(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 101068142 B
(45)授权公告日 2012.09.05

(21)申请号 200710102627.8

(22)申请日 2007.04.24

(30)优先权数据
11/429,478 2006.05.05 US
11/429,477 2006.05.05 US
11/474,033 2006.06.23 US
11/491,052 2006.07.20 US
11/506,661 2006.08.18 US
11/506,729 2006.08.18 US
11/527,137 2006.09.26 US

(73)专利权人 美国博通公司
地址 美国加州尔湾市奥尔顿公园路 16215 号

(72)发明人 詹姆士·D·贝内特

(74)专利代理机构 深圳市顺天达专利商标代理有限公司 44217
代理人 蔡晓红

(51)Int.Cl.
H04L 9/00(2006.01)
H04L 12/56(2006.01)

(56)对比文件
US 2002/0032880 A1,2002.03.14, 说明书 0004 至 0077 段、图 1-10.
US 2005/0157647 A1,2005.07.21, 全文.
US 2005/0210533 A1,2005.09.22, 全文.

审查员 张明霞

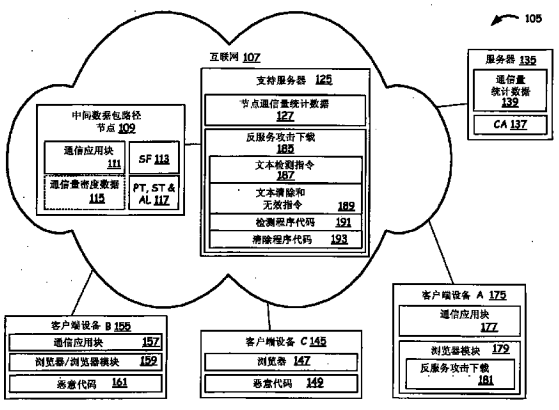
权利要求书 3 页 说明书 13 页 附图 11 页

(54)发明名称

一种通信架构及其内的中间路由节点和方法

(57)摘要

本发明涉及一种通信架构及其内的中间路由节点和方法。所述通信架构包括在源设备和多个目的设备之间路由多个数据包的中间路由节点，存储在所述中间路由节点上的多个模板以及服务功能模块。所述中间路由节点例如交换机、路由器、接入点、桥接器或网关，通过比较数据包与多个模板，来识别包含有网页请求的该数据包，其中该请求为服务攻击尝试。然后，所述中间路由节点通过与服务器和客户端设备的交互拒绝服务攻击。也即，所述中间路由节点发送带有口令机制的消息给服务器，基于其响应或其它，发送消息和反服务攻击下载程序给客户端设备，并接收客户端设备的响应。



CN 101068142 B

1. 一种通信架构，其特征在于，包括：

多个客户端设备；

服务器；

多个中间路由节点；

所述多个中间路由节点中的第一中间路由节点接收来自所述多个客户端设备的数据包；

所述第一中间路由节点分析每个收到的数据包，所述分析至少包括将所述每个数据包与至少一个模板进行比较，所述比较包括：(a)比较当前通信量密度与服务器设置的当前数据和时间的通信量密度阈值，所述阈值从服务器或中间路由节点获得；(b)自动从服务器访问当前时间和数据的统计通信数据，并将其与当前通信量密度比较；(c)自动从服务器访问当前时间和数据的节点通信量统计数据，并将其与当前通信量密度进行比较；(d)使用与模板相关的逻辑内可用的计数机制；(e)与存储在中间路由节点的针对当前时间的一个短时间窗期间的通信量密度数据进行比较，从中间路由节点处出现的通信量密度的突然升高来确定；

所述第一中间路由节点至少部分地基于所述分析结果，识别出至少服务器上服务攻击的可能性；

所述第一中间路由节点通过调用服务攻击功能来响应所述识别，所述服务攻击功能由用户选择下列中的至少一个：

丢弃网页请求或含有网页请求的数据包；

发送消息给客户端设备，对服务器的当前问题进行解释；

发送带有人为口令的服务攻击消息给客户端设备，以确保该网页请求是由该客户端设备的用户作出的；

改变数据包内的服务器地址，将请求转移至另一个服务器；

改变第一中间节点处的阈值以向服务器的用户提供可增加特定时间周期内相关通信量的选项。

2. 根据权利要求 1 所述的通信架构，其特征在于，所述第一中间路由节点还基于与目的地为所述服务器的至少某些数据包的接收有关的时序信息，识别出至少服务器上服务攻击的可能性。

3. 根据权利要求 1 所述的通信架构，其特征在于，所述第一中间路由节点基于所述分析结果的统计分析，至少识别出服务器上服务攻击的可能性。

4. 根据权利要求 1 所述的通信架构，其特征在于，所述至少一个模板包括目标为服务器的网络地址的第一模板，和目标为网页请求的至少一部分的第二模板。

5. 一种用于从源设备路由数据包到目的地设备的通信架构中的中间路由节点，其特征在于，所述中间路由节点包括：

网路接口；

包含有多个模板和之前通信量数据的存储器；

连接至所述存储器和所述网络接口的处理电路；

所述处理电路接收数据包；

所述处理电路比较所述数据包与多个模板中的至少一个，所述比较包括：(a)比较当

前通信量密度与服务器设置的当前数据和时间的通信量密度阈值，所述阈值从服务器或中间路由节点获得；(b) 自动从服务器访问当前时间和数据的统计通信数据，并将其与当前通信量密度比较；(c) 自动从服务器访问当前时间和数据的节点通信量统计数据，并将其与当前通信量密度进行比较；(d)使用与模板相关的逻辑内可用的计数机制；(e)与存储在中间路由节点的针对当前时间的一个短时间窗期间的通信量密度数据进行比较，从中间路由节点处出现的通信量密度的突然升高来确定；

所述处理电路至少部分地基于所述比较结果和之前的通信量数据，触发服务功能模块，所述服务功能模块由用户选择下列中的至少一个功能：

丢弃网页请求或含有网页请求的数据包；

发送消息给客户端设备，对服务器的当前问题进行解释；

发送带有人为口令的服务攻击消息给客户端设备，以确保该网页请求是由该客户端设备的用户作出的；

改变数据包内的服务器地址，将请求转移至另一个服务器；

改变第一中间节点处的阈值以向服务器的用户提供可增加特定时间周期内相关通信量的选项。

6. 根据权利要求 5 所述的中间路由节点，其特征在于，所述中间路由节点包括路由器。

7. 根据权利要求 5 所述的中间路由节点，其特征在于，所述中间路由节点包括接入点。

8. 根据权利要求 5 所述的中间路由节点，其特征在于，所述服务功能模块尝试解决拒绝服务攻击。

9. 一种分组交换通信路径内的中间路由节点所执行的方法，所述分组交换通信路径将数据包从源设备路由到目的地设备，其特征在于，所述方法包括：

接收数据包；

比较所述数据包与至少一个模板，所述比较包括：(a) 比较当前通信量密度与服务器设置的当前数据和时间的通信量密度阈值，所述阈值从服务器或中间路由节点获得；(b) 自动从服务器访问当前时间和数据的统计通信数据，并将其与当前通信量密度比较；(c) 自动从服务器访问当前时间和数据的节点通信量统计数据，并将其与当前通信量密度进行比较；(d)使用与模板相关的逻辑内可用的计数机制；(e)与存储在中间路由节点的针对当前时间的一个短时间窗期间的通信量密度数据进行比较，从中间路由节点处出现的通信量密度的突然升高来确定；

考虑与目的地设备有关的通信量数据；

基于所述比较结果和所述考虑，触发服务功能模块，所述服务功能模块由用户选择下列中的至少一个功能：

丢弃网页请求或含有网页请求的数据包；

发送消息给客户端设备，对服务器的当前问题进行解释；

发送带有人为口令的服务攻击消息给客户端设备，以确保该网页请求是由该客户端设备的用户作出的；

改变数据包内的服务器地址，将请求转移至另一个服务器；

改变第一中间节点处的阈值以向服务器的用户提供可增加特定时间周期内相关通信量的选项。

10. 根据权利要求 9 所述的方法，其特征在于，所述服务功能模块尝试解决潜在的拒绝服务攻击，所述通信量数据包括与之前接收的发送给所述目的地设备的数据包有关的信息。

一种通信架构及其内的中间路由节点和方法

技术领域

[0001] 本发明涉及通信架构，更具体地说，涉及分组交换通信网络内的交换节点操作。

背景技术

[0002] 互联网在今天已经广泛用于在彼此远离的各个地点之间传输语音、视频和数据包。互联网架构通常包括交换设备，例如路由器、交换机、分组交换机，以及接入点和互联网服务提供商网络（ISPN）、互联网通信路径和终端设备。用作终端设备的客户端设备包括例如个人或笔记本电脑、服务器、机顶盒和手持数据／通信设备。服务器通常向多个客户端设备提供网页内容，由客户端设备使用网页浏览器进行浏览。

[0003] 被故意引入大量客户端设备的某些类型的恶意代码通过同时（基于系统时钟）向未感染的服务器计算机发送请求来攻击该服务器，致使其过载。这些攻击对服务器和客户端设备双方的用户都造成极大的困扰和损失。通常，客户端设备无法清除这些恶意代码。因而用户需要频繁的购买多个恶意代码清除包，因为当前的恶意代码清除包可能不能够处理逐渐增加的所有恶意代码。尽管有些时候这些清除包是免费的，但大多数都是很贵的，特别是考虑到要买多个清除包。

[0004] 在通过与本发明的系统进行比较后，现有和传统的手段的其它局限和缺点是很明显的。

发明内容

[0005] 本发明提供一种操作装置和方法，结合至少一副附图给出了充分地显示和／或描述，并更完整地在权利要求中阐明。

[0006] 根据本发明提出的一种在源设备和多个目的设备之间路由多个数据包的通信架构，其中包括中间路由节点、存储在所述中间路由节点中的多个模板（template）、以及服务功能模块。所述中间路由节点接收多个数据包中的第一数据包，其内包含有网页请求，所述请求为服务器攻击尝试。然后，所述中间路由节点通过将第一数据包的内容与多个模板中的至少一个模板进行比较，来识别所述网页请求。所述中间路由节点识别出服务器攻击尝试，并通过触发服务功能模块对服务器攻击尝试的识别做出响应。

[0007] 根据本发明提出的一种通信架构内的中间路由节点，用于路由来自源设备的数据包，所述中间路由节点包括网络接口、包含有多个模板和通信量数据的存储器以及处理电路。所述处理电路接收含有网页请求的数据包，所述网页请求为服务器攻击尝试。接着，所述处理电路将所述数据包的内容与多个模板中的至少一个模板进行比较，识别所述网页请求。然后，所述处理电路通过使用所述通信量数据标识出服务器攻击尝试，并通过触发服务功能模块对所述网页请求做出响应。

[0008] 根据本发明一个方面，提出一种通信架构，包括：

[0009] 多个客户端设备；

[0010] 服务器；

[0011] 多个中间路由节点；

[0012] 所述多个中间路由节点中的第一中间路由节点接收来自所述多个客户端设备的数据包；

[0013] 所述第一中间路由节点分析每个收到的数据包，所述分析至少包括将所述每个数据包与至少一个模板进行比较；

[0014] 所述第一中间路由节点至少部分地基于所述分析结果，至少识别出服务器上服务攻击的可能性；

[0015] 所述第一中间路由节点通过调用服务攻击功能来响应所述识别。

[0016] 上述通信架构中，所述第一中间路由节点还基于与目的地为所述服务器的至少某些数据包的接收有关的时序信息，识别出至少服务器上服务攻击的可能性。

[0017] 上述通信架构中，所述第一中间路由节点基于统计分析，至少识别出服务器上服务攻击的可能性。

[0018] 上述通信架构中，所述至少一个模板包括目标为服务器的网络地址的第一模板，和目标为网页请求的至少一部分的第二模板。

[0019] 上述通信架构中，所述第一中间路由节点基于非正常高频率地接收到目的地为服务器的数据包，至少识别出服务器上服务攻击的可能性。

[0020] 上述通信架构中，所述第一中间路由节点基于非正常高频率地接收到与第一模板和第二模板均匹配的数据包，至少识别出服务器上服务攻击的可能性。

[0021] 上述通信架构进一步包括提供恶意代码识别服务的支持服务器。

[0022] 上述通信架构中，支持服务器提供恶意代码清除服务。

[0023] 上述通信架构中，支持服务器具有服务攻击功能的至少一部分。

[0024] 上述通信架构中，所述第一中间路由节点提供所述服务攻击功能的至少一部分。

[0025] 上述通信架构中，所述服务攻击功能包括人为口令 (human challenge)。

[0026] 上述通信架构中，所述服务功能模块发出服务攻击消息。

[0027] 上述通信架构中，所述服务功能模块发出针对恶意代码的软件。

[0028] 根据本发明一个方面，提出一种通信架构中的中间路由节点，用于将数据包从源设备路由到目的设备，所述中间路由节点包括：

[0029] 网路接口；

[0030] 包含有多个模板和在先通信量数据的存储器；

[0031] 连接至所述存储器和所述网络接口的处理电路；

[0032] 所述处理电路接收数据包；

[0033] 所述处理电路比较所述数据包与多个模板中的至少一个；

[0034] 所述处理电路至少部分地基于所述比较结果和在先通信量数据，触发服务功能模块。

[0035] 上述中间路由节点包括路由器。

[0036] 上述中间路由节点包括接入点。

[0037] 上述中间路由节点中，所述服务功能模块尝试解决拒绝服务攻击。

[0038] 上述中间路由节点中，所述服务功能模块尝试解决与目的设备相关的限制。

[0039] 上述中间路由节点中，所述限制包括通信带宽限制。

[0040] 上述中间路由节点中，所述限制包括处理限制。

[0041] 上述中间路由节点中，所述服务功能模块包括人为口令。

[0042] 上述中间路由节点中，所述服务功能模块包括针对恶意代码的程序代码下载。

[0043] 根据本发明一个方面，提供一种由分组交换通信路径内的中间路由节点执行的方法，所述分组交换通信路径将数据包从源设备路由到目的设备，所述方法包括：

[0044] 接收数据包；

[0045] 比较所述数据包与至少一个模板；

[0046] 考虑与目的设备有关的通信量数据；

[0047] 基于所述比较结果和所述考虑，触发服务功能模块。

[0048] 上述方法中，所述服务功能模块尝试解决潜在的拒绝服务攻击，所述通信量数据包括与之前接收的目的地为所述目的设备的数据包有关的信息。

[0049] 上述方法中，所述信息包括数据包接收频率。

[0050] 上述方法中，所述触发包括发送请求给支持服务器。

[0051] 上述方法中，所述触发包括执行所述服务功能模块的至少一部分。

[0052] 根据后续结合附图对本发明具体实施例的详细介绍，本发明的特征和优点可以显而易见。

附图说明

[0053] 图 1 是根据本发明构建的通信架构的一个实施例的示意图，其中中间数据包路径节点处理来自多个客户端设备并发往服务器的包含有网页请求的数据包，以抵制恶意引入的服务攻击；

[0054] 图 2 是分布在图 1 所示的通信架构的服务器和中间数据包路径节点之间的通信应用的功能框图；

[0055] 图 3 是分布在图 1 所示的通信架构的一个客户端设备和中间数据包路径节点之间的通信应用的功能框图；

[0056] 图 4 是分布在图 1 所示的通信架构的中间数据包路径节点和服务器与客户端设备内的通信应用之间的交互的示意图；

[0057] 图 5 是根据本发明图 1 所示的实施例构建的网络节点（交换机 / 路由器 /ISPN/AP）的框图；

[0058] 图 6 是根据本发明图 1 所示的实施例构建的支持服务器的框图；

[0059] 图 7 是根据本发明图 1 所示的实施例构建的路由器的框图；

[0060] 图 8 是根据本发明图 1 所示的实施例构建的终端设备（服务器和 / 或客户端设备）的框图；

[0061] 图 9 是图 1 所示的中间数据包路径节点的总功能流程图；

[0062] 图 10 是图 1 所示的中间数据包路径节点的详细功能流程图；

[0063] 图 11 是图 1 所示的中间数据包路径节点的通信量密度数据处理电路的功能流程图。

具体实施方式

[0064] 图 1 是根据本发明构建的通信架构的一个实施例 105 的框图，其中中间数据包路径节点 109 处理从多个客户端设备 145、155、175 发送到服务器 135 的包含有网页请求的数据包，以抵制恶意引入的服务攻击。触发服务攻击的恶意代码 149 和 161 可以在预定时间和预定日期出现在来自多个客户端设备例如客户端设备 A、B 和 C 175、155、145 的数据中，采用从服务器 135 请求特定网页的形式。根据本发明，作为互联网 107 的一部分的中间数据包路径节点 109 和支持服务器 125 一起为服务器 135 提供帮助，通过本申请中介绍的多种方法之一检测服务攻击尝试，并采取一系列步骤抵制该服务攻击尝试。

[0065] 恶意代码可包括病毒代码和广告软件代码。例如，某些广告软件经常会弹出指向特定地址的窗口，其动机是为了增加点击量或导致拒绝服务攻击。这样的恶意代码可以是病毒，或者仅仅是不想要的广告软件。例如，恶意代码可以是在客户端设备间传播的病毒，使用内部时钟使攻击同步，或者是攻击性广告软件，从目标服务器中加载一个弹出窗口。服务攻击为自动恶意引入的对服务器 135 网页的请求。因此，通信应用块 (CA)111、137、157 和 177 等允许作为拒绝服务攻击一系列步骤中的一部分的中间数据包路径节点 109 与服务器 135 交互，并根据该响应或另外与客户端设备 155 和 175 交互，该交互包括人为口令以确保人的干预。为了服务攻击尝试的检测，中间数据包路径节点 109 使用内置数据库或实时通信量数据 (traffic data) 例如通信量密度数据 (trafficdensity data)115，或统计的节点通信量数据 127(即，与支持服务器 125 的数据相关的统计流量)，服务器 135 的统计通信量数据 139。中间数据包路径节点 109 还包含有主模板、次模板和相关逻辑 (PT、ST 和 AL)117 以及服务功能模块 (SF)113，帮助确定网页请求和服务攻击尝试。此外，客户端设备 145、155 和 175 可包含浏览器和 / 或浏览器模块例如 147、159 和 179。某些客户端设备，例如客户端设备 C 175，还可从支持服务器 125 下载反服务攻击下载程序 181，以帮助清除恶意代码，阻拦任何进一步的服务攻击尝试。某些传统的客户端设备，例如客户端设备 C 145，不含有通信应用块。

[0066] 本申请中会交换使用中间数据包路径节点、中间路由节点、中间节点和网络节点这几个名字。此外，源终端设备、源设备和服务器可交换使用，目的终端设备、目的设备和客户端设备可交换使用。然而，基于来自中间节点 109 或服务器 135 的请求，内置于互联网 107 的支持服务器 125 假设有责任向中间节点 109 提供抵制服务攻击的帮助。支持服务器还向客户端设备 145、155、175 以及服务器 135 提供恶意代码检测和清除帮助。依据反服务攻击下载程序 185，该恶意代码检测和清除帮助包括不同的级别，例如提供 :a) 文本检测指令 185 ;b) 文本清除或无效指令 187 ;c) 检测程序代码 191 ;d) 移除程序代码 193。当识别到服务攻击的可能性时，将提供这些反服务攻击下载程序 185，后续将结合图 3 给出介绍。

[0067] 服务攻击尝试的检测开始于中间节点 109 识别向服务器 135 请求网页的请求。为了识别网页请求，中间节点 109 将来自客户端设备 145、155 或 175 中的一个设备的到达数据包载荷载荷与本地可用的主模板进行比较。该主模板包含有比特序列，若能够成功匹配，则可帮助确定到达数据包是否包含有对服务器 135 的网页请求。如果通过比较该数据包载荷与主模板无法做出上述确定，与该主模板相关的逻辑将该数据包传给次模板。然后进行与主模板类似的与至少一个次模板的比较，并且该相关逻辑将数据包与次模板进行多个比较。一旦网页请求的成功确定完成后，相关逻辑以及主模板或次模板的应用将帮助确定该网页请求是否是服务攻击尝试。

[0068] 为了确定该网页请求是否是服务攻击尝试，与主模板或次模板相关的逻辑控制中间节点 109 执行以下方法之一：(a) 比较当前通信量密度与服务器 135 设置的当前数据和时间的通信量密度阈值，该阈值可从支持服务器 125 获得或在中间节点 109 自身处；(b) 自动从服务器 135 访问当前时间和数据的统计通信量数据，并将其与当前通信量密度进行比较（在中间节点靠近服务器时特别适用）；(c) 自动从支持服务器 125 访问当前时间和数据的节点通信量统计数据 127，并将其与当前通信量密度进行比较；(d) 使用与主模板或次模板相关的逻辑内可用的计数机制；和 / 或 (e) 与存储在中间节点 109 内的针对当前时间之前的一个短时间窗期间的通信量密度数据 115 进行比较，从节点处出现的通信量密度的突然升高来确定。服务器 135 自动设置通信量密度阈值，或由服务器 135 的用户针对每个时间周期提前手动设置。该数据可在服务器 135 自身处，或可从支持服务器 125 获得。为了自动设置阈值，服务器 125 可使用可从服务器 135 获得的通信量统计数据 139。

[0069] 成功确认服务攻击尝试后，中间节点 109 中断任何其它向服务器 135 请求网页的请求。这一操作由与主模板或次模板相关的逻辑通过调用一个或多个服务功能来执行。该服务功能模块接着在中断其它进一步的网页请求后，调用通信应用块 111 和 137。然后，通信应用块 111 发送带有人为口令的消息给服务器 135，并在对被中断的请求进行进一步处理之前，等待响应。该消息可包括有标题（例如“服务攻击消息 / 警告…！”）和中间节点 109 所遇到的情形的简短描述。该描述可以是例如“在 < 当前日期和时间 >，服务器 (www.domainname.com) 正经历超出平均的对网页 < 网页路径名 > 的请求。这可能是对服务器的服务攻击尝试，请选择以下一个或多个选项，并通过输入人为口令代码作出快速响应。”提供给服务器 135 用户的选择包括一个或多个选项：(a) 阻止任何进一步的网页请求；(b) 发送消息给客户端设备，对服务器的当前问提进行解释，例如“服务器出现技术问题，请稍微再试……”；(c) 发送带有人为口令的服务攻击消息给客户端设备，以确保该网页请求是由该客户端设备的用户作出的；(d) 为该网页请求创建到其它服务器的路径，例如，从某特定区域的请求；和 / 或 (e) 将支持服务器或中间节点处的阈值改为另一个值。

[0070] 选择 (a) 允许中间节点 109 简单地丢弃任何其它的网页请求。选择 (d) 允许中间节点改变数据包内的服务器地址，将通信量转移给另一个服务器。这一选择可应用于通信量来自特定区域的情况，允许服务器 135 的用户提供基于区域的 IP 地址。例如，某个特定地理位置具有 IP 地址 xxx.xxx.yyy.yyy，该 IP 地址的前两个部分（即 xxx.xxx）定义了地理区域。在选择 (e) 中，改变支持服务器 125 或中间节点 109 处的阈值，向服务器 135 的用户提供了可增加特定时间周期内网页相关通信量的选项。这一选项在特定场合例如商业广告竞赛、选举或体育赛事期间是有用的。

[0071] 选择选项 (c) 后，中间节点 109 发送服务攻击消息给客户端设备 145、155 和 175。客户端设备 145、155 或 175 接收到的服务攻击消息可包括有标题（例如“服务攻击消息……！”）和中间节点 109 与服务器 135 所遇到的情形的简短描述。该描述可以是例如“您的系统正尝试在繁忙通信量期间访问服务器 (www.domainname.com)。通信量繁忙的原因可能是恶意引入的服务攻击。为了确保您正在作出该请求而不是恶意代码，我们向您提供人为口令。请输入以下给出的代码并点击“是”按钮。如果您希望稍后再访问该网页，请点击“否”按扭。”此外，该消息还可以包含有反服务攻击下载链接，以帮助客户端设备 145、155 和 175 的用户清除该恶意代码。

[0072] 人为口令确保了来自客户端设备 145、155 和 / 或 175 的用户的人为响应。该人为口令包括几个数字或字母，其方向不同于计算机上文字的显示方向，并期望自然人用户通过键入这些字符来作出响应，从而同意数据包的传输。在通信量非预期猛增的期间，这一过程使得中间节点 109 能够确定，网页请求是单独来自客户端设备的用户的，并非恶意代码引入的服务攻击。通过该人为口令机制，中间网络节点 109 在需要的情况下还可以收集某些用户信息。此外，中间节点 109 使用该人为口令机制，可针对该恶意代码发送消息、信息、警告和帮助（以反服务攻击下载程序的形式）。

[0073] 中间节点 109 通过上述方式完成服务攻击处理，无需沿通信路径重复任何这些处理步骤。该无重复处理通过在服务攻击处理执行之后，在数据包中加入比较表版本代码来实现。该比较表版本代码结合有关于与该数据包比较过的主模板和次模板的信息，以及前一节点对该数据包所使用的功能相关的信息。包含在比较表版本代码内的信息包括模板的版本、相关逻辑的版本、本地服务功能的版本以及本地或远程应用的服务功能。如果通信路径内的任一节点包含有增强的或最近版本的模板，该节点可决定只需与这些增强的模板进行比较。同样的考虑也适用于相关逻辑和服务功能。如果数据包内没有比较表版本代码，则执行处理的中间节点可确定，前面的节点尚未进行数据包分析。相反，如果数据包中有比较表版本代码，执行处理的中间节点将解码该代码以确定之前已经发生了服务攻击处理。然后，如果还需要任何其它的服务攻击处理，则只用执行该其它的服务攻击处理。

[0074] 为了执行上述的服务攻击处理方法，中间节点 109 可在数据包被加密的情况下解密数据包，并可调用本地或远程服务来实现该解密处理。若到达中间节点的数据包是经过加密的，并且若已指出了进一步分析，则网络节点继续解密该数据包。尽管公钥可以从服务器 135 或客户端设备 145、155、175 中任一方获得，但是私钥仅为客户端设备 153 所知悉。

[0075] 抵制服务攻击之外，中间节点 109 和支持服务器 125 还处理涉及非预期高流量的情况。服务功能模块 113 在这样的情况下可发出消息例如“请稍后再试”。该不可支持的流量可基于服务器的处理和通信带宽来确定。

[0076] 图 2 是分布在图 1 所示的通信架构的服务器 235 和中间数据包路径节点 209 之间的通信应用块 211 和 237 的功能框图 205。服务器 235 包括通信应用块 237，与出现在互联网骨干网 207 内的中间节点 209 的通信应用块 211 结合起来工作，抵制对服务器 235 的服务攻击。通信应用块 237 和 211 提供与服务攻击有关的消息，并从服务器 235 收集响应，其帮助中间节点 209 确定对服务攻击尝试的响应。针对来自中间节点 209 的拒绝服务攻击响应的统计数据，可从本地可获得的通信量密度数据 215，或从支持服务器 225 的 SNT 数据（节点通信量统计数据）239，或从服务器 235 的通信量统计数据 239 中获得。此外，主模板、次模板和相关逻辑 (PT、ST 和 AL)217 以及服务功能模块 (SF)213 帮助中间节点 209 确定从服务器 235 请求网页的请求，并抵制对服务器 235 的服务攻击。

[0077] 当尝试对服务器 235 进行服务攻击并且该尝试已被中间节点 209 识别出来时，通信应用块 211 和 237 在采取任何进一步的措施之间，从服务器 235 的用户（或管理者）获取响应。为了从服务器 235 的用户获得响应，中间节点 209 发送消息给服务器 235。该消息可包括有标题（例如“服务攻击消息……！”）和中间节点 209 所遇到的情况的简短描述。该描述可以是例如“当前时间和日期，服务器 (www.domainname.com) 正接收超出阈值 (x％）的请求。请选择您的选项，输入以下给出的代码并点击“是”按钮，否则请点击“否”

按钮以忽略。”提供给服务器 235 的用户的选择包括以下一个或多个选项 :(a) 阻止所有的请求 ;(b) 发送消息“服务器出现技术问题,请稍后再试……”;(c) 发送带有人为口令的“服务攻击消息”;(d) 创建路径,将请求从 <xxx. xxx. xxx. xxx> 转移至 <xxx. xyz. com> ;和 / 或 (e) 改变支持服务器上的阈值 <x>%。

[0078] 选项 (a) 允许中间节点 209 简单地丢弃任何其它含有网页请求的数据包。选项 (b) 基于网页请求,发送消息给对应的客户端设备 (图 3 中的 355),指出服务器 235 出现某些技术问题,如后续结合图 3 所述。选项 (c) 发送带有人为口令的消息给客户端设备,并从客户端设备获得响应,以确保请求来自网页的用户。有关发送给客户端设备的服务攻击消息的详细介绍,请参见图 3 的描述。选项 (d) 允许中间节点改变数据包内的服务器地址,将通信量转移给另一个服务器。这一选择可应用于通信量来自特定区域的情况,允许服务器 235 的用户提供部分 IP 地址。例如,某个特定地理位置具有 IP 地址 129. 133. xxx. xxx,该 IP 地址的前两个部分便定义了地理区域。在选项 (e) 中,改变支持服务器 225 或中间节点 209 处的阈值,向服务器 235 的用户提供了可增加特定时间周期内网页相关通信量的选项。这一选项在特定场合例如商业广告竞赛、选举或体育赛事期间是有用的。

[0079] 图 3 是分布在图 1 所示的通信架构的客户端设备 355 和中间数据包路径节点 309 之间的通信应用块 311、357 的功能框图 305。客户端设备 355 包含有通信应用块 357,其与位于互联网骨干 307 内的中间节点 309 的通信应用块 311 一起协同工作,以提示与服务攻击问题有关的消息并从客户端设备 355 获取响应。通信应用块 311 和 357 还通过提供链接和 / 或反服务攻击下载程序来帮助客户端设备 355。客户端设备 355 还包含有浏览器模块 359,其通过附加功能辅助浏览器。浏览器模块 359 进一步包含有反服务攻击下载程序以帮助清除恶意代码 361。此外,主模板、次模板和相关逻辑 (PT、ST 和 AL)317 以及服务功能模块 (SF)313 帮助中间节点 309 判断来自客户端设备 355 的网页请求,并拒绝对服务器的攻击。

[0080] 当客户端设备 355 尝试进行服务攻击且该尝试已被中间节点 309 识别出来时,根据服务器的选择,通信应用块 311 和 357 得以运行并从客户端设备 355 的用户处获得响应,如前对图 2 的描述所示。发送给客户端设备 355 的服务攻击消息可包括有标题例如“服务攻击消息……!”和中间节点 309 所遇到的情况的简短描述。该描述可以是例如“服务器正经受可能因恶意代码引起的非正常高通信量,请输入以下的数字并点击‘是’按钮来验证该请求是由您做出的。否则,请点击‘否’取消该请求,或点击以下的链接来确认当前是否已受病毒或其它恶意代码感染,如果是,请修复。”此外,该消息中还可包括有反服务攻击下载链接,以帮助客户端设备 355 的用户清除恶意代码。这些链接提供有上述的消息,例如“点击此处以识别并清除存在的任何恶意代码”。通过点击该链接,中间节点 309 或支持服务器 325 提供如何识别和清除的文本指令,或为该搜索和清除步骤提供下载程序代码 (例如 java 代码)。图 4 是图 1 所示的通信架构内服务器 475 与客户端设备 407、以及中间数据包路径节点和 / 或支持服务器 441 内的通信应用块 409、449 和 477 之间的交互的示意图 405。具体来说,该图示出了包含有多个中间数据包路径节点 (简称为中间节点) 和 / 或支持服务器 441、服务器 (或源设备)475 以及客户端设备 407(可以是图 1 中的客户端设备 B 155 或 C 175) 的通信架构的各个组件之间的交互操作。服务器 475 包含有组件例如通信应用块 477 与通信量统计数据 479。客户端设备 407 包括通信应用块 409、浏览器模块 411,并还

可包括有发起服务攻击的恶意代码 413。通信量统计数据 479 可以是数据库表，其内包含有与通信量有关的数据和统计值。

[0081] 交互操作开始于客户端设备 407 通过中间节点 441 向服务器 475 传送网页请求。中间节点 411 接收带有服务器地址 429 的数据包，并开始分析该包含有请求 433 的数据包。中间节点 441 将接收的包含网页请求的数据包载荷与 PT 和 ST（主模板和次模板）进行比较，并应用 AL（相关逻辑）。与主模板或次模板相关的逻辑使用在中间节点 441 处获得的通信量密度数据，以做出接收的网页请求是服务攻击尝试的决定。或者，中间节点可将该数据包传给支持服务器来分析该包含网页请求的数据包是否为服务攻击。与主和次模板相关的逻辑然后可引导通信应用块 449 执行与服务器 475 的交互 447、431，并基于响应，发送服务攻击消息和反服务攻击下载程序 447、433 给客户端设备 407。

[0082] 中间节点和 / 或支持服务器 441 在检测到病毒或其它恶意代码时，可以完全保护服务器免受感染。例如，中间节点和 / 或支持服务器 411 停止或者至少中断目的地为服务器 475 的每个数据包。中间节点和 / 或支持服务器 411 的这一处理取决于如图 2 所述的与选项栏相关的设置。为了避免单次会话过程中出现的对客户端设备 407 的重复人为口令，可在第一次人为口令验证之后，向浏览器（经修改可与浏览器模块 411 一起支持这一功能的）发出允许的会话 ID。随后，浏览器可在每个数据包中加入该会话 ID，中间节点和 / 或支持服务器便不会中断后续的操作。

[0083] 图 5 是根据本发明图 1 所示的实施例构建的网络节点（交换机 / 路由器 /ISPN/AP)507 的框图 505。此外，该图中示出了将网络节点 507 通信连接至具有相似的隔离功能的邻近节点 557 的通信路径 555。网络节点电路 507 可代表用于路由数据包的任一互联网节点，该电路可以部分或全部集合到任意网络设备中，例如交换机、路由器和 ISPN 或接入点。网络节点电路 507 一般包括处理电路 509、本地存储器 517、管理员接口 549 和网络接口 541。这些部件通过一个或多个系统总线、专用通信路径或其它直接或间接通信路径彼此通信连接。在不同实施例中，处理电路 509 可以是微处理器、数字信号处理器、状态机、专用集成电路、现场可编程门阵列或其它处理电路。处理电路 509 通信连接至编码 / 加密管线 511、解码 / 解密管线 513、以及通信量密度数据处理电路和通信量密度数据 515。这些硬件部件 511、513 和 515 可以硬连接以增加服务攻击处理和路由的速度。

[0084] 本地存储器 517 可以是随机访问存储器、只读存储器、闪存、硬盘驱动器、光驱或可存储计算机指令和数据的其它类型存储器。本地存储器 517 包含有服务模块管理器 (SMM)519，通过将报头内容和载荷内容与合适的模板进行比较来分析入站数据包。这些模板和相关逻辑包括主模板和相关逻辑 521、次模板和相关逻辑 523。如果在与主模板的比较过程中出现任何匹配，相关逻辑将该数据包传送给选择的次模板组进行进一步的分析。在与次模板进行比较后，应用与次模板相关的逻辑。这一处理过程不断重复直至得出结论。得出的结论可以确定所接收的数据包包含有网页请求且该请求为服务攻击尝试。然后，应用合适的服务功能模块 525 或远程隔离服务功能模块（图中未示出，可以从图 1 所示的支持服务器或其它中间节点获得）。通信应用块 527 将消息和人为口令显示在屏幕上，例如弹出窗口，而无需浏览器。存储器 517 还包含有节点通信量统计数据 529，其包含有与各个服务器和网页的节点通信量有关的其它统计数据。

[0085] 网络接口 541 包括有线和无线分组交换接口 545、有线和无线电路交换接口 547。

此外，网络接口 541 还可包括有内置的和单独的接口处理电路 543。网络接口 541 允许网络设备与其它网络设备通信，并允许处理电路 509 接收和发送数据包，该数据包可能包含有网页请求。当某些功能在本地存储器 517 中不可用时，网路接口 541 允许使用外部的服务功能模块来进行分析和处理。管理器接口 549 包括显示器和键盘接口。这些管理员接口 549 允许位于网络交换机一侧的用户对本发明的方案进行控制。

[0086] 其它实施例中，网络节点 507 可包括更少或更多的部件，同样可包括更少或更多的功能。换句话说，图示的网络设备仅仅是根据本发明实现的可能功能性的一个示例。网络节点的其它可能的实施例将结合图 7 进行描述。

[0087] 网络节点 507 通过通信路径 555 通信连接至外部网络设备，例如邻近节点 557 或支持服务器（未示出）。邻近节点 557 还包括本发明的其它组件，例如通信量密度数据处理电路和通信量密度数据 575、本地存储器 577、SMM（服务模块管理器）579、PT、ST 和 AL（主模块、次模块和相关逻辑）581、SF（服务功能）583、SNTD（节点通信量统计数据）585 和 CA（通信应用块）587。此外，邻近节点 557 还具有网络节点 507 的其它部件，例如加密管线和解密管线（未示出）。

[0088] 网络节点 507 通过比较数据包内容与多个主模板开始进行分析。通过这样的主模板比较，节点 507 判断该数据包是否含有网页请求，若含有，并进一步判断该请求是否为服务攻击尝试。出现匹配时，节点 507 应用与主模板相关的逻辑。接着，将进行次模板比较，将数据包的载荷内容与选择的次模板组进行比较。然后，应用与次模板相关的逻辑。不断重复次模板比较和应用相关逻辑的过程，直至得出关于网页请求和服务攻击尝试的结论。然后，通过使用本地可用的服务功能模块 525，或通过将数据包传送给邻近节点 557 使用外部可用的服务功能模块例如 SF 583，对数据包应用服务功能模块。

[0089] 一旦成功确定服务攻击尝试后，中间节点 507 将中断后续对该网页的任何其它请求。这一步骤通过与主模板或次模板相关的逻辑调用一个或多个服务功能模块 525 来实现。在中断进一步的网页请求后，该服务功能模块可调用通信应用块 527，在对被中断的请求采取进一步的处理之前，发送带有人为口令的消息给服务器（图 1 的 135），并等待应答。然后，中间节点 507 发送服务攻击消息给客户端设备（图 1 所示的 145、155 或 175）。客户端接收的该服务攻击消息可包括有标题例如“服务攻击消息……！”和中间节点 507 以及服务器所遇到的情况的简短描述。

[0090] 图 6 是根据本发明图 1 所示的实施例构建的支持服务器 655 的框图 605。支持服务器电路 655 执行部分或全部的服务攻击处理，例如检测数据包内的网页请求，确定该请求是否为服务攻击尝试，对网页数据包、服务器和客户端设备执行通信应用处理，收集并分析与多个服务器有关的通信量统计数据。支持服务器电路 655 一般包括处理电路 657、本地存储器 661、用户接口 649 和网络接口 641。这些部件通过一个或多个系统总线、专用通信路径或其它直接或间接的通信路径彼此通信连接。各种实施例中，处理电路 657 可以是微处理器、数字信号处理器、状态机、专用集成电路、现场可编程门阵列或其它处理电路。处理电路 657 通信连接至通信量密度数据处理电路和通信量密度数据 659。

[0091] 本地存储器 661 可以是随机访问存储器、只读存储器、闪存、硬盘驱动器、光驱、或可存储计算机指令和数据的其它类型存储器。本地存储器 661 包含有本发明的各种其它组件，例如服务模块管理器 663、主、次模板及其相关逻辑 665、通信应用块 667、统计值收集功

能 669、浏览器模块 671 和节点通信量统计数据（例如通信量密度阈值数据）675 和服务功能模块 679。浏览器模块 671 进一步包含反服务攻击下载 673。通过提供如下不同级别的反服务攻击下载 673，为恶意代码检测和清除提供帮助 :a) 文本检测指令 ;b) 文本清除或无效指令 ;c) 检测程序代码 ;d) 清除程序代码。这些反服务攻击下载 673 在识别到服务攻击可能性时提供。

[0092] 支持服务器电路 655 所执行的服务攻击处理与结合图 5 所述的网络节点执行的处理相似，开始于比较数据包内容与主模板。若在主模板比较过程中出现任何匹配，相关的逻辑将该数据包传送给选定的次模板组进行必要的进一步分析，并在次模板比较完成后，应用与次模板相关的逻辑。这一过程重复执行，直至得出结论。然后，应用合适的服务功能模块 679。一旦确认为服务攻击尝试，便开始服务攻击处理。作为服务功能应用的一部分，通信应用块 667 发送消息给服务器和客户端设备，并将带有人为口令的统计数据收集界面显示在显示屏上，例如在有或没有浏览器的情况下显示弹出窗口。该统计值收集功能 669 还可结合服务器的通信量统计数据一起自动工作，以收集关于服务器内网页的通信量统计数据。

[0093] 网络接口 641 包含有线和无线分组交换接口 645、有线和无线电路交换接口 647。此外，网络接口 641 还可包括有内置的和单独的接口处理电路 643。网络接口 641 允许网络设备与其它网络设备、服务器和客户端设备通信。用户接口 649 包括显示器和键盘接口。这些用户接口 649 允许用户对本发明的支持服务器 655 的各个方面进行控制，例如手动 / 自动 / 半自动统计数据收集和分析，主模板和次模板以及相关逻辑等。

[0094] 其它实施例中，本发明的支持服务器电路 655 可包括更少或更多的部件，同样可包括更少或更多的功能。换句话说，图示的支持服务器 655 仅仅是根据本发明实现的可能功能性的一个示例。

[0095] 支持服务器 655 通过通信路径 635 通信连接至外部网络设备，例如中间节点 607。中间节点 607 包括处理电路 609、本地存储器 617、TDD 处理电路和 TDD 615。本地存储器 617 进一步包含有 SMM（服务模块管理器）619、PT、ST 和 AL（主模块、次模块和相关逻辑）621、SF（服务功能）623、SNTD（节点通信量统计数据）625 和 CA（通信应用块）627。中间节点 607 还具有其它部件，例如加密管线和解密管线（未示出）。

[0096] 支持服务器 655 具有三个主要功能 :(a) 收集与节点和服务器相关的通信量数据和统计值 ;(b) 提供次模板和逻辑以完成服务攻击尝试的检测 ;(c) 基于收集并分析后的通信量数据和统计值，生成并分配模板和逻辑给中间节点，其中该生成操作可手动、全自动或带有人为确认和编辑的半自动方式实现。模板和逻辑的自动生成通过通信应用块（通过与终端用户交互来参与统计数据的收集）例如 627 来完成。

[0097] 图 7 是根据本发明图 1 所示的实施例构建的路由器 755 的框图 705。路由器 755 可以是分组交换机或接入点。路由器电路 775 一般包括通用主处理卡 755、交换机 709 和多个线卡 715 至 781。线卡 715 至 781 在某些情况下可以完全不同。第一线卡 715 包括网络接口 725，其能够与有线和无线网络例如 10Mbit、1000Mbit 以太网和 5Gbit DWDM（密集波分复用）光纤网连接。第一线卡 715 还包括交换机接口 745，允许第一线卡与互连交换机 709 连接。此外，第一线卡 715 还包括次处理电路 735，用于在互连交换机 709 路由数据包之前对该数据包进行预处理。次处理电路 735 包含有转发引擎 737 和路由缓存。次处理电

路 735 除了对数据包进行预处理外，还包含有 PT 和 AL（主模板及相关逻辑）741。入站数据包先与主模板进行比较并应用相关逻辑。若出现网页请求和服务攻击尝试匹配的情况，则将该数据包传给通用主处理卡 755 进行进一步处理。次处理电路 735 还包含有节点通信量统计数据 739 和本地服务功能模块，以用于快速服务攻击处理。

[0098] 通用主处理卡 755 包括核心主处理电路 757，其通信连接至 TDD（通信量密度数据）处理电路和通信量密度数据 759。通用主处理卡 755 还包含服务模块管理器 (SMM)783、SP 和 AL（次模板和相关逻辑）785、SF（服务功能块）787 和 SNTD（节点通信量统计数据）789。若第一线卡 715 有转发数据包来，SMM 783 结合 SP 和 AL 785 以及 SF 787 一起，对网页请求和服务攻击尝试进行次级的分析和处理。

[0099] 图 8 是根据本发明图 1 所示的实施例构建的终端设备（服务器和 / 或客户端设备）807 的框图 805。终端设备电路 807 可指任何可发送和 / 或接收数据包的设备电路，该电路可部分或全部集成在图 1-4 所述的任何终端设备内。终端设备电路 807 一般包括处理电路 809、本地存储器 811、用户接口 831、和网络接口 855。这些部件通过一个或多个系统总线、专用通信路径或其它直接或间接通信路径彼此通信连接。在不同实施例中，处理电路 809 可以是微处理器、数字信号处理器、状态机、专用集成电路、现场可编程门阵列或其它处理电路。

[0100] 网络接口 855 包括有线和无线分组交换接口 859、有线和无线电路交换接口 861。此外，网络接口 859 还可包括内置的和单独的接口处理电路 857。网络接口 855 允许终端设备与任何其它终端设备通信。用户接口 831 包括显示器和键盘接口。

[0101] 本地存储器 811 可以是随机访问存储器、只读存储器、闪存、硬盘驱动器、光驱或可存储计算机指令和数据的其它类型的存储器。本地存储器 811 包含有通信应用块 813 和浏览器模块 815。本地存储器 811 还包含有浏览器应用块 827、以及操作系统 821 和浏览器 825。浏览器应用块 827 能够执行或编译下载的反服务攻击下载程序 817，帮助清除恶意代码，将该恶意代码通知给用户，并修复与恶意服务攻击相关的问题。这些下载程序 817 可由网络节点例如 811 在其检测到发往或发自终端设备电路 807 的数据包内的服务攻击尝试时提供。通信应用块 813 将消息和人为口令显示在显示屏上，例如无浏览器情况下的弹出窗口。

[0102] 其它实施例中，终端设备电路 807 可包括更少或更多的部件，同样可包括更少或更多的功能，并可应用于数据包交换而并非仅仅是语音包交换。换句话说，图示的终端设备仅仅是根据本发明实现的可能功能性的一个示例。

[0103] 终端设备 807 通过网络 875 通信连接至外部网络设备，例如远程设备 881。外部远程设备 881 还包括本发明的其它组件，例如处理电路 883 和本地存储器 895，该本地存储器 895 包括有 SMM（服务模块管理器）885、PT、ST 和 AL887、SF 891、SNTD（节点通信量统计数据）889 和 CA（通信应用块）893，以及本发明的其它功能块。服务器和客户端设备一般通过交换数据包彼此进行通信。这些数据包中可包含有网页请求和恶意代码引起的服务攻击尝试，其可能是故意的，也可能是无意的。当网络节点例如远程设备 881 检测到该服务攻击尝试时，其将采取多种可能处理步骤之一，如前结合图 4 所述。

[0104] 图 9 是图 1 所示的中间数据包路径节点的总的功能流程图 905。该流程开始于步骤 911，中间节点接收包含有网页请求的数据包，且该请求是服务攻击尝试。下一步骤 913

中，中间节点比较接收到的数据包与主模板，并通过使用通信量密度数据来应用相关逻辑。下一步骤 915 中，若主模板的相关逻辑有指示，中间节点将该数据包与次模板进行比较，并通过使用通信量密度数据来应用相关逻辑。

[0105] 步骤 917 中，中间节点对该数据包应用选择的服务功能，包括调用通信应用块。下一步骤 919 中，中间节点在必要的情况下发送带有口令机制的消息给服务器。基于响应，中间节点发送带有人为口令的消息给消息以及反服务攻击下载给客户端设备。然后，步骤 921 中，中间节点继续向服务器路由该数据包。

[0106] 图 10 是图 1 所示的中间数据包路径节点的详细功能流程图。网络设备的该功能流程开始于步骤 1007。下一步骤 1009 中，该中间节点通过网络接口接收传送的数据包。步骤 1011 中，该中间节点分析该数据包，将其与主模板进行比较。判断步骤 1013 中，中间节点验证是否有任何的匹配情况。若无网页请求匹配情况出现，则在步骤 1029 中，中间节点路由该数据包，然后该流程在步骤 1031 结束。

[0107] 如果在判断步骤 1013 发现有匹配，则在步骤 1015 中，中间节点通过使用通信量密度数据来应用与主模板相关的逻辑。下一步骤 1017 中，中间节点验证是否需要进行次模板比较。若是，则在步骤 1019 中，中间节点将该数据包与次模板进行比较来进一步分析该数据包。若无需进行次模板比较，该流程将跳转至下一步骤 1025。

[0108] 在判断步骤 1021 中，中间节点验证是否有匹配情况。若无网页请求或服务攻击尝试匹配，该流程跳转至步骤 1025。否则在步骤 1023 中，中间节点通过使用通信量密度数据来应用与次模板有关的逻辑。该通信量密度数据用于验证该网页请求是否为服务攻击尝试。

[0109] 下一步骤 1025 中，中间节点执行与服务器的通信应用交互操作。也即，在必要的情况下发送带有口令机制的消息给服务器。步骤 1027 中，中间节点执行与客户端设备的通信应用交互操作。该中间节点基于来自服务器或其它的响应，发送消息和反服务攻击下载程序给客户端设备，并接收客户端设备的响应。步骤 1029 中，中间节点路由该数据包，该流程进入结束步骤 1031。

[0110] 图 11 是图 1 所示的中间数据包路径节点通过使用通信量密度数据的通信量密度数据处理电路的功能流程图 1105。通信量密度数据处理电路的功能流程开始于步骤 1107。然后在步骤 1109 中，该通信量密度数据处理电路接收来自服务模块管理器的数据包。步骤 1111 中，该通信量密度数据处理电路使用通信量密度数据和 / 或节点通信量统计数据来判断服务器是否正遭受服务攻击。

[0111] 步骤 1113 中，该通信量密度数据处理电路执行或者提示通信应用块执行与服务器的通信应用交互操作。也即，在必要的情况下发送具有口令机制的消息给服务器，并请求服务器对当前网页请求的响应。步骤 1115 中，通信量密度数据处理电路执行或提示通信应用块执行与客户端设备的通信应用交互操作。通信量密度数据处理电路基于来自服务器的响应或其它，发送消息和反服务攻击下载程序给客户端设备并接收客户端设备的响应。然后，步骤 1117 中，通信量密度数据处理电路指示处理电路向服务器路由数据包。如有设置要求，通信量密度数据处理电路丢弃包含有网页请求的数据包，或将该数据包重新路由给另一服务器。此外，通信量密度数据处理电路可向客户端设备提供帮助以修复恶意代码。该通信量密度数据处理电路的功能流程在步骤 1119 中结束。

[0112] 本领域普通技术人员可知，本申请中所使用的短语“通信连接”包括有线的和无线的、直接的连接和通过其它组件、元件或模块的间接连接。本领域普通技术人员还可知，推定连接（即推定一个部件与另一个部件连接）包括两个部件之间与“通信连接”方式相同的无线的和有线的、直接的和间接的连接。

[0113] 本发明通过借助方法步骤展示了本发明的特定功能及其关系。所述方法步骤的范围和顺序是为了便于描述任意定义的。只要能够执行特定的功能和顺序，也可应用其它界限和顺序。任何所述或选的界限或顺序因此落入本发明的范围和精神实质。

[0114] 本发明还借助功能模块对某些重要的功能进行了描述。所述功能模块的界限和各种功能模块的关系是为了便于描述任意定义的。只要能够执行特定的功能，也可应用其它的界限或关系。所述其它的界限或关系也因此落入本发明的范围和精神实质。

[0115] 本领域普通技术人员还可知，本申请中的功能模块和其它展示性模块和组件可实现为离散组件、专用集成电路、执行恰当软件的处理器和前述的任意组合。

[0116] 此外，尽管以上是通过一些实施例对本发明进行的描述，本领域技术人员知悉，本发明不局限于这些实施例，在不脱离本发明的精神和范围的情况下，可以对这些特征和实施例进行各种改变或等效替换。本发明的保护范围仅由本申请的权利要求书来限定。

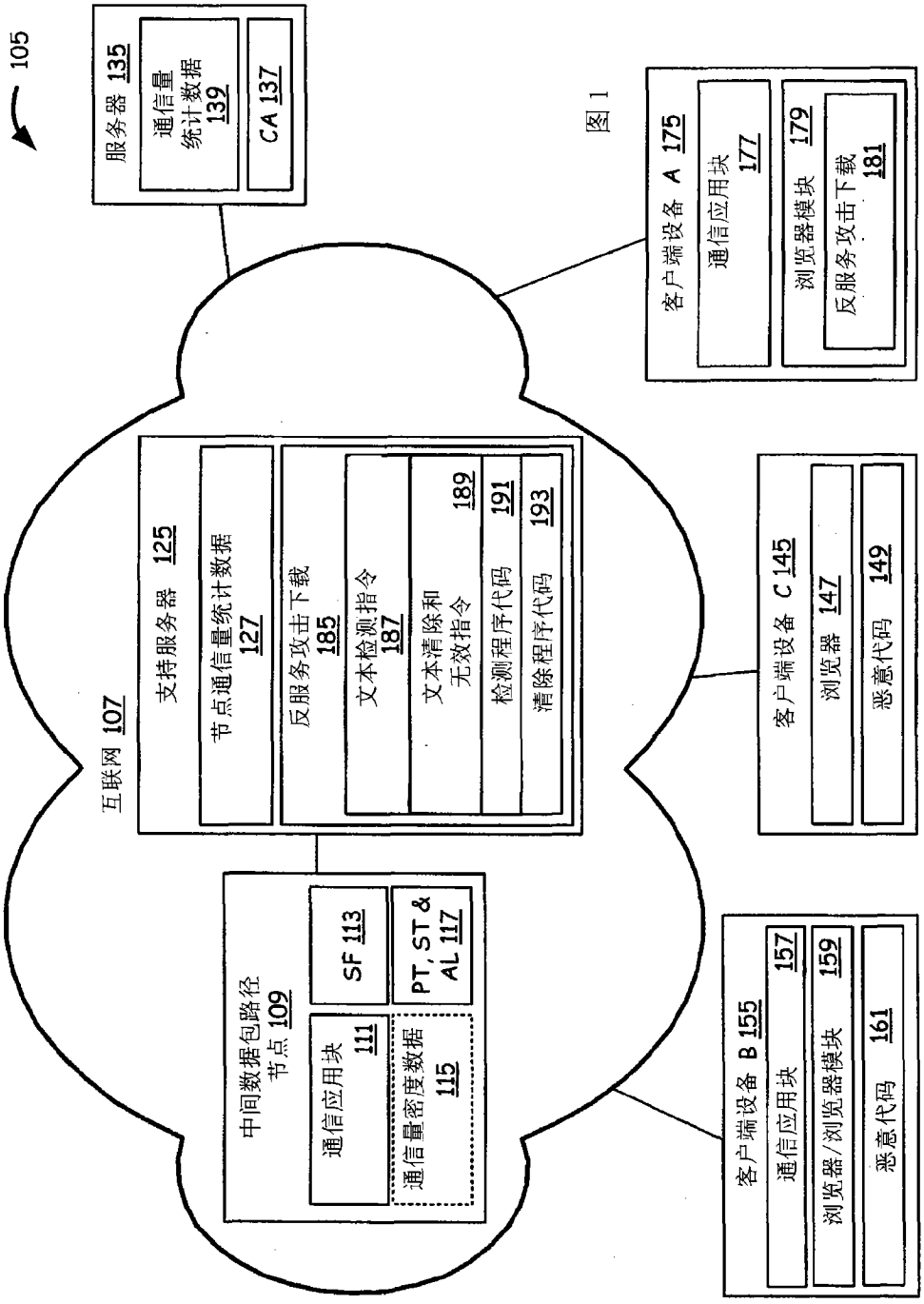

105
服务器 135
通信量统计数据 139
CA 137
互联网 107
支持服务器 125
节点通信量统计数据 127
反服务攻击下载 185
文本检测指令 187
文本清除和无效指令 189
检测程序代码 191
清除程序代码 193
中间数据包路径节点 109
通信应用块 111
通信量密度数据 115
SF 113
PT, ST & AL 117
客户端设备 A 175
通信应用块 177
浏览器模块 179
反服务攻击下载 181
客户端设备 C 145
浏览器 147
恶意代码 149
客户端设备 B 155
通信应用块 157
浏览器/浏览器模块 159
恶意代码 161

图 1

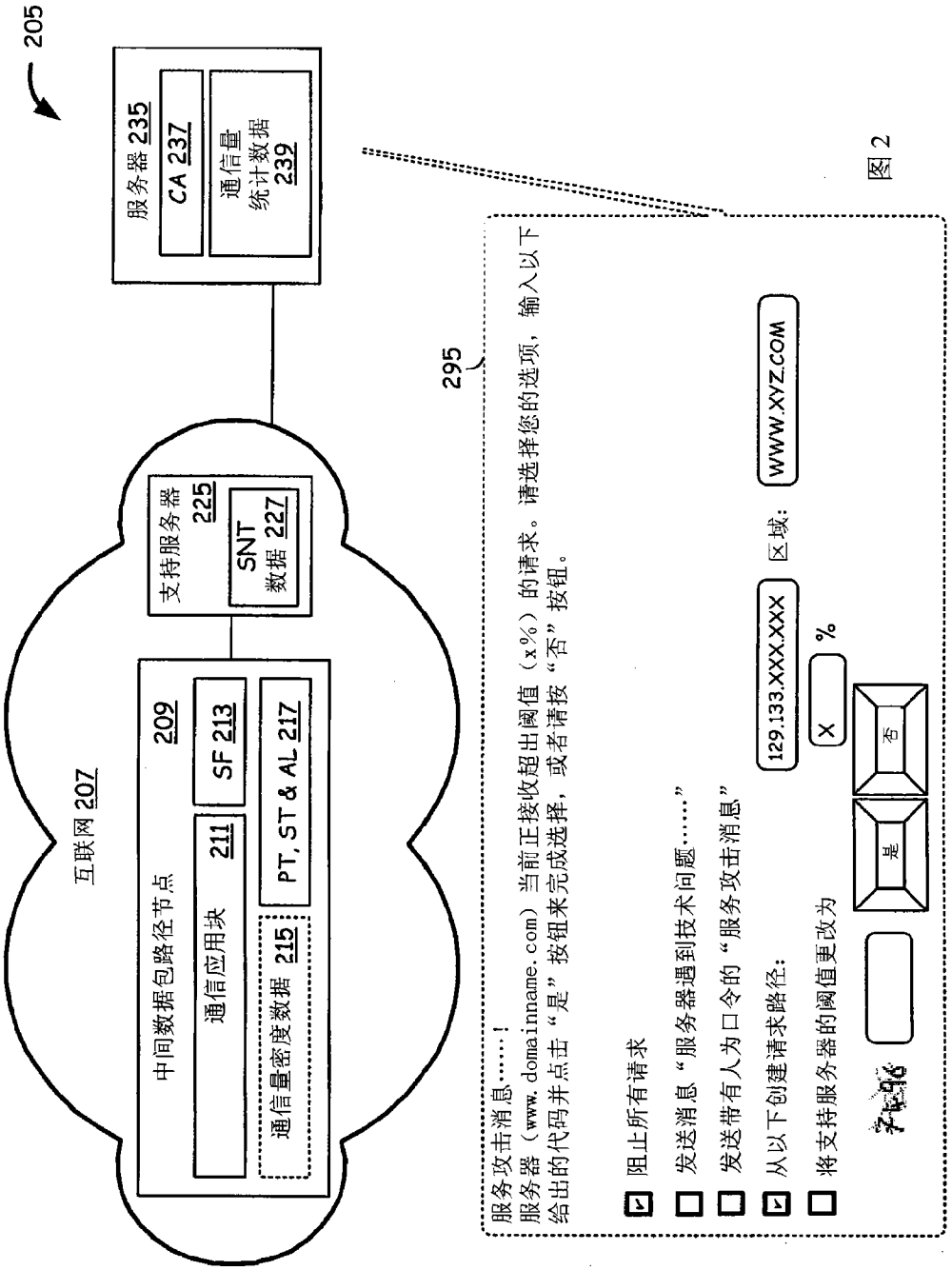

205
服务器 235
CA 237
通信量统计数据 239
互联网 207
中间数据包路径节点 209
通信应用块 211
SF 213
通信量密度数据 215
PT, ST & AL 217
支持服务器 225
SNT 数据 227
295
服务攻击消息……!
服务器（www.domainname.com）当前正接收超出阈值（x%）的请求。请选择您的选项，输入以下给出的代码并点击“是”按钮来完成选择，或者请按“否”按钮。
阻止所有请求
发送消息“服务器遇到技术问题……”
发送带有人为口令的“服务攻击消息”
从以下创建请求路径:
129.133.XXX.XXX
区域:
WWW.XYZ.COM
将支持服务器的阈值更改为
X
%
是
否

图 2

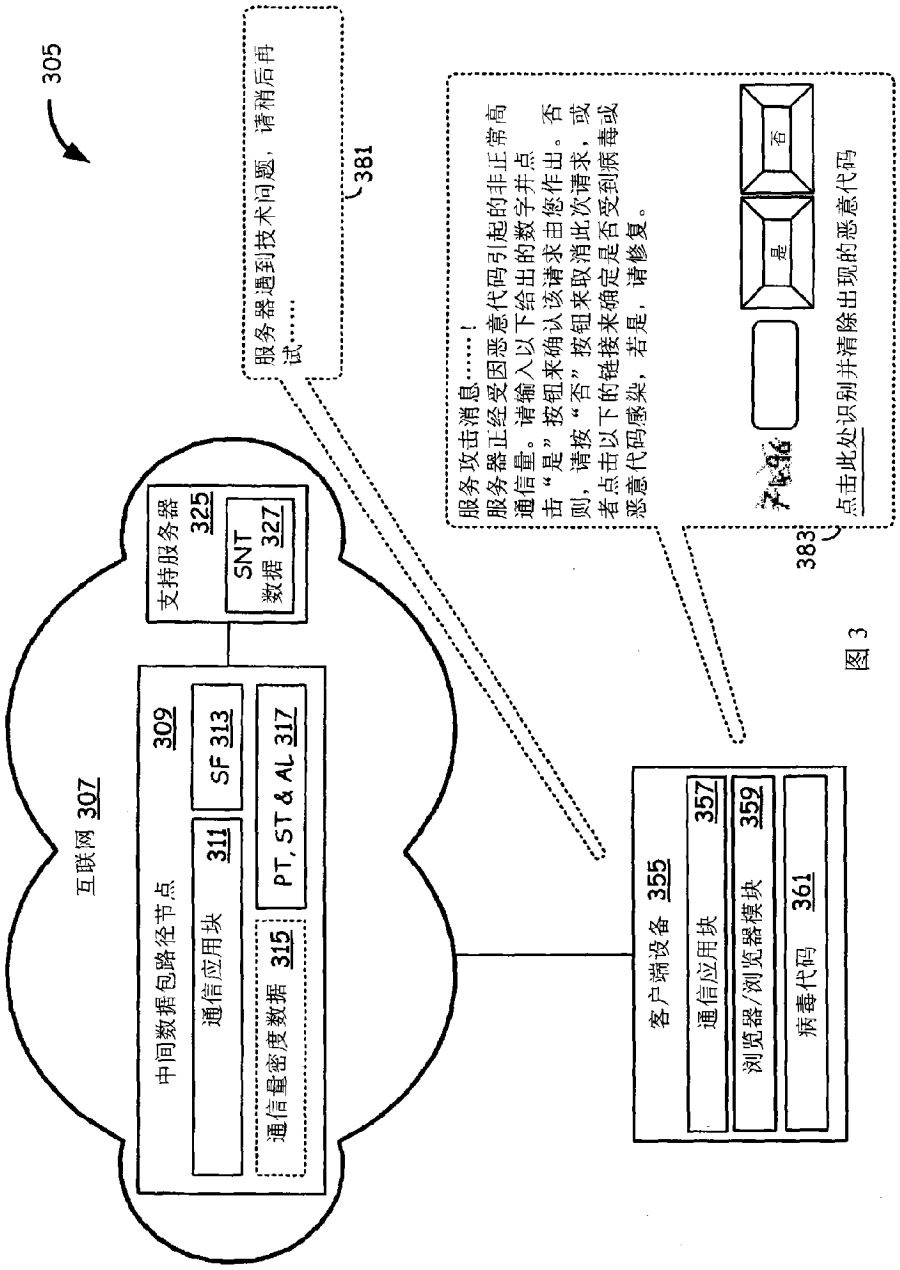

305
互联网 307
中间数据包路径节点 309
通信应用块 311
SF 313
通信量密度数据 315
PT, ST & AL 317
支持服务器 325
SNT 数据 327
客户端设备 355
通信应用块 357
浏览器/浏览器模块 359
病毒代码 361
服务器遇到技术问题，请稍后再试……
381
服务攻击消息……！
服务器正经受因恶意代码引起的非正常高通信量。请输入以下给出的数字并点击“是”按钮来确认该请求由您作出。否则，请按“否”按钮来取消此次请求，或者点击以下的链接来确定是否受到病毒或恶意代码感染，若是，请修复。
是
否
383
点击此处识别并清除出现的恶意代码

图 3

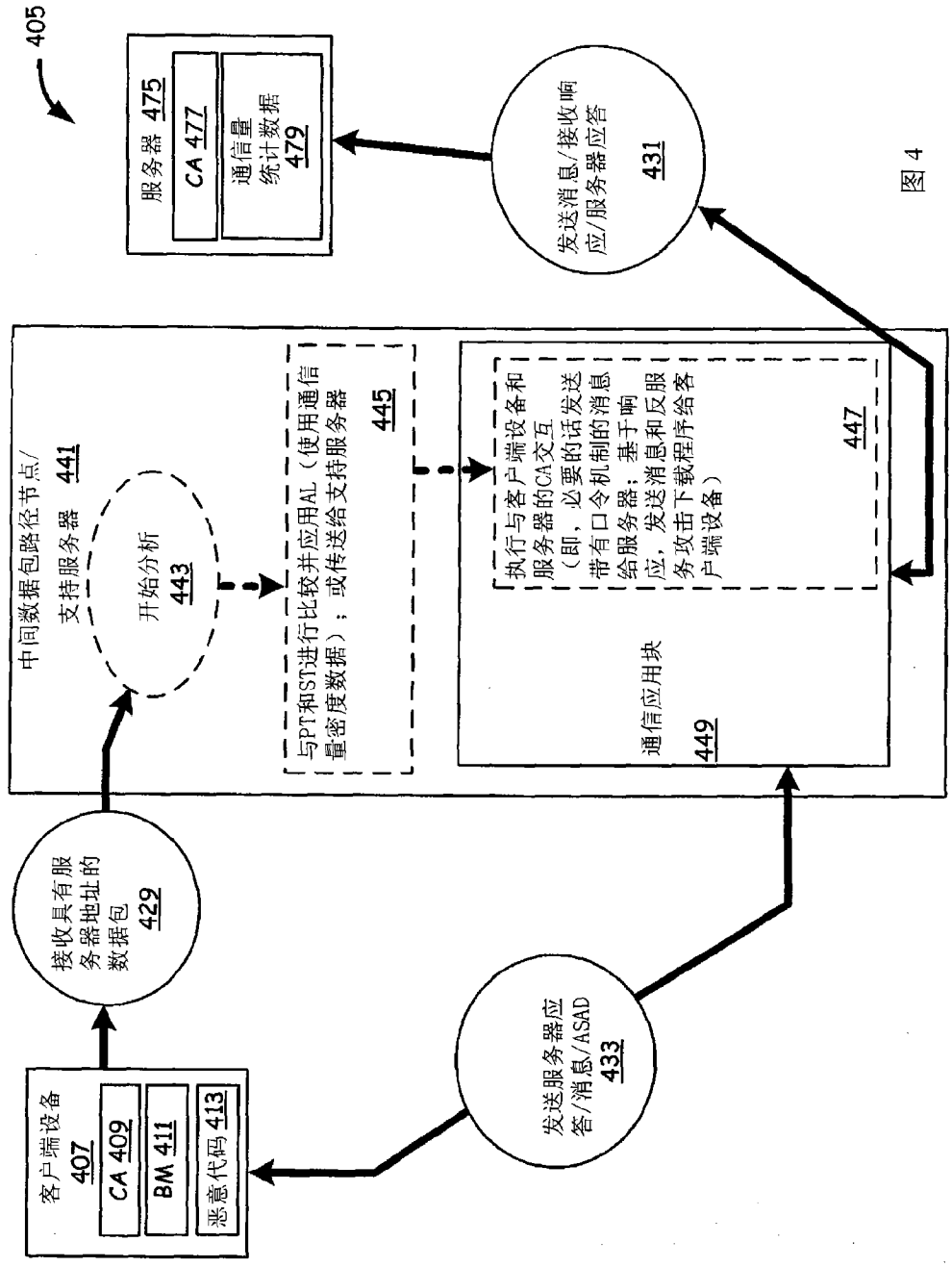

405
服务器 475
CA 477
通信量统计数据 479
发送消息/接收响应/服务器应答 431
中间数据包路径节点/支持服务器 441
开始分析 443
与PT和ST进行比较并应用AL（使用通信量密度数据）；或传送给支持服务器 445
执行与客户端设备和服务器的CA交互（即，必要的话发送带有口令机制的消息给服务器；基于响应，发送消息和反服务攻击下载程序给客户端设备） 447
通信应用块 449
接收具有服务器地址的数据包 429
发送服务器应答/消息/ASAD 433
客户端设备 407
CA 409
BM 411
恶意代码 413

图 4

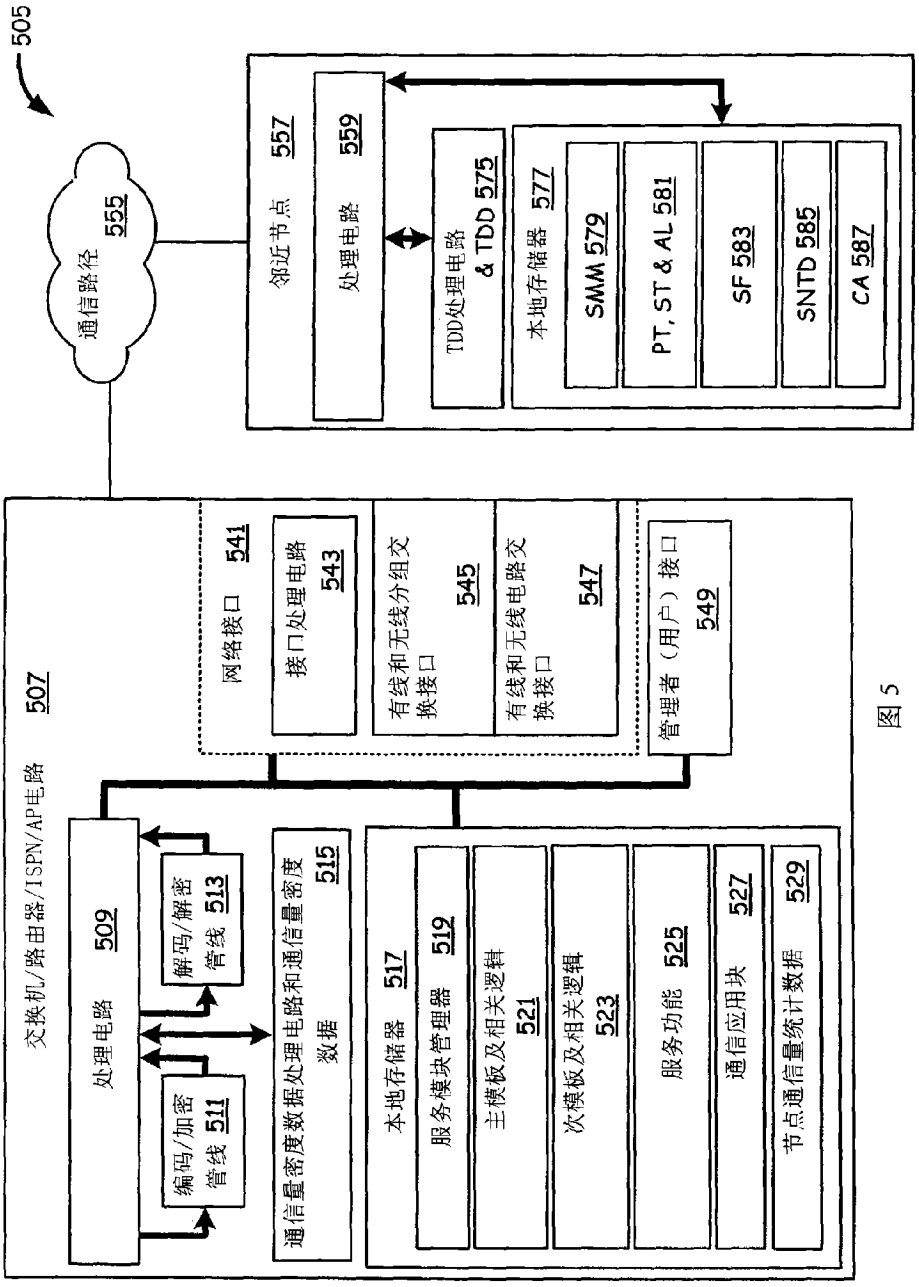

505
通信路径 555
邻近节点 557
处理电路 559
TDD处理电路 & TDD 575
本地存储器 577
SMM 579
PT, ST & AL 581
SF 583
SNTD 585
CA 587
交换机/路由器/ISPN/AP电路 507
处理电路 509
编码/加密管线 511
解码/解密管线 513
通信量密度数据处理电路和通信量密度数据 515
网络接口 541
接口处理电路 543
有线和无线分组交换接口 545
有线和无线电路交换接口 547
管理者（用户）接口 549
本地存储器 517
服务模块管理器 519
主模板及相关逻辑 521
次模板及相关逻辑 523
服务功能 525
通信应用块 527
节点通信量统计数据 529

图 5

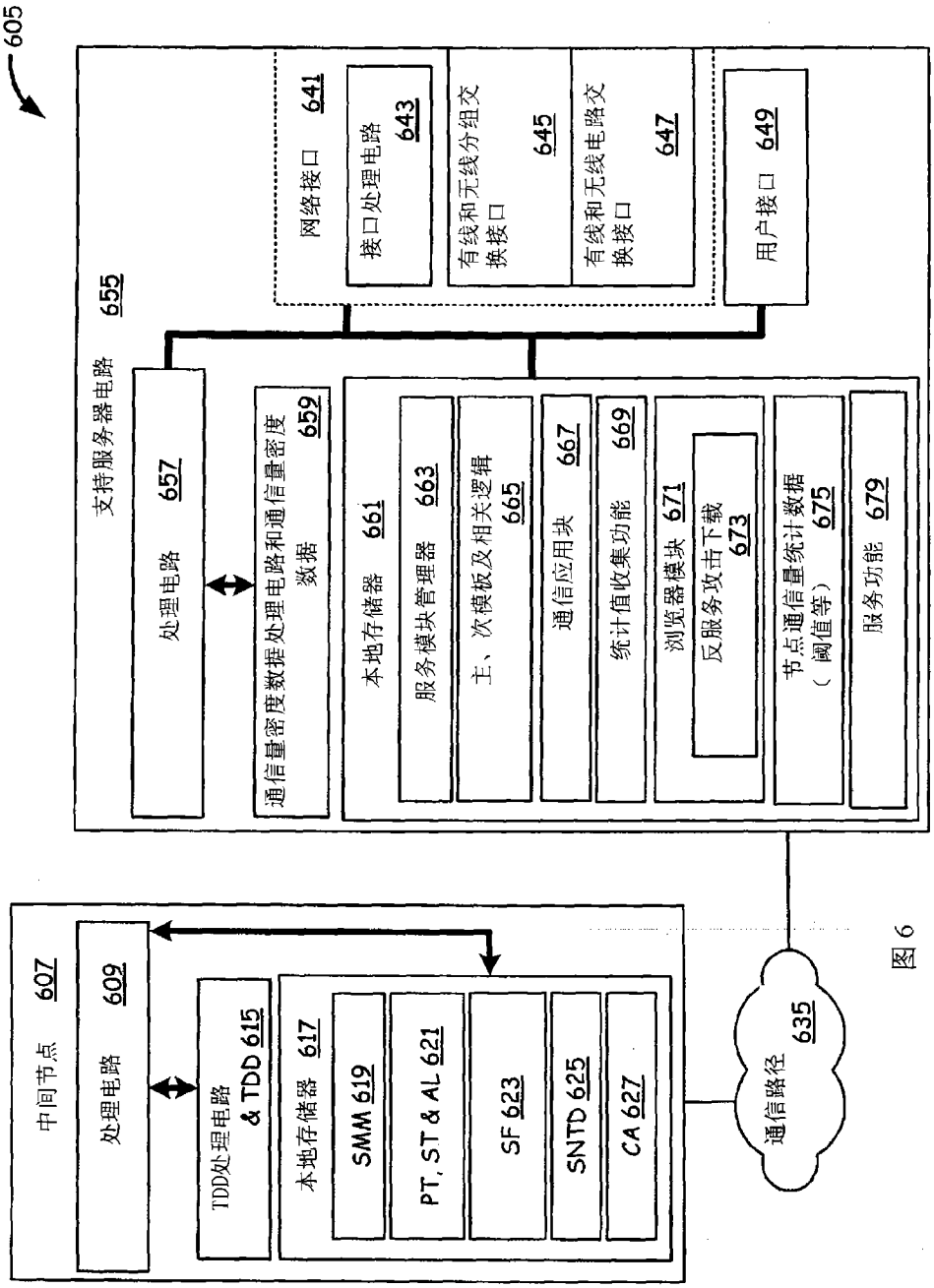

605
支持服务器电路 655
处理电路 657
通信量密度数据处理电路和通信量密度数据 659
本地存储器 661
服务模块管理器 663
主、次模板及相关逻辑 665
通信应用块 667
统计值收集功能 669
浏览器模块 671
反服务攻击下载 673
节点通信量统计数据（阈值等） 675
服务功能 679
网络接口 641
接口处理电路 643
有线和无线分组交换接口 645
有线和无线电路交换接口 647
用户接口 649
中间节点 607
处理电路 609
TDD处理电路 & TDD 615
本地存储器 617
SMM 619
PT, ST & AL 621
SF 623
SNTD 625
CA 627
通信路径 635

图 6

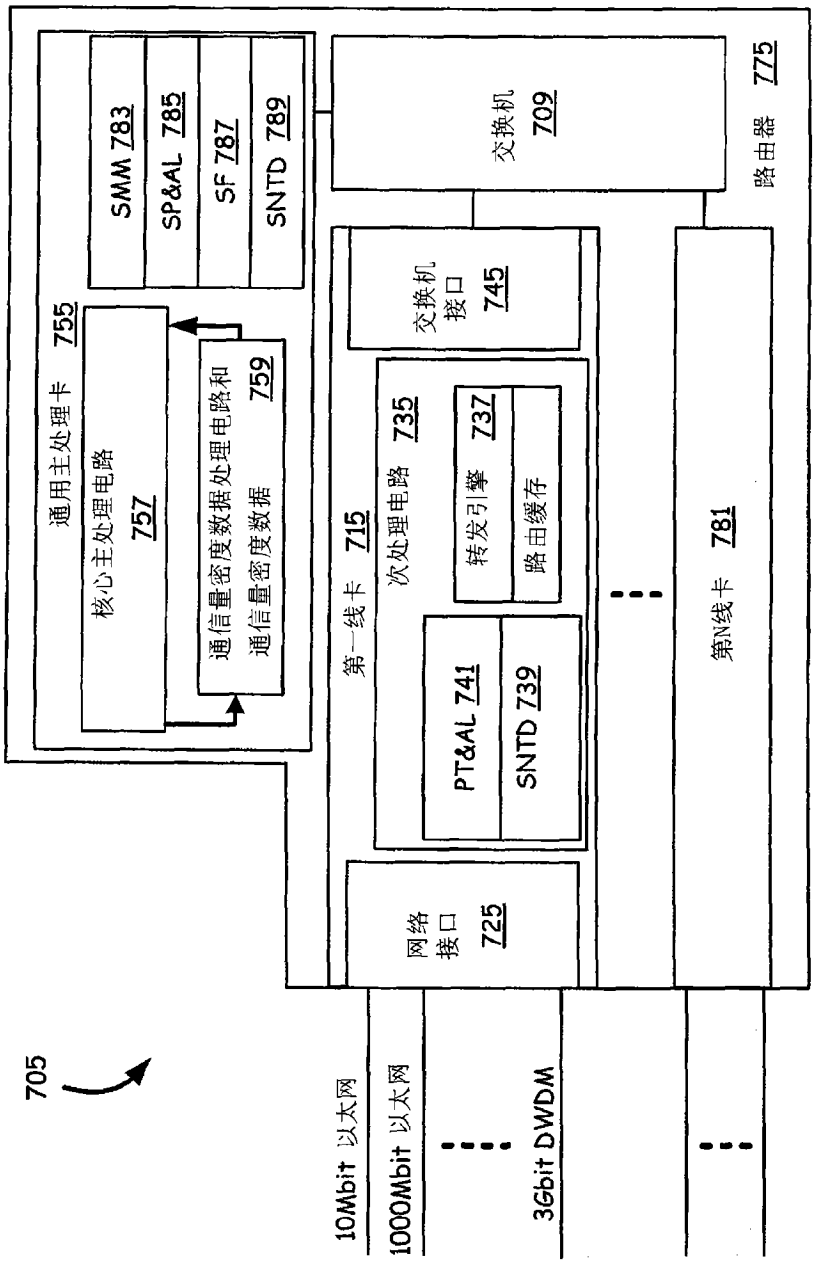

705
通用主处理卡 755
核心主处理电路 757
通信量密度数据处理电路和通信量密度数据 759
SMM 783
SP&AL 785
SF 787
SNTD 789
交换机 709
路由器 775
交换机接口 745
第一线卡 715
次处理电路 735
转发引擎 737
路由缓存
PT&AL 741
SNTD 739
网络接口 725
第N线卡 781
10Mbit 以太网
1000Mbit 以太网
3Gbit DWDM

图 7

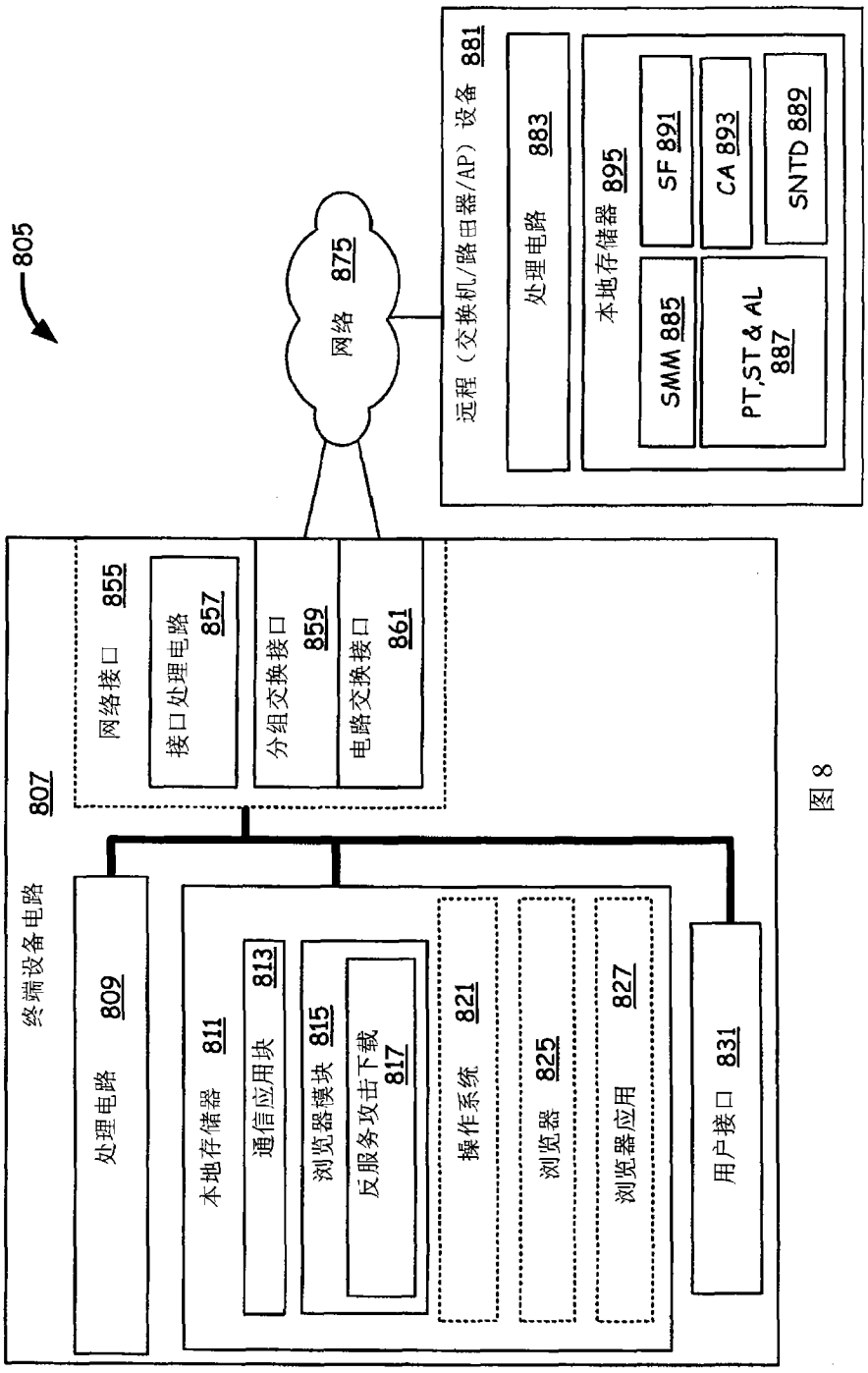

805
网络 875
远程（交换机/路由器/AP）设备 881
处理电路 883
本地存储器 895
SF 891
CA 893
SNTD 889
SMM 885
PT,ST & AL 887
终端设备电路 807
网络接口 855
接口处理电路 857
分组交换接口 859
电路交换接口 861
处理电路 809
本地存储器 811
通信应用块 813
浏览器模块 815
反服务攻击下载 817
操作系统 821
浏览器 825
浏览器应用 827
用户接口 831

图 8

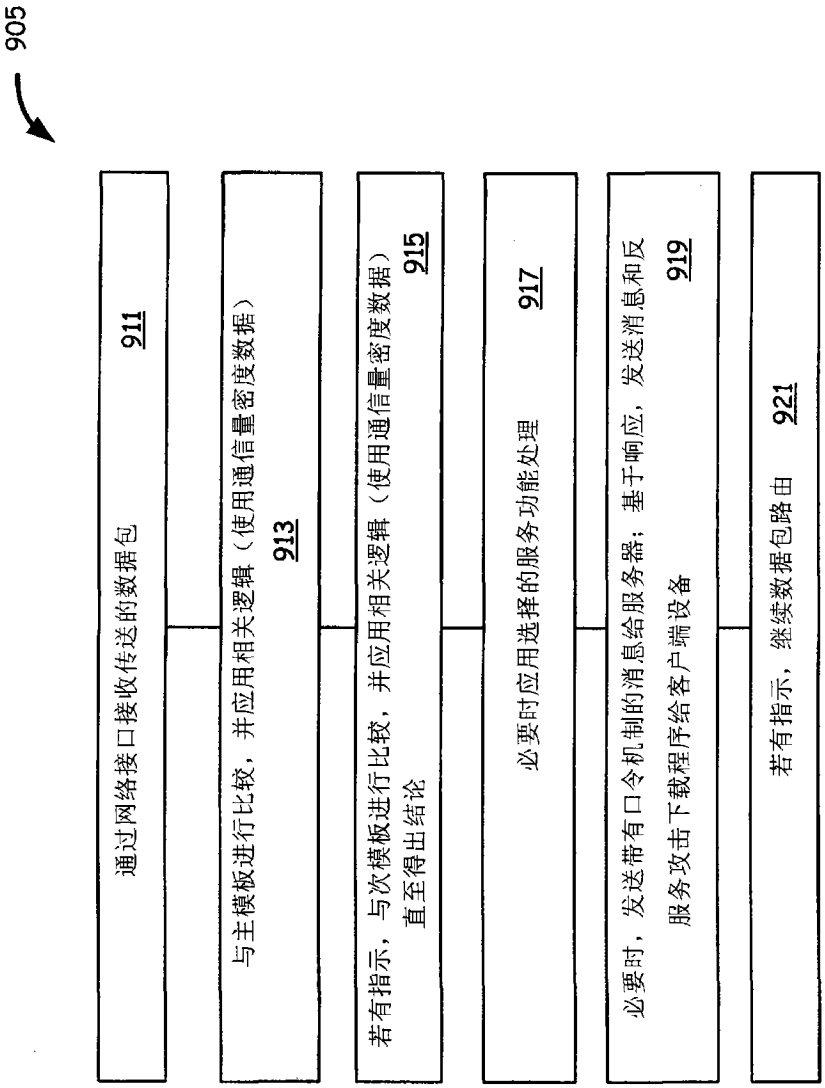

905
通过网络接口接收传送的数据包 911
与主模板进行比较，并应用相关逻辑（使用通信量密度数据） 913
若有指示，与次模板进行比较，并应用相关逻辑（使用通信量密度数据）直至得出结论 915
必要时应用选择的服务功能处理 917
必要时，发送带有口令机制的消息给服务器；基于响应，发送消息和反服务攻击下载程序给客户端设备 919
若有指示，继续数据包路由 921

图 9

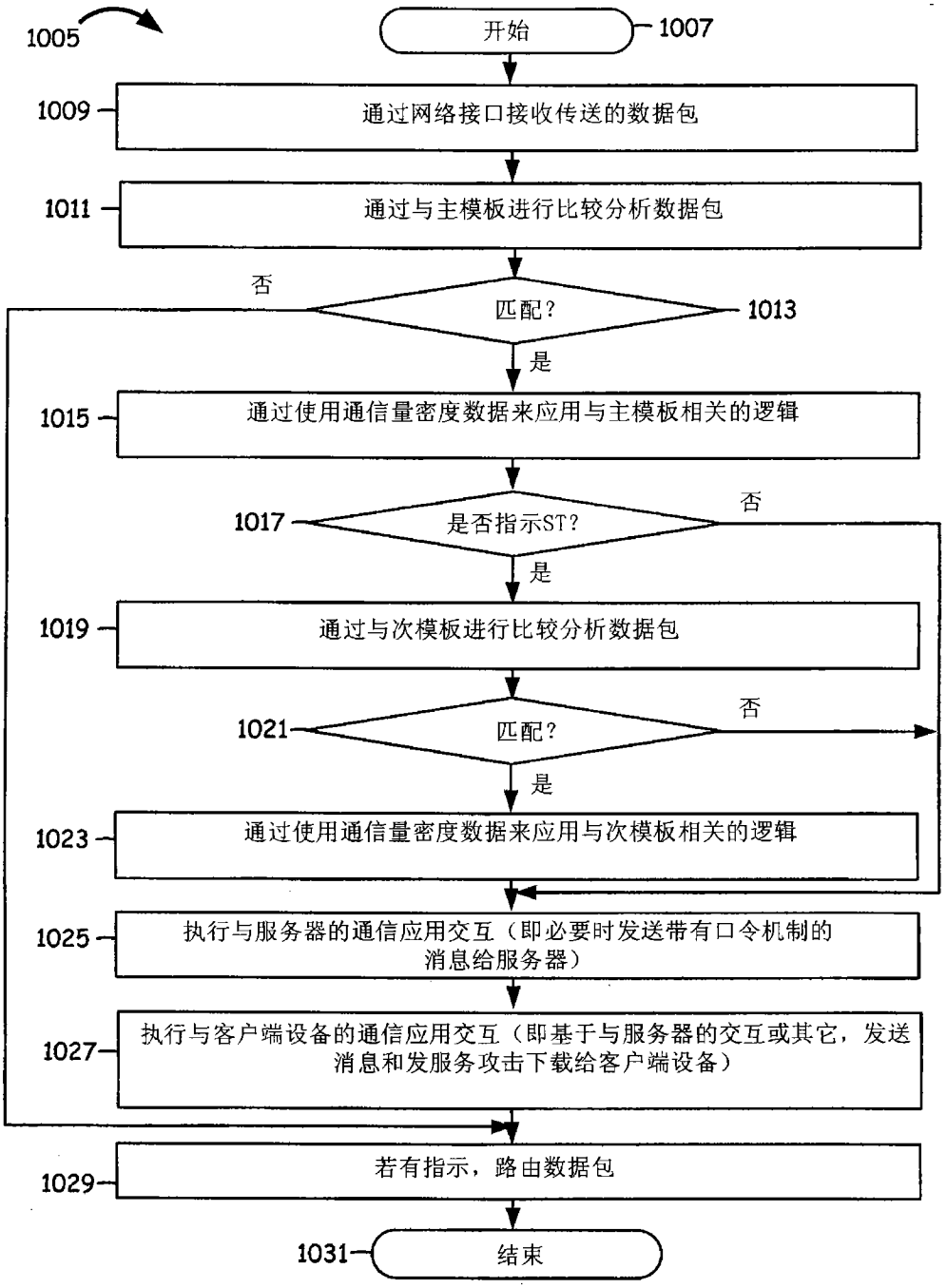

1005
开始
1007
1009
通过网络接口接收传送的数据包
1011
通过与主模板进行比较分析数据包
否
匹配?
1013
是
1015
通过使用通信量密度数据来应用与主模板相关的逻辑
1017
是否指示ST?
否
是
1019
通过与次模板进行比较分析数据包
1021
匹配?
否
是
1023
通过使用通信量密度数据来应用与次模板相关的逻辑
1025
执行与服务器的通信应用交互（即必要时发送带有口令机制的消息给服务器）
1027
执行与客户端设备的通信应用交互（即基于与服务器的交互或其它，发送消息和发服务攻击下载给客户端设备）
1029
若有指示，路由数据包
1031
结束

图 10

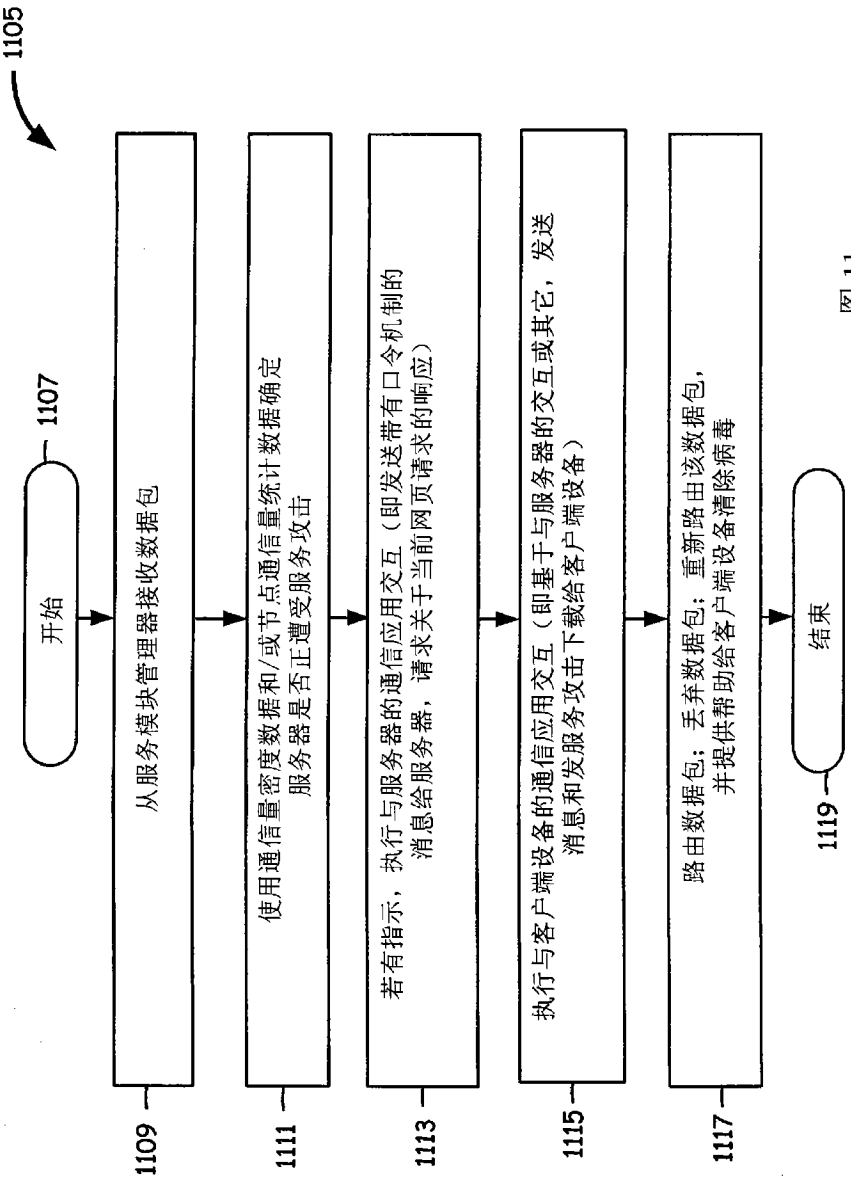

1105
开始
1107
从服务模块管理器接收数据包
1109
使用通信量密度数据和/或节点通信量统计数据确定服务器是否正遭受服务攻击
1111
若有指示，执行与服务器的通信应用交互（即发送带有口令机制的消息给服务器，请求关于当前网页请求的响应）
1113
执行与客户端设备的通信应用交互（即基于与服务器的交互或其它，发送消息和发服务攻击下载给客户端设备）
1115
路由数据包；丢弃数据包；重新路由该数据包，并提供帮助给客户端设备清除病毒
1117
结束
1119

图 11