[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 9/00 (2006.01)

[12] 发明专利申请公布说明书

[21] 申请号 200580010423.0

[43] 公开日 2007 年 3 月 28 日

[11] 公开号 CN 1938982A

[22] 申请日 2005.3.17
[21] 申请号 200580010423.0
[30] 优先权
[32] 2004. 4. 7 [33] US [31] 10/820,980
[86] 国际申请 PCT/US2005/008859 2005.3.17
[87] 国际公布 WO2005/101721 英 2005.10.27
[85] 进入国家阶段日期 2006.9.29
[71] 申请人 思科技术公司
地址 美国加利福尼亚州
[72] 发明人 阿莫·卡里 米特什·德拉尔
阿纳恩萨·拉迈阿
沙拉德·阿拉瓦特

[74] 专利代理机构 北京东方亿思知识产权代理有限责任公司
代理人 王 怡

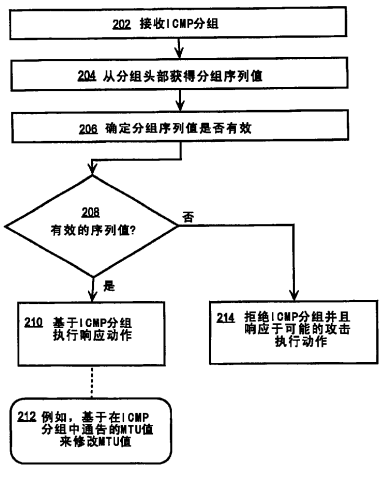
权利要求书 3 页 说明书 11 页 附图 4 页

[54] 发明名称

通过认证因特网控制消息协议分组来防止网络攻击的方法和装置

[57] 摘要

本发明公开了一种用于防止网络上的攻击的方法。该方法包括计算机实现的以下步骤：接收包括有与面向连接的传输协议的连接相关联的头部的拷贝的 ICMP 分组(202)；从该头部获得分组序列值(204)；确定该分组序列值是否有效(206)；以及仅在该分组序列值被确定为有效时才更新与传输协议连接相关联的参数值。使用所公开的方法使得能够对 ICMP 分组(202)进行认证，以使得仅在 ICMP 分组(202)被确定为可信的时才执行诸如调整 MTU 值之类的网络元件的响应措施。



1. 一种用于防止网络上的攻击的计算机系统，该计算机系统包括数据处理器、耦合到分组交换网络的网络接口、以及存储可由所述数据处理器执行的一个或多个指令序列的存储器，所述存储器特征在于用于下述过程的指令：接收包括有与面向连接的传输协议的连接相关联的头部的拷贝的 ICMP 分组；从所述头部获得分组序列值；确定所述分组序列值是否有效；以及仅在所述分组序列值被确定为有效时才更新与所述传输协议连接相关联的参数值。

2. 如权利要求 1 所述的计算机系统，其中，所述 ICMP 分组包括与 TCP 连接相关联的 TCP 头部的拷贝。

3. 如权利要求 1 所述的计算机系统，其中，所述 ICMP 分组是 ICMP “端点不可达”错误分组。

4. 如权利要求 1 所述的计算机系统，其中，所述 ICMP 分组指定需要分段。

5. 如权利要求 1 所述的计算机系统，其中，所述存储器特征在于用于下述过程的指令：确定所述分组序列值是否在所述连接的传输协议允许的分组序列值的范围内。

6. 如权利要求 1 所述的计算机系统，其中，所述存储器特征在于用于下述过程的指令：确定所述分组序列值是否在所述连接的已发送但是尚未确认的 TCP 分组序列值的范围内。

7. 如权利要求 1 所述的计算机系统，其中，所述存储器特征在于用于下述过程的指令：从导致接收到所述 ICMP 分组的先前已发送的片段的序列值开始，确定所述分组序列值是否与当前存储在 TCP 重传缓冲区中的一个或多个分组的一个或多个分组序列值精确相等。

8. 如权利要求 1 所述的计算机系统，其中，所述计算机系统是充当 TCP 端点节点的路由器。

9. 如权利要求 1 所述的计算机系统，其中，所述计算机系统是防火墙设备。

10. 一种用于防止网络上的攻击的计算机系统，用于防止网络上的攻击，该计算机系统包括数据处理器、耦合到分组交换网络的网络接口、以及存储可由所述数据处理器执行的一个或多个指令序列的存储器，所述存储器特征在于用于下述过程的指令：在 TCP/IP 分组交换网络中的 TCP 端点节点处接收包括有与 TCP 连接相关联的 TCP 头部的拷贝的 ICMP 分组；从所述 TCP 头部获得分组序列号；确定所述分组序列号是否有效；以及仅在所述分组序列号被确定为有效时才更新与所述 TCP 连接相关联的最大传输单元（MTU）值。

11. 如权利要求 10 所述的计算机系统，其中，所述 ICMP 分组是 ICMP“端点不可达”错误分组。

12. 如权利要求 10 所述的计算机系统，其中，所述 ICMP 分组指定需要分段。

13. 如权利要求 10 所述的计算机系统，其中，所述存储器特征在于用于下述过程的指令：确定所述分组序列号是否在所述连接允许的 TCP 分组序列号的范围内。

14. 如权利要求 10 所述的计算机系统，其中，所述存储器特征在于用于下述过程的指令：确定所述分组序列号是否在所述连接的已发送但是尚未确认的 TCP 分组序列值的范围内。

15. 如权利要求 10 所述的计算机系统，其中，所述存储器特征在于用于下述过程的指令：从导致接收到所述 ICMP 分组的先前已发送的片段的序列值开始，确定所述分组序列号是否与当前存储在 TCP 重传缓冲区中的一个或多个分组的一个或多个序列号精确相等。

16. 如权利要求 10 所述的计算机系统，其中，所述计算机系统包括充当 TCP 端点节点的路由器。

17. 如权利要求 10 所述的计算机系统，其中，所述计算机系统包括防火墙设备。

18. 一种承载一个或多个指令序列的计算机可读介质，所述指令在由一个或多个处理器执行时致使所述一个或多个处理器执行下述步骤：接收包括有与面向连接的传输协议的连接相关联的头部的拷贝的 ICMP 分组；

从所述头部获得分组序列值；确定所述分组序列值是否有效；以及仅在所述分组序列值被确定为有效时才更新与所述传输协议连接相关联的参数值。

19. 一种用于防止网络上的攻击的装置，包括：

用于接收包括有与面向连接的传输协议的连接相关联的头部的拷贝的ICMP 分组的装置；

用于从所述头部获得分组序列值的装置；

用于确定所述分组序列值是否有效的装置；以及

用于仅在所述分组序列值被确定为有效时才更新与所述传输协议连接相关联的参数值的装置。

20. 如权利要求 19 所述的装置，其中，所述用于接收 ICMP 分组的装置包括用于接收包括有与 TCP 连接相关联的 TCP 头部的拷贝的 ICMP 分组的装置。

21. 如权利要求 19 所述的装置，其中，所述用于接收 ICMP 分组的装置包括用于接收 ICMP“端点不可达”错误分组的装置。

22. 如权利要求 19 所述的装置，其中，所述用于接收 ICMP 分组的装置包括用于接收指定需要分段的 ICMP 分组的装置。

23. 如权利要求 19 所述的装置，其中，所述用于确定所述分组序列值是否有效的装置包括用于确定所述分组序列值是否在所述连接的传输协议允许的分组序列值的范围内的装置。

24. 如权利要求 19 所述的装置，其中，所述用于确定所述分组序列值是否有效的装置包括用于确定所述分组序列值是否在所述连接的已发送但是尚未确认的 TCP 分组序列值的范围内的装置。

25. 如权利要求 19 所述的装置，其中，所述用于确定所述分组序列值是否有效的装置包括用于确定所述分组序列值是否与当前存储在 TCP 重传缓冲区中的一个或多个分组的一个或多个序列值相等的装置。

26. 如权利要求 19 所述的装置，包括充当 TCP 端点节点的路由器。

27. 如权利要求 19 所述的装置，包括防火墙设备。

通过认证因特网控制消息协议分组来防止网络攻击的方法和装置

技术领域

本发明一般地涉及防止计算机网络上的攻击。更具体地说，本发明涉及用于防止通过因特网控制消息协议实行的网络攻击的方法。

背景技术

本发明所述方法可以被实现，但是不一定是先前已设想出或者已实现了的方法。因此，除非在这里另行指出，本发明所述方法不是本申请的权利要求的现有技术，并且不因为被包括在该部分中而承认是现有技术。

基于传输控制协议和因特网协议（TCP/IP）的网络和互连网依赖于用于处理网络中的错误状况的因特网控制消息协议（“ICMP”）。ICMP 是在因特网工程任务组（IETF）的 RFC（请求注解）792 中定义的。参与互连网或全球因特网的路由器、交换机和其他网络元件使用 ICMP 来交换错误处理信息。在这些网络元件上运行的 ICMP 代理可以产生错误消息和通知消息，所述错误消息例如是 ICMP 目的地不可达消息，所述通知消息例如是 ICMP 回送请求和答复消息。

路由器接收到 ICMP 错误消息分组时作出的响应取决于在该 ICMP 分组中承载的类型值。在 RFC 792 中，未要求对 ICMP 分组的源进行认证，并且 ICMP 的实现方式也不提供这种认证。多数 ICMP 实现方式对 ICMP 分组中承载的 IP 地址进行验证，有时也验证其中的 TCP 端口号，但是这种验证级别不足以防止大多数类型的攻击。结果，虚假的 ICMP 分组可能给出错误状况的假象，导致路由器以不希望的方式对不存在的错误状况作出响应。某些响应可能导致拒绝对客户端的服务，或者导致较差的服务质量。因此，网络管理员希望具有一种方式，用于路由器或其他网络元件在执行响应动作之前确定 ICMP 分组的可信性。

下面是仅仅一个虚假的 ICMP 分组可能如何导致灾难性结果的示例。

路径 MTU 发现（PMTU）是这样一种方法，该方法由 TCP 用来智能发现特定连接的路径最大传输单元（MTU）。其目的是找到一条路径的 MTU 值，以便使用该 MTU 值作为 TCP 片段大小，而不是使用默认的为 536 的 TCP 片段大小。PMTU 试图找到比 536 大的最小 MTU，从而导致较高的沿该路径的数据吞吐量。

PMTU 发现是通过发送下述 ICMP 分组实现的：在该 ICMP 分组中，IP 头部中的“不分段”（DF）位被设置，并且具有连续较大的分段大小值。当接收到包括已导致指定分段大小值错误的接口的 MTU 的 ICMP“不可达”型分组时，较小的 MTU 被发现。TCP 实现方式采取的纠正动作是在接下来数分钟内使用嵌入在 ICMP 分组中的 MTU 值，然后尝试使用较大的值。典型情况下在 10 分钟内使用相同的 MTU 值。

然而，ICMP 不可达分组易受未经授权的或者说恶意方欺骗。欺骗该分组仅需的特定信息是一个四元组的值，包括两个 IP 地址和两个端口号。一个端口号一般是公知的端口号，另一个端口号可以容易地猜出，因为大多 TCP 实现方式仅递增公知的端口号以创建用于后继连接的端口号。此外，恶意方通常可以从在因特网内公开的边界网关协议（BGP）流映射获得参与 TCP 连接的路由器的 IP 地址。

TCP 主机被允许接受最小为 68 的 MTU，该值反映出 40 字节的 TCP-IP 头部数据后的 28 字节的数据。因此，通告一个 70 字节的 MTU 的虚假的 ICMP 分组将导致 TCP 实现方式在 10 分钟内使用 30 个字节作为分段大小。在 10 分钟后接收并处理另一个 MTU 为 70 的虚假的 ICMP 分组将导致连接在另一个 10 分钟内继续处于减速状况中。

使用 PMTU 的 TCP 应用的示例包括 BGP 和 FTP，它们通常需要交换大量的数据。这些应用和其他应用可能易受到这里所述的攻击。对于类似于 BGP 的协议，分组传输时间尤其关键，因此使连接减速可能导致灾难性后果。在 FreeBSD 操作系统及其派生操作系统中的 TCP 实现方式都易受到上述攻击。许多其他 TCP 栈实现方式都表现出相同的可能行为。在因特网协议版本 6（IPv6）下，ICMP 分组被用在邻居发现过程、路径 MTU 发现和多播监听者发现（MLD）协议中。IPv6 路由器使用 MLD 来发现直接

附接的链路上的多播监听者，包括希望接收去往特定多播地址的多播分组的节点。基本 IPv6 分组头部的下一头部字段中的值 58 标识出 IPv6 ICMP 分组。类似的标识符用在 IPv4 中。就 ICMP 分组紧随所有扩展头部并且是 IPv6 分组中的最后一个信息段来说，IPv6 中的 ICMP 分组类似于传输层分组。

在 IPv6 ICMP 分组内，ICMPv6 类型和 ICMPv6 代码字段标识 IPv6 ICMP 分组细节，例如 ICMP 消息类型。校验和字段中的值是从 IPv6 ICMP 分组和 IPv6 头部中的字段导出的。ICMPv6 数据字段包含与 IP 分组处理相关的错误或诊断信息。

由于基于 ICMP 的攻击，所以 ICMPv4 和 ICMPv6 二者通常都被企业防火墙中实现的安全策略阻挡。对于使用 IPv4 的路由器，不存在广泛使用的技术用以防止基于 ICMP 的网络攻击。尽管 ICMPv6 具有使用 IPSec 认证和加密的能力（该认证和加密降低了基于 ICMPv6 的攻击的可能性），但是，已布署的 IPv4 路由器的基数非常大，这些路由器需要防止基于 ICMP 的攻击的解决方案。

根据 RFC 792，IPv4 ICMP 错误分组包括已产生错误的原始分组的 IP 头部的拷贝，以及来自该原始 IP 分组的有效载荷的至少 8 字节的数据。在一种现有方法中，IP 头部中承载的 IP 地址和传输头部中承载的 TCP 端口号（如果存在的话）被用来选择路由器中的具体应用或服务。然而，该现有方法不对分组执行任何形式的认证。

附图说明

在附图的图示中，通过示例而不是限制示出了本发明，在附图中相似的标号指示类似的元素，其中：

图 1 是示出了使用面向连接的传输协议用于分组数据通信的节点的网络的概况的框图；

图 2 是示出了通过认证 ICMP 分组来防止网络攻击的方法的一个实施例的高级别概况的流程图；

图 3 是用于认证 ICMP 分组的替换方法的流程图；以及

图 4 是示出了可以在其上实现本发明实施例的计算机系统的框图。

具体实施方式

下面描述通过认证因特网控制消息协议分组来防止网络攻击的方法和装置。在下面的描述中，为了说明目的，阐述了各种特定细节以便提供对本发明的全面理解。但是，没有这些特定细节也可以实施本发明，对于本领域的技术人员来说是很明显的。在另外一些实例中，以框图形式示出了公知的结构和设备，以免不必要地混淆了本发明。

在这里根据以下提纲对实施例进行描述：

1.0 综述

2.0 通过认证 ICMP 分组来防止网络攻击的方法

3.0 实现机制-硬件概述

4.0 扩展和替换

1.0 综述

在本发明中实现了前述背景部分中所述需求、以及从下面的描述将变清楚的其他需求和目的，本发明在一个方面中包括一种用于防止网络上的攻击的方法，该方法包括计算机实现的以下步骤：接收包括有与面向连接的传输协议的连接相关联的头部的拷贝的 ICMP 分组；从该头部获得分组序列值；确定分组序列值是否有效；以及仅在该分组序列值被确定为有效时才更新与传输协议连接相关联的参数值。所公开方法的使用使得能够对 ICMP 分组进行认证，以使得仅在 ICMP 分组被确定为可信的时才执行诸如调整 MTU 值之类的网络元件的响应措施。与现有方案不同，嵌入在 ICMP 分组中的传输层或应用层协议信息被用来认证分组。

根据一个特征，接收 ICMP 分组的步骤包括接收包括有与 TCP 连接相关联的 TCP 头部的拷贝的 ICMP 分组。在另一个特征中，接收 ICMP 分组的步骤包括接收 ICMP“端点不可达”错误分组。在又一个特征中，接收 ICMP 分组的步骤包括接收指定需要分段的 ICMP 分组。

在一个特征中，确定分组序列值是否有效的步骤包括确定该分组序列

值是否在所述连接的传输协议允许的分组序列值的范围内。在另一个特征中，确定分组序列值是否有效包括确定该分组序列值是否在所述连接的已发送但是尚未确认的 TCP 分组序列值的范围内。在又一个特征中，确定分组序列值是否有效包括确定该分组序列值是否与当前存储在 TCP 重传缓冲区中的一个或多个分组的一个或多个序列值相等。

在一个实施例中，前述步骤在充当 TCP 端点节点的路由器中执行。在另一个实施例中，这些步骤在防火墙设备中执行。

在其他方面中，本发明包括被配置为执行前述步骤的计算机装置和计算机可读介质。

2.0 通过认证 ICMP 分组来防止网络攻击的方法

2.1 结构概述

图 1 是示出了使用面向连接的传输协议来进行分组数据通信的节点的网络的概况的框图。第一网络元件 102 直接或间接通过网络 104 被通信耦合到第二网络元件 106。网络 104 可以包括一个或多个局域网、广域网、互连网、或者它们的组合，这些网络使用任何形式的通信链路，包括线缆、光链路、红外链路或者射频无线链路。

在一个实施例中，网络元件 102 和 106 每个都包括路由器、交换机或者网络基础设施的其他元件。为了说明简单清楚的示例的目的，图 1 仅示出了两个网络元件 102 和 106。但是，在其他实施例中，任意数目的网络元件可以与网络 104 通信，或者参与到网络 104 中。此外，为了清楚，省略了完整网络系统的其他公共元件，例如，个人计算机、工作站、打印机、服务器，以及其他末端站或内容源。

在一个实施例中，网络 104 是 TCP/IP 分组交换网络，元件 102 和 106 使用 IP、TCP 和 ICMP 通过该网络通信。为了支持这种通信，网络元件 106 充当 TCP 端点节点，终止发源于网络元件 102 或者网络元件 102 的末端站客户端处的 TCP 连接。网络元件 106 容纳或执行操作系统 108，操作系统 108 管理一个或多个应用，所述应用包括实现 TCP 的 TCP/IP 代理 110。TCP/IP 代理 110 包括 ICMP 处理逻辑 112 或者可以访问 ICMP 处理逻

辑 112，ICMP 处理逻辑 112 实现 ICMP。在替换实施例中，网络元件 106 可以包括实现了提供对 IP、TCP 和 ICMP 的实现的 TCP/IP 栈的个人计算机或者工作站。

在该环境中，网络元件 102 和 106 可以使用包括 ICMP 消息的 IP 分组和 TCP 片段进行通信。许多这种消息可以是合适并合法的，并且可以导致网络元件 106 执行适当的响应动作，例如，调整 MTU 值来顾及网络元件 102 或网络 104 的带宽限制。然而，通信耦合到网络 104 的未授权用户 120 可能通过确定出网络元件 102 和网络元件 106 正用来通信的 IP 地址和端口号值来发送一个或多个虚假 ICMP 分组 122 到网络元件 106。如果虚假的 ICMP 分组 122 包含不合理的小 MTU 值，则网络元件 106 可能使其使用的 MTU 值减小，从而导致性能问题。

2.2 功能概述

在一种方案中，提供了一种认证 ICMP 分组的方法。认证 ICMP 分组使得网络节点能够防止执行任何纠错动作，而纠错动作通常是响应于虚假 ICMP 分组而要求执行的。具体而言，ICMP 分组中嵌入的传输信息或应用层信息可以用于认证 ICMP 分组。在过去的方案中，仅这种信息的一部分（如传输层端口号）被以有限方式用来对 ICMP 分组解复用，以纠正传输协议或应用。

在这里的方案的一个实施例中，TCP 头部的前 8 个字节可以被用来认证 ICMP 分组，从而消除未经授权的发送者实行使用 TCP 的应用的拒绝服务攻击的可能性。如 TCP RFC 所定义，TCP 头部的前 8 个字节包含与两个网络节点之间的 TCP 连接相关的两个端口号值和 TCP 序列号。该序列号标识已导致下游节点标识出错误并且响应于该错误产生 ICMP 分组的 TCP 片段。

根据各种实施例，提供了两种方案用于使用 TCP 序列号来认证 ICMP 分组。在第一方案中，序列号被测试来确定其是否在已发送但是未被确认并且对于关联的 TCP 连接当前有效的序列号的范围内。在 TCP 的某些实现方式中，已发送但是未被确认的序列号的范围由软件变量定义，该软件变量名为“snduna”和“sndnxt”。

在第二方案中，提供了一种更严格的测试，试图使接收到的序列号与在由 TCP 实现方式维护的重传队列或缓冲区中存储的每个 TCP 片段中出现的序列号匹配。TCP 重传队列以其发送时的原始形式保存每个片段的拷贝。如果接收到的 ICMP 分组是可信的，则 ICMP 分组中的序列号必然与重传队列中的某一分段的序列号匹配。

图 2 是示出了用于通过认证 ICMP 分组来防止网络攻击的方法的一个实施例的高级别概况的流程图。图 3 是用于认证 ICMP 分组的替换方案的流程图。图 2 和图 3 的过程都可以使用一个或多个机器、计算机程序、过程或者软件元件实现。在一个实施例中，图 2 和图 3 的过程被实现为作为 ICMP 处理逻辑 112 的一部分的程序指令序列。

首先参考图 2，在步骤 202 中，接收 ICMP 分组。例如，在步骤 202 中，网络元件 106 接收到来自网络元件 102 或未经授权的用户 120 的 ICMP 分组。在一个实施例中，仅针对接收到的下述 ICMP 分组执行图 2 的过程：所述分组具有指示其是 ICMP“不可达”类型错误分组的类型代码和指示需要对片段分段和/或改变 MTU 的值。

在步骤 204 中，从接收到的分组的头部获得分组序列值。例如，实现图 2 的过程的网络元件从 ICMP 分组中承载的 IP 头部抽取 TCP 序列号。

在步骤 206 和步骤 208 中，执行测试来确定分组序列值是否有效。如果序列值有效，则在步骤 210 中基于 ICMP 分组执行响应动作。例如，该响应动作可以包括基于在 ICMP 分组中通告的 MTU 值来修改执行步骤 202-210 的网络元件的 MTU 值，如步骤 212 所示。但是，步骤 212 仅是一个示例，并且在其他实施例中可以执行任何其他适当的响应动作。

如果步骤 206-208 的测试结果为否，则在步骤 214 中，拒绝 ICMP 分组，并且可以响应于可能的攻击执行可选的动作。拒绝 ICMP 分组可以包括丢弃分组，不执行传统上响应于 ICMP 分组执行的响应动作，或者仅在在步骤 222 中发现所接收到的序列值的精确匹配时等情况下才执行诸如修改 MTU 值之类的响应动作。在步骤 214 中执行的可选响应动作可以包括创建日志条目等。

在步骤 206 中可以使用若干方案来确定分组序列值是否有效。现在参

考图 3，该图示出了两种替换方案作为示例。在步骤 220 所表示的一种方案中，步骤 206 包括确定所接收到的 ICMP 分组的序列值是否在已由 TCP 实现方发送但是接收节点尚未确认的序列值的允许范围内。在使用传统变量名的 TCP 软件实现方式中，步骤 220 的测试可以包括确定接收到的 ICMP 分组的序列值是否在由该实现方式维护的值“sndnxt”和“snduna”内。

在步骤 222 所表示的另一种方案中，执行测试来确定所接收到的序列值是否等于由 TCP 实现方式维护的 TCP 重传缓冲区中的分组的任何序列值。TCP 重传缓冲区将包含已实际发送的所有 TCP 片段的拷贝，因此可以充当所有已知有效的序列值的引用仓库。该方案要求比第一种方案稍多的处理资源，因为对于重传缓冲区中的所有片段都要求进行比较。但是，在典型的实现方式中，该额外的处理时间并不繁重。

在执行了步骤 220 或步骤 222 的方案后，控制前进到上面参考图 2 已描述的步骤 208-214。

尽管在使用 TCP 的通信的上下文中给出了上述示例，但是，取决于各自头部中可用的信息，这里所述方案可以与任何其他传输协议和应用信息一起工作。使用序列值的等同物的任何面向连接的传输层协议都可以使用。例如，这些方案可能适用于任何面向连接的传输协议。这些方案提供了对诸如 BGP、VPN、OSPF 之类的应用，各种基于 IP 的语音协议，或者依赖于 TCP 的其他高层协议的保护，并且还提供了可以被检查或者可以结合可以被检查的 IP 头部信息的头部信息或序列值。这里的方案可以消除网络节点响应于虚假的 ICMP 分组而执行灾难性的纠错动作的可能性。

这里的方案提供了有效的安全性解决方案，该方案适用于大多数传输协议和使用面向连接的传输协议并且依赖于 ICMP 反馈或错误消息的应用。这里的方案可以被应用到若干场景中，例如，拒绝服务攻击防止、增强对故障警报的健壮性、以及 TCP 代理机制。

3.0 实现机制-硬件概述

图 4 是示出了可以在其上实现本发明的实施例的计算机系统 400 的框

图。该优选实施例是使用在诸如路由器设备之类的网络元件中运行的一个或多个计算机程序实现的。因此，在本实施例中，计算机系统 400 是路由器。

计算机系统 400 包括总线 402 或用于传输信息的其他机制，以及与总线 402 耦合用于处理信息的处理器 404。计算机系统 400 还包括耦合到总线 402 用于存储信息和要由处理器 404 执行的指令的主存储器 406，例如，随机访问存储器（RAM）、闪存或者其他动态存储器件。主存储器 406 还可以用于存储在执行要由处理器 404 执行的指令期间的临时变量或其他中间信息。计算机系统 400 还包括耦合到总线 402 的只读存储器（ROM）408 或其他静态存储器件，用于存储静态信息和用于处理器 404 的指令。还提供了存储设备 410，例如，磁盘、闪存或光盘，该存储设备 410 被耦合到总线 402 用于存储信息和指令。

通信接口 418 可以被耦合到总线 402，用于传输信息和命令选择到处理器 404。接口 418 是传统的串行接口，如 RS-232 或 RS-422 接口。外部终端 412 或其他计算机系统连接到计算机系统 400，并且使用接口 414 向其提供命令。在计算机系统 400 中运行的固件或软件提供终端接口或基于字符的命令界面，使得外部命令可以被提供给该计算机系统。

交换系统 416 被耦合到总线 402，并且具有到一个或多个外部网络元件的输入接口 414 和输出接口 419。外部网络元件可以包括耦合到一个或多个主机 424 的本地网络 422，或者具有一个或多个服务器 430 的诸如因特网 428 之类的全球网。交换系统 416 根据预定协议和公知传统将到达输入接口 414 的信息流量交换到输出接口 419。例如，交换系统 416 与处理器 404 协作可以确定出到达输入接口 414 的数据分组的目的地，并且使用输出接口 419 将其发送向正确的目的地。目的地可以包括主机 424、服务器 430、其他末端站、或者本地网络 422 或因特网 428 中的其他路由选择和交换设备。

本发明涉及使用计算机系统 400 来通过认证因特网控制消息协议分组而防止网络攻击。根据本发明一个实施例，通过认证因特网控制消息协议分组来防止网络攻击是由计算机系统 400 响应于处理器 404 执行主存储器

406 中包含的一条或多条指令的一个或多个序列而提供的。这些指令可以从另一个计算机可读介质（如存储设备 410）读取到主存储器 406 中。执行主存储器 406 中包含的指令序列致使处理器 404 执行这里所述的过程步骤。也可以采用多处理布置中的一个或多个处理器来执行主存储器 406 中包含的指令序列。在替换实施例中，硬连线电路可以被用来替代软件指令或者与软件指令组合来实现本发明。因此，本发明的实施例不限于硬件电路和软件的任何特定组合。

这里使用的术语“计算机可读介质”指参与向处理器 404 提供指令以执行的任何介质。这种介质可以采用任何形式，包括但不限于非易失性介质、易失性介质和传输介质。非易失性介质包括例如光盘或磁盘，例如存储设备 410。易失性介质包括动态存储器，例如主存储器 406。传输介质包括同轴电缆、铜线和光线，包括包含总线 402 在内的线路。传输介质还可以采用声波或光波的形式，例如在无线电波和红外数据通信期间产生的那些波。

计算机可读介质的常见形式包括例如软盘、柔性盘、硬盘、磁带、或者任何其他磁介质、CD-ROM、任何其他光介质、穿孔卡、纸带、具有孔状图案的任何其他物理介质、RAM、PROM、以及 EPROM、闪存-EPROM、任何其他存储器芯片或盒带、下文所述载波、或者计算机可以从其读取的任何其他介质。

各种形式的计算机可读介质可以被用于传输一条或多条指令的一个或多个序列到处理器 404 以供执行。例如，指令最初可以被存储在远程计算机的磁盘上。远程计算机可以将指令加载到其动态存储器中，然后使用调制解调器通过电话线发送这些指令。计算机系统 400 本地的调制解调器可以接收到电话线上的数据，并且使用红外发射器将该数据转换成红外信号。耦合到总线 402 的红外探测器可以接收红外信号中承载的数据，并且将数据放置到总线 402 上。总线 402 将数据传输到主存储器 406，处理器 404 从主存储器 406 提取并执行指令。主存储器 406 接收到的指令可以可选地在被处理器 404 执行之前或之后被存储到存储设备 410 中。

通信接口 418 还提供到网络链路 420 的双向数据通信耦合，网络链路

420 被连接到本地网络 422。例如，通信接口 418 可以是综合业务数字网（ISDN）卡或者调制解调器，用于向对应类型的电话线提供数据通信连接。作为另一个示例，通信接口 418 可以是局域网（LAN）卡，用于提供到兼容 LAN 的数据通信连接。还可以实现无线链路。在任何这种实现方式中，通信接口 418 发送并接收电、电磁或光信号，这些信号承载表示各种类型信息的数字数据流。

网络链路 420 一般提供通过一个或多个网络到其他数据设备的数据通信。例如，网络链路 420 可以提供通过本地网络 422 到主机计算机 424 的连接，或者到由因特网服务提供商（ISP）426 操作的数据装备的连接。ISP 426 又通过当前普遍称作“因特网”428 的全球分组数据通信网络提供数据通信服务。本地网络 422 和因特网 428 二者都使用承载数字数据流的电、电磁或光信号。通过各种网络的信号和在网络链路 420 上的和通过通信接口 418 的信号承载去往和来自计算机系统 400 的数字数据，这些信号都是传输信息的载波的示例形式。

计算机系统 400 可以通过（一个或多个）网络、网络链路 420 和通信接口 418 发送消息和接收数据，包括程序代码。在因特网示例中，服务器 430 可能通过因特网 428、ISP 426、本地网络 422 和通信接口 418 传输所请求的应用程序代码。根据本发明，一个这种下载的程序提供这里所述的通过认证因特网控制消息协议分组来防止网络攻击。

接收到的代码可在该代码被接收到时由处理器 404 执行，和/或者被存储在存储设备 410 或其他非易失性存储设备中用于以后执行。这样，计算机系统 400 可以以载波形式获得应用代码。

4.0 扩展和替换

在前面的说明书中，已参考本发明的特定实施例描述了本发明。但是，很清楚，在不脱离本发明的广泛精神和范围的情况下，可以对其作出各种修改和改变。因此，应当认为说明书和附图是说明性的而非限制性的。

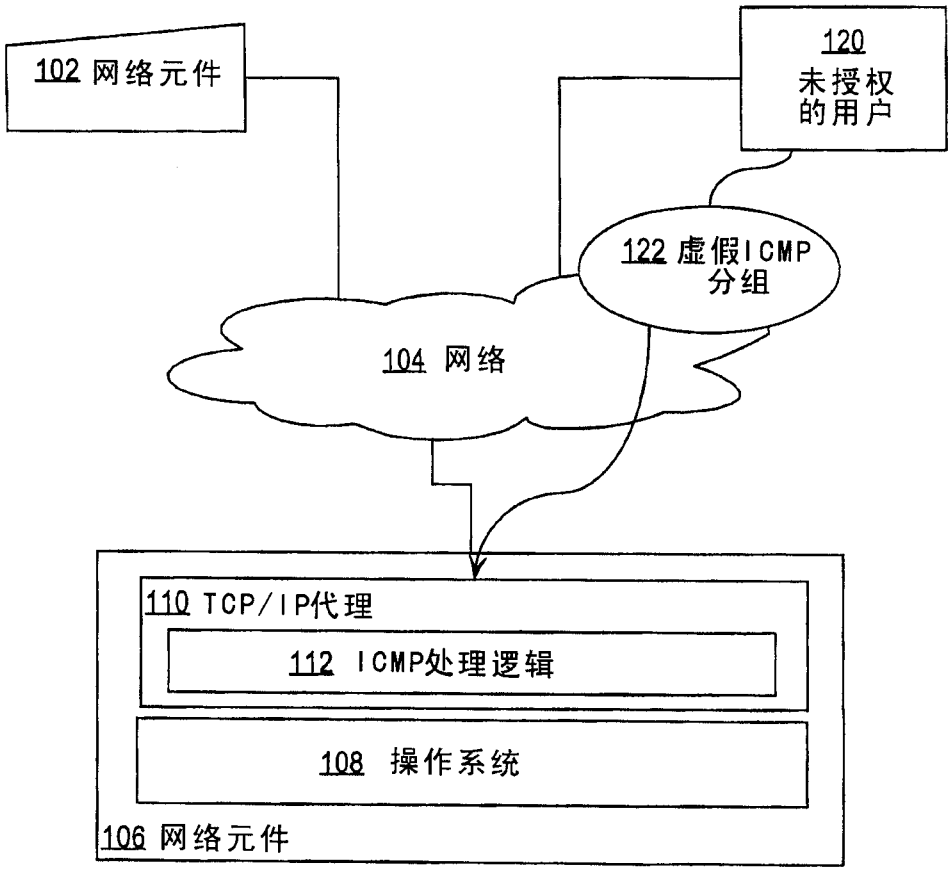

102 网络元件
120
未授权
的用户
122 虚假ICMP
分组
104 网络
110 TCP/IP代理
112 ICMP处理逻辑
108 操作系统
106 网络元件

图1

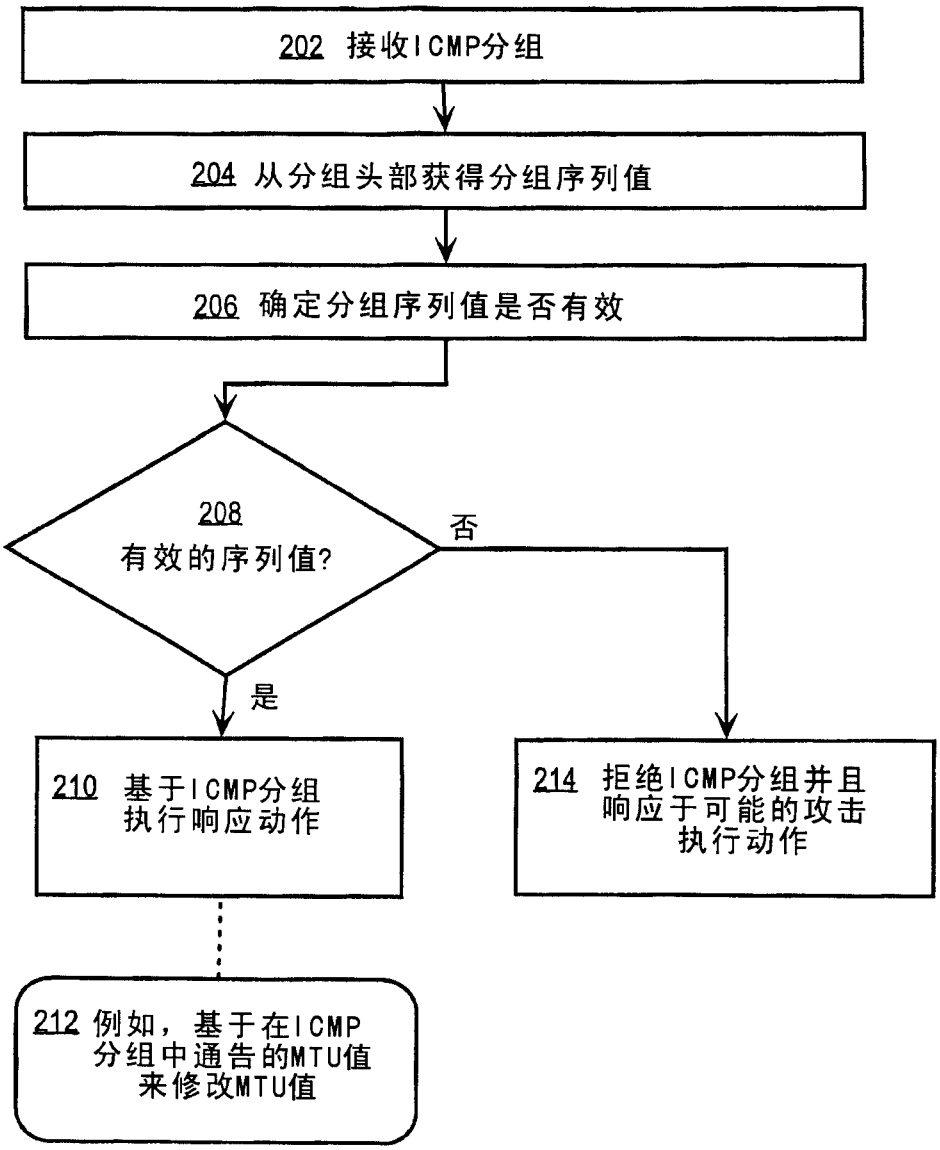

202 接收ICMP分组
204 从分组头部获得分组序列值
206 确定分组序列值是否有效
208
有效的序列值?
否
是
210 基于ICMP分组
执行响应动作
214 拒绝ICMP分组并且
响应于可能的攻击
执行动作
212 例如，基于在ICMP
分组中通告的MTU值
来修改MTU值

图2

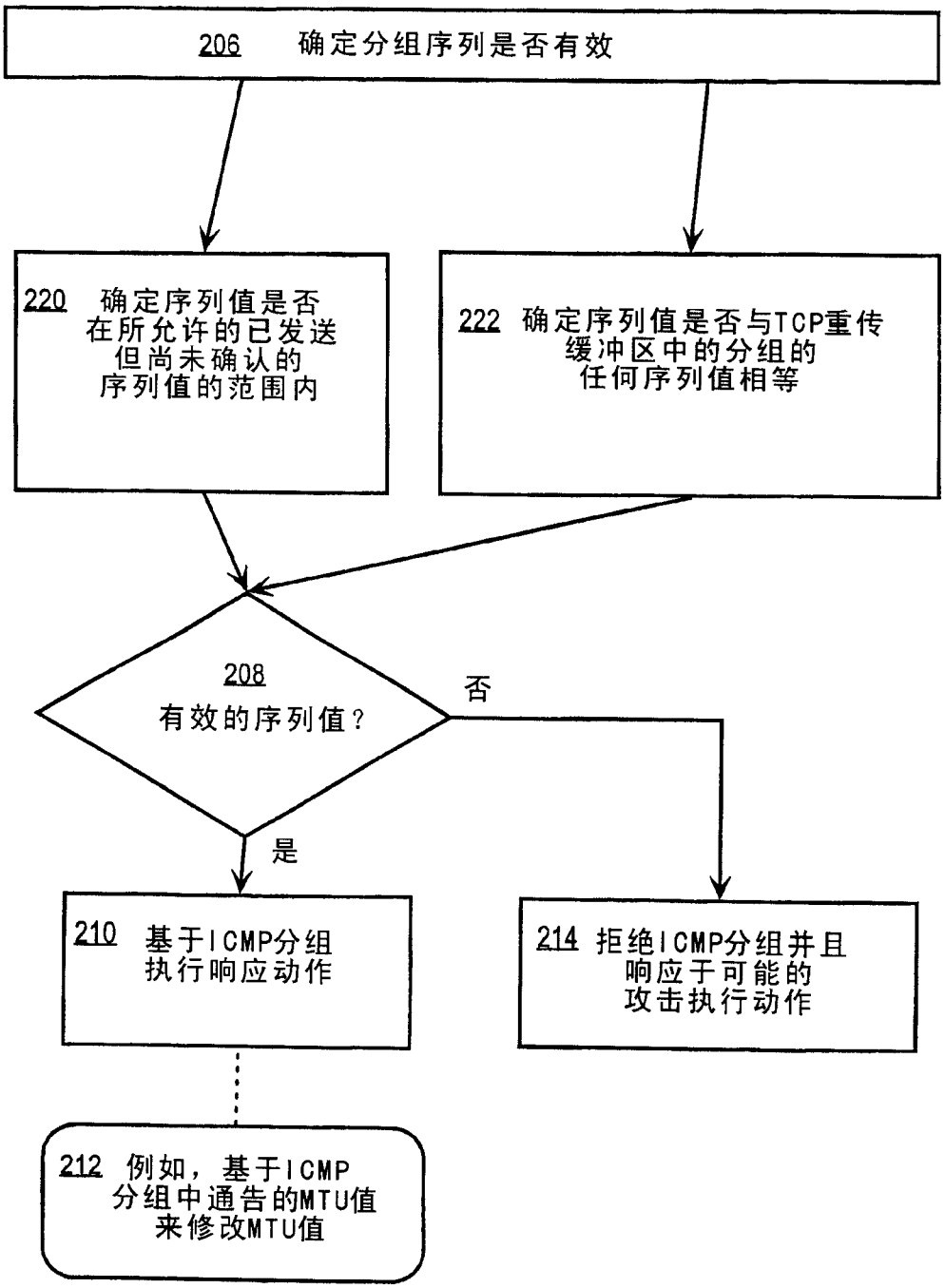

206 确定分组序列是否有效
220 确定序列值是否在所允许的已发送但尚未确认的序列值的范围内
222 确定序列值是否与TCP重传缓冲区中的分组的任何序列值相等
208 有效的序列值？
否
是
210 基于ICMP分组执行响应动作
214 拒绝ICMP分组并且响应于可能的攻击执行动作
212 例如，基于ICMP分组中通告的MTU值来修改MTU值

图3

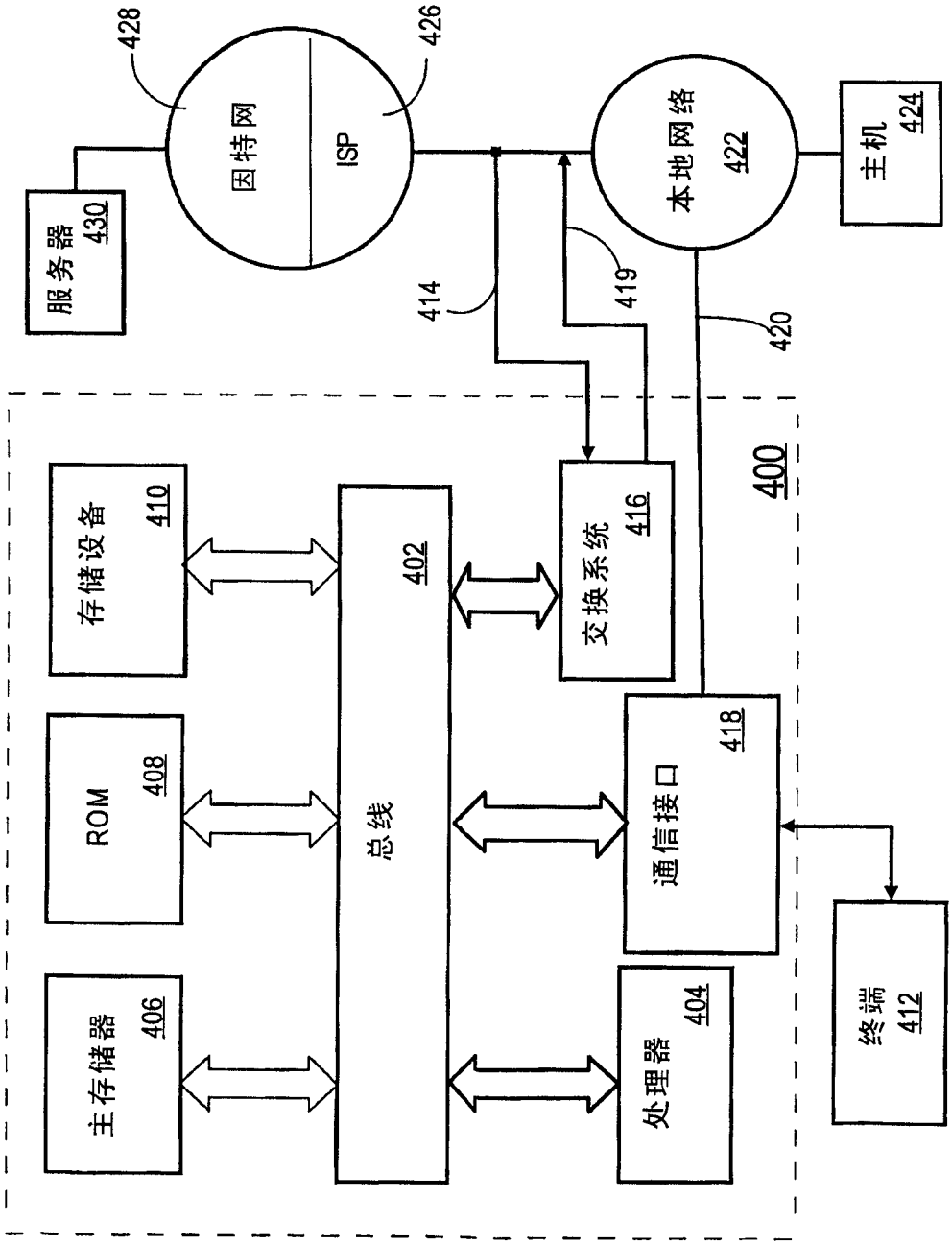

428
因特网
ISP
426
服务器
430
本地网络
422
主机
424
414
419
420
400
存储设备
410
402
交换系统
416
ROM
408
总线
通信接口
418
主存储器
406
处理器
404
终端
412

图4