[19] 中华人民共和国国家知识产权局

[51] Int. Cl[7]
H04L 12/56

[12] 发明专利申请公开说明书

[21] 申请号 200410031300.2

[43] 公开日 2004 年 10 月 13 日

[11] 公开号 CN 1536847A

[22] 申请日 2004.3.26
[21] 申请号 200410031300.2
[30] 优先权
[32] 2003. 3.27 [33] US [31] 10/401,919
[71] 申请人 阿瓦雅技术公司
地址 美国新泽西州
[72] 发明人 克里斯托弗·J.·东利
库尔特·H.·哈瑟罗特
罗伯特·R.·吉尔曼
约翰·M.·沃尔顿

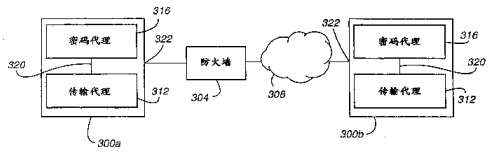
[74] 专利代理机构 中国国际贸易促进委员会专利商标事务所
代理人 董 莘

权利要求书 5 页 说明书 12 页 附图 8 页

[54] 发明名称 鉴权分组有效负荷的方法

[57] 摘要

提供了一种用于鉴权分组的体系结构，其包括：可用于接收分组的输入端 322，所述分组包括传输、会话和显示标题部分中的至少一个；传输代理 312，其可用于基于所述分组的至少一部分内容计算第一消息鉴权码，并将所述第一消息鉴权码与所述传输、会话和显示标题部分中的至少一个内的第二消息鉴权码相比较，以鉴权所述分组。



ISSN1008-4274

1. 一种用于鉴权分组的体系结构，包括:

接收分组，所述分组包括标题和有效负荷;

至少部分地基于从一些所述分组标题中得到的伪标题来计算第一消息鉴权码；其中所述伪标题中的源与目的地端口字段中的至少一个具有与所述分组标题中的对应源与目的地端口字段不同的值；以及

比较所述第一消息鉴权码与所述标题中的第二消息鉴权码，以鉴权所述分组。

2. 根据权利要求 1 的方法，其中所述标题包括传输标题部分，且所述第二鉴权码在所述传输标题部分中。

3. 根据权利要求 1 的方法，其中所述第二鉴权码是基于伪标题计算的，在所述伪标题中，源与目的地端口字段中的至少一个被设置为具有与所述标题中的对应源或目的地端口字段不同的值。

4. 根据权利要求 3 的方法，其中在所述伪标题中，源与目的地字段中的至少一个具有独立于所述标题中的对应源和目的地字段的值。

5. 根据权利要求 4 的方法，其中所述源与目的地字段中的至少一个被设置为零，且其中所述传输标题部分由 OSI 传输层与 TCP/IP 主机到主机传输层中的一个定义。

6. 根据权利要求 1 的方法，其中所述第一与第二鉴权码是散列消息鉴权码;

其中所述第一与第二鉴权码被截断为具有预定数量的比特;

其中使用所述传输标题部分来确定所述第一与第二消息鉴权码;

其中在所述比较步骤中，当所述第一与第二消息鉴权码不同时，所

述分组被认为是无效的，且还包括:

将指示分组无效的实例的计数器递增。

7. 根据权利要求 1 的方法，在所述接收步骤之后还包括:

在第一种模式中，当所述标题并不包括有效鉴权选项时，丢弃所述分组，所述鉴权选项包括所述第二消息鉴权码；以及

在第二种不同的模式中，当所述标题包括鉴权选项时，丢弃所述分组，其中所述计算与比较步骤仅发生在所述第一种模式中。

8. 根据权利要求 7 的方法，其中所述第二模式是有效的，其还包括:

从较高层接收中止所述第二模式并启动所述第一模式的指令；以及

响应于所述指令，中止所述第二模式并启动所述第一模式；以及

其中所述指令由应用层生成，其为传送鉴权指令与接收鉴权指令的其中一个。

9. 根据权利要求 7 的方法，在所述第一模式中还包括:

基于一些所述分组的内容来计算第一消息鉴权码；以及

比较所述第一消息鉴权码与所述传输标题部分中的第二消息鉴权码，以鉴权所述分组，其中所述第二鉴权码在所述传输标题部分内。

10. 根据权利要求 1 的方法，还包括:

汇编所述分组，所述分组标题包括传输标题部分；且其中

在第一种模式中，在所述传输标题部分中包括有效鉴权选项字段；以及

在第二种不同的模式中，并不在所述传输标题部分内包括有效鉴权选项字段；以及

随后传送所述分组。

11. 一种分组，其包括:

传输层标题部分，所述传输层标题部分包括:

源端口字段;

目的地端口字段;

序列号字段；以及

选项字段，其中所述选项字段包括鉴权选项，所述鉴权选项包括消息鉴权码；以及

有效负荷。

12. 根据权利要求 11 的分组，其中所述消息鉴权码是基于伪标题计算的，在所述伪标题中，源与目的地端口字段中的至少一个被设置为具有与所述分组标题中的对应源或目的地端口字段不同的值。

13. 一种用于鉴权分组的体系结构，其包括:

用于接收分组的输入装置，所述分组包括标题和有效负荷;

计算装置，其用于至少部分地基于从一些所述分组标题中得到的伪标题来计算第一消息鉴权码；其中所述伪标题中的源与目的地端口字段中的至少一个具有与所述分组标题中的对应源与目的地端口字段不同的值；以及

比较装置，其用于比较所述第一消息鉴权码与所述标题中的第二消息鉴权码，以鉴权所述分组。

14. 根据权利要求 13 的系统，其中所述标题包括传输标题部分;

其中所述第二鉴权码在所述传输标题部分内；以及

其中所述第二鉴权码是基于伪标题计算的，在所述伪标题中，源与目的地端口字段中的至少一个被设置为具有与所述标题中的对应源或目的地端口字段不同的值。

15. 根据权利要求 14 的体系结构，其中在所述伪标题中，源与目的地字段中的至少一个具有独立于所述标题中的对应源和目的地字段的

值。

16. 根据权利要求 15 的体系结构，其中所述源与目的地字段中的至少一个被设置为零，且其中所述传输标题部分由 OSI 传输层与 TCP/IP 主机到主机传输层中的一个定义。

17. 根据权利要求 13 的体系结构，其中所述第一与第二鉴权码是散列消息鉴权码；

其中所述第一与第二鉴权码被截断为具有预定数量的比特；

其中使用所述传输标题部分来确定所述第一与第二消息鉴权码；以及

其中当所述第一与第二消息鉴权码不同时，所述分组被认为是无效的，且还包括：

用于将指示分组无效的实例的计数器递增的计数装置。

18. 根据权利要求 13 的体系结构，还包括分组丢弃装置，其在第一种模式中，当所述标题并不包括有效鉴权选项时，丢弃所述分组，所述鉴权选项包括所述第二消息鉴权码，而在第二种不同的模式中，当所述标题包括鉴权选项时，丢弃所述分组；以及

其中所述计算与比较装置仅在所述第一模式中操作，且所述丢弃操作在接收到所述分组之后发生。

19. 根据权利要求 18 的体系结构，其中所述第二模式是有效的；

其中所述丢弃装置从较高层接收中止所述第二模式并启动所述第一模式的指令，且响应于所述指令，中止所述第二模式并启动所述第一模式；以及

其中所述指令由应用层生成，其为传送鉴权指令与接收鉴权指令的其中一个。

20. 根据权利要求 **18** 的体系结构，其中所述丢弃装置在所述第一模式中基于一些所述分组的内容计算第一消息鉴权码，并比较所述第一消息鉴权码与所述传输标题部分中的第二消息鉴权码，以鉴权所述分组，其中所述第二鉴权码在所述传输标题部分内。

21. 根据权利要求 **13** 的体系结构，还包括:

用于汇编所述分组的装置，所述分组标题包括传输标题部分;

用于在第一种模式中使所述传输标题部分内包括有效鉴权选项字段，并在第二种不同的模式中使所述传输标题部分内不包括有效鉴权选项字段的装置；以及

用于随后传送所述分组的装置。

鉴权分组有效负荷的方法

技术领域

本发明涉及鉴权，尤其涉及分组有效负荷的鉴权。

背景技术

近年来，对于有效网络安全性的需要逐步变得重要，这归因于网络黑客、病毒以及其它类型网络攻击的频繁发生和更为复杂。电子商务已引进了一种新型网络攻击，称为业务否定或 DoS 攻击。在 DoS 攻击中，当使用标准传输控制协议或 TCP 在两个应用之间提供数据的顺序传输时，恶意第三方可以将错误分组注入或“合并”到所述分组流内。为了逃避驾驭 TCP（例如安全套接层或 SSL，或是传输层安全或 TLS）的安全协议的检测，所述错误分组被适当构造，从而使其包括正确的地址对和序列号（从而使得所述分组显示为是有效的），但包括虚假数据。当正确分组稍后到达时，所述分组被作为重新传送的复本而删除。因为所述虚假数据无法成功鉴权，所述安全协议通过发送错误消息到所述发动节点来终止所述会话。所述安全协议无法选择性地请求所丢弃（正确）数据的重新传输。因此，所述 DoS 攻击必须通过长密码协商会话来重新建立所述 TLS 连接，这需要大量的处理资源。DoS 攻击不仅无必要地消耗处理资源，还使得电子商务每年损失百万美金收入。

一种用于挫败 DoS 攻击的方法是以传输模式使用 IP 安全或 IPSec 协议以鉴权每个 IP 分组。IPSec 不仅可以加密实际用户数据或有效负荷，还可以加密一些用于泄露技术会话攻击简表内的客户地址的协议栈信息项。IPSec 作为开放系统互连或 OSI 体系结构的第三层（“IP”上的互联网协议）和第四层（TCP 或 UDP）之间的“垫片”，并包括一套协议，所述协议共同规定鉴权标题（AH）、封装的安全有效负荷（ESP）以及互联网密钥交换（IKE）。IPSec 提供了经由 AH 的地址鉴权、经由 ESP 的

数据加密、使用 IKE 的发送者和接收者节点之间的自动密钥交换。

图 2A 示出了具有鉴权标题 204 的 IPv4 分组 200。所述鉴权标题 204 包括下一标题字段 208（其具有一个字节的长度，并识别符合所述 AH 的较高级协议）、有效负荷长度字段 212（其具有一个字节的长度，并规定所述鉴权数据字段 216 的长度）、预留字段 220（其具有为将来使用预留的两个字节）、安全参数索引或 SPI 字段 224（其具有四个字节的长度，并识别用于所述分组的安全协议）、序列号字段 228（其具有四个字节的长度，并作为一个计数器，所述计数器识别其已接收的负载相同目的地和 SPI 数据的 IP AH 分组的数量）、鉴权数据字段 216（其具有可变的长度，并包括完整性检查值或 ICV（其是使用 DES、MD5 或安全散列算法（SHA-1）生成的分组的数字签名））。

图 2B 示出了具有封装的安全有效负荷或 ESP 标题 254 的 IPv4 分组 250。所述封装的安全有效负荷标题包括上述的 SPI 和序列号字段 224 和 228、TCP 或用户数据报协议（UDP）标题 230、有效负荷数据字段 258（其包括用户的原始数据的加密后版本）、填充字段 262（其提供加密算法的任何必需的填充需要，或是提供字节界限校准）、填充长度字段 266（其规定用于所述填充字段的填充字节的数量）、下一标题字段 270（其通过识别包括在所述有效负荷数据字段内的数据的类型来参考所述有效负荷数据）、鉴权数据 274（其为应用于整个 ESP 标题的数字签名）。

但是，IPSec 无法通过防火墙，尤其是执行网络-地址翻译或网络-地址-端口翻译的代理服务器防火墙。以下将参照图 1 来讨论该问题。参照图 1，防火墙（或代理服务器）100 位与网络 104 和各种有防火墙保护的网络节点 108a-n 之间。每个节点 108a-n 都具有对应 IP 地址和端口号。当节点 108a-N 将分组发送出所述网络时，所述防火墙可能仅改变所述 IP 地址，或改变所述 IP 地址和端口号两者。所述新 IP 地址通常是代理服务器的 IP 地址。因为 IPSec 在第三层和第四层内操作，且 IPSec 并不具有用于端口技术规范的设备，因而所述代理服务器尝试改变端口失败，且所述分组并不被传送。所述 ESP 标题 254 通常允许改变 IP 地址，但不允许改变端口号。另一方面，所述 AH 204 通常不允许改变 IP 地址或

是端口号。

发明内容

上述需要以及其它需要由本发明的各个实施例与配置来满足。本发明指向一种方法，其用于在所述应用层之下的层内鉴权分组，例如在 OSI 传输以及 TCP/IP 主机到主机传输层内。

在本发明的一个实施例中，提供了一种用于鉴权分组的方法，所述方法包括步骤:

（a）接收分组，所述分组包括标题和有效负荷，而所述标题包括传输标题部分;

（b）基于所述分组的至少一部分内容计算第一消息鉴权码；以及

（c）比较所述第一消息鉴权码与所述传输标题部分内的第二消息鉴权码来鉴权所述分组。

所述传输标题部分可由任何适当的软件模型来定义，例如所述 OSI 传输层以及 TCP/IP 主机到主机传输层。

所述消息鉴权码可使用任何适当的算法来计算，例如（安全）散列算法。所述第一和第二鉴权码通常被截短为预定数量比特。

所述第一和第二消息鉴权码可基于所述标题的全部或所选择部分和/或所述有效负荷的全部或所选择部分。通常至少基于所述传输标题部分来确定所述第一和第二消息鉴权码。

在一种配置中，所述第一和第二鉴权码是基于伪标题计算的，在所述伪标题中，源端口和/或目的地端口字段被设置为与所述标题中对应源端口或目的地端口字段不同的值。另一种方式是，所述源和/或目的地字段具有独立于所述标题中对应源和目的地字段的值。例如，所述源和/或目的地字段被设置为零。并不被所述防火墙处理的所述分组内的字段在所述伪标题内通常不会被设置为不同的值或忽略。

在可能与上述实施例一起使用的另一实施例中，本发明指向一种用于所接收分组的鉴权方法，所述方法包括步骤:

（a）在第一模式中，当所述标题并不包括有效鉴权选项时，丢弃所

述分组，所述鉴权选项包括所述第二消息鉴权码；以及

（b）在第二不同模式中，当所述标题包括鉴权选项时丢弃所述分组。上述实施例中的计算和比较步骤仅发生在所述第一模式中。所述操作模式通常是由较高层确定的，例如由所述应用层或会话层，或是由传输层自身。

在可与上述实施例中的任何一个一起使用的又一个实施例中，本发明指向一种用于将被传送的分组的鉴权方法，所述方法包括步骤：

（a）组合包括标题和有效负荷的分组，所述标题包括传输标题部分，其中

（b）在第一模式中，所述传输标题部分包括有效鉴权选项字段；以及

（c）在第二不同模式中，所述传输标题部分内并不包括有效鉴权选项字段；以及

（d）随后传送所述分组。

所述各个实施例相对于现有技术都具有大量优点。例如，所述标题的传输部分内包括鉴权选项可有效阻止未授权地操作传送中的数据，并提供对于由第三方注入未经鉴权数据所引起的会话破坏的更高抵抗力，例如在 DoS 攻击的情况下。在生成分组时，计算消息鉴权码并将其插入所述标题。在接收所述分组时，验证所附的消息鉴权码。当所述验证失败时，所述分组显然已被修改（或被虚假地注入所述分组流），因此不再确认即丢弃所述分组。鉴权或未确认分组将由所述发送者重新传送。所述消息鉴权码可以一种方式来定义，从而使得所述分组流过地址和/或端口翻译防火墙，而无需将所述分组内的机密公开给所述防火墙。根据这样一种定义，由代理服务器型防火墙操作或改变的所述源端口和/或目的地端口字段以及其它任何字段的值被设置为与所述标题中的值不同，例如被设置为零，或被在所述消息鉴权码所基于的伪标题内完全忽略。用于计算所述消息鉴权码的所述共享机密或密钥由所述传输层之上的协议层提供。因此，提供允许以未鉴权模式使用所述传输层，以协商所述共享机密。在完成所述协商时，传输层鉴权可被激活，以使所有后续分组

化的信息得到鉴权。这样，本发明最大地使用了现有协议，例如 TLS 和 TCP， 而无需备选解决方案或是生成新协议。

本文所公开的发明内容将使得上述优点以及其它优点变得清晰。

上述实施例和配置并不是完全的，亦非穷举的。应当理解的是，本发明的其它实施例也可以单独或组合使用一个或多个上述或以下详述的特征。

附图说明

图 1 是常规代理服务器型防火墙的方框图；

图 2A 是常规分组与鉴权标题的方框图；

图 2B 是常规分组与封装安全协议标题的方框图；

图 3 是根据本发明实施例的代理服务器型防火墙的方框图；

图 4 是根据传输控制协议的常规传输层标题的方框图；

图 5 是根据本发明的鉴权 TCP 选项字段的方框图；

图 6 是用于计算消息鉴权码的伪标题的方框图；

图 7 是描述密码代理的操作的流程图；以及

图 8A 和 B 是描述跟踪代理的操作的流程图。

具体实施方式

图 3 描述了一种根据本发明的第一实施例的体系结构。所述体系结构至少包括第一和第二端点或节点 300a、b，以及位于所述节点 300a、b 之间的防火墙 304 和网络 308。

所述第一和第二节点 300a、b 可以是任何计算部件，例如个人计算机或 PC、服务器、膝上电脑、个人数字助理或 PDA、IP 电话、VoIP 媒介网关、H.323 门卫等。每个节点都包括传输代理 312、密码代理 316 以及输入端或接口 322。

所述传输代理 312（a）提供数据的无错传送，（b）从相邻的较高层接受数据，例如从所述 OSI 的会话层或第 5 层或是从 TCP/IP 的应用层，如果需要将所述数据分割到较小分组内，将所述分组传送至相邻的较低

层，例如所述 OSI 的网络层或第 3 层或是 TCP/IP 的互连网络层，并确认所述分组完全并正确地到达其目的地，以及（c）鉴权所述分组的所选择内容。

所述密码代理 316 包括协议，例如安全套接层或 SSL（用于安全性）和/或传输层安全或 TLS（用于安全性）（通常统称为“SSL/TLS”）、公共管理协议或 CMIP（用于网络管理），文件传送、接入以及管理（用于远程文件处理），X.400（用于电子邮件），和/或定义具体的面向用户的应用业务和进程的 SASL。所述密码代理 316 可以在 OSI 面向业务层（例如层 5、6 和/或 7）的任何应用内或 TCP/IP 的应用层内操作。

套接 320 代表所述鉴权和传输代理之间的接口。

应当理解的是，所述 OSI 分层过程在源机器的应用层或第 7 层内开始，在所述的层内，消息由应用程序生成。所述消息通过该层向下移动，直至其到达第 1 层。第 1 层是实际物理通信媒介。所述分组化的数据然后被通过所述媒介传送至所述接收主机，在所述接收主机内，所述信息向上移动通过所述的层，即从第 1 层到第 7 层。当消息在所述源机器内通过所述的层向下移动时，所述消息被以与特定的层相关的标题封装，例如 IP 标题 232，AH 204，TCP 或 UDP 标题 236，或 ESPH 254（图 2A 和 2B）。当所述消息在所述主机内通过所述的层向上移动时，标题由每个对应的层去除。所述 TCP/IP 层以非常相似的方式操作。

防火墙 304 可以是任何类型的防火墙。例如，所述防火墙可以是帧过滤防火墙、分组过滤防火墙、电路网关防火墙、状态防火墙或是应用网关或代理服务器防火墙。

网络 308 可以是数字或模拟的任意分布式处理网络，例如互联网。

以下将参照图 4-6 来描述由所述传输代理 312 用于鉴权的所述 TCP 标题。图 4 描述了所述 TCP 标题 400 的现有技术格式。所述 TCP 标题 400 包括的字段为：源端口 404、目的地端口 408、分组序列号 412（上述的）、字节确认号 416（其指示在发送确认之前接收和接受的最后字节号）、数据偏移 420（其指示数据在所述分组内的开始位置）、标志字段 422、预留 424、窗口 428（其指示可以接收和缓存的字节数）、校验和 432、

紧急指针 436（其指示所述分组内出现紧急数据）、选项 440（其包括与所述协议相关的各个选项）以及填充 444（以足够的零比特填充所述选项字段以确保所述标题具有所需长度的可变长度字段）。根据本发明，通过在所述选项字段 440 内包括鉴权选项来实现 TCP 分组数据单元（"PDU"）或分组的鉴权。应当理解的是，所述选项字段内的选项可以具有两种形式中的一种，即后跟选项长度的字节的单个字节值选项类型，或是后跟选项数据的（选项长度-2）字节的字节选项类型。在一种配置中，所述的鉴权选项具有第二种形式。

图 5 描述了第二种形式的鉴权选项。所述的鉴权选项 500 包括以下字段，即选项指示符 504、长度 508 以及消息鉴权码 512。所述选项指示符字段 504 是指配的选项数字比特或/所述分组鉴权选项的值，所述长度字段 508 是所述消息鉴权码或 MAC 的长度，而所述消息鉴权码 512 字段包括所述消息鉴权码自身。所述 MAC 可以任何技术计算，包括键控散列消息鉴权码，例如 HMAC-MD5 和 HMAC-SHA1 算法，它们被截断为 N 个比特，分别表示为 HMAC-MD5-N 和 HMAC-SHA1-N。其它支持的消息鉴权码包括任何键控的、密码安全 MAC，例如那些基于密码反馈加密的 MAC。这些代码同样优选的是被截断为 N 个比特。散列消息鉴权码的截短阻止了攻击者解密所述散列密钥信息。用于生成所述代码的所述密钥是从所述密码代理处接收的。

以下将参照图 6 来讨论所述 MAC 的计算。所述 MAC 的计算可在全部或部分所述 TCP 标题和有效负荷上执行，而所选择字段被设置为零（或被设置为零比特）。在图 6 中，所述 MAC 是在代表所述整个 TCP 标题、有效负荷以及所述分组的主体的伪标题 600 上执行，而所述伪标题内的源端口字段 604、目的地端口字段 608 、校验和字段 612 都被设置为零（或零比特）。因此，可由某些类型防火墙处理的所述源端口和目的地端口以及涵盖其的所述校验和被从所述 MAC 计算中排除。这允许在所述 TCP 标题通过地址或地址与端口翻译防火墙时，以常规方式操作所述 TCP 标题，而不会影响鉴权。

并不由所述防火墙操作的所述分组内的字段被设置为不同的值，所

述字段例如是紧急指针标志（其指示所述紧急指针字段是有效的）、PSH 标志（其指示数据应当被推至使用层）、结束标志、确认标志、“syn”标志（其指示同步序列号应当被发送）、RST 标志（重新设置连接）、序列号、确认号、数据偏移、窗口、选项、填充。一般而言，所述确认字段与 ack 字段应当被鉴权（连同其它标志）覆盖。

应当理解的是，依据应用可将所述伪标题 600 内的源端口字段 604、目的地端口字段 608 和校验和字段 612 中的一个或多个设置为非零值。在计算所述 MAC 时，所述源端口字段 604 和目的地端口字段 608 都应当由防火墙 304 每一侧的每个节点保持不变，以避免确定 MAC 时的矛盾。每个所述字段内的值通常都是不同的，且不依赖于所述防火墙 60 与第一和第二节点 300a、b 的地址。例如，从所述第一节点传送到第二节点的分组应当具有所述伪标题 600 内的被设置为常量的源端口字段，而从所述第二节点传送到第一节点的分组应当具有所述伪标题 600 内的被设置为常量的目的地端口字段，以避免防火墙 304 的端口翻译的复杂性。

所述鉴权选项 500（图 5）包括在伪标题的选项字段内。尽管并不要求所述选项-数据字段不会由所述防火墙改变，所述选项-数据字段具有适当的长度，通常被设置为零（或是零比特）。使用实际标题计算标准 TCP 校验和。

所述密码代理 316 通过提供（多个）算法的选择以及所述算法的（多个）密码资料，在 TCP 连接的一个或两个方向上激活鉴权。一旦由传送密码代理 316 激活，所有所传送的分组都必须包括有效鉴权选项 500，而当传送密码代理并未激活时，未生成的 TCP 标题可能包括鉴权选项 500。如果鉴权由接收密码代理 316 激活，则所有所接收的分组必须包括有效鉴权选项 500，如上所述，其中包括的 MAC 必须匹配于所接收分组，或所述分组由传输代理 312 判断为无效。当鉴权由所述接收密码代理 316 激活时，任何未通过鉴权或并不包括有效鉴权选项 500 的分组与带有无效校验和的分组由传输代理 312 以相同的方式处理。鉴权错误可能由所述传输代理 312 记录或计数，所述传输代理 312 使所述密码代理 316 或使用层在请求时可得到所述日志/计数。在所述密码代理 316 协调所述激

活的假定下，所述传输代理 312 尚未报告给所述密码代理 316 的任何所接收数据被丢弃（所接收的序列号相应地并不增加），因此所述数据一定已被攻击者在传送中注入或破坏。当鉴权并不由所述接收密码代理 316 激活时，所有具有鉴权选项 500 的分组都被丢弃。这是因为所述传送密码代理 316 显然期望具有鉴权后的分组，而所述接收密码代理 316 可能尚未为此提供必需的鉴权参数。

以下将参照图 7 和 8 描述所述传输代理 312 和密码代理 316 的操作。

图 7 描述每个节点内的密码代理所执行的操作。在图 7 的步骤 700 中，第一节点 300a 与第二节点 300b 的密码代理 316 使用常规技术经由安全信道协商协议参数。协商通常涉及每方交换密钥，在一些情况下还涉及数字证书。根据交换后的密钥来计算共享主密钥。当所述第一与第二节点所交换的完成消息内的散列一致时，完成协商。通常借助数字签名在密码代理层上验证所述交换。

在完成协商时，在所述第一与第二节点之间交换多个消息。在步骤 704 中，所述第一与第二节点将开始密码或改变密码指令发送到所述第二节点，反之亦然。当所述第一或第二节点内的密码代理 316 发送所述开始密码指令时，所述代理 316 在步骤 708 中指令对应传输代理 312 启动传送鉴权，并将必需的信息（通常为共享机密，例如消息鉴权码算法的传送密钥与识别）提供给所述代理 312，以在将被传送到另一节点的分组上执行鉴权操作。当所述第一或第二节点内的密码代理 316 在步骤 712 中从另一节点接收所述开始密码指令时，所述代理 316 在步骤 716 中指令对应传输代理 312 启动接收鉴权，并将必需的信息（通常为共享机密，例如消息鉴权码算法的接收密钥（其可能不同于所述传送密钥）与识别）提供给所述代理 312，以在所接收分组上执行鉴权操作。在所述第一或第二节点执行步骤 708 之后，在步骤 702 中为对应传输代理 312 提供将被鉴权的数据，用于传输到另一节点。在执行步骤 720 或 716 之后，所述密码代理 316 在步骤 724 中等待从另一节点接收数据。

图 8A 和 B 描述每个节点内的传输代理所执行的操作。

参照图 8A，在步骤 800 中，所述传输代理 312 接收所述传送鉴权指

令与鉴权信息。作为响应，所述传输代理 312 进入传送鉴权模式（或第一模式），其中鉴权选项 500 包括在每个被传送到所述第二节点的分组的选项字段 440 内。在步骤 808 中，所述传输代理 312 通过生成鉴权选项 500 来鉴权所述数据，所述鉴权数据包括在所述分组标题的选项字段 440 内。如上所述，在建立所述选项 500 时，所述传输代理 312 基于图 6 的伪标题与共享机密，计算所述消息鉴权码，将其截断为 N 比特。在步骤 812 中，所述传输代理 312 将所述分组格式化，并将所述分组发送到另一节点的传输代理。在执行步骤 312 之后，发送传输代理 312 在步骤 816 中等待来自密码代理 316 的更多数据。

参照图 8B，在步骤 802 中，所述传输代理 312 接收所述接收鉴权指令与鉴权信息。作为响应，所述传输代理 312 进入接收鉴权模式，其中鉴权选项 500 必须包括在所述第二节点所接收的每个分组的选项字段 440 内。应当理解的是，所有的所接收分组都可进入此模式，或是只有从所述第二节点接收的分组方可进入此模式。在步骤 824 中，所述传输代理从另一节点的发送传输代理接收分组。在判定菱形框 828 中，所述接收传输代理 312 确定所接收的分组是否包括鉴权选项。在所述分组包括鉴权选项时，所述传输代理 312 在步骤 832 中通过基于分组伪标题和其它内容以及共享机密计算截短为 N 比特的消息鉴权码，并将所计算的消息鉴权码与鉴权选项的字段 512 内的消息鉴权码相比较，从而鉴权所述分组。在判定菱形框 828 中，所述传输代理 312 确定分组鉴权是否成功。当所述消息鉴权码不同时，分组鉴权失败，所述代理 312 继续步骤 840（如下所述）。当所述消息鉴权码相同时，分组鉴权成功，所述代理 312 继续步骤 844。在步骤 844 中，所述分组内包括的数据被转发到接收节点的对应密码代理 316。当在判定菱形框 828 中所述分组并不包括鉴权选项 500 时，或当在判定菱形框 836 中鉴权失败时，所述传输代理 312 在步骤 840 中丢弃所述分组，在步骤 848 中记录和计数鉴权错误，在步骤 852 中并不增加序列号。在丢弃所述分组时，由于所述发送节点从未接收到成功接收所丢弃分组的确认，所以其将会重新发送所述分组，从而显著恶化并降低 DoS 攻击者的能力。所述代理 312 然后继续步骤 856，并等

待下一个将接收的分组。

因为由代理服务器处理的所述源和目的地地址字段和校验和字段在所述消息鉴权码所基于的所述伪标题 600 内被设置为零（或零比特），所以防火墙地址和/或端口翻译在所述密码代理 316 内并不会与诸如 SSL 和 TLS 的安全协议的操作相干扰。

应当理解的是，响应于由所述密码代理 316 接收的停止密码指令（例如下一改变密码指令或结束指令），所述传输代理 312 被重新设置为所述第一或无鉴权模式。停止鉴权指令然后由所述接收密码代理发送至所述对应密码代理。

因为所有以传送鉴权模式传送，并以接收鉴权模式接收的分组必须包括鉴权选项，所以以这些模式传送/接收的确认分组必须在其标题内包括鉴权选项。这阻止了 DoS 攻击者通过将错误确认发送至所述发送节点来阻塞会话或引起会话终止。

可以使用本发明的多种改变和修改。可以提供本发明的一些特征而不提供其它特征。

例如在一个备选实施例中，所述传输代理 312 可以上述协议之外的协议实施。例如，用于所述传输代理的其它协议包括 TCP、UDP、互联网控制消息协议或 ICMP 或是会话控制传输协议或 SCTP 的其它版本。数据传输和确认内主要基于 SCTP。STP 的一种改变是定义两个新的有效负荷类型，并限制主要内容。一种有效负荷类型用于鉴权分组流，另一有效负荷类型用于确认所述分组流。

同样在其它实施例中，所述密码代理可使用多个适当安全协议的任何一种，例如 IPsec 等。

在另一备选实施例中，鉴权选项的实施方式不仅在传输层标题内，而且可作为栈内的 Bump，或 OSI 第 3 层和第 4 层之间的 BITS 实施方式。

在有一备选实施例中，所述鉴权选项在对应于 OSI 传输层的 TCP/IP 层内。例如，所述鉴权选项可在 TCP/IP 主机到主机传输层内。

在又一备选实施例中，可能是由或可能不是由 OSI 第 3、4、5、6、

和/或 7 层定义的伪标题仅代表所述标题和/或有效负荷的一部分，并可能包括一个或多个与图 6 所示的字段不同的字段。

在另一备选实施例中，所述传输代理和/或密码代理或是其部分被体现为逻辑电路以及或替代软件，所述逻辑电路例如是专用集成电路。

在各种实施例中，本发明包括本文充分描述和叙述的元件、方法、过程、系统和/或装置，包括各种实施例、子组合及其子集。本领域技术人员在理解本公开之后应当理解如何使用本发明。在各种实施例中，在忽略并未在本文或其各实施例中说明和/或描述的项目的情况下，包括在忽略现有设备或过程所使用的所述项目的情况下，本发明提供了例如用于提高性能、便于实现和/或降低实施成本的设备与过程。

本发明的以上讨论是出于示例与描述目的而提供的。以上并非用于将本发明限制为本文公开的一个或多个形式。例如在以上的详细描述中，本发明的各种特征可在一个或多个实施例中结合在一起，以将此公开连成整体。所公开的方法不应当被解释为权利要求的本发明需要比在每个权利要求内明确陈述的特征更多的特征。而是如权利要求书所反映，发明方面决不在于单个上述实施例的所有特征。因此，将权利要求书引入具体实施方式，其中每个权利要求都可独立作为本发明的优选实施例。

此外，尽管本发明的描述已包括一个或多个实施例以及特定改变与修改，但本领域技术人员在理解本发明之后，可了解其它改变与修改同样在本发明的范围内。旨在得到达到所允许程度的包括备选实施例的权利，包括所要求权利的备选、可交换和/或等同的结构、功能、范围或步骤，不论其是否在本文得到描述，而非旨在公开共享任何专利内容。

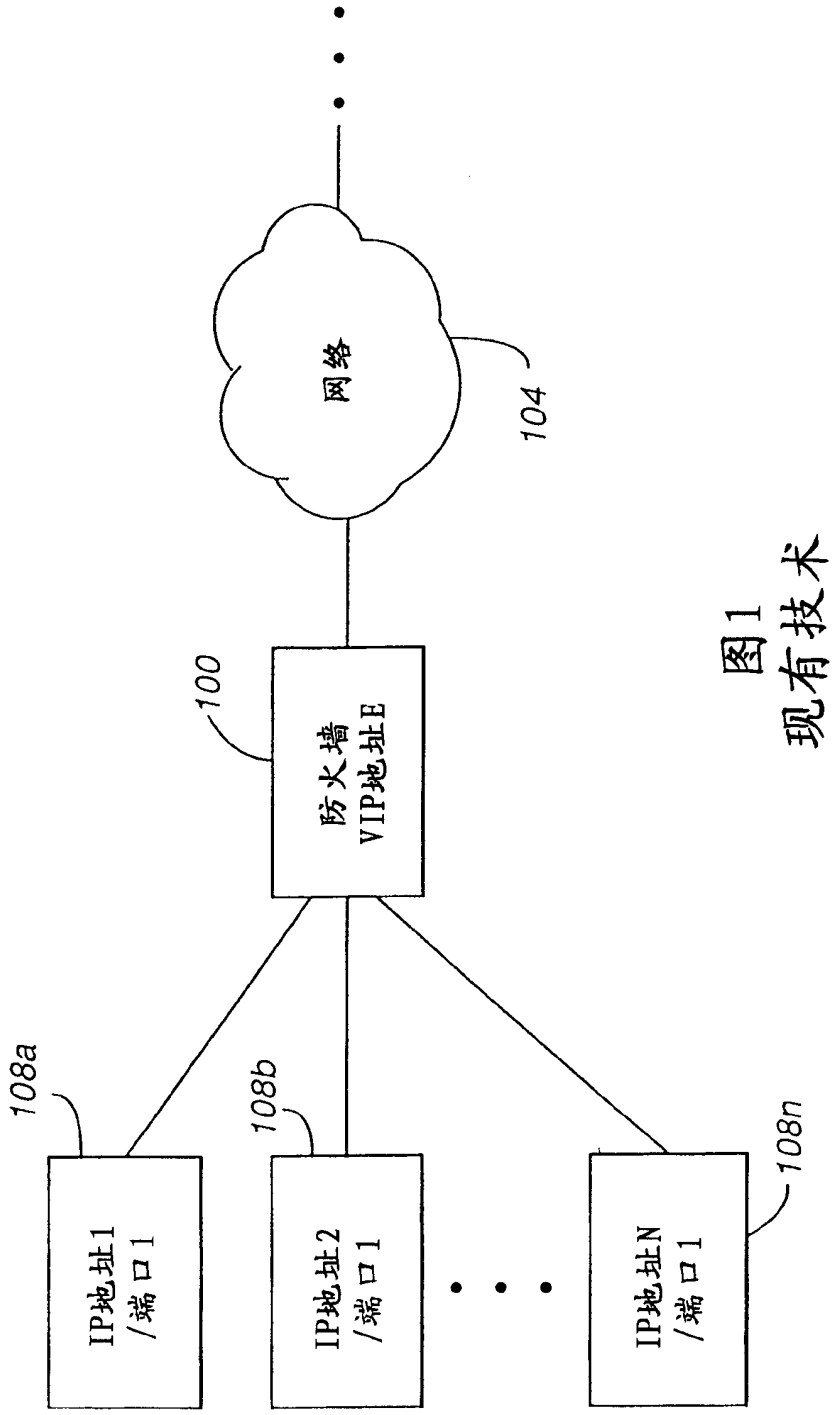

网络
104
100
防火墙
VIP地址E
108a
108b
108n
IP地址1
/端口1
IP地址2
/端口1
IP地址N
/端口1

图1
现有技术

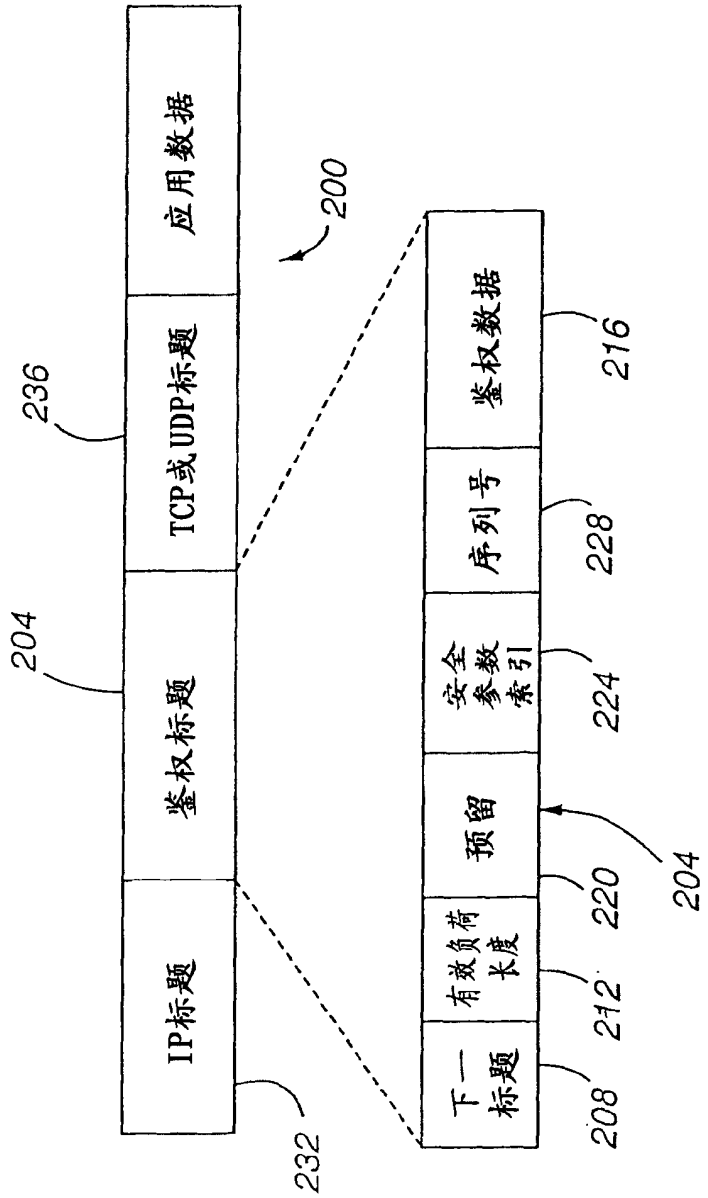

IP标题
鉴权标题
TCP或UDP标题
应用数据
下一标题
有效负荷长度
预留
安全参数索引
序列号
鉴权数据
200
204
236
232
208
212
220
224
228
216

图2A
现有技术

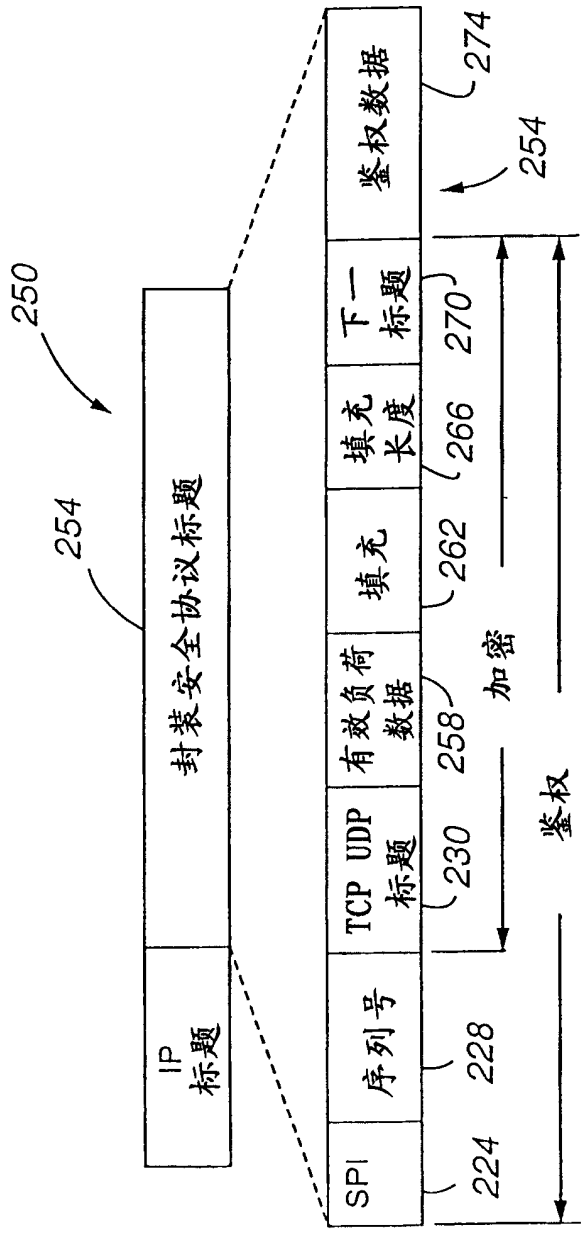

250
254
封装安全协议标题
IP 标题
SPI
序列号
TCP UDP 标题
有效负荷数据
填充
填充长度
下一标题
鉴权数据
224
228
230
258
262
266
270
274
254
加密
鉴权

图 2B

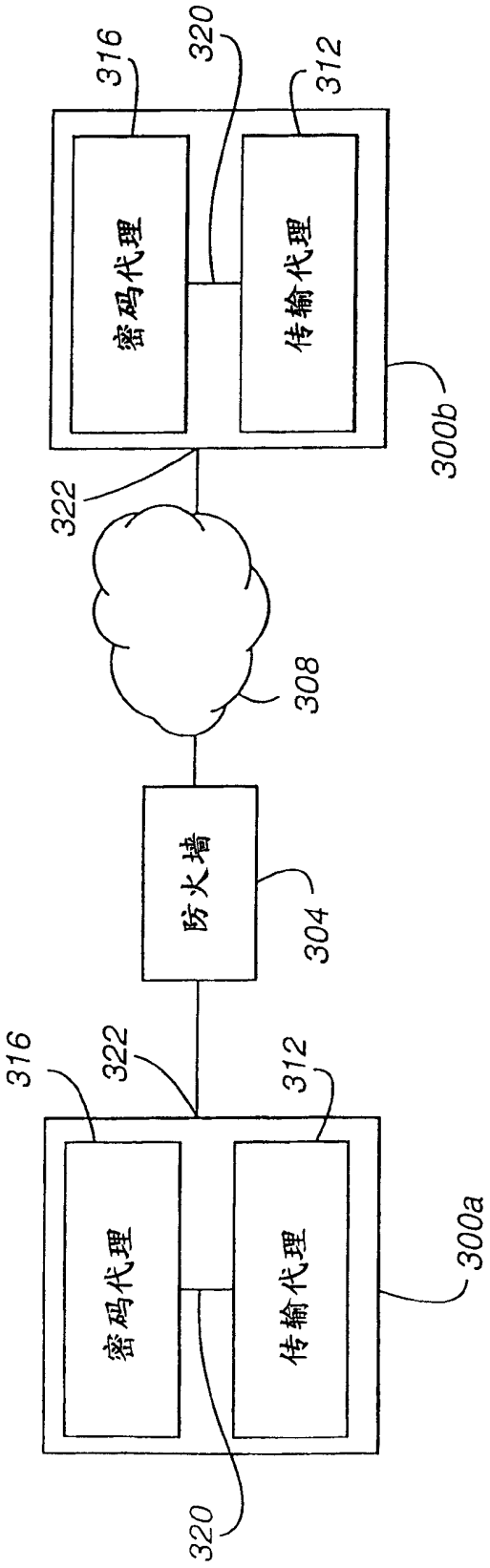

316
320
312
密码代理
传输代理
300b
322
308
防火墙
304
316
322
312
密码代理
传输代理
300a
320

图 3

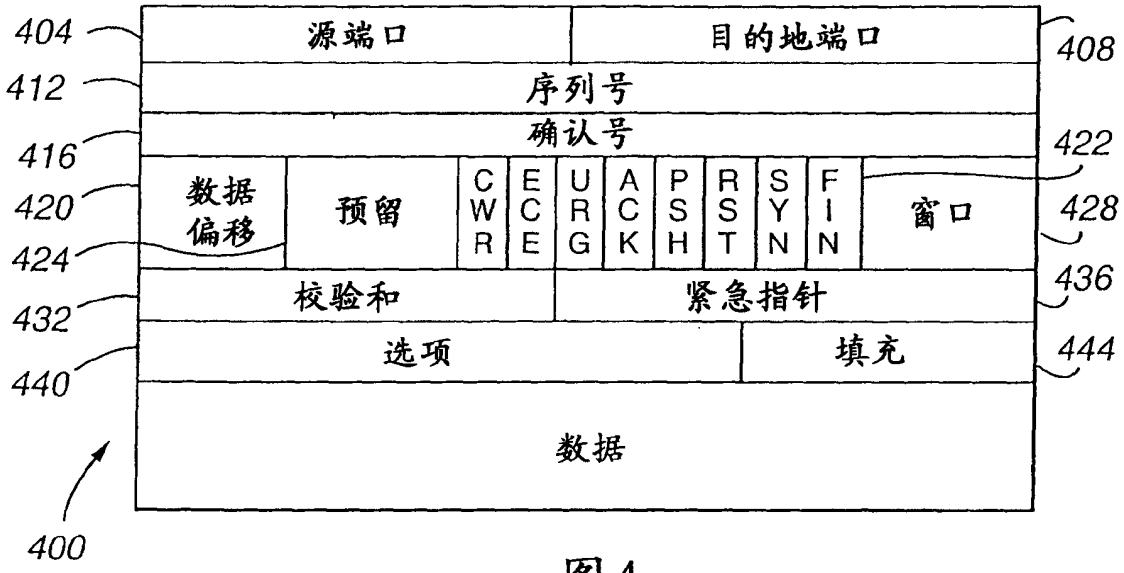

404
源端口
目的地端口
408
412
序列号
确认号
416
422
420
数据偏移
预留
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
窗口
428
424
436
432
校验和
紧急指针
440
选项
填充
444
数据
400

图4
现有技术

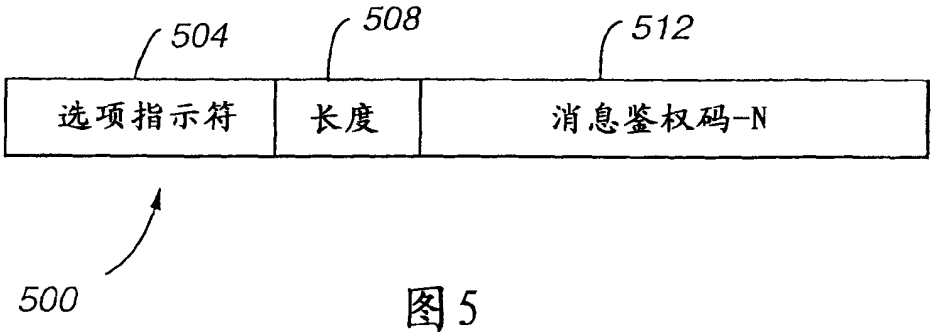

504
508
512
选项指示符
长度
消息鉴权码-N
500

图5

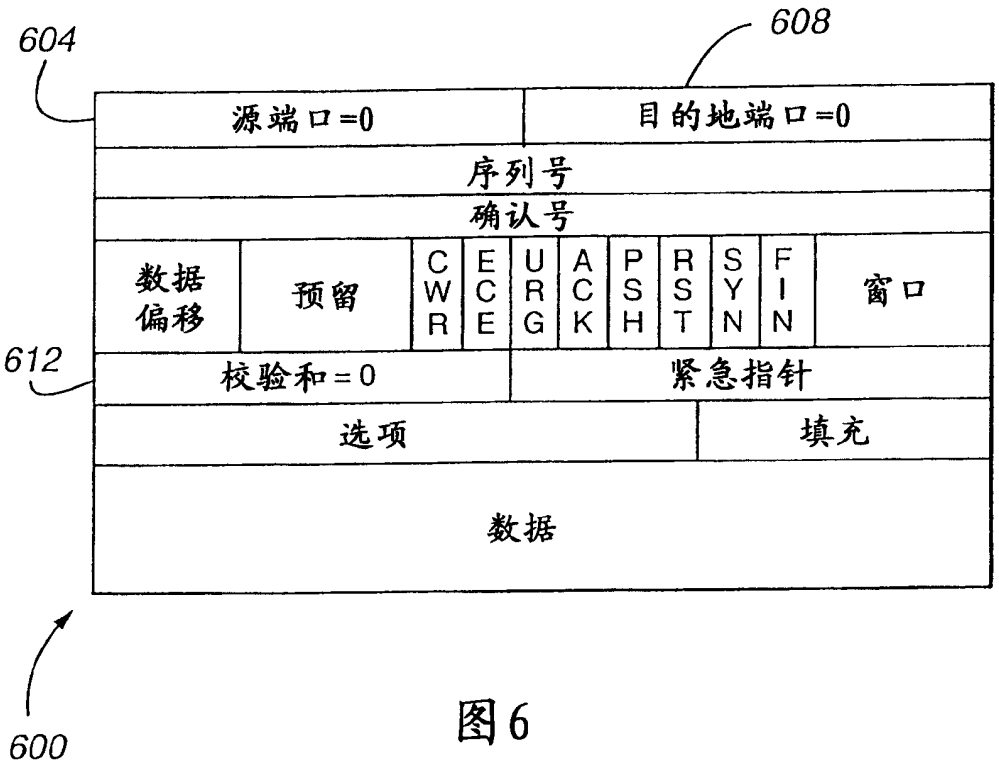

604
608
源端口=0
目的地端口=0
序列号
确认号
数据偏移
预留
CWR
ECE
URG
ACK
PSH
RST
SYN
FIN
窗口
612
校验和=0
紧急指针
选项
填充
数据
600

图6

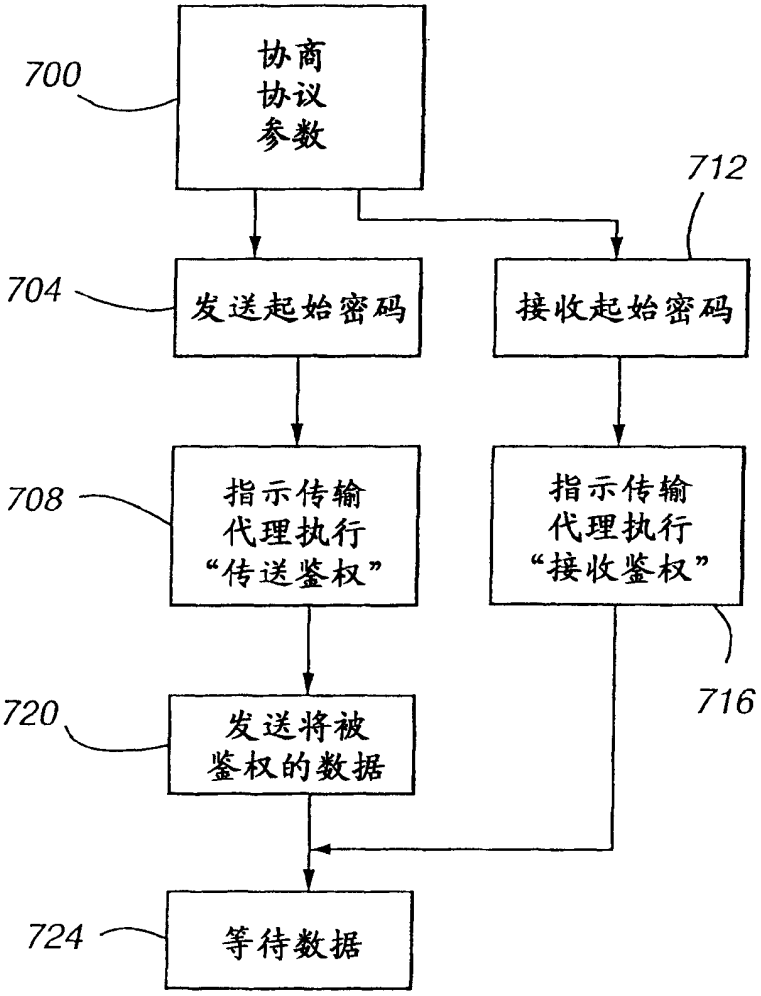

700
协商
协议
参数
712
704
发送起始密码
接收起始密码
708
指示传输
代理执行
“传送鉴权”
指示传输
代理执行
“接收鉴权”
716
720
发送将被
鉴权的数据
724
等待数据

图7

图8A

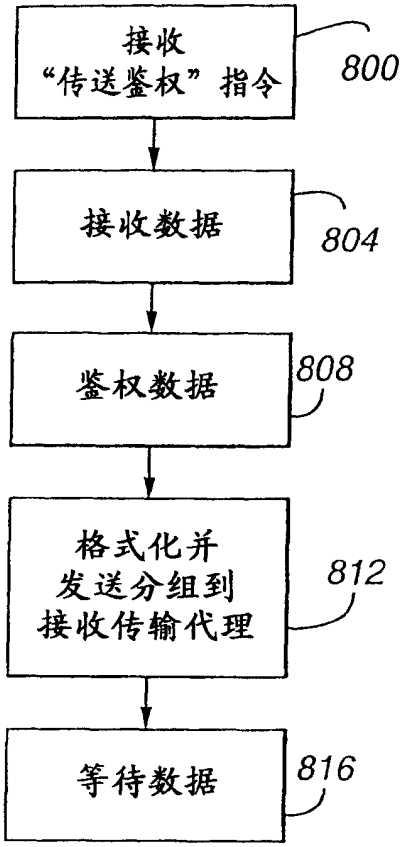
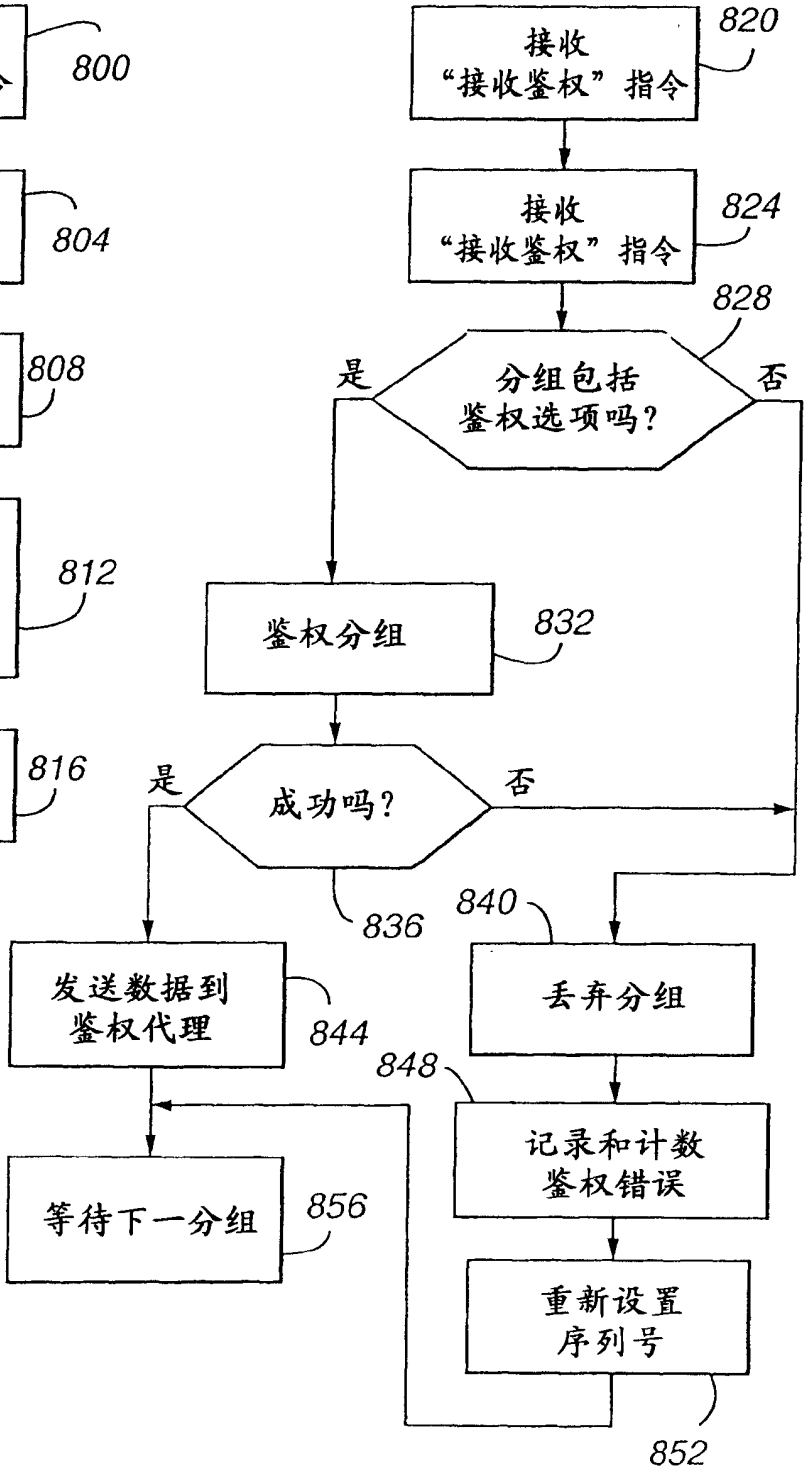

接收
“传送鉴权”指令
800
接收数据
804
鉴权数据
808
格式化并
发送分组到
接收传输代理
812
等待数据
816

图8B


接收
“接收鉴权”指令
820
接收
“接收鉴权”指令
824
828
分组包括
鉴权选项吗？
是
否
鉴权分组
832
成功吗？
是
否
836
840
发送数据到
鉴权代理
844
丢弃分组
848
记录和计数
鉴权错误
等待下一分组
856
重新设置
序列号
852