[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
H04L 12/24 (2006.01)
H04L 12/26 (2006.01)

[12] 发明专利申请公开说明书

[21] 申请号 200510072684.7

[43] 公开日 2006 年 1 月 11 日

[11] 公开号 CN 1719783A

[22] 申请日 2005.5.16
[21] 申请号 200510072684.7
[30] 优先权
[32] 2004. 7. 9 [33] EP [31] 04405438.5
[71] 申请人 国际商业机器公司
地址 美国纽约阿芒克
[72] 发明人 约翰·G·罗尼
克里斯托弗·J·吉布林
马塞尔·沃尔德沃格尔
保罗·T·赫尔利
[74] 专利代理机构 北京市柳沈律师事务所
代理人 郭定辉 黄小临

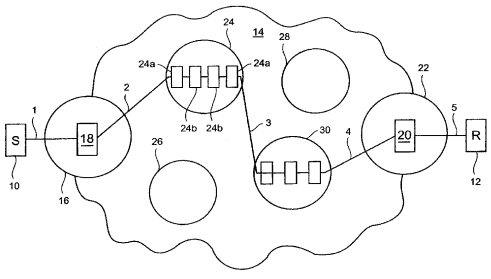
权利要求书 8 页 说明书 23 页 附图 8 页

[54] 发明名称

识别网络内分布式拒绝服务攻击和防御攻击的方法和系统

[57] 摘要

本发明提供了通过在因特网主干连接中的一个或数个点上取样分组以确定分组度量参数，在因特网内检测分布式拒绝服务(DDoS)攻击的系统。 在所选时间间隔上相对于发送分组的主机所处的指定地理位置分析可以包括接收的分组的数量的分组度量参数。 预期行为可以应用于识别揭示 DDoS 攻击的业务失真。 在补充方面，本发明提供了在路由器上验证分组以便提高验证分组的 QoS 的方法。 这个方法可以用于阻止和过滤分组和可以与 DDoS 攻击检测系统结合在一起用于分布式地防御因特网内的 DDoS 攻击。



1. 一种在因特网（14）中检测分布式拒绝服务（DDoS）攻击的方法，其特征在于，该方法包括如下步骤:

在第一预定时间段的数个时间间隔内在因特网（14）中的一个点（2，3，4）上取样分组（100），以便获取与分组的源地址和它们的相关时间间隔有关的数据;

分析所述数据，以便在每个时间间隔内获取与在所述点上从各自指定地理区接收的分组的分组度量有关的至少一个参数；和

对于下一个预定时间段的一个时间间隔，将在那个时间间隔内从指定地理区接收的分组的分组度量参数与从在第一预定时间段的相应时间间隔内获得的至少一个分组度量参数中导出的阈值相比较，所述比较的结果用于确定DDoS 攻击的存在。

2. 根据权利要求 1 所述的方法，其特征在于，分组度量包括接收的分组的数量、接收的分组的大小或任何其它分组度量之一或组合。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，在因特网中的一个点上取样分组的步骤包括在两个因特网相连网络（16，24，22，30）之间的边界（2，3，4）上取样分组。

4. 根据权利要求 3 所述的方法，其特征在于，两个网络的每一个包括自主系统（AS）。

5. 根据权利要求 1 到 4 的任何一项所述的方法，其特征在于，两个网络的每一个包括企业网络、因特网服务提供者（ISP）或网络服务提供者（NSP）的任何一个。

6. 根据权利要求 1 到 5 的任何一项所述的方法，其特征在于，以因特网主干速率执行取样分组的步骤。

7. 根据权利要求 1 到 6 的任何一项所述的方法，其特征在于，取样在因特网中的某点上接收的所有分组，以获取与它们的源地址和所述分组的相关时间间隔有关的数据。

8. 根据权利要求 1 到 7 的任何一项所述的方法，其特征在于，在因特网中的某点上取样分组的步骤包括取样在构成第一预定时间段的每个时间间隔内接收的分组。

9. 根据权利要求 1 到 7 的任何一项所述的方法，其特征在于，在因特网中的某点上取样分组的步骤包括取样在构成第一预定时间段的时间间隔的每第 n 时间间隔内接收的分组，其中 n 是大于 1 的整数。

10. 根据权利要求 1 到 9 的任何一项所述的方法，其特征在于，指定地理区是从与在因特网中的所述点上接收的分组的源地址有关的数据中确定的，其中，所述数据包括每个这样分组的 32 位 IP 源地址的一部分。

11. 根据权利要求 10 所述的方法，其特征在于，指定地理区是根据在因特网中的所述点上接收的每个分组的 32 位数字源地址的前八位位组确定的。

12. 根据权利要求 1 到 11 的任何一项所述的方法，其特征在于，第一预定时间段包括在所述间隔的每个时间间隔内获取与在因特网中的所述点上从各自指定地理区接收的分组的分组度量有关的至少一个参数的训练间隔。

13. 根据权利要求 1 到 12 的任何一项所述的方法，其特征在于，将在时间间隔内从指定地理区接收的分组的分组业务度量参数与从在第一预定时间段的相应时间间隔内获得的分组度量参数中导出的阈值相比较的步骤是针对随后预定时间段的时间间隔实现的。

14. 根据权利要求 13 所述的方法，其特征在于，第一预定时间段、下一个预定时间段和/或随后预定时间段的持续时间是 24 小时、一个星期、一个公历月或一年之一。

15. 根据权利要求 13 或 14 所述的方法，其特征在于，第一预定时间段、下一个预定时间段和/或随后预定时间段的持续时间包括是预定时间段的一部分的预定持续时间。

16. 根据权利要求 12 到 15 的任何一项所述的方法，其特征在于，利用为下一个和/或随后预定时间段的对立时间间隔确定的分组度量参数，更新在第一预定时间段的每个时间间隔内在因特网的所述点上从各自特定地理区接收的至少一个分组度量参数。

17. 根据权利要求 1 到 16 的任何一项所述的方法，其特征在于，从在第一预定时间段的时间间隔内获得的分组度量参数中导出的阈值包括指定地理区的分组的数量与同一时间间隔内另一个地理区的分组的数量相比的比率，或来自指定地理区的分组的数量的方差与另一个地理区的分组的数量的方差的比率。

18. 根据权利要求 1 到 17 的任何一项所述的方法，其特征在于，将在时

间间隔内从指定地理区接收的分组的分组度量变化参数与从至少一个分组度量参数中导出的阈值相比较的步骤包括将所述分组度量参数与从在第一预定时间段的相应时间间隔内获得的至少一个分组度量参数中导出的数个阈值相比较，组合所述比较的结果以确定 DDoS 攻击的存在。

19. 根据权利要求 1 到 18 的任何一项所述的方法，其特征在于，将在时间间隔内从指定地理区接收的分组的分组度量参数与从在第一预定时间段的相应时间间隔内获得的至少一个分组度量参数中导出的阈值相比较的步骤根据从至少一个其它 DDoS 攻击检测系统（200）接收的数据，通过概率函数来修改。

20. 根据权利要求 1 到 19 的任何一项所述的方法，其特征在于，它包括将来自 DDoS 攻击检测系统（200）、包括有关那个系统检测的 DDoS 攻击的信息的数据发送到位于因特网（14）中的其它点上的协同 DDoS 攻击检测系统（200）的步骤。

21. 根据权利要求 1 到 20 的任何一项所述的方法，其特征在于，它包括将来自 DDoS 攻击检测系统（200）的数据发送到其它网络节点，以便响应在所述 DDoS 攻击检测系统（200）上检测的 DDoS 攻击将所述节点重新配置成过滤分组业务的步骤。

22. 根据权利要求 1 到 21 的任何一项所述的方法，其特征在于，它包括响应在 DDoS 攻击检测系统（200）上接收的与那个系统或协同 DDoS 攻击检测系统（200）检测的 DDoS 攻击的级别有关的信息，改变在因特网（14）上所述点（2，3，4）上分组的取样速率的步骤。

23. 根据权利要求 1 到 22 的任何一项所述的方法，其特征在于，它包括一旦检测到对准特定 IP 目的地地址的 DDoS 攻击，就阻止具有那个 IP 目的地地址的在取样点上接收的所有分组的步骤。

24. 根据权利要求 1 到 22 的任何一项所述的方法，其特征在于，它包括一旦根据已知源 IP 地址度量检测到 DDoS 攻击，就阻止在取样点上很少遇到的具有源 IP 地址的在取样点上接收的分组的步骤。

25. 根据权利要求 1 到 24 的任何一项所述的方法，其特征在于，时间间隔可以包括一系列相继时间间隔。

26. 根据权利要求 1 到 25 的任何一项所述的方法，其特征在于，分析器（220）响应 DDoS 系统（200）对存在 DDoS 攻击的确定，启动因特网中的

至少一个路由器实现根据权利要求 50 到 66 的任何一项所述的方法。

27. 一种在因特网中检测分布式拒绝服务（DDoS）攻击的系统，其特征在于，该系统（200）包括:

分组取样器（210），用于在第一预定时间段的数个时间间隔内在因特网（14）中的一个点（2，3，4）上取样分组，以便获取与分组的源地址和它们的相关时间间隔有关的数据；和

分析器（220），用于分析所述数据，以便在每个时间间隔内获取与在所述点上从各自指定地理区接收的分组的分组度量有关的至少一个参数；和将在下一个预定时间段的一个时间间隔内从指定地理区接收的分组的分组度量参数与从在第一预定时间段的相应时间间隔内获得的至少一个分组度量参数中导出的阈值相比较，所述比较的结果可用于确定 DDoS 攻击的存在。

28. 根据权利要求 27 所述的系统，其特征在于，由分析器（220）用于获取分组度量参数的分组度量包括接收的分组的数量、接收的分组的大小或任何其它分组度量之一或组合。

29. 根据权利要求 27 或 28 所述的系统，其特征在于，分组取样器（210）被安排成在包括在两个因特网相连网络（16，24，22，30）之间的边界在内的因特网中的一个点上取样分组。

30. 根据权利要求 27 到 29 的任何一项所述的系统，其特征在于，网络取样器包括网络处理器（212）和包括数据存储设施（214），用于存储与取样分组的源地址和它们的相关时间间隔有关的数据。

31. 根据权利要求 29 或 30 所述的系统，其特征在于，两个网络（16，24，22，30）的每一个包括自主系统（AS）。

32. 根据权利要求 27 到 30 的任何一项所述的系统，其特征在于，两个网络（16，24，22，30）的每一个包括企业网络、因特网服务提供者（ISP）或网络服务提供者（NSP）的任何一个。

33. 根据权利要求 27 到 32 的任何一项所述的系统，其特征在于，分组取样器（210）被安排成取样在构成第一预定时间段的每个时间间隔内在因特网中的某点上接收的分组。

34. 根据权利要求 27 到 32 的任何一项所述的系统，其特征在于，分组取样器（210）被安排成在构成第一预定时间段的时间间隔的每第 n 时间间隔内在因特网中的某点上接收的分组，其中 n 是大于 1 的整数。

35. 根据权利要求 27 到 34 的任何一项所述的系统，其特征在于，分组取样器（210）被安排成从与在因特网中的所述点上接收的分组的源地址有关的数据中确定指定地理区，其中，所述数据包括每个这样分组的 32 位 IP 源地址的一部分。

36. 根据权利要求 27 到 35 的任何一项所述的系统，其特征在于，分析器（220）包括事件管理器（228），用于将来自特定 DDoS 攻击检测系统（200）或另一个 DDoS 攻击检测系统（200）、包括有关那个系统检测的 DDoS 攻击的信息的数据发送到位于因特网（14）中的其它点上的协同 DDoS 攻击检测系统（200）。

37. 根据权利要求 36 所述的系统，其特征在于，事件管理器（228）将来自特定 DDoS 攻击检测系统（200）或另一个 DDoS 攻击检测系统（200）的数据发送到其它网络节点，以便响应在所述 DDoS 攻击检测系统（200）上检测的 DDoS 攻击将所述节点重新配置成过滤分组业务。

38. 根据权利要求 36 或 37 所述的系统，其特征在于，分析器（220）的处理单元（224）被安排成响应事件管理器（228）从特定 DDoS 攻击检测系统（200）或另一个 DDoS 攻击检测系统（200）接收的与那个系统（200）或协同 DDoS 攻击检测系统（200）检测的 DDoS 攻击的级别有关的信息，改变分组取样器（210）的取样速率。

39. 根据权利要求 36 到 38 的任何一项所述的系统，其特征在于，网络取样器（210）被安排成响应事件管理器（228）从特定 DDoS 攻击检测系统（200）或另一个 DDoS 攻击检测系统（200）接收的与对准特定 IP 目的地地址的 DDoS 攻击有关的信息，阻止到达特定 IP 目的地地址的所有分组。

40. 根据权利要求 36 到 39 的任何一项所述的系统，其特征在于，网络取样器（210）被安排成响应事件管理器（228）从特定 DDoS 攻击检测系统（200）或另一个 DDoS 攻击检测系统（200）接收的与 DDoS 攻击的检测有关的信息，阻止在取样点上很少遇到的具有源 IP 地址的在取样点上接收的分组。

41. 一种在因特网中检测分布式拒绝服务（DDoS）攻击的分析器，其特征在于，它包括:

安排成从数据存储设施（214）中检索数据的处理单元（224），所述数据与在因特网中的一个点上接收的数个取样分组的每一个的源地址和取样每个

分组的时间间隔有关，所述多个时间间隔构成预定时间段；和

安排成执行构成分析程序的软件代码的处理单元（224），所述分析程序用于在每个时间间隔内获取与在所述点上从各自指定地理区接收的分组的分组度量有关的至少一个参数；和将在下一个预定时间段的一个时间间隔内从指定地理区接收的分组的分组度量参数与从在（第一）预定时间段的相应时间间隔内获得的至少一个分组度量参数中导出的阈值相比较，所述比较的结果用于确定 DDoS 攻击的存在。

42. 一种在发送主机（10）和接收主机（12）之间的连接中的路由器上验证分组的方法，其特征在于，它包括如下步骤：

由发送主机从插在所述分组（100）的首标（300；400；500；600）中的令牌数据（340；400；500；600）集中读取令牌的值，所述令牌数据集是从开始连接时构成连接（1-5）的数个路由器（24a，b，c，d）中获得的；

在路由器上核实所述读取令牌；和

在核实步骤的结果是真的情况下，将提高的服务质量（QoS）提供给所述分组。

43. 根据权利要求 42 所述的方法，其特征在于，在路由器上核实读取令牌的步骤包括根据存储在路由器上的秘密值核实所述读取令牌。

44. 根据权利要求 42 或 43 所述的方法，其特征在于，在接收主机（12）从发送主机（10）接收到至少一个分组后，由接收主机（12）将令牌数据集提供给发送主机(10)，以便发送主机将其插入发送到接收主机的随后分组中。

45. 根据权利要求 44 所述的方法，其特征在于，令牌数据集包括构成发送主机和接收主机之间的连接的路由器的 IP 地址。

46. 根据权利要求 43 到 44 的任何一项所述的方法，其特征在于，从构成发送主机和接收主机之间的连接的路由器获得的令牌数据集对于每个路由器包括第二非地址相关值，其中，第二值与构成连接的一系列路由器中该路由器的位置有关。

47. 根据权利要求 46 所述的方法，其特征在于，第二值包括存活时间（TTL）或路径距离值。

48. 根据权利要求 43 到 47 的任何一项所述的方法，其特征在于，令牌数据集含有与之相联系的代码，所述代码向遇到包含代码字段的分组的路由器指示所述路由器对插入所述分组的令牌数据集的令牌执行核实步骤。

49. 根据权利要求 43 到 48 的任何一项所述的方法，其特征在于，由发送主机插入分组中的令牌数据集包括从连接中的路由器可能实现的数个可能 QoS 级别中选择的所需 QoS 级别。

50. 根据权利要求 43 到 49 的任何一项所述的方法，其特征在于，核实步骤包括对读取令牌进行密码计算。

51. 根据权利要求 43 到 50 的任何一项所述的方法，其特征在于，在核实步骤返回假结果的情况下，路由器不向分组提供提高的 QoS。

52. 根据权利要求 51 所述的方法，其特征在于，在核实步骤返回假结果的情况下，路由器降低分组的 QoS 级别。

53. 根据权利要求 43 到 52 的任何一项所述的方法，其特征在于，令牌数据集对于连接的每个路由器包括短期令牌和长期令牌。

54. 根据权利要求 51 到 52 的任何一项所述的方法，其特征在于，令牌数据集对于连接的每个路由器包括短期令牌和长期令牌，其中，所述短期令牌和长期令牌对应于每一个所述路由器存储的各自秘密值。

55. 根据权利要求 54 所述的方法，其特征在于，核实步骤包括首先核实短期令牌，和如果取得真结果，则向分组提供提高的 QoS。

56. 根据权利要求 55 所述的方法，其特征在于，在对短期令牌的核实步骤返回假结果的情况下，接着对长期令牌执行核实步骤，和如果取得真结果，则向分组提供提高的 QoS。

57. 根据权利要求 56 所述的方法，其特征在于，响应来自对长期令牌的核实步骤的真结果向分组提供的 QoS 处在比在对短期令牌的核实步骤返回真结果的情况下提供给分组的 QoS 低的 QoS 级别。

58. 一种验证在发送主机（10）和接收主机（12）之间的连接中的路由器上接收的分组的路由器，其特征在于，它包括：安排成执行如下步骤的处理单元（224）:

由发送主机从插在所述分组（100）的首标（300; 400; 500; 600）中的令牌数据（340; 400; 500; 600）集中读取令牌的值，所述令牌数据集是从该路由器和开始连接时构成连接（1-5）的数个其它路由器（24a，b，c，d）中获得的;

在路由器上核实所述读取令牌; 和

在核实步骤的结果是真的情况下，将提高的服务质量（QoS）提供给所

述分组。

59. 根据权利要求 58 所述的路由器，包括存储器，用于存储据此执行核实读取令牌的步骤的秘密值。

60. 根据权利要求 58 到 59 的任何一项所述的路由器，其特征在于，处理单元（224）被安排成识别与令牌数据集相联系的代码字段，和当识别出所述代码字段时，对令牌数据集的令牌执行核实步骤。

61. 根据权利要求 58 到 60 的任何一项所述的路由器，其特征在于，处理单元（224）被安排成对读取令牌进行密码计算。

62. 根据权利要求 59 到 61 的任何一项所述的路由器，其特征在于，路由器将与短期令牌相对应的第一秘密值和与长期令牌相对应的第二秘密值存储在它的存储器中。

63. 根据权利要求 62 所述的路由器，其特征在于，处理单元（224）被安排成首先对照第一秘密值核实短期令牌，和如果取得真结果，则向分组提供提高的 QoS。

64. 根据权利要求 63 所述的路由器，其特征在于，在处理单元（224）返回来自对照第一秘密值核实短期令牌的步骤的假结果的情况下，接着对照第二秘密值对长期令牌执行核实步骤，和如果取得真结果，则向分组提供提高的 QoS。

65. 一种包括存储器的计算机，所述存储器存储用于实现根据权利要求 43 到 57 或 1 到 25 的任何一项所述的方法、可由处理器（224，212）执行的程序代码。

66. 一种包含用于实现根据权利要求 43 到 57 或 1 到 25 的任何一项所述的方法、可由处理单元（224）执行的程序代码的计算机可读媒体。

识别网络内分布式拒绝服务攻击和防御攻击的方法和系统

技术领域

本发明涉及识别分组数据网络内的分布式拒绝服务（DDoS）攻击和防御这种攻击的方法。具体地说，本发明涉及识别对目标（受害）设备的 DDoS 攻击的方法、与因特网连接的系统和/或网络和减轻这种攻击对目标的影响的方法。

背景技术

拒绝服务（DoS）攻击是一个或多个攻击者阻止或损害主计算机、路由器、服务器和网络等的合法使用的明显企图。虽然这种攻击可以从目标网络本身内发起，但绝大多数攻击是从与通过因特网与目标连接的外部系统和网络发起的。今天，因特网连接设备、系统和网络正面临着迅速扩张和来自 DoS 攻击的真正威胁。这种攻击不仅伤害既定目标，而且威胁着因特网本身的稳定性。大多数 DoS 攻击的动机似乎仍然是受例如黑客“炫耀”、表达愤怒或企图报复的欲望的驱动，但是，存在着网上犯罪分子正越来越多地使用 DoS 攻击来勒索从在线（基于因特网）活动中获取它们大部分收入的企业的迹象，和令人害怕的是恐怖分子将 DoS 攻击用作破坏政府机构的良好管理的手段。

可以容易地从因特网中发起 DoS 攻击是使因特网取得如此成功的特征的直接后果。在设计因特网时，在人们的脑海中考虑的是功能，而不是安全。它仿效端到端范例，从而，通信端主机部署复杂的功能来达到所需的服务保证，而连接所述端主机的中间网络（因特网）提供极少量的、最有效的服务。这样，可以分布式地管理因特网，使得在它的用户之间不用强行执行公共策略。这种使用户容易共享因特网中的设计自由提供了诸如 DoS 攻击之类滥用的机会。

DoS 攻击者利用了因特网由有限资源组成的事实的优点。包括因特网和网络的核心、与之连接的系统和设备的互连自主系统（AS）由有限带宽、处理能力和存储容量组成，它们都是设计成消耗足够多目标可用资源以引起某种程度的服务崩溃的 DoS 攻击的共同目标。此外，因特网中的安全性是高度

独立的。这样，DoS 攻击通常从通过安全相关约定而被破坏的系统发起。防侵入系统不仅有助于保护它们具体支持的因特网资源，而且有助于防止这样的资源被用于攻击其它因特网相连系统和网络。因此，无论因特网资源被保护得多好，它的安全性也依赖于其余因特网中的安全状态。对在因特网中可以容易地启动 DoS 攻击有影响的其它因素是端主机之间的服务保证所需的大多数情报位于端主机内而不是因特网中和因特网在可以将极大量消息携带给目标的中间网络之间应用高带宽路径的事实。

早期 DoS 攻击技术涉及到生成分组和将分组从单个源头发送到单个目的地的简单工具。这些攻击往往人工配置，这限制了它们的频率和有效性，并且，可以容易地通过例如源地址分组过滤来防御。但是，近年来，演变出对一个或多个目标自动进行多源攻击，即所谓分布式 DoS（DDoS）攻击的工具包。通过从黑客网站下载这些工具包可容易地获得它们，并且，使用简单，连初学因特网用户也可以设置 DDoS 攻击。

目前，对单个目标的多源攻击是对因特网相连设备、系统和网络发起的 DDoS 攻击的最普通形式。这种攻击利用了因特网和目标之间的资源不对称的优点，因为将足够大量的约定主机集中起来，一般说来同时地向目标发送无用分组。综合业务的数量往往足以引起目标系统或网络崩溃和/或充满它的因特网连接，从而，至少在攻击期间有效地从因特网中除去目标。这些类型的攻击通常被称为分组泛滥 DDoS 攻击。

尽管对于单源 DoS 攻击，可以跟踪分组包含实际源地址的攻击源和应用例如分组过滤来弃掉从那个源接收的分组，但 DDoS 攻击更恶毒，因为向目标发送无用分组的被破坏的主机的数量可能有数万个，甚至有数十万个，和因为还往往应用隐藏被破坏的主机的身份的地址假冒。即使可以识别无用分组的源头，也无助于目标防护它自己，因为像在所谓反射器或间接 DDoS 攻击中发生的那样，接收分组可能来自提示向目标发送分组的合法源。阻止来自这些源的分组也阻止了来自合法用户的分组。

在目标上容易检测到成功的 DDoS，因为它能了解使它变饱和和失效的所有攻击分组。尽管 DDoS 攻击的检测使目标可以实现诸如分组过滤之类的防护，虽然存在一些没有被攻击击垮的可用分组处理资源，但攻击的检测未必导致攻击分组被有效过滤以便在目标上保持某种程度的服务。由于攻击的分布式性质，在目标上或其附近的分组过滤通常使攻击分组减少之外，也使

正常（合法）分组减少，因为分组过滤器不能区分它们，导致至少对目标上的服务造成损害。因此，目标上 DDoS 的检测一般说来不那么有效，因为对于目标来说，总是晚得难以建立有效防护。

目标网络面临的两难境地是，检测装置与目标网络越接近，检测 DDoS 攻击的能力就越强，而与目标网络越接近，过滤分组以弃掉攻击分组的有效性随着攻击分组减少而下降，也就是说，过滤与攻击源接近的攻击分组更有效得多，因为这样的过滤较不可能使指定到目标的合法分组减少。

经常，一旦检测到 DDoS 攻击，目标网络的因特网服务提供者（ISP）网络就减少指定到目标网络指定的所有分组，从而有效地中止目标网络上的服务，并且，在任何情况下，取消目标网络自身防御 DDoS 攻击的努力。

解决在攻击分组的总效应击垮目标之前检测 DDoS 的问题的一种方案是在网络中远离目标地部署系统。这样的系统使用有关因特网中的某个选点上网络业务的期望行为的信息来确定什么时候出现攻击。当前可用的这种类型的系统，一般称之为“因特网防火墙”。作为检测 DDoS 攻击的方法，所有这样的系统监视穿过因特网中的一个或多个点的分组，分析总分组流行为的某个方面，和设法确定是否明显地偏离了正常行为。关键问题是找出构成正常行为的特征。虽然业务模式由于诸如新网站越来越受欢迎或部署了新应用之类的合法原因迅速发生变化，但诸如到达给定目的地地址的分组的预期数量或用户数据报协议（UDP）分组与传输控制协议（TCP）分组之间的比率之类的绝对度量却是有限值。诸如记录 TCP SYN 消息与 ACK 消息的比率之类的其它技术也可以识别某些 DoS 攻击，但攻击者已经表明了利用这样的独特参数迅速地绕过检测工具的令人佩服的能力。

与在什么地方和如何检测 DDoS 攻击无关，除了简单弃掉指定到目标的所有分组（合法和攻击两者）之外，防御这种攻击的当前推荐方法至少包括进行进入分组过滤的目标和/它的 ISP。这涉及到 ISP 核实分组的源地址是否适合那个输入目标系统链路。但是，这要求 ISP 几乎没有动机地升级它的装备，因为 ISP 本身几乎不会被对其客户（用户）之一的 DDoS 攻击击垮。因此，可以得出，这是 ISP 不愿承担的责任。

防御 DDoS 攻击的另一种手段包括增加分组的路由信息，使甚至远程的 ISP 也能够识别带有特定源地址的分组来源于此的可能链路。但是，这再次要求 ISP 为很少看得见的利益升级它们的装备，尤其与目标没有什么酬劳关系

的那些 ISP。

利用因特网协议（IP）首标中它们的预定使用之外的现有字段来包括倘若分组足够多，使接收器能够重构分组经过的路径的数段信息是可以使接收器滤出攻击分组采取的手段。但是，攻击者仍然可以滥用这种手段，将大量虚假信息传送给目标（接收器），因此，效果有限。

后面跟着带有特定控制分组的一小组现有分组也有助于接收器滤出攻击分组，特定控制分组通过，比方说，指出分组经过的一个路由器，指出分组的来源。但是，这种手段解决不了识别合法路由器和造成从网络容量的观点来看，只在 DDoS 攻击期间是优点，而在其它时间是缺点的产生附加业务的问题。

因此，问题仍然是如何识别 DDoS 攻击和当发生 DDoS 攻击时如何阻止或减轻它的影响。

在因特网中的某个选点（或某些选点）上检测 DDoS 攻击的现有手段基于随着时间迅速变化和易于随因特网技术的进步而逐渐过时的参数。因此，我们需要的是基于随技术的改变而保持不变，并且一般说来足以高概率地检测到许多 DDoS 攻击两者的参数。

尽管需要搬动以将 DDoS 攻击检测系统放入因特网中，但大多数 DDoS 检测和防护系统都位于想要保护他们的网络、系统和设备免遭这种攻击的端主机（接收器，可能是目标）运行的因特网的边缘。如果过滤系统本身没有将被击垮，防护系统主要依靠在泛滥分组攻击的性质一定的情况下，必须具有高处理能力的防御攻击的分组过滤。当前，几乎不可能由于 ISP 出于竞争的动机将他们的网络升级成防御 DDoS 攻击，尽管随着在世界范围立法机关施加压力要求负担，这种情况可能会发生改变。因此，需要提供使接收器能够更智能地过滤接收分组和为因特网的其它相连系统和网络创造动机以帮助这个过程的方法。

发明内容

本发明试图提供减轻和/或消除与已知检测系统，尤其，包括当前可用的因特网防火墙的侵入检测系统相联系的缺点、在因特网中的适当点上检测 DDoS 的方法。本发明还试图提供实现这样方法的新装置。

本发明还试图提供减轻和/或消除与现有 DDoS 防护系统相联系的缺点、

在目标网络等上更智能地过滤接收分组的方法，和提供实现该方法的新装置。

根据本发明的第一方面，提供了在因特网中检测分布式拒绝服务（DDoS）攻击的方法，其特征在于，该方法包括如下步骤：在第一预定时间段的数个时间间隔内在因特网中的一个点上取样分组，以便获取与分组的源地址和它们的相关时间间隔有关的数据；分析所述数据，以便在每个时间间隔内获取与在所述点上从各自指定地理区接收的分组的分组度量有关的至少一个参数；和对于下一个预定时间段的一个时间间隔，将在那个时间间隔内从指定地理区接收的分组的分组度量参数与从在第一预定时间段的相应时间间隔内获得的至少一个分组度量参数中导出的阈值相比较，所述比较的结果用于确定 DDoS 攻击的存在。

根据本发明的第二方面，提供了在因特网中检测分布式拒绝服务（DDoS）攻击的系统，其特征在于，该系统包括：分组取样器，用于在第一预定时间段的数个时间间隔内在因特网中的一个点上取样分组，以便获取与分组的源地址和它们的相关时间间隔有关的数据；和分析器，用于分析所述数据，以便在每个时间间隔内获取与在所述点上从各自指定地理区接收的分组的分组度量有关的至少一个参数；和将在下一个预定时间段的一个时间间隔内从指定地理区接收的分组的分组度量参数与从在第一预定时间段的相应时间间隔内获得的至少一个分组度量参数中导出的阈值相比较，所述比较的结果用于确定 DDoS 攻击的存在。

根据本发明的第三方面，提供了在因特网中检测分布式拒绝服务（DDoS）攻击的分析器，其特征在于，它包括：安排成从数据存储设施中检索数据的处理单元，所述数据与在因特网中的一个点上接收的数个取样分组的每一个的源地址和取样每个分组的时间间隔有关，所述多个时间间隔构成预定时间段；和安排成执行构成分析程序的软件代码的处理单元，所述分析程序用于在每个时间间隔内获取与在所述点上从各自指定地理区接收的分组的分组度量有关的至少一个参数；和将在下一个预定时间段的一个时间间隔内从指定地理区接收的分组的分组度量参数与从在（第一）预定时间段的相应时间间隔内获得的至少一个分组度量参数中导出的阈值相比较，所述比较的结果用于确定 DDoS 攻击的存在。

根据本发明的第四方面，提供了包括存储器的计算机，所述存储器存储用于实现根据本发明第一方面的方法、可由处理器执行的程序代码。

根据本发明的第五方面，提供了包含用于实现根据本发明第一方面的方法、可由处理器执行的程序代码的计算机可读媒体。

根据本发明的第六方面，提供了在发送主机和接收主机之间的连接中的路由器上验证分组的方法，其特征在于，它包括如下步骤：由所述发送主机从插在所述分组的首标中的令牌数据集中读取令牌的值，所述令牌数据集是从开始连接时构成连接的数个路由器中获得的；在路由器上核实所述读取令牌；和在核实步骤的结果是真的情况下，将提高的服务质量（QoS）提供给所述分组。

根据本发明的第七方面，提供了验证在发送主机和接收主机之间的连接中的路由器上接收的分组的路由器，其特征在于，它包括：安排成执行如下步骤的处理单元：由所述主机从插在所述分组的首标中的令牌数据集中读取令牌的值，所述令牌数据集是从路由器和开始连接时构成连接的数个其它路由器中获得的；在路由器上核实所述读取令牌；和在核实步骤的结果是真的情况下，将提高的服务质量（QoS）提供给所述分组。

根据本发明的第八方面，提供了包括存储器的计算机，所述存储器存储用于实现根据本发明第六方面的方法、可由处理器执行的程序代码。

根据本发明的第九方面，提供了包含用于实现根据本发明第六方面的方法、可由处理器执行的程序代码的计算机可读媒体。

本发明的其它特征可从从属权利要求中明显看出。

附图说明

图 1 是横跨因特网的端到端分组交换连接的示意性例示；

图 2 是 IPv4 数据报的结构的示意图；

图 3 是直接型的 DDoS 攻击网络的示意性例示；

图 4 是间接或反射器型的 DDoS 攻击网络的示意性例示；

图 5 是包含基于本发明第一主要方面的 DDoS 检测系统的因特网的示意性例示；

图 6 是基于本发明第一主要方面的 DDoS 检测系统的方块示意图；

图 7 是实现基于本发明第二主要方面的方法的分组的第一附加首标部分的示意性表示；

图 8 示出了构成图 7 的首标部分的数据空间的一个数据字段的数据元；

图9a是实现基于本发明第二主要方面的方法的分组的第二附加首标部分的示意性表示;

图 9b 是实现基于本发明第二主要方面的方法的可替代第二附加首标部分的示意性表示;

图 10 是实现基于本发明第二主要方面的改进方法的分组的第一附加首标部分的示意性表示;

图 11 示出了构成图 10 的首标部分的数据空间的一个数据字段的数据元;和

图 12 是实现基于本发明第二主要方面的改进方法的分组的第二附加首标部分的示意性表示。

具体实施方式

因特网是由通过称为因特网协议（IP）的简单公用层-3 协议互连许多各种层-2 网络的网络组成的环球网。传输控制协议（TCP）是构成应用在因特网中以保证以完整形式接收和以正确顺序重新组装发送的信息的构成分组的软件系统的基础的协议，而 IP 是构成允许信息的所述分组从一个 IP 地址到另一个 IP 地址获得的软件系统的基础的协议。将唯一的 32 位 IP 地址分配给因特网上的每个计算设备，IP 地址通常被写成用句点分开的 4 个数，例如，193.32.2. 36。取决于计算设备和它的因特网服务提供者（ISP）之间的连接的性质，分配给所述设备的 IP 地址可以是永久的或临时的，但是，在每一种情况下，它都是唯一的。因特网号码分配管理局（IANA）是负责发放 IP 地址的全局实体。因此，因特网是基于 TCP/IP 的分组数据网，这样，与诸如公共交换电话系统（PSTN）之类的传统电话网相比，它包括分组交换网，而不是电路交换网。

参照附图，图 1 是横跨因特网（被表示成云状）14 的包括发送（源）端主机（S）10 和接收（目的地）端主机（R）12 之间的链路 1、2、3、4 和 5 的端到端分组交换连接的示意性例示。发送主机 10 和/或接收主机 12 可以包括诸如个人计算机（PC）之类的独立设备或在与因特网 14 连接的系统和/或网络内那样的设备。可替代地，发送主机 10 和/或接收主机 12 可以包括例如企业网络的万维网服务器或路由器，或具有 IP 地址和能够发送和接收 IP 分组的任何其它 IP 启用设备。

发送主机 10 通过因特网服务提供者（ISP）16 与因特网 14 连接，因特网服务提供者（ISP）包括发送来自所述源主机 10 的 IP 分组和接收寻址到所述源主机 10 的 IP 分组的因特网边缘网关路由器 18。源主机 10 和 ISP 16 之间的链路 1 可以包括本领域的普通技术人员已知的任何适当链路，例如，包括通过 PSTN 的调制解调器到调制解调器链路、以太局域网（LAN）连接等。源主机 10 和/或接收主机 12 可以包括因特网相连网络，并且，事实上，正如与因特网连接的大型企业、研究院和政府机构网络常见的那样，是它自己的 ISP。接收主机 12 通过链路 5 与 ISP 22 的因特网边缘网关路由器 20 连接。

因特网 14 是由诸如 ISP 16、24 之类的网络和其它中间网络 24、26、28、30 组成的网络。端到端分组交换连接 1-5 通过这些网络的一部分形成，用于将 IP 分组从源主机 10 发送到接收主机 12。类似地，分组交换连接（未示出）可以在接收主机 12 和源主机 12 之间形成，用于沿着相反方向发送 IP 分组，但是，这种“相反”连接无需沿着与“正向”连接 1-5 相同的路径。中间网络 24、26、28、30 本身可以包括 ISP 和/或网络服务提供者（NSP）。

如图 2 所示，IPv4 数据报（分组）100 含有首标部分 102 和有效负载（要发送到接收节点的数据）部分 104（未按比例表示）。首标部分 102 包括各种各样的字段，这些字段包括:

1. 版本字段 106，它一般被设置成“4”，标识应用在因特网中的 IP（IPv4）的当前最广泛使用的版本。

2. IP 首标长度（IHL）字段 108，它标识形成首标部分 102 的 32 位字的个数。这通常是 5。

3. 包含代码点（DSCP）的有差别服务字段 110，它通常被设置成“0”，但它可以表示网络所需的特定服务质量（QoS）。

4. 数据报大小字段 112，它示出 IP 分组 100 的 IP 首标部分 102 和有效负载部分 104 用字节表示的总大小。

5. 标识字段 114，它包括与源地址一起唯一地标识分组的 16 位数。在重新组装成碎片分组期间，在接收器上使用这个字段。

6. 存活时间（TTL）字段 116，它包括分组可以路由转换的跳段（hop）/链路的个数。这个字段逐渐被分组遇到的路由器递减，作为防止偶然路由循环的手段。当这个字段中的值递减到零时，弃掉该分组。

7. 协议字段 118 或服务访问点（SAP），指示携带的传输分组的类型。

这个字段的公用值是 1 = ICMP; 2 = IGMP; 6 = TCP; 和 7 = UDP。ICMP 是用于与网络操作或误操作有关的带外消息的因特网控制消息协议。IGMP 是为因特网上的多播消息传送设置标准的因特网成组消息协议。

8. 源地址字段 120，它包含分组的发送者的 32 位句点隔开数字 IP 地址。

9. 目的地地址字段 122，它包含分组的最后目的地的 32 位句点隔开数字 IP 地址。

10. 选项字段 124，尽管"Record Route"选项可以被设置成跟踪 IP 数据报所取的路由，但除非 IHL 多于 5 个 32 位字，一般不使用它。这个选项包含数据报流过的路由器的 IP 地址。

应该识别到，上面列出的字段没有穷尽在 IPv4 首标部分 102 中找到的字段，它还包括像与路由器可以打碎 IP 分组的时间有关的碎片化标志字段和碎片化补偿字段那样的字段（在图 2 中未示出）。

再参照图 1，从源主机 10 发送到接收主机 12 的 IP 分组一个跳段一个跳段地转发。在发送主机 10 是具有唯一 IP 地址的 IP 启用设备的情况下，所述主机 10 在将它自己的 IP 地址作为源地址和在本例中包括接收主机 12 的预定目的地的 IP 地址插入分组的首标部分 102 中之后，在链路 1 上将分组发送到它的 ISP 16 的网关路由器 18。一旦接收到分组，网关路由器 18 就检查 IP 目的地地址和检验它的路由表，路由器由目的地地址/下一个跳段对组成。如果在网关路由器的路由表中找到目的地 IP 地址，那么，在相关的下一个跳段（链路 2）上将分组转发给路径中朝向接收主机 12 的下一个路由器。如果在网关路由器的路由表中没有找到目的地 IP 地址，那么，在在中间网络 26、28、30、32 的层面之上的默认路线上将分组转发给有希望知道将分组转发到什么地方的路由器。在接收分组的每个路由器上重复这个过程，直到它到达（通过链路 3、4 和 5）它的预定目的地或分组的 IP 首标中的 TTL 值递减到零为止。

每个中间网络 26、28、30、32 是由以自主系统（AS）形式出现的路由器组成的网络。在 1996 年 3 月发行的因特网工程部（IETF）征求意见（RFC）文件第 1930 号中，AS 被定义成在单种技术管理下，将内部网关协议（IGP）和公用度量用于在 AS 内路由分组和将外部网关协议（EGP）用于将分组路由到其它 AS 的一组路由器。虽然实际上许多 AS 在 AS 内使用几个 IGP 和数组度量，但 AS 的管理在其它 AS 看来应该像具有单个连贯内部路由计划和呈现出可通过它到达各个网络的一致画面。在图 1 中，中间网络 24 可以被看作包

括含有数个外部网关路由器 24a 和数个内部网关路由器 24b 的 AS。ISP 16、22 也可以包括 AS。

现在参照图 3，图 3 示意性地例示了攻击目标机器（T）50 的攻击者 40 在因特网 14 上像管弦乐队那样编排的直接型分布式拒绝服务（DDoS）攻击网络。可以包括简单独立 PC 的攻击者 40 建立包括许多管理或主设备 42 和大量代理设备（往往称为蛇神或精灵）44 的 DDoS 攻击网络。管理设备 42 是攻击者 40 用来扫描其它易受攻击主机（代理器）和安装诸如 Trinoo、Tribe Flood Network 3000 和 Stracheldracht 之类的程序的约定计算机。计算机病毒和蠕虫常常用于安装这种后门和/或控制程序。

一旦攻击网络已准备好，攻击者就识别目标机器 50 和向管理设备 42 发出带有目标 IP 地址、攻击持续时间、攻击方法和其它指令的攻击命令。每个管理设备 42 将它的指令传给它的代理设备 44。攻击者 40、管理设备 42 和代理设备 44 之间的通信通常通过诸如因特网中继信道（IRC）之类，对于管理器 42 和代理器 44 的拥有者来说难以或不可能识别从攻击者 40 接收的命令的来源的信道。

通常用在 DDoS 攻击中的分组流的类型包括带有寻址到目标 50 的各种标志集的 TCP 分组、ICMP 回音请求/回答（查验（ping））分组和 UDP 分组的流。在 TCP 的情况中，SYN 泛滥是最众所周知的攻击。攻击者 40 往往通过在分组中假冒源地址字段隐藏代理设备 44 的身份，以便将来对相同或不同目标的攻击中可以重新使用代理设备 44。虽然一方面管理设备 42 和另一方面代理设备 44 被显示成位于各自对齐的网络云 43、45 内，但应该明白，这仅仅是为了易于例示，管理器 42 和代理器 44 两者都包括与因特网 14 连接的约定计算机。这些计算机可以位于因特网中的任何地方（与因特网连接），和可以位于不同网络内，甚至包括独立机器。通常，家用 PC 的拥有者没有安全意识，因此，忽略了他们的 PC 可以被容易地约定成 DDoS 攻击网络的组成部分的可能性。

当发出攻击时，目标 50 面临着充满它的因特网连接 5 的巨大无用分组和击垮它的处理能力。

在如图 4 所示的间接或反射器型攻击中，诸如路由器和/或服务器之类的大量中间节点 46 被无过地用作攻击发出者。攻击者 40 像以前那样建立攻击网络，但使代理设备 44 将请求分组发送到要求对设置成目标机器 50 的 IP 地

址的请求分组的内嵌源地址作出响应的中间节点 46。在不知道请求分组是假冒成目标地址的源地址的情况下，中间节点 46 根据请求分组的类型使目标机器 50 充满响应分组。TCP 和 UDP 可以被开发成发出间接攻击。虽然在图 4 中中间节点 46 被显示成与代理设备 44 一一对应关系，但应该明白，这仅仅是为了易于例示。

正如上文所讨论的那样，在目标网络、系统或设备附近检测 DDoS 攻击最有效，但是，在因特网中的这个点进行检测通常导致在目标可以建立有效防护之前就被击垮了。按照本发明的第一主要方面，本发明提供了位于因特网中的 DDoS 检测系统，以便在攻击的总效应可以击垮它的目标之前检测到 DDoS 攻击，和以便可以与其它类似检测系统共享 DDoS 攻击检测信息。

参照图 5，在本发明的第一主要方面中，本发明包括 DDoS 检测系统 200。DDoS 检测系统 200 位于因特网 14 中可以取样例如在诸如 ISP 16、22 和 NSP 24、30 之类的两个网络之间或诸如 NSP 24 和 30 之类的两个 AS 之间的链路上发送的分组的点上。检测系统 200 在物理上可以与路由器/网关一起位于任何这样的 ISP、NSP 和 AS 网络的边缘，成为与网络的周围交接的路由器/网关。

如图 6 所示，检测系统 200 包括捕获数据的分组取样器 210 和分析取样器 210 捕获的数据的分析器 220。取样器 210 包括网络处理器 212。正是网络处理器 212 位于因特网 14 中，使得能够在两个网络（AS 等）之间的链路 3 上从网络流中取样分组。网络处理器 212 位于两个 AS 的各自外部网关路由器（EGR）之间，以便它在它的连接点上接收通过因特网 14 发送的所有分组。网络处理器 212 被安排成至少读取所述分组的一些，以便导出至少与所述分组的源 IP 地址和所述分组的接收时间有关的数据。这个数据可以包括源和目的地端口、协议类型和分组大小。最好，网络处理器 212 能够以因特网主干线速率工作和被安排成读取所有这样的分组，以便获取源相关 IP 地址数据和接收时间。

取样器 210 包括诸如数据库之类的数据存储设施 214，用于存储累积源相关 IP 地址数据和分组接收时间。数据存储设施 214 通过专用链路 216 与网络处理器 212 连接，但是，在一些实施例中，数据存储设施 214 可以与网络处理器 212 处在一起，或可以远离网络处理器 212 和通过因特网连接与网络处理器 212 连接。

分析器 220 可以包括例如 Linux PC，Linux PC 通过诸如公共对象请求代理体系结构（CORBA）启用接口 222 之类的分布式处理环境（DPE）与取样器 210 的存储设施 214 通信，以便检索累积数据。但是，应该识别到，分析器 220 可以包括任何适用的计算设备，无需是 Linux 操作设备。CORBA 是计算机应用程序可以使用以便在网络上一起工作的销售商无关体系结构和基础设施标准。分析器 220 含有执行分析程序的处理单元 224，分析程序包括适合以如下所述的方式分析从存储设施 214 中检索的数据的程序代码。当处理单元 224 检测到 DDoS 攻击时，将构成事件消息的数据（DDoS 攻击数据）转发给接着向事件管理器 228 公布事件的事件散布器 226。至少一个事件管理器 228 含有在因特网 14 中的其它位置上与其它协作检测系统 200 交接，以便这样的系统 200 可以在它们各自的处理单元中利用事件数据的接口 230。至少一个事件管理器 228 含有重新配置带有适当过滤器的网络部件以阻止 DDoS 攻击分组的接口 232。事件散布器 226 和事件管理器 228 是基于软件的功能。重新配置网络部件（设备）的至少一个事件管理器 228 可能通过这样的设备支持的适当管理接口来完成这项工作。这个接口可以是诸如简单网络管理协议（SMNP）启用接口或 Cisco IOS 启用接口之类的任何适当管理接口。

与诸如因特网防火墙之类，根据随时间（以分钟的数量级）迅速变化的参数识别网络业务中的异常，以便检测 DDoS 攻击的侵入检测系统应用的现有方法相比，按照本发明第一主要方面的方法不是观看计算机的行为，而是观看人的行为，作为获取随应用的因特网技术的改变而保持不变和具有高概率地检测 DDoS 攻击的一般性质的适用参数的手段。基于人的行为的一个已知因特网不变量是昼夜行为，即，环球网中的业务模式'跟着太阳走'，使得在任何指定地理区（世界的某个区域）中，你可以预期在那个地理区中，在，比如说，下午 3 点产生的业务量比在，比如说，早晨 3 点产生的业务量大。由于历史原因，IANA IPv4 域命名空间的一些部分被留作供某些地理区使用。例如，在它们的 IP 地址中将八位位组"193"用作前八位位组的所有 IP 地址位于欧洲，而在位于美国的设备的 IP 地址中可以找到八位位组"199"，对于位于亚洲的设备是"61"。通过简单审查 IP 地址的重要部分可以识别发送主机的地理位置。

本发明的方法利用了这种 IP 寻址的全局特征。它包括如下步骤：在因特网 14 中诸如 AS 之类的两个主要网络的边缘路由器之间的点上观察分组流，

以便编译在具有指示它们各自的全局地理位置的IP源地址的各自数量的分组的第一规定（预定）时间段上的简档。第一规定时间段最好是24小时，因为这代表观察到的人与因特网14交互的一个完整周期。为此，网络处理器212被安排成在两个AS之间的链路3上读取观察网络分组流中的一部分分组，和在存储设施214中累积与读取分组的源IP地址和它们的接收（截获）时间有关的数据。这个累积数据保存在存储设施214中，直到分析器计算机220检索它为止。在一个优选实施例中，网络处理器212读取观察网络分组流上的所有分组。

为了提高网络处理器212捕获与读取分组的源IP地址和它们的接收时间有关的数据的效率，不记录精确的接收时间。取而代之，网络处理器212被安排成在第一规定时间段的整个持续时间内的一系列时间间隔中收集数据。因此，这个数据包括与读取分组的源IP地址有关的数据和与所述分组的读取相联系的时间间隔。各时间间隔总体可能构成整个所述规定时间段，或总体上可能构成一部分所述规定间隔。换句话说，第一规定时间段可以划分成数个相等的长度，相邻数据捕获时间间隔为，比方说，1分钟使24小时的规定时间段变成总共1440个数据捕获时间间隔，或者，可以在构成规定时间段的时间间隔中每隔n-1个时间间隔进行一次数据捕获，其中，n是大于1的整数。网络处理器212还捕获与读取分组的源IP地址和在下一个和随后规定时间段内进行读取的时间间隔有关的数据。下一个和随后规定时间段具有等于第一规定时间段，最好，24小时的持续时间，并且，最好被安排成具有相同数据捕获时间间隔模式。

将第一规定时间段当作假设没有发生涉及观察网络链路3的DDoS攻击的学习间隔。分析器220的处理单元224检索累积在存储设施214中的数据和处理它，以便获取与来自各自地理位置的分组的数量有关的参数。这些参数包括在第一规定时间段的各个时间间隔上来自各自地理位置的分组的数量相互之间的方差。这些参数允许作出这样的观察，当在下一个或随后规定时间段内的特定时间间隔或一系列相继时间间隔中观察到指定地理位置的分组的数量发生改变时，来自其它地理位置的分组的数量很有可能也发生改变。从这些观察中导出作为检测利用观察链路3的DDoS攻击的手段，将来概率判定可以基于此的阈值。

对于下一个规定时间段，分析器220的处理单元224从存储设施214中

检索累积数据和分析所述数据，以便将例如在所述规定时间段的各个时间间隔上来自各自地理位置的分组的数量相互之间的方差相互关联。对于所述下一个规定时间段的给定时间间隔或一系列相继时间间隔，将具有指示特指定地理位置的IP源地址的分组的数量的变化量与从与在训练间隔内在相应时间间隔或一系列时间间隔内观察的业务的数量有关的参数中导出的一个或多个阈值相比较。例如，假设具有指示亚洲的IP源地址的分组的数量在第n-1时间段和第n时间段之间增加了，比如说，10％，可以预期，具有指示欧洲的IP源地址的分组的数量在那个相同的时间段内将增加3-5％，而具有指示美国的IP源地址的分组的数量可能增加得非常少，比如说，1％。但是，DDoS攻击将使表面上从通过它们的IP源地址所指的指定地理区发出的分组的数量失真。因此，如果分组数量的变化量大于阈值，那么，处理单元24确定可能正在发生DDoS攻击和在观察链路3上正在发送分组。每个阈值可以包括给定时间间隔或一系列时间间隔内指定地理区的分组的数量与另一个地理区的分组的数量的比率。可替代地，每个阈值可以包括从一个时间间隔或一系列时间间隔到下一个来自指定地理区的分组的数量的方差与来自另一个地理区的业务的相似度量的比率。在测量三个地理区的业务量的情况下，为比较步骤生成两个阈值，可以使用这两个阈值之一或两者。

对于每个随后的规定时间段，重复这个过程。维持在训练间隔内建立的比率，并且，可以用在下一个规定时间段内获得的比率更新它。更新比率和因此从中导出阈值可以包括为各自时间间隔内的相应比率确定总值。比率和从中导出的阈值可以存储在处理单元的查用表中，查用表中的项目与时间间隔的序列相联系地排列着。虽然在优选实施例中，规定时间段被设置成24小时。但应该明白，所述规定时间段的持续时间可以包括其它持续时间，譬如，一个星期、一个公历月或甚至一年。

按照本发明的DDoS攻击检测方法使用了在因特网14中的两个主要网络之间的点上，在24小时的规定时间段内，具有指示各自全局地理位置的IP源地址的分组的数量的预期比率与那些比率的预期增量变化的组合。虽然只提供四分之一分配IP（源）地址来提供指示地理位置，但这个比例高到足以能够作出有用观察。鉴于此，对于DDoS攻击者来说，难以将攻击伪装成分配攻击源ID地址，无论是否假冒，都不可能轻易地与在监视网络层链路3上观察的模式相对应。例如，如果攻击者从整个可用IP地址范围中随机地将假

冒源地址分配给约定代理设备 44，那么，来自所有地理区的所有分组数量在一般说来相同的时间上等量地增加，在因特网用户的昼夜行为一定的情况下，这是异乎寻常的。即使攻击者企图使按假冒地址操作的代理设备 44 的数量随每天的时间而改变，以便模仿因特网用户昼夜行为，攻击者也无法知道在网络链路 3 上观察到的精确比率，因此，模仿的企图也无法把攻击伪装起来。

当确定正在发生利用观察链路 3 的 DDoS 攻击时，管理单元 224 将构成事件的数据消息发送给接着向数个事件管理器 228 公布事件的事件散布器 226。除了可能正在发生 DDoS 攻击的警告之外，事件消息可以包括与网络中可疑 DDoS 攻击的位置有关的信息、这个可疑 DDoS 攻击就是攻击的概率和用于计算所述概率的算法。至少一个事件管理器 228 含有与其它协同检测系统联系，警告它们检测 DDoS 攻击的接口 230。类似地，事件管理器 228 可以在这个接口上接收来自协同检测系统的事件消息。这样，协同检测系统可以共享有关在因特网 14 中的不同点上发生 DDoS 攻击的情报。接口 230 可以包括 CORBA 兼容接口。接口 230 也可以包括因特网连接。

分析器 220 的处理单元 224 可以被安排成考虑来自其它协同检测系统的有关发生 DDoS 攻击的情报，根据阈值比较修改判定，以便是否正在发生 DDoS 攻击的判定不是唯一地基于业务量变化参数与一个或多个阈值的比较，而是包括从现有知识中导出的概率函数。例如，如果事件管理器 228 接收到指示在附近网络中检测到 DDoS 攻击的事件消息，使应用于网络数量变化参数与一个或多个阈值的比较的概率函数的权重更大，以产生比没有接收到这样的事件消息时更肯定的结果。概率函数不仅可以考虑接收的事件消息的数量和在事件消息中标识的网络的接近度，而且考虑自从接收到这样的事件消息以来经过的时间。概率函数可以从 Bayes（贝叶斯）定理的应用中导出。处理单元 224 执行的比较步骤可以包括将不止一种的算法应用于业务量变化参数，以便对 DDoS 攻击的存在与否作出确定。这些算法可以包括将前文所述的许多不同阈值平行地应用于业务量变化参数、将概率函数应用于业务量变化参数和/或应用经过概率函数修改的阈值。组合将这些算法平行应用于业务量变化参数所得的结果，形成有关 DDoS 攻击检测的判定。

处理单元 224 可以被安排成响应检测系统 200 和协同系统检测的 DDoS 攻击的增殖变更网络处理器 212 的取样速率，从而使取样速率随检测到的攻击次数增加而增加或反之。但是，应该观察到，从网络处理器 212 到处理单

元 224 的通信是异步的，通信流量有利于处理单元 224。

至少一个事件管理器 228 含有将重新配置消息转发给其它网络部件，以便应用过滤器来阻止 DDoS 分组的接口 232。在描绘在图 6 中的检测系统的实施例中，可以看出，接口 232 与网络处理器 212 链接，网络处理器 212 可以包括为了滤出 DDoS 攻击分组通过事件管理器 228 重新配置的网络部件之一。这使事件管理器 228 能够更新由网络处理器 212 应用于接收分组的过滤规则。

检测系统 200 可以位于因特网 14 中便于取样诸如 AS 之类的两个主要网络之间的一个或多个分组流的任何方便的点上。将基于本发明的协同检测系统 200 安装在因特网 14 中的多个位置上使 DDoS 攻击得到协调检测。需要应用于因特网 14 的检测系统 200 的数量不需要像最初看起来那么多。当前，全局因特网包括大约 10,000 个 AS。由于 AS 与其它 AS 的连接的数量遵从负幂函数规律，利用基于本发明的检测设备 200 监视少数高额相连 AS 的连接，可以达到良好的因特网 14 的覆盖。

在确定了正在发生攻击之后，检测系统 200 可以开始阻止指定到目标设备 50 的所有分组。尽管这只阻止了包括合法分组和攻击分组两者的穿过链路 3 指定到目标设备 50 的分组，但它有助于通过目标设备 50 本身实现的阻断努力，而不会干扰合法（或攻击）分组穿越其它路径。但是，在许多基于本发明的协同检测系统对目标设备 50 实现分组阻断的情况下，这足以防止指定到目标设备 50 的其它攻击分组使它的因特网连接饱和或击垮它的处理能力。因此，基于本发明的协同检测系统 200 起分布式分组过滤系统的作用，以减轻对目标设备 50 的攻击造成的影响。检测系统 200 可以利用存储在存储设施 214 或处理单元 224 中的以前获得源 IP 地址度量，对 DDoS 攻击的检测作出更智能的响应，实现分组过滤以阻止源 IP 地址在链路 3 上很少见的分组。

基于本发明的协同检测系统 200 可以通过 ISP 实现成对客户的税收生成服务。该服务可以包括监视到客户网端的业务和根据任何已知过滤方法或基于本发明第二主要方面的方法帮助客户阻止攻击业务。

基于本发明第二主要方面的方法认识到最关注阻止 DDoS 攻击的因特网相连实体是后面有存在酬劳关系的 ISP 的目标设备、系统或网络本身。其它因特网实体几乎没有什么动机来帮助目标实体阻止 DDoS 攻击，除非存在为此获得的利益。基于本发明第二主要方面的方法不仅提供了 DDoS 目标 50 防

御DDoS攻击的更智能方法，而且被设计成具有发送主机10和中间节点也实现这种方法的优点。

下面特别参照图7到9和一般参照图1到6描述基于本发明第二主要方面的方法。当发送主机10想要开始在服务（服务质量，QoS）不止一个的基本或未经验证级别上将分组发送到接收端主机12的数据传输联系例如连接1-5时，应用为了易于描述这里称为"分组A"的分组，以及为从连接1-5上分组A遇到的路由器18、24、30、20中收集证件配备的附加首标部分300（图7）。如图7所示的首标部分300包括代码字段310，代码字段310可以被设置成向处理分组A的路由器指示通过那个路由器将数据（证件）提供给首标部分300。首标部分300可以可选地包括长度字段320，长度字段320指示首标部分300用八位位组（字节）表示的实际和/或总许可长度。包括在首标部分300中的还有指向数据部分340的下一个未填充数据字段340_{N-X}的指针字段330。指针字段330指向从下一个路由器将它的证件插入的、下一个数据字段340_{N-X}开始的八位位组。除了这种字段方式操作之外，也可以进行信息的算术编码，这不需要"下一个"指针。

在分组A遇到的每个路由器上，路由器将路由器在沿着同一路径（连接1-5）的随后分组中必须看到使它能够赋予这样的分组以更高服务级别的、下文称为"令牌"的值插入指针字段330所指的下一个自由数据字段340_{N-X}（图）中。在接收主机12上，首标部分300的数据字段$340_{1到N}$从而包括连接1-5上分组A遇到的路由器1到N依次插入的N个令牌串。从路由器中收集令牌数据可以通过修正IPv4或IPv6"记录路线"选项实现。IP网络中的记录路线选项通过使用指针字段和数字空间（数据字段）收集路径中的路由器的IP地址。

除了令牌之外，每个路由器可以可选地将它的IP地址插入下一个自由数据字段340_{N-X}中，作为相互参考所述令牌的手段，以便能够在那个路由器上对沿着同一路径的随后分组作出该令牌的确是那个路由器插入的令牌，而不是偶尔具有相同值的其它路由器插入的令牌的确定。实际上，这个值不是必不可少的，因为可以通过分组首标中其它地方的TTL（或IPv6跳段计数）字段来索引，由于可以利用索引操作直接访问字段，而不是必须搜索插入令牌的列表，使首标部分300更加紧凑，并且还使处理速度加快。这还使得不需要字段300。但是，在优选实施例中，路由器将第二非地址相关值插入数据字段340_{N-X}中，作为相互参考的方式，其中，所述第二值与一系列路由器中

连接 1-5 上分组遇到的路由器的位置有关。第二值可以包括 TTL（存活时间或路径距离）值，因为 IPv4 首标中的这个字段被每个路由器一个接一个地递减，因此，与路由器相对于接收主机 12 的位置有关。因此，在随后分组在因特网 14 上沿着同一条路径的情况下，在每个路由器上看到的 TTL 值在那个路由器上对于每个这样的分组将是相同的，因此，可以假设插入的令牌对应于插入它们的路由器。但是，在这样的分组沿着不同路径的情况下，就像路由器和插入令牌之间的对应关系那样，TTL 值和连接 1-5 的路由器之间的对应关系也丧失了。

接收主机 12 一旦接收到分组 A 或预定个这样的分组，就将一个消息返回给发送主机 10，使它识别将插入寻址到接收主机 12 的随后分组中的令牌串，作为使连接 1-5 中的路由器能够赋予沿着同一条路径的随后分组以更高服务级别的手段。该消息可以包括按在接收主机 10 上接收的顺序的令牌串和被发送主机 10 插入每个随后分组的第二附加首标部分 400（图 9a）中。可替代地，该消息可以包括被发送主机 10 插入每一个随后分组的第二附加首标部分 400 中的按它们的 TTL 值索引的令牌的阵列（图 9b）。第二附加首标部分 400 可以包括代码字段 410，代码字段 410 当被设置时，向随后分组遇到的路由器指示一旦令牌数据集中的下一个令牌得到核实，就在更高服务级别上处理分组。不愿赋予发送器 10 以更加优先级的接收主机 12 可以不返回任何信息或虚假信息，这两者都将导致处理质量下降。

令牌数据收集分组（本文称为“分组 A”）应该具有防止发送主机 10 没有通过接收主机 12 完成反馈循环偶然学习所述分组收集的一些或所有令牌数据的形式。例如，在令牌数据收集分组使连接 1-5 中的中间路由器发送错误消息的情况下，可以使令牌数据过早地返回到发送主机 10。在因特网中，因特网控制消息协议（ICMP）使错误消息发送到包含许多原始消息的发送主机 10。接收这样包含大多数或所有令牌数据的错误消息可以使恶意发送主机能够确定获取提高 QoS 所需的令牌数据，这将使本发明的意图受挫。

上面的问题可以通过对令牌数据收集分组施加某些限制来解决。例如，可以使收集分组的最初 TTL/跳段计数更高，比如说，对于这个字段来说是最大值的 255，以免在中间路由器上生成 ICMP“超过 TTL/跳段计数”分组。或者，可以使它的消息大小低于最少链路最大发送单元（MTU）大小，以免发出 ICMP“碎片化所需”分组。一种可替代的方法是在收集分组结束时收集令牌数

据，以便当原始分组的主要部分作为 ICMP 分组的一部分被回送到发送器时，切除这样的分组。进一步的可替代方法是使收集分组成为 ICMP 分组本身，从而防止它起动错误回答分组。

一旦接收到沿着同一条路径的随后分组，连接 1-5 中的每个路由器都在第二附加首标 400 中识别令牌数据的存在，并且对通过它的 TTL 值索引的令牌进行核实测试。如果核实结果是真的，那么，给予分组以更高服务级别。服务级别可以是两个级别之一，即，基本的或提高的。在核实步骤是假的情况下，尽管提高质量级别指示符包含在分组首标中，也只给予分组以基本服务级别。此外，可以将路由器在首标中检测到虚假声明的事实通知下游路由器。

在正如在 DDoS 攻击期间可能发生的那样，连接 1-5 发生阻塞的情况下，一旦在路径上发送具有提高服务级别的分组，不发送或只发送指示基本服务级别的分组和使核实测试失败的那些分组。

除了已经描述过的两个服务级别之外，可以按照在基本级别之上的数个逐步提升质量级别在路径上发送分组。对于在发送主机 10 和接收主机 12 之间沿着同一条路径的随后分组，这样分组的所需服务质量级别的指示符包括在传送令牌数据集的来自接收主机 12 的消息中。在发送主机 10 上在所述消息中接收的服务质量指示符值由发送主机 10 插入每个随后分组的 QoS 字段中。因此，连接 1-5 中的每个路由器一旦核实它的 TTL 值所指示的令牌是真的，就给予那个分组以它的 QoS 值所指示的服务级别。在核实测试导致假匹配的情况下，将那个分组的 QoS 值降低到较低的级别，甚至基本级别。这甚至可应用于只存在两个级别的情况。

对于沿着同一条连接 1-5 的随后分组，通过 TTL 值索引的令牌串或令牌的阵列总是映射到将所述令牌提供给接收主机 12 的路由器，而来自其它发送主机的分组，或来自相同发送主机 10，但沿着其它路径通过一些所述路由器的分组在整个路径上对应关系不成立。因此，在每个路由器上，对令牌的核实测试可以简单地包括确定字符串或阵列中相关位置上的令牌是否具有与由那个路由器存储的秘密值相同的值。这是根据核实测试在计算上简单的形式。在从，比如说，v 个值的空间中选择令牌和路由器（节点）是连接 1-5 中的允许节点号 k，即，在它之前存在 k-1 个允许节点的情况下，源（例如，代理设备 44）能够虚假地声明在那个节点上具有更高服务级别的概率由如下函数的

值确定：概率 = v^k。例如，在路由器个数等于 6 和令牌包括单位值，即，“1”或“0”的情况下，源只能虚假地获得每 64 个分组中 1 个的提高服务。当今的典型路径穿过大约 20 个路由器。如果这些路由器的每一个都启用这种系统，虚假地获得提高服务的概率是每 2^20 个中 1 个 = 1048576 中 1 个，从而使攻击失效。所需的存储器只是 20 个位或 2.5 个字节（没有计及可能包括指针等的固定首标大小）。

在核实测试包括简单比较令牌的值和由路由器存储的秘密值的情况下，存在代理设备 44 通过试错法可以容易地学习或容易地猜测路由器存储的秘密值的缺点。因此，在优选实施例中，核实测试包括结合其源 IP 地址和其目的地 IP 地址对与分组相联系的令牌进行的计算。在核实测试的这种实现中，仍然只需要在每个路由器上存储单个全局秘密值。尽管这不需要繁重的计算，但计算的结果应该不容易猜测，因此，密码函数是首选。对令牌和 IP 地址进行计算的适当函数包括如下：

令牌值 = H（源地址，目的地地址，秘密值），

其中，H（）是散列函数；和

令牌值 = E_{秘密值}*（源地址，目的地地址），

其中，E_{密钥}是加密函数。

作为将接收主机 12 提供的令牌数据集（字串数据或阵列数据）插入每个随后分组的第二附加首标部分 400 中的可替代方法，发送主机 10 可以改为将这个数据插入第一附加首标部分 300 中，从而，不需要包括第二附加首标部分 400。令牌数据集被发送主机 10 插入第一附加首标部分 300 的相应数据字段 $340_{1\text{到}N}$ 中，并且，还将代码字段 310 设置成向路由器指示它们不将数据写入首标部分 300 的数据部分 340 中，而是读取那个字段中的数据供对包含在其中的令牌进行核实测试用的值。指针字段 330 也可以被两个新代码字段值禁用。第一附加首标部分 300 还可以包括发送主机 10 可以将从接收主机 12 接收的 QoS 指示符值插入的 QoS 字段 325（图 7）。

在繁重业务和/或 DDoS 攻击在路径 1-5 上引起阻塞的状况下，来自由接收主机 12 已经赋予更高服务级别的发送主机 10 的分组比来自其它发送主机，

无论是合法源还是攻击源的分组得到更有利对待。来自这些源的分组默认为基本服务级别，并且，即使攻击源企图虚假地要求具有更高服务级别，它的分组基本上通不过路由器实现的核实测试，因此，也得到较不利对待。因此，本发明的方法提供了减轻 DDoS 攻击对目标 50 的影响的分布式措施，因为在因特网 44 中的许多节点上和在远离目标 50 和与攻击源接近的位置上作出对攻击分组实现基本服务级别或对所述分组降低虚假声明的服务级别的判定。停止或减缓离目标 50 越远的攻击，对与目标 50 越接近的其它链路和节点的影响就越小。

基于本发明第二主要方面的方法是在包括发送主机 10、接收主机 12 和路径 1-5 中的任何中间节点（路由器）的连接节点的每一个上，按照由所述节点的分组处理单元执行的软件，通过 ISP 16，22 和 NSP 24，30 实现的。这样，实现该方法的软件与现有因特网软件和基础设施完全向后兼容。但是，不实现该方法的那些发送主机的分组具有它们被路径 1-5 中的路由器降级了的或甚至降到基本级别的服务级别，因此，在繁重业务和/或 DDoS 攻击下受到严重影响。因此，那些发送主机，以及中间节点，尤其 ISP 的关注在于实现该方法，以便不处于不利地位。因此，基于本发明第二主要方面的方法为发送主机和中间节点创建动机，将它们的软件更新成包括实现前述方法的软件，以免从 QoS 的视角来看变成低级节点。

就额外装载而言，目标 50 上的 DDoS 负载对于它的 ISP 22 很少成问题。ISP 通常拥有一组各色各样输入路由。通过至少在目标 ISP 22 的路由器中部署基于本发明第二主要方面的方法，为 DDoS 攻击的分组泛滥效应的显著减小创造条件，而不会加重 ISP 22 或它的其它客户机（DDoS 攻击的未来可能目标）的负担。如上所述，阻止或减缓离目标 50 越远的 DDoS 攻击，对目标 50 和其它系统链路和节点的影响就越小。因此，该方法适合于通过分散远离目标 50 的 DDoS 攻击的防御支持接收主机 12。

该方法的缺点是用于实现该方法的分组大小增加了，但是，当通过基于本发明第一主要方面的方法检测 DDoS 攻击时，这可以利用基于本发明这个方面的方法来解决。检测系统 200 的事件管理器 228 被安排成将包括目标 50 的网络节点重新配置成当通过协同检测系统 200 的任何一个检测 DDoS 攻击时，实现基于本发明第二主要方面的方法。

基于本发明第二主要方面的方法可以修改成提高它的可应用性和能够在

来自最近与接收主机 12 通信的发送主机 10 的分组和来自在某个时间段内没有与接收主机 12 通信的发送主机的那些分组之间应用鉴别度。如图 10 到 12 所示，当发送主机 10 想要开始与接收主机 12 连接时，它像前面那样将分组 A 发送到接收主机 12，以提供来自连接 5 上分组 A 遇到的路由器的证件。在分组 A 遇到的每个路由器上，路由器将短期令牌（T_{ST}）值和长期令牌（T_{LT}）值插入如附加首标部分 500 的指针字段 530 所指示的下一个自由数据字段 540_{N-X} 中。短期令牌与可以由路由器每几个小时改变一次和由路由器存储的第一秘密值相联系，和长期令牌与可以几天或甚至更长时间之后改变的第二秘密值相联系。路由器必须至少了解随后分组中的令牌之一或两者，以便使路由器能够将一些更高服务级别提供给这样的分组。

如图 12 所示，来自分组 A 的在接收主机 12 上接收的令牌数据集包括通过各自 TTL 值索引的短期令牌和长期令牌的阵列。这个数据集被发送到发送主机 10，发送主机 10 将它插入寻址到接收主机 12 的每个随后分组的第二附加首标 600 中。可替代地，可以在代码字段 510 据此设置的每个分组的第一附加首标部分 500 中携带令牌数据集。

如上所述，路径 1-5 上的每个路由器访问包含在第二附加首标 600 中的令牌数据集，和对短期令牌 T_{ST} 和长期令牌 T_{LT} 的至少一个进行核实测试。在优选实施例中，路由器与第一秘密值相联系地对短期令牌进行核实测试，并且，如果取得成功，给予分组以那个分组的 QoS 值所指示的服务级别。在这个第一核实测试非真的情况下，路由器与存储在那个路由器中的第二秘密值相联系地对长期令牌进行核实测试，并且，如果这个测试取得成功，给予分组以比基本级别更高的服务级别。在后一种情况下，路由器可以被安排成降低分组的 QoS 值所指示的服务级别，作为更有利对待在短期令牌有效的间隔内最后与接收主机通信的发送主机 10 发出的分组的手段。在两个核实测试都非真的情况下，分组接受降低了的服务级别或甚至基本服务级别。

短期令牌和长期令牌的使用使路由器特别优待最近与接收主机通信的发送主机，但仍然能使在某个时间内没有与接收主机通信的发送主机声明在基本服务级别之上的服务级别。在该方法的进一步改进中，路由器可以存储一系列过去短期秘密值和/或过去长期秘密值，和一旦开始发送主机和接收主机之间的新连接，就将与所述旧秘密值相联系的一系列令牌值分配给分组 A。接收主机将包括每个路由器发放的这种令牌的列表的令牌数据集发送给发送

主机，以便像前面那样将其插入随后分组中。在每个路由器上处理寻址到接收主机的随后分组，以对照当前短期令牌值进行核实，以便找出真结果。一旦失败，对与过去短期秘密值相联系的任何短期令牌的每一个进行核实测试，然后，对与过去长期秘密值相联系的任何令牌进行核实测试，以便找出真结果。这个过程一直持续到获得真结果或所有测试都以失败告终为止。任何核实测试的成功都验证了比所有核实测试都失败的分组得到更有利对待的分组，但根据为了获得真结果而要求令牌的列表往下到什么程度，降低适用于已验证分组的服务级别。

在该方法的进一步改进中，一旦开始发送主机和接收主机之间的新连接，每个路由器就将与各自秘密值相联系的一系列令牌值分配给分组 A，各自秘密值又与各自 QoS 级别相联系。这使接收主机能够从接收主机中为随后分组选择服务级别。因此，接收主机向发送主机发送包括从路由器提供的数组令牌中选择的令牌值的令牌数据集，其中，所述所选令牌值在每种情况下对应于接收主机为那个发送主机选择的 QoS 级别。QoS 级别值也作为令牌数据集的一部分传送到发送主机，以便插入寻址到接收主机的随后分组中。

在从值空间 v 中选择令牌，每个秘密值具有历史长度 h，和存在 q 个 QoS 级别的情况下，由其源利用随机值分配的分组与给定 QoS 级别匹配的概率由如下关系定义：如果对所有 QoS 级别加以比较，概率 = $1-(1/v)^{hq}$。然而，如果只对当前 QoS 级别加以比较，关系调整为：概率 = $1-(1/v)^{h}$。因此，对于具有 k 个跳段（进行核实测试的节点）的路径，在所有 k 个节点上分组虚假记录真结果的概率由如下关系给出：概率 = $1-(s)^{k}$，其中，$s = 1-(1/v)^{h}$。

在该方法的进一步改进中，路由器的每一个被安排成一旦在那个路由器上出现第一核实测试假结果，不马上降级分组。该路由器可以包括一旦出现假结果就递增 1 的核实测试结果计数器。当这个计数器达到预定阈值时，开始执行降低记录假结果的分组的步骤。这种改进使该方法更能抵抗单跳段路径改变或使路由器在业务正在流动的同时改变它的秘密值。

在另一个实施例中，每个路由器可能具有三个可能值 v，即，0、1 和 2，存储在它的“个人字段”中。取代将 2 个位分配给每个“个人字段”，第 i 路由器将整个“存储字段（storage field）”330 当作一个数字，然后，通过将 $v^{*}(3\hat{}i)$ 加入“存储字段”中插入它的值。当执行比较步骤时，将 v 与 INTEGER("storage field"/3^i)MOD 3 比较。

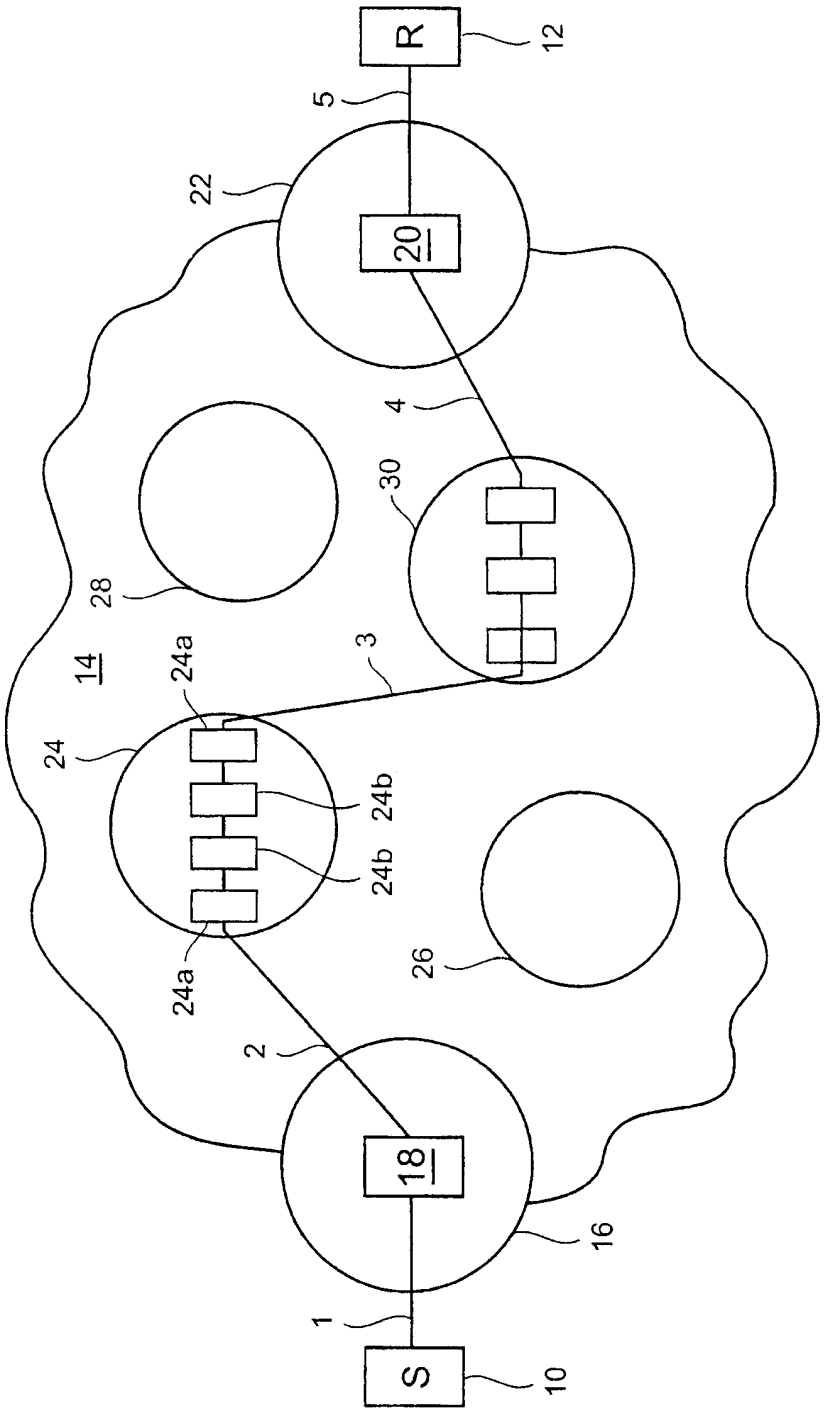


图 1

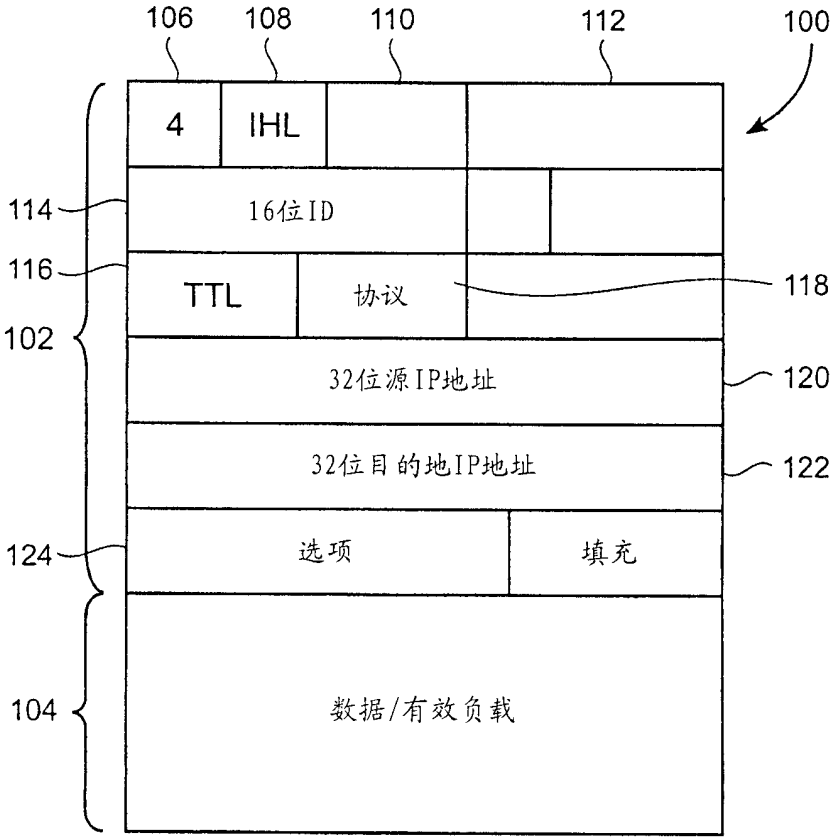

106
108
110
112
100
4
IHL
114
16位ID
116
TTL
协议
118
102
32位源IP地址
120
32位目的地IP地址
122
124
选项
填充
104
数据/有效负载

图 2

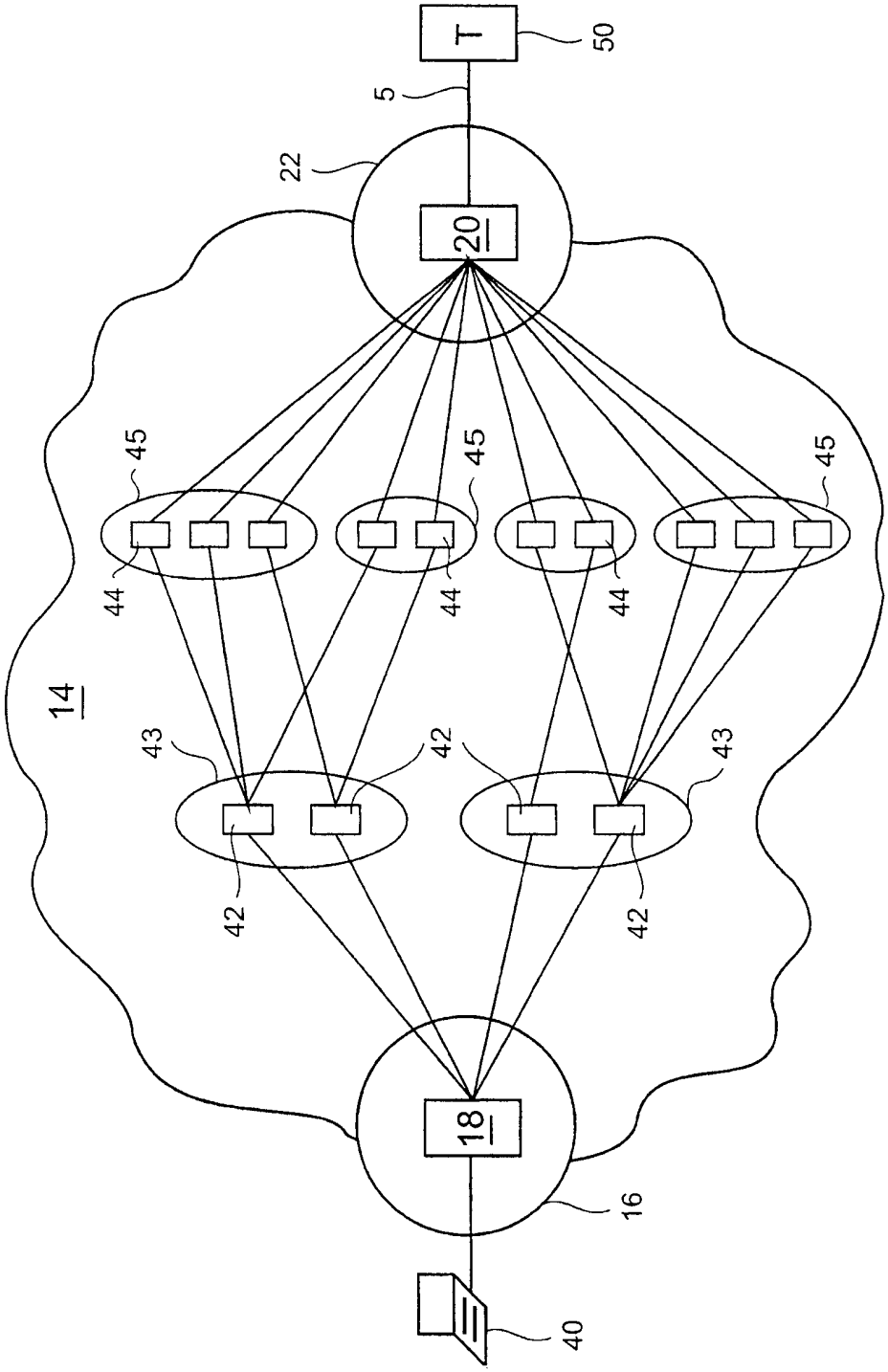


图 3

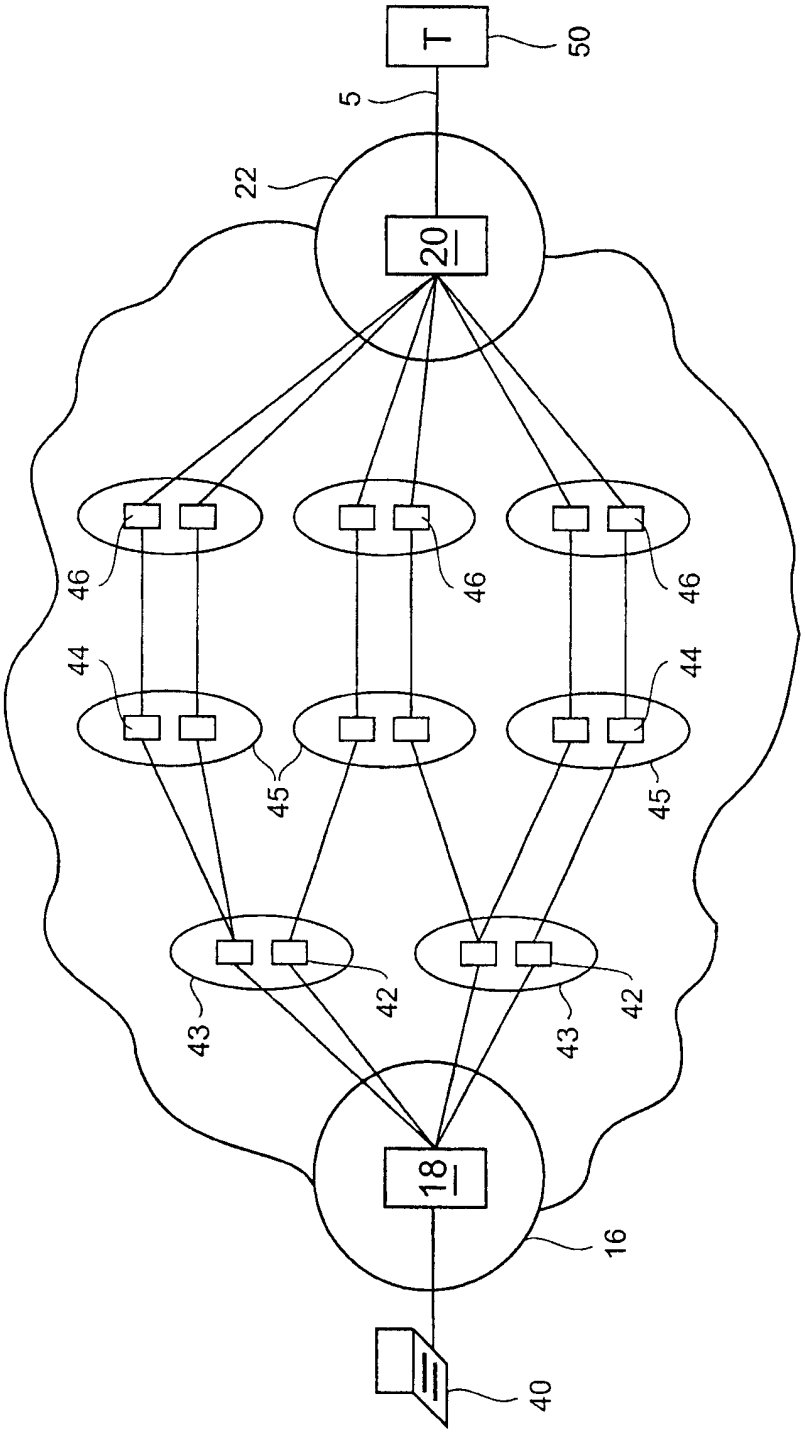


图 4

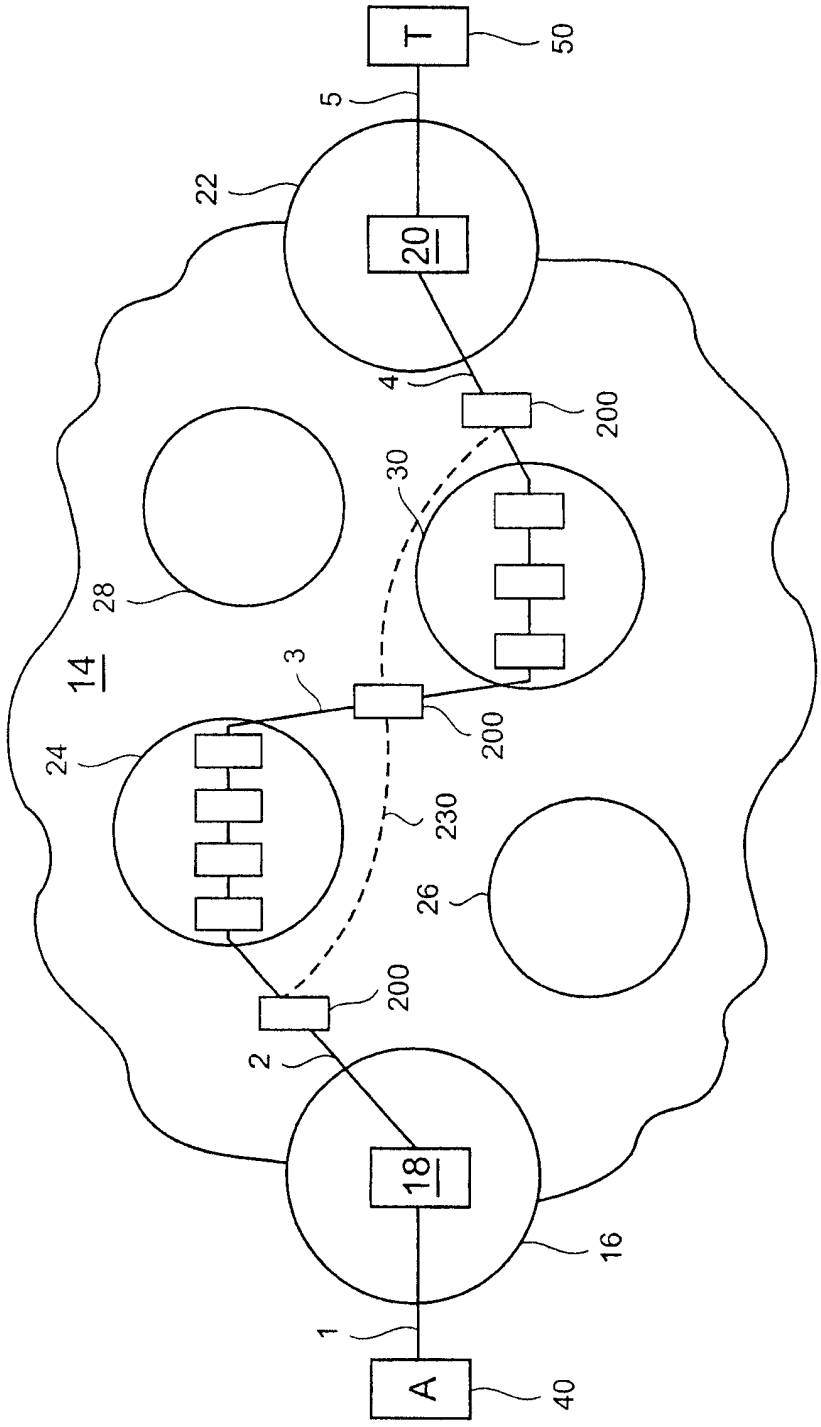


图 5

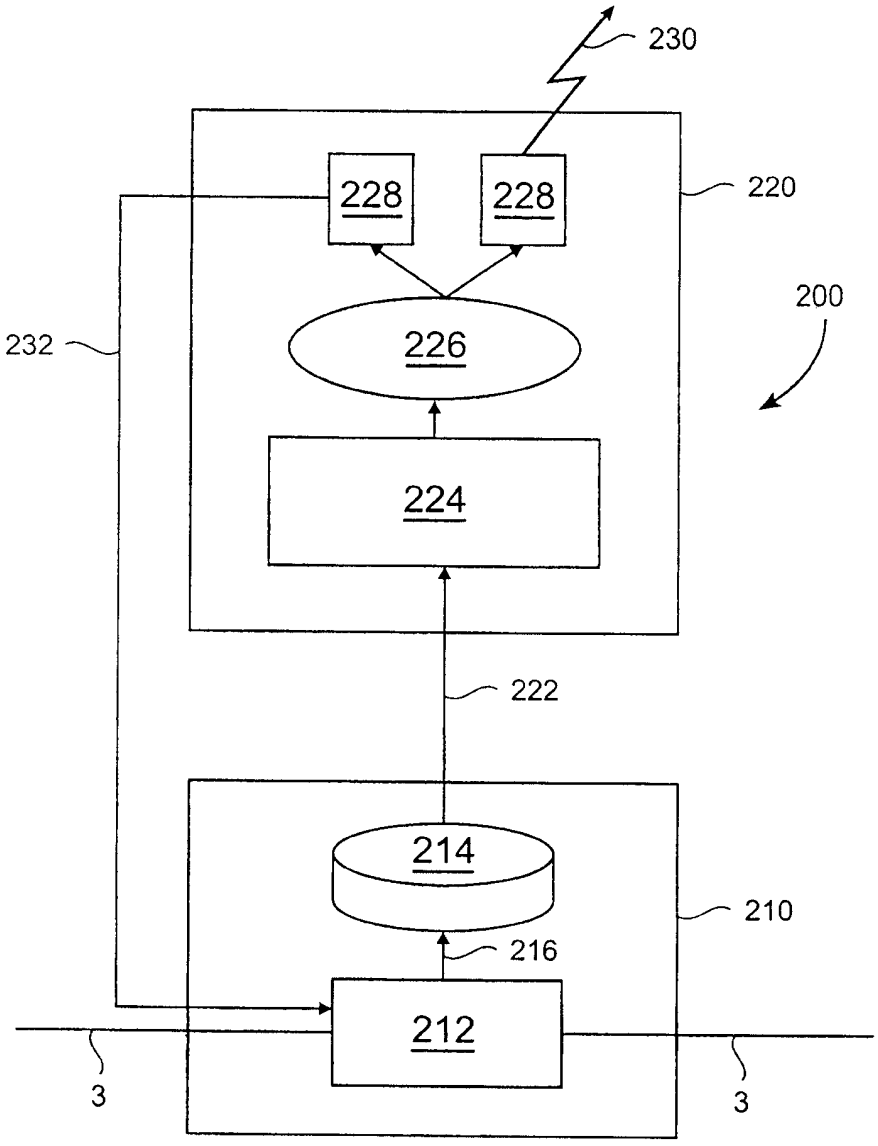


图 6

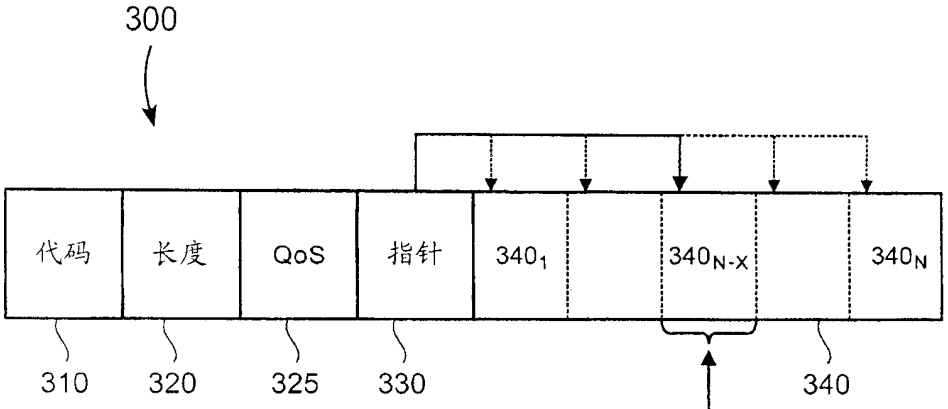

300
代码
长度
QoS
指针
340_1
340_{N-X}
340_N
310
320
325
330
340

图 7

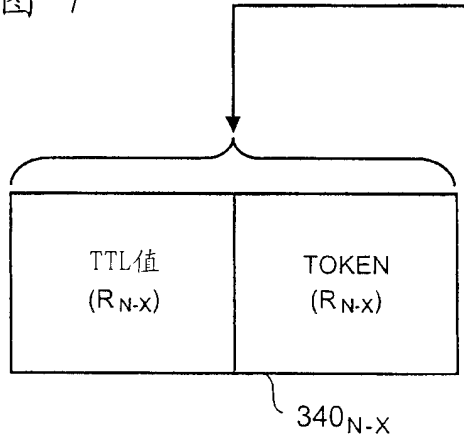

TTL值
(R_{N-X})
TOKEN
(R_{N-X})
340_{N-X}

图 8

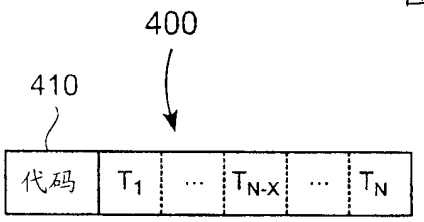

400
410
代码
T_1
...
T_{N-X}
...
T_N

图 9a

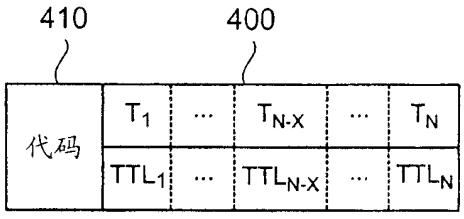

410
400
代码
T_1
...
T_{N-X}
...
T_N
TTL_1
...
TTL_{N-X}
...
TTL_N

图 9b

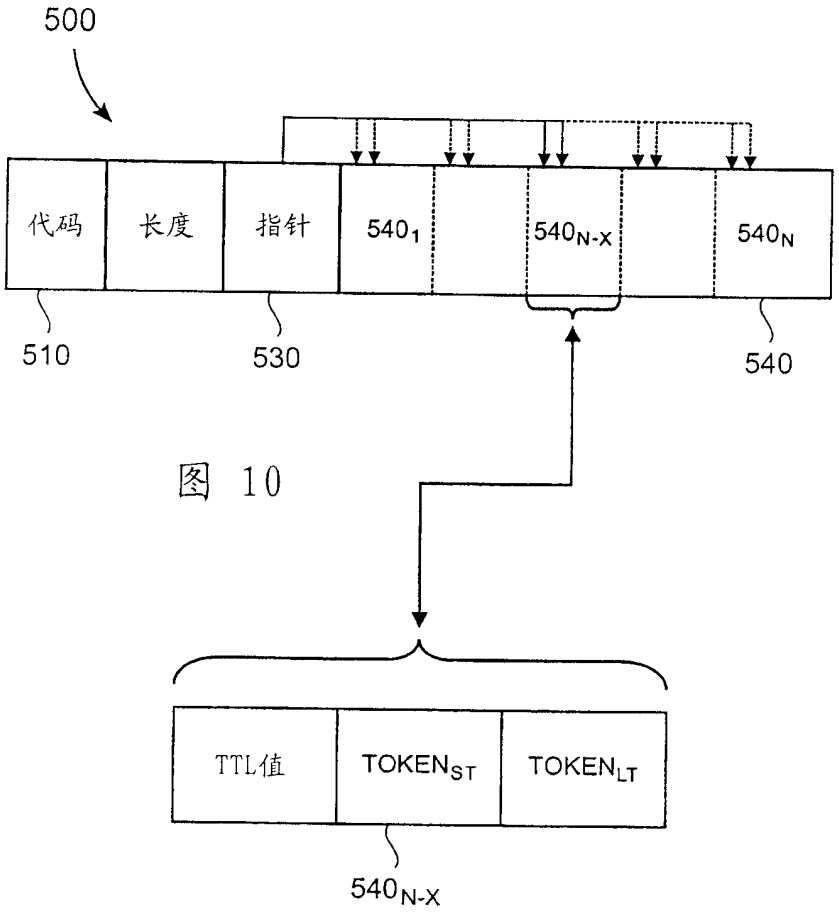

500
代码
长度
指针
540_1
540_{N-X}
540_N
510
530
540
TTL值
$TOKEN_{ST}$
$TOKEN_{LT}$
540_{N-X}

图 10

图 11

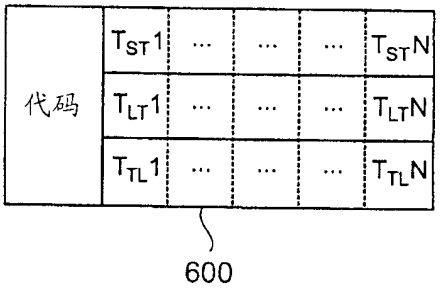

代码
$T_{ST}1$
$T_{ST}N$
$T_{LT}1$
$T_{LT}N$
$T_{TL}1$
$T_{TL}N$
600

图 12