(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 104247367 B
(45)授权公告日 2017.08.04

(21)申请号 201380015156.0

(22)申请日 2013.03.28

(65)同一申请的已公布的文献号
申请公布号 CN 104247367 A

(43)申请公布日 2014.12.24

(30)优先权数据
61/618,359 2012.03.30 US

(85)PCT国际申请进入国家阶段日
2014.09.19

(86)PCT国际申请的申请数据
PCT/US2013/034415 2013.03.28

(87)PCT国际申请的公布数据
WO2013/149041 EN 2013.10.03

(73)专利权人 华为技术有限公司
地址 518129 广东省深圳市龙岗区坂田华为总部办公楼

(72)发明人 宋继飞 易晓勇 张向阳

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
US 2002097724 A1,2002.07.25,
US 2010169446 A1,2010.07.01,
US 2010088288 A1,2010.04.08,

审查员 孙凯

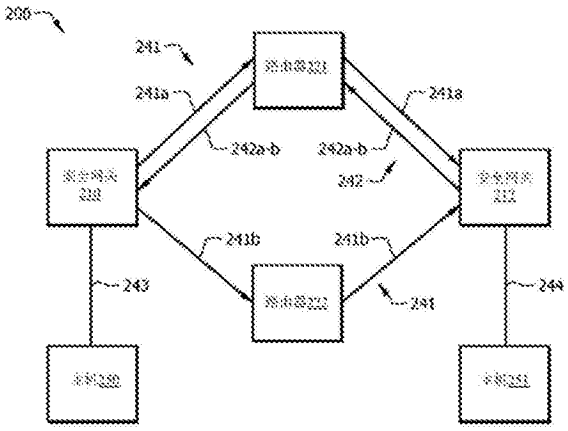
权利要求书2页 说明书9页 附图4页

(54)发明名称

提升IPsec性能和防窃听安全性

(57)摘要

一种网元(NE),包括:所述网元(NE)包括:存储器设备,用于存储指令;处理器,用于通过将数据流的第一多个数据包划分为第一多个子流,并使所述第一多个子流经由网络传输至第二NE来执行指令,其中所述第一多个子流使用包括多个并行子SA的第一因特网协议安全协议(IPsec)安全联盟(SA)集群进行传输。本发明还包括一种网元(NE),包括处理器,用于使用因特网密钥交换协议(IKE)或IKE版本2(IKEv2)在所述NE和第二NE之间创建包括第一多个子SA的IPsec SA集群,其中所述第一子SA是单向的,以及所述第一子SA用于在同一方向传输第一多个数据包。



CN 104247367 B

1.一种网元(NE),其特征在于,包括:

存储器设备,用于存储指令;以及

处理器,用于通过如下方式执行所述指令:

将数据流的第一多个数据包划分为第一多个子流;以及

使所述第一多个子流经由网络传输至第二NE,

其中所述第一多个子流使用包括多个并行子SA的第一因特网协议安全协议(IPsec)安全联盟(SA)集群进行传输,所述多个并行子SA中的每个子SA针对所述第一多个子流中的每个子流独立建立。

2.根据权利要求1所述的NE,其特征在于,所述多个并行子SA中的第一子SA与第二子SA经过不同的网络路径。

3.根据权利要求1所述的NE,其特征在于,所述多个并行子SA中的第一子SA与第二子SA经过相同的网络路径。

4.根据权利要求1所述的NE,其特征在于,所述子SA不是嵌套的。

5.根据权利要求1所述的NE,其特征在于,所述数据流的所述数据包通过使用选择算法在所述第一多个子SA之间分发。

6.根据权利要求5所述的NE,其特征在于,所述选择算法包括轮询选择算法、随机选择算法或其组合。

7.根据权利要求1所述的NE,其特征在于,所述多个子SA中的每个包括安全参数指标(SPI),以及所述每个子SA SPI包括不同于其他每个子SA SPI的值。

8.根据权利要求1所述的NE,其特征在于,所述处理器进一步用于经由第二IPsec SA集群接收来自所述第二NE的第二多个子流。

9.根据权利要求8所述的NE,其特征在于,所述第二多个子流包括第二多个数据包,以及所述处理器进一步用于通过使用防重放位图在所述第二多个数据包上执行防重放功能来执行所述指令。

10.根据权利要求1所述的NE,其特征在于,所述第一多个数据包每个都包括序列号,以及所述序列号基于与数据包相关联的所述子流确定,而非基于所述数据流确定。

11.一种网元(NE),其特征在于,包括:

处理器,用于使用因特网密钥交换协议(IKE)或IKE版本2(IKEv2)在所述NE和第二NE之间创建包括第一多个并行子SA的因特网协议安全协议(IPsec)安全联盟(SA)集群,

其中所述第一多个并行子SA是单向的,以及

所述第一多个并行子SA用于在同一方向传输第一多个数据包,

所述第一多个并行子SA中的每个子SA针对与所述第一多个数据包相关联的多个子流中的一个子流独立建立。

12.根据权利要求11所述的NE,其特征在于,所述处理器进一步用于在通信会话期间经由网络使用所述第一多个并行子SA将所述第一多个数据包传输到所述第二NE。

13.根据权利要求12所述的NE,其特征在于,所述处理器进一步用于在所述通信会话期间经由所述网络接收来自所述第二NE的第二多个数据包,以及所述第二多个数据包经由包括第二多个并行子SA的第二IPsec SA集群接收。

14.根据权利要求13所述的NE,其特征在于,所述第二多个并行子SA是单向的,所述第

二多个并行子SA用于在公共方向传输数据包，以及所述第二多个并行子SA用于在与所述第一多个并行子SA相反的方向传输数据包。

15.根据权利要求13所述的NE，其特征在于，在数据库中对所述第一多个并行子SA的查找并行执行，所述第一多个数据包的序列号并行生成，所述第二多个数据包的防重放检查并行执行，或其组合。

16.根据权利要求11所述的NE，其特征在于，所述处理器进一步用于通过处理saCount属性创建所述SA集群，以及与所述saCount属性相关联的值指示所述SA集群中第一多个并行子SA的数目。

17.根据权利要求11所述的NE，其特征在于，所述处理器进一步用于通过处理selectSA属性创建所述SA集群，以及与所述selectSA属性相关联的值指示用于选择传输与所述第一多个数据包相关联的子流的子SA的选择算法。

18.一种通信方法，其特征在于，包括：

将数据流的第一多个数据包划分为第一多个子流；以及

使所述第一多个子流经由网络传输至第二NE，

其中所述第一多个子流使用包括多个并行子SA的第一因特网协议安全协议(IPsec)安全联盟(SA)集群进行传输，所述多个并行子SA中的每个子SA针对所述第一多个子流中的每个子流独立建立。

19.根据权利要求18所述的方法，其特征在于，所述多个并行子SA中的第一子SA与第二子SA经过不同的网络路径。

20.根据权利要求18所述的方法，其特征在于，所述多个并行子SA中的第一子SA与第二子SA经过相同的网络路径。

21.根据权利要求18所述的方法，其特征在于，所述子SA不是嵌套的。

22.根据权利要求18所述的方法，其特征在于，所述数据流的所述数据包通过使用选择算法在所述第一多个子SA之间分发。

23.根据权利要求22所述的方法，其特征在于，所述选择算法包括轮询选择算法、随机选择算法或其组合。

24.根据权利要求18所述的方法，其特征在于，所述多个子SA中的每个包括安全参数指标(SPI)，以及所述每个子SA SPI包括不同于其他每个子SA SPI的值。

25.根据权利要求18所述的方法，其特征在于，所述方法还包括经由第二IPsec SA集群接收来自所述第二NE的第二多个子流。

26.根据权利要求25所述的方法，其特征在于，所述第二多个子流包括第二多个数据包，以及所述方法还包括通过使用防重放位图在所述第二多个数据包上执行防重放功能。

27.根据权利要求18所述的方法，其特征在于，所述第一多个数据包每个都包括序列号，以及所述序列号基于与数据包相关联的所述子流确定，而非基于所述数据流确定。

提升IPsec性能和防窃听安全性

[0001] 相关申请案的交叉参考

[0002] 本发明要求2012年3月30日由张向阳等人递交的发明名称为“多路径IP层安全”的第61/618359号美国临时专利申请案的在先申请优先权，其以引用方式并入本文本中，如全文再现一般。

[0003] 关于由联邦政府赞助的

[0004] 研究或开发的声明

[0005] 不适用。

[0006] 缩微平片附件的引用

[0007] 不适用。

背景技术

[0008] 可要求联网设备跨多个网络进行通信。某些设备可能要求这类通信保持安全。经由安全网络互连的设备可依赖该安全网络中固有的安全措施来为任意跨网络通信提供这种安全。还可要求这些设备跨不安全的网络进行通信。例如，一台主机可经由互联网和另一主机、客户端、网络等通信，这可能是部分、不均衡和/或完全不安全的。通信可仅如提供给发送方和接收方之间任意点通信的最低安全级别那样安全。网络设备可采用各种安全协议来维持通过不安全网络的通信的安全性。例如，源网络设备可与目标网络设备协商安全连接和/或通信，只要这两个网络设备都配置为采用相同的安全协议(一个或多个)。

发明内容

[0009] 在一项实施例中，本发明包括一种网元(NE)，包括：存储器设备，用于存储指令；处理器，用于通过将数据流的第一多个数据包划分为第一多个子流，并使所述第一多个子流经由网络传输至第二NE来执行指令，其中所述第一多个子流使用包括多个并行子SA的第一因特网协议安全协议(IPsec)安全联盟(SA)集群进行传输。

[0010] 在另一项实施例中，本发明包括一种网元(NE)，包括处理器，用于使用因特网密钥交换协议(IKE)或IKE版本2(IKEv2)在所述NE和第二NE之间创建包括第一多个子SA的IPsec SA集群，其中所述第一子SA是单向的，以及所述第一子SA用于在同一方向传输第一多个数据包。

[0011] 在另一项实施例中，本发明包括一种方法，包括建立多个IPsec SA子隧道以及将所述SA子隧道聚集在一起形成SA集群。

[0012] 结合附图和权利要求书，可从以下的详细描述中更清楚地理解这些和其他特征。

附图说明

[0013] 为了更完整地理解本发明，现在参考以下结合附图和详细描述进行的简要描述，其中相同参考标号表示相同部分。

[0014] 图1是IPsec安全架构的实施例的示意图。

[0015] 图2是IPsec安全架构的另一实施例的示意图。

[0016] 图3是创建SA集群的方法的实施例的流程图。

[0017] 图4是为数据子流选择子SA的方法的实施例的流程图。

[0018] 图5是经由SA集群接收数据的方法的实施例的流程图。

[0019] 图6是NE的实施例的示意图。

具体实施方式

[0020] IPsec是一种安全协议组，包括保护跨越各种网络的互联网协议(IP)通信安全的安全协议，如互联网工程任务组(IETF)文档请求注解(RFC)4301中所述，该文档以引用的方式并入。IPsec可保护IP层中的(例如，第三层和/或开放系统互连(OSI)模型的网络层)通信安全。IPsec可以是保护安全网关之间的数据流(例如，信息)的端到端安全方案。IPsec可采用单向SA对保护包括数据包的数据流。例如，本地安全网关可采用第一SA保护传输到远端安全网关的信息，采用第二SA保护从远端安全网关接收的信息。IPsec还可允许SA束，该SA束可包括嵌套在SA内的SA)(例如，隧道内的隧道)。IPsec可能限于采用SA对和/或SA束对。IPsec可以一种连续方式在SA上传输包。另外，可为每个SA指配唯一的安全参数索引(SPI)。因此，窃听节点可通过监控单个网络节点来接收SA保护的通过隧道的所有包并可使用SPI关联这些包。如果窃听节点突破了SA安全措施，该窃听节点可完全自由访问整个数据流。

[0021] 本文本中公开了增强保护不安全网络上传输的数据流量的一种方法和/或系统。可通过将数据流分割成多个子流并且并行传输这些子流(例如，经由子隧道和/或传输信息)来增强对IPsec数据的保护。可针对每个子流独立建立每个子SA。可合并子SA以形成SA集群。每个子SA可包括唯一的SPI。SA集群的子SA可采用或不采用本地安全网关和远端安全网关之间不同的网络路径。因此，窃听节点可能不能通过监控沿网络路径的单个节点来访问所有子流且可能意识不到其他网络路径的存在、数目或路线。由于每个子SA可包括唯一的SPI，从多个子流获取包的窃听节点也不能关联数据包以确定它们和同一个流相关。另外，子流的并行传输可允许传输效率相比串行传输有所提升。SA集群可在IETF文档draft-zhang-ipsecme-multi-path-ipsec-02中进一步描述，该文档以引用方式并入。

[0022] 该方法和/或系统可通过将数据流量扩展到多个路径上来提升安全服务。例如，这种扩展可能增加攻击者成功拦截所有包的难度，因为可能使用了不同的路线。即便当使用相同的路线时，攻击者/窃听者可能难以确定哪个SA集是某特定集群SA的一部分，哪个可能增加解密拦截到的包的难度。并且，多个路径的选择可提供(例如，链路失败时)增强的可靠性。多个SA的使用还可为优化的性能和最优网络控制提供额外的选择。这些技术可提升IPsec提供的安全服务。SA集群可提供在不同包上执行不同密码变换的选择。另外，SA集群还可提供沿不同路径传输包的选择。

[0023] 图1是IPsec安全架构100的一项实施例的示意图。IPsec安全架构100可包括主机150和主机151，其可经由安全网关110和112在位于不安全网络130中的路由器120上进行通信。主机150和151可分别经由安全连接143和144连接到安全网关110和112。主机150和151可能希望在不安全网络130上通信。安全网关110可(例如，通过使用IKE和/或IKEv2)为向安全网关112的传输建立单向SA141。类似地，安全网关112可为向安全网关110的传输建立单向SA142，这可能产生SA对。主机150可通过经由安全连接143与安全网关110通信来向主机

151传输数据，主机150可使用SA141经由路由器120在不安全的网络130上向安全网关112传输信息。这类信息随后可经由安全连接144路由到主机151，保证所传输的信息的端到端安全。主机151可以大体相同的方式向主机152传输数据包，但可能采用SA142而非SA141。

[0024] 主机(例如，主机150和151)可以是经由网络与另一台主机通信的任意设备。例如，主机150和/或151可包括服务器、客户端终端或其组合。主机150和151可用于出于分享资源、响应业务请求、应用托管等目的的数据通信。例如，主机150可包括客户端终端，主机151可包括服务器，且主机151可托管应用并响应来自主机150的应用请求。又如，主机150和151每个都可包括虚拟机(VM)、存储空间、处理资源等资源，并且可在网络连接上动态重定位数据、应用等。

[0025] 安全网关(例如，安全网关110和112)可以是位于安全网络边缘的任意NE。安全网络可包括安全连接，例如安全连接143和144。安全网关110和112可为位于安全网络内的任意设备和/或遍历安全网络的通信提供安全。安全网关110和112可防止未经授权访问安全网络(例如，防火墙)并且为离开安全网络的通信实施安全协议。例如，如果主机150和151每个都位于数据中心，安全网关110和112可位于数据中心网络的边缘，使得离开安全网络的所有流量都经过网关110和/或112。安全网关110和112可分别从主机150和151接收数据，并且通过在不安全网络130(例如，互联网)上创建IPsec SA141和142来发起通信会话。安全网关110和112可通过使用IKE和/或IKEv2等交换安全密钥以创建这类SA。

[0026] IPsec SA(例如，SA141和142)可在传输模式或隧道模式下运行。在传输模式下，数据包的净荷(例如，正被传输的实际数据)可加密，而包括数据包路由信息的数据包的头则可不加密。在隧道模式下，整个数据包都可加密。SA还可包括数据和/或算法以支持报文认证头协议(AH)和/或封装安全载荷协议(ESP)操作。AH可提供无连接完整性和数据流的数据源认证。ESP可提供数据包机密性(例如，封装)、数据源认证、无连接完整性、防重放业务和流机密性。SA141和142每个都可是单向的。因此，可要求一对SA141和142在安全网关110和112之间传送数据包。在一项实施例中，SA141和142每个可包括SA束。SA束可包括两个嵌套的SA(例如，隧道内的隧道)。例如，SA束可在ESP SA内包括AH SA。IPsec安全架构100可限于为安全网关110和112之间的每个安全通信提供单个SA对和/或单个SA对束(例如，SA141和SA142)。每个SA可包括单独的SPI，该SPI可用作SA数据库(SAD)中的索引且可和SA目标地址结合用于唯一地标识SA以及确定加密密钥和与SA相关联的协议。

[0027] 路由器120可以是位于不安全网络130中的任意NE或NE组。路由器可从安全网关110接收数据包并将该数据包转发到安全网关112，反之亦然。路由器120可使用OSI第二层、第2.5层和/或第三层技术对包进行路由。路由器120可基于数据包的头做出路由决策。如果数据包已封装(例如，ESP)，则路由器120可基于该封装包的头做出路由决策，无需了解存储在该数据包头和/或净荷中的数据。路由器120可提供安全网关110和安全网关112之间的端到端连接。路由器120可分别为SA141和SA142组成单个网络路径。SA141的网络路径和SA142的网络路径可能是或不是同一条路径。

[0028] IPsec协议组指明了遵循IPsec的系统的基础架构100的一个示例。IPsec协议组描述了如何(例如，在IP层，在IP版本4(IPv4)和IP版本6(IPv6)环境中)为流量提供一组安全服务。如本文所述，IPsec协议组将SA定义为IPsec的概念。SA(例如，SA141和142)可定义单工连接，其可向该连接携载的流量提供安全服务。SA可通过使用AH或ESP提供安全服务，但

不可在单个SA中同时使用这两者提供安全服务。AH和ESP可在IETF文档RFC4302和RFC4303中进一步描述，IETF文档RFC4302和RFC4303以引用的方式并入本文本中。如果要将AH和ESP保护都应用到业务流上，则可创建两个SA，并通过迭代应用安全协议(例如，嵌套的SA)协调二者以实现保护。由于一个SA可用于携载单播流量，因此可在点对点通信中创建一对SA(例如，SA141和142)。这两个SA141和142可在安全网关110和112二者之间创建一个单播IPsec隧道。为区分不同的SA，接收方可使用SPI来识别输入数据包应绑定的SA，其中SPI可包括32位的值。SPI指配可在SA的创建者处完成，该创建者可以是接收侧。在发送侧，附加的目标IP地址信息可用于解决任意SPI冲突。这样，发送侧可选择正确的SA，IP包将在此SA下处理。在另一项实施例中，每个安全网关110和112都可指配本地SPI，且每个都保持知晓对方的SPI。发送包时，每一方(例如，网关110或112)可在数据包头中采用对方(例如，网关112或110)的SPI。

[0029] 应注意，尽管图1仅描绘了位于安全网关110和112之间的SA(例如，SA141和142)，在某些实施例中，主机(例如主机150和/或151)可经由SA直接和网关(例如网关110和/或112)通信。例如，作为主机的客户端终端可以不位于安全网络上。在这种情况下，客户端终端可使用SA在不安全网络130上直接和安全网关通信。

[0030] 图2是IPsec安全架构200的另一项实施例的示意图。架构200可包括主机250和251、安全连接243和244、安全网关210和212以及路由器221和222，它们分别和主机140和141、安全连接143和144、安全网关110和112以及路由器120大体相似。安全网关210和212可经由SA集群241和SA集群242通信。

[0031] SA集群241和242每个都包括多个并行子SA。并行子SA可以是具有相同源节点(例如，安全网关210)、相同目标节点(例如，安全网关212)的多个单向子SA，且每个并行子SA可传输同一数据流的一部分。例如，SA集群241可包括并行子SA241a和241b，而SA集群242可包括并行子SA242a和242b。SA集群与SA束的区别可在于，SA集群的子SA可以不是嵌套的。然而，在某些实施例中，子SA可包括SA束。虽然仅为每个SA集群描绘了两个子SA，但指定通信需要多少子SA，SA集群241和242就可包括多少子SA。子SA241a和241b每个可类似于SA141，而子SA242a和242b可类似于SA242。然而，每个子SA只可以传输和/或封装数据流的一部分。例如，安全网关210可能希望经由SA集群241向安全网关212传输包括多个数据包的数据流。安全网关210可在子SA241a和241b之间交替包，在子SA241a上发送比在子SA241b上更多的包，将流划分成离散数据包块并在子SA241a-241b之间交替块等。每个子SA可包括不同的SPI，因此SA集群241和/或242可包括多个SPI。SA集群的子SA可在安全网关之间采用相同路线或不同路线。例如，SA集群241可分别包括子SA241a和子SA241b，子SA241a可采用经由路由器221的路线，而子SA241b采用经由路由器222的路线。又如，SA集群242可包括子SA242a和242b，两者都可采用经由路由器221的路线。

[0032] 架构200可允许数据流分割并以窃听节点不可预测的方式路由。由于每个SA集群可包括未知数目的子SA，窃听节点可能不知道和特定数据流相关的数据包的确切数目。进一步地，由于每个SA集群可包括多个SPI，窃听节点可能无法关联任何获取的数据包，且可能无法确定这些数据包和同一数据流相关。另外，由于某些子SA可能遍历不同于其他子SA的网络路线，窃听节点可能无法通过监控单个网络节点获取流的所有数据包，并且可能无法确定应该监控其他哪些网络节点以获取剩余的数据包。因此，SA集群241和/或242的使用

可显著增加窃听和/或黑客攻击过程的不确定性，并可因此强化不安全网络的安全性。同样地，在并行子SA中传输数据包的能力可允许传输优化。例如，如果路由器221变得拥堵，传出数据包可从子SA241a转向241b而不终止通信会话。进一步地，和架构100可能所需的数据流包的串行处理相比，数据流包的并行传输可通过并行处理器允许处理效率的提升。例如，当并行传输数据流包时，可并行执行SA查找，序列号生成和/或防重放检查。

[0033] 架构200可采用抽象语法编码1(ASN.1)实施SA集群的创建和使用。以下ASN.1定义可基于子SA(例如，分别为子SA241a和241b或242a和242b)的数目创建SA集群(例如，SA集群241和/或242)，还可选择合适的子SA用于子流传输：

[0034]
```
Processing ::= SEQUENCE {
extSeqNum     BOOLEAN,--真: 64 位计数器, 假: 32 位计数器
seqOverflow   BOOLEAN,--真: 密钥更新, 假: 终止&审计
fragCheck     BOOLEAN,--真: 状态片段检查,
                      --假: 无状态片段检查
Lifetime      SALifetime,
spi           ManualSPI,
algorithms    ProcessingAlgs,
tunnel        TunnelOptions    OPTIONAL,--如为空, 使用传输模式
saCount       INTEGER     OPTIONAL,     --如为空, 使用 1
selectSA      SASelAlgoType  OPTIONAL--如果 saCount 为 1, 忽略,
                                      --如为空, 使用轮询
}
```

[0035]
```
SASelAlgoType ::= INTEGER {
round-robin   (0),
random        (1),
others        (2)
}
```

[0036] 在上述ASN.1定义中，extSeqNum、seqOverflow和fragCheck属性可以是布尔值(例如，可包含true或false值)，并且可设置为分别指示创建SA集群的实体(例如，子流发送方)是否应该设置64位或32位的计数器，在序列号溢出时进行密钥更新或终止集群，和是否有状态地检查流分割。Lifetime属性可指示SA集群和/或特定子SA的生命周期，其中生命周期可以是SA集群和/或子SA在不接收和/或传输数据时保持活动的时间量。SA集群可设置为永不超时。管理员可采用SPI属性手动设置SPI值，如果SPI是自动生成的，则可忽略。algorithms属性可指示用于创建和/或采用SA集群和/或子SA的其他处理算法。tunnel属性可用于指示SA集群和/或子SA是否使用隧道和/或传输模式以及与隧道模式相关联的任意选项。saCount属性可以是变量，且可设置为整数或其他值以指示要为SA集群创建的子SA的数目。selectSA属性可以是变量，且可设置为整数或其他值以与SASelAlgoType相符。发送方可使用selectSA为特定子流的传输选择子SA。SASelAlgoType可以是变量，且可设置为整数或其他值以指示特定选择算法。例如，SASelAlgoType可设置为值0以指示轮询选择算法，设置为值1以指示随机选择算法，设置为其他值以指示其他选择算法(例如，用户自定义的，

基于SA路径时延的分摊，基于SA路径保证的服务质量分摊等)。轮询可以是将数据流的各部分均等指派给每个子SA的选择算法。

[0037] 数据机密性可保护传输的数据不受被动式攻击，如窃听。在IPsec实施中(例如，架构100)，所有的IP数据报都可在一个IPsec隧道内传输，其可受到一个SA的保护。为提升机密安全服务，可采用SA集(例如，子SA241a、241b、242a和/或242b)保护流量。可在两个实体间建立多个隧道并将这些隧道聚集在一起形成一个集群隧道(例如，SA集群241和/或242)。一个IP包仍由单个SA保护。发送实体可在所有这些子SA之间分割流量。接收实体可复用来自多个IPsec隧道的流量。聚集在一起的各隧道可定义为子隧道。子隧道的SA可定义为子SA。可在一个集群隧道内保护的IP流量可在所有子隧道间分割。术语SA集群可用于描述SA的合并，通过合并SA，必须处理流量以满足安全策略。由于在两个安全实体间为同一个流量流建立了多个子隧道，因此物理路径可能不同。这些集群SA的处理顺序可以是本地事件，因为所有这些SA都可能是或者不是嵌套的SA。

[0038] 应注意，SA集群可由发送方执行，接收实体可不知道SA集群存在于IP层。例如，流量复用可由上层进程执行，而非直接由IPsec进程执行，因为接收器可能没有用以关联IP层的多个子SA上的SA集群流量的机制。然而，上层进程可采用其他方法(例如，通过关联与上层进程相关的序列号等)收集和复用流量。

[0039] 如果子SA通过IKE协商进行协商，该子SA可包括其自身的软硬生命周期。然而，SA集群可能没有生命周期。架构200可能不变更对每个子SA的维护。如果一个子SA变成无效(例如，超时)，则这种子SA可能不用于进一步的包处理。如果SA集群停止容纳任何有效的子SA，则该SA集群可变成无效。

[0040] 图3是创建SA集群的方法300的实施例的流程图。在方法300中，NE(例如安全网关210和/或212)可(例如，从主机240)接收与另一NE(例如，步骤310处的安全网关212)创建SA的请求。在步骤312处，方法300可检索SA的安全策略。安全策略可存储于安全策略数据库(SPD)中，该安全策略数据库(SPD)可位于NE上和/或从另一NE(如管理NE)访问。安全策略可用于确定处理参数和/或将与SA相关联的加密密钥材料。在步骤314处，方法300可检查安全策略以确定saCount变量是否存在。如果saCount变量不存在，方法300可前进至步骤316；如果saCount存在，则前进至步骤320。

[0041] 在步骤316处，saCount变量不存在，这可能意味着单个SA(例如，SA141)已由安全策略指定。因此，方法300可(例如，通过使用IKE和/或IKEv2)创建SA，前进至步骤318并结束。

[0042] 在步骤320处，saCount变量可能存在，这可能意味着SA集群由安全策略指定。saCount变量的值可指示SA集群中子SA的数目。如果saCount变量的值不大于或等于1，方法300可前进至步骤322并返回错误，因为集群可能需要至少一个子SA。如果saCount的值大于或等于1，方法300可前进至步骤324。在步骤324处，方法300可创建计数变量并将该计数变量的值设为saCount变量的值。在步骤326处，方法300可(例如，通过使用IKE和/或IKEv2)创建子SA。在步骤328处，计数变量的值可按1递减。在步骤330处，方法300可确定计数变量的值是否大于0。如果计数变量的值保持大于0，方法300可返回到步骤326并根据计数变量的值创建额外的SA。一旦计数变量的值在步骤330处达到0，方法300可前进至步骤318处并结束。因此，子SA可基于安全策略创建并添加到SA集群。

[0043] 如上所述，SA集群可包括多个子SA建立。子隧道可独立建立。在建立后，子隧道可逐个添加到集群。将子SA添加进SA集群的准确方式可以是本地事件。所有协作子隧道可包括不同的SPI值。对于一个集群隧道可使用多少子隧道，可能无限制。在任意IPsec流量通过任意子隧道传输之前，发送实体和接收实体都可在SA集群规格上达成一致。可建立新的子SA并将其加入到SA集群中，即便在流量开始在集群隧道内流动之后。尽管子隧道可以是独立的，但它们可共享仅一个序列号源。集群隧道内携载的每个IPsec包都可包括唯一的序列号。

[0044] 所有子隧道都可独立建立。通过不同子隧道的流量可采用相同的路线。流量也可基于路由策略采用不同路线，例如，通过使用等价多路径路由。当SA集群仅包括一个子SA时，如果为架构100设计的设备不支持SA集群，SA集群可在架构100下与IPsec实施完全互操作。

[0045] 图4是为数据子流选择子SA的方法400的实施例的流程图。在步骤410处，传出包可由安全网关210和/或212等接收。在步骤412处，方法400可查询SPD以找到与来自步骤410的包所属的流相匹配的SPD条目。在步骤414处，方法400可确定存储于SPD条目中的saCount值是否大于1。如果saCount值不大于1，该方法可前进至步骤418；如果saCount值大于1，则前进至步骤416。在步骤418处，方法400可使用SA的SPI和流信息查询SA数据库(SAD)以找到执行SA封装和/或传输的数据。如果计数值为1或更小，可能只有1个SA，无需SA选择。如果计数值大于1，方法400在步骤416处可根据子SA选择算法(例如，selectSA和/或SASelAlgoType)为子流选择子SA。一旦选择了子SA，该方法可前进至步骤418并使用所选子SA的SPI查询SAD。通过这一方式，流的数据包可通过使用选择算法在子SA之间分发。选择算法可出于上述数据流量效率和安全原因在子SA之间交替包。

[0046] 如上所述，发送实体可通过多个子隧道分割和/或交替IPsec流量。当基于安全策略配置为流量处理选择了SA集群时，可为指定包选择一个子SA以进行传出IPsec处理。本地实施可确定应将哪个SA应用到指定IP包上。除了序列编号可在所有子SA之间共享，其他与架构100相关联的处理流程不可更改。发送实体处的本地实施可选择任意方法获取包的序列号，这可独立于子SA选择。在替代性实施例中，每个子SA都可生成自己的序列编号，这可不要求在各子SA间共享序列号。

[0047] 图5是经由SA集群接收数据的方法500的实施例的流程图。防重放可以是IPsec的功能，且可用于防止接收NE多次处理相同的包。如果采用单个SA，包可按顺序接收，这就允许接收NE丢弃新接收到的、序列号小于上一个接收到的包的序列号的任意包。当采用SA集群时，可并行传输包。因此，如果采用序列号共享，则数据包可无序接收。当通过使用防重放位图采用SA集群时，可采用方法500实施防重放功能。

[0048] 在步骤510处，可由安全网关210和/或212等接收传入包。在步骤512处，该方法可(例如，通过使用SPI查询SPD)确定SA是否采用防重放。如果没有为SA采用防重放，方法500可前进至步骤514并处理包。如果采用了防重放，方法500可前进至步骤516。在步骤516处，方法500可获取数据包的序列号并将序列号和防重放位图进行比较。例如，防重放位图可包括所有具有对应值的可能的序列号(例如，每个都设为值0、值1或其组合)以指示是否已接收到序列号对应的包。在步骤518处，方法500可确定是否在防重放位图中设置序列号。如果设置了序列号(例如，为值1)，该方法可确定已经接收到具有序列号的包，前进至步骤520，

然后丢弃包。如果序列号未设置(例如,为值1),该方法可确定尚未接收到具有序列号的包,然后可前进至步骤522。在步骤522处,该方法可(例如,通过将对应值设为值0)更新防重放位图以指示已经接收到与序列号相关联的包。方法500随即可前进至步骤514并处理包。

[0049] 如上所述,在接收器侧选择子SA这一过程可类似于选择单个SA,两者都可基于SPI和IP地址信息。除了对序列号处理的变更,其他方面可能都不变。使用多个子隧道可能导致两个实体之间的安全通信信道无序传递IPsec包。作为补救,如果接收实体需要维持发送顺序,可使用数据包IPsec头内的序列号。如果启用了防重放,所有的子隧道都可在接收实体处使用一个共享的防重放位图。防重放检查可针对SA集群而非特定的子SA完成。

[0050] 尽管多路径解决方案可能带来无序传递的问题,但无序问题也可能会产生于单个SA中。重排序过程可基于特定网络的拓扑、以类似于TCP重排序和/或IP重组的方式在聚合节点和/或最终主机处(例如,主机240和/或241)完成。

[0051] 图6是网元(NE)600的实施例的示意图,网元(NE)600可包括:安全网关110、112、210和/或212;主机140、141、240和/或241;和/或路由器120、221和/或222。本领域的技术人员将认识到术语NE包含广泛的设备,NE600只是其中一个示例。包含NE600只是为了清楚地进行论述,而决非将本发明的应用限于一项特定的NE实施例或一类NE实施例。本发明描述的特征/方法中至少一些特征/方法,例如,用于创建SA集群的方法300,用于为子流选择子SA的方法400和/或用于从SA集群接收数据的方法500,可在网络装置或部件(例如NE600)中整体或部分实施。例如,可使用硬件、固件和/或安装用于在硬件上运行的软件来实施本发明的特征/方法。NE600可以是通过网络传输帧的任意设备,例如,交换机、路由器、网桥、服务器、客户端等。如图6所示,NE600可包括收发器(Tx/Rx)610,其可以是发射器、接收器、或其组合。Tx/Rx610可耦合到多个下游端口620用于传输和/或接收来自其他节点的帧,而Tx/Rx610耦合到多个上游端口650用于传输和/或接收来自其他节点的帧。处理器630可耦合到Tx/Rx610以处理帧和/或确定将帧发送到哪些节点。处理器630可包括一个或多个多核处理器和/或存储器设备632,其可作为数据存储器、缓冲器等。处理器630可实施为通用处理器,或者可以是一个或多个专用集成电路(ASIC)和/或数字信号处理器(DSP)的一部分。下游端口620和/或上游端口650可包含电和/或光发射和/或接收部件。NE600可以是或可以不是做出路由决策的路由部件。

[0052] 据了解,通过将可执行指令编程和/或加载至NE600,处理器630、下游端口620、Tx/Rx610、存储器632和/或上游端口650中的至少之一被改变,将NE600部分转换成特定机器或装置,例如,本发明宣扬的拥有新颖功能的多核转发架构。加载可执行软件至计算机所实现的功能可以通过公知设计规则转换成硬件实施,这在电力工程和软件工程领域是很基础的。决定使用软件还是硬件来实施一个概念通常取决于对设计稳定性及待生产的单元数量的考虑,而不是从软件领域转换至硬件领域中所涉及的任何问题。一般来说,经常变动的设计更适于在软件中实施,因为重新编写硬件实施比重新编写软件设计更为昂贵。通常,稳定及大规模生产的设计更适于在如ASIC这样的硬件中实施,因为运行硬件实施的大规模生产比软件实施更为便宜。设计通常可以以软件形式进行开发和测试,之后通过公知设计规则转变成专用集成电路中等同的硬件实施,该集成电路硬线软件指令。由新ASIC控制的机器是一特定的机器或装置,同样地,编程和/或加载有可执行指令的电脑可视为特定的机器或装置。

[0053] 本发明公开至少一项实施例，且所属领域的普通技术人员对所述实施例和/或所述实施例的特征作出的变化、组合和/或修改均在本发明公开的范围内。因组合、合并和/或省略所述实施例的特征而得到的替代性实施例也在本发明的范围内。应当理解的是，本发明已明确阐明了数值范围或限制，此类明确的范围或限制应包括涵盖在上述范围或限制(如从大约1至大约10的范围包括2、3、4等；大于0.10的范围包括0.11、0.12、0.13等)内的类似数量级的迭代范围或限制。例如，每当揭示具有下限R1和上限Ru的数值范围时，具体是揭示落入所述范围内的任何数字。具体而言，特别公开所述范围内的以下数字：R＝R1+k*(Ru-R1)，其中k是从1％到100％以1％增量递增的变量，即，k是1％、2％、3％、4％、7％、……、70％、71％、72％、……、95％、96％、97％、98％、99％或100％。此外，还特此公开了，上文定义的两个R值所定义的任何数值范围。除非另有说明否则术语“约”是指其后数字的±10％。相对于权利要求的某一要素，术语“可选择”的使用表示该要素可以是“需要的”，或者也可以是“不需要的”，二者均在所述权利要求的范围内。使用如“包括”、“包含”和“具有”等较广术语应被理解为提供对如“由…组成”、“基本上由…组成”以及“大体上由…组成”等较窄术语的支持。因此，保护范围不受上文所述的限制，而是由所附权利要求书定义，所述范围包含所附权利要求书的标的物的所有等效物。每项和每条权利要求作为进一步公开的内容并入说明书中，且权利要求书是本发明的实施例。所述揭示内容中的参考的论述并不是承认其为现有技术，尤其是具有在本申请案的在先申请优先权日期之后的公开日期的任何参考。本发明中所引用的所有专利、专利申请案和公开案的揭示内容特此以引用的方式并入本文本中，其提供补充本发明的示例性、程序性或其他细节。

[0054] 虽然本发明多个具体实施例，但应当理解，所公开的系统和方法也可通过其他多种具体形式体现，而不会脱离本发明的精神或范围。本发明的实例应被视为说明性而非限制性的，且本发明并不限于本文本所给出的细节。例如，各种元件或部件可以在另一系统中组合或合并，或者某些特征可以省略或不实施。

[0055] 此外，在不脱离本发明的范围的情况下，各种实施例中描述和说明为离散或单独的技术、系统和方法可以与其他系统、模块、技术或方法进行组合或合并。展示或论述为彼此耦合或直接耦合或通信的其他项也可以采用电方式、机械方式或其他方式通过某一接口、装置或中间部件间接地耦合或通信。其他变更、替换、更替示例对本领域技术人员而言是显而易见的，均不脱离此处公开的精神和范围。

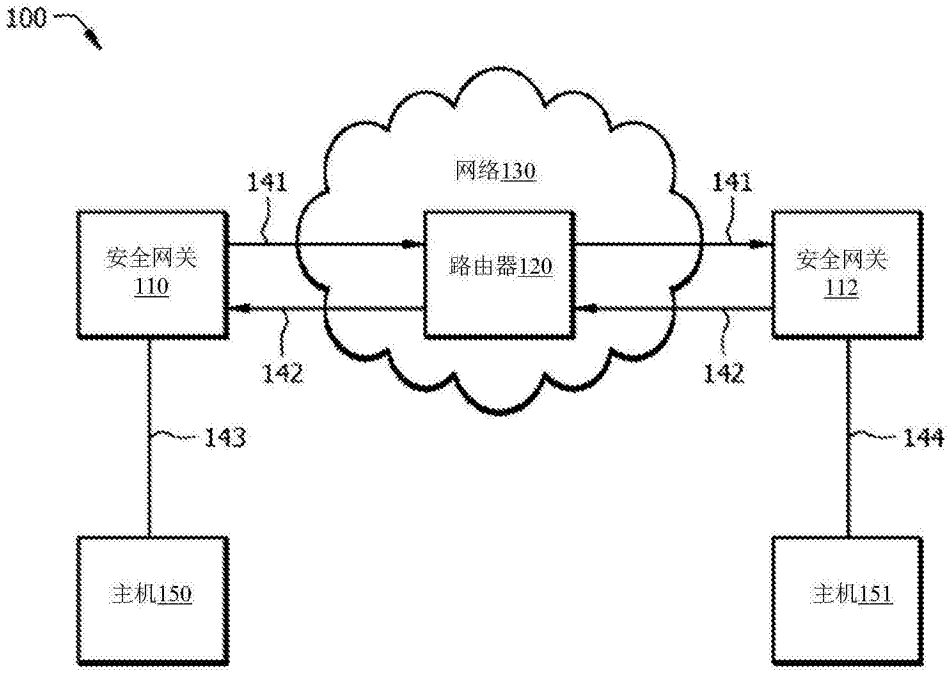

100
网络130
141
141
安全网关
110
路由器120
安全网关
112
142
142
143
144
主机150
主机151

图1

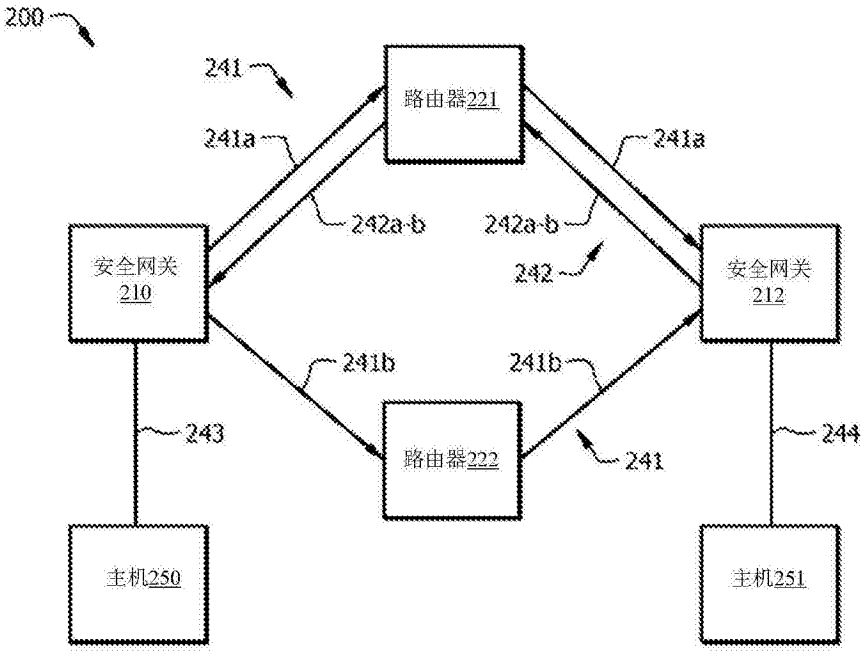

200
241
路由器221
241a
241a
242a-b
242a-b
242
安全网关
210
安全网关
212
241b
241b
243
244
路由器222
241
主机250
主机251

图2

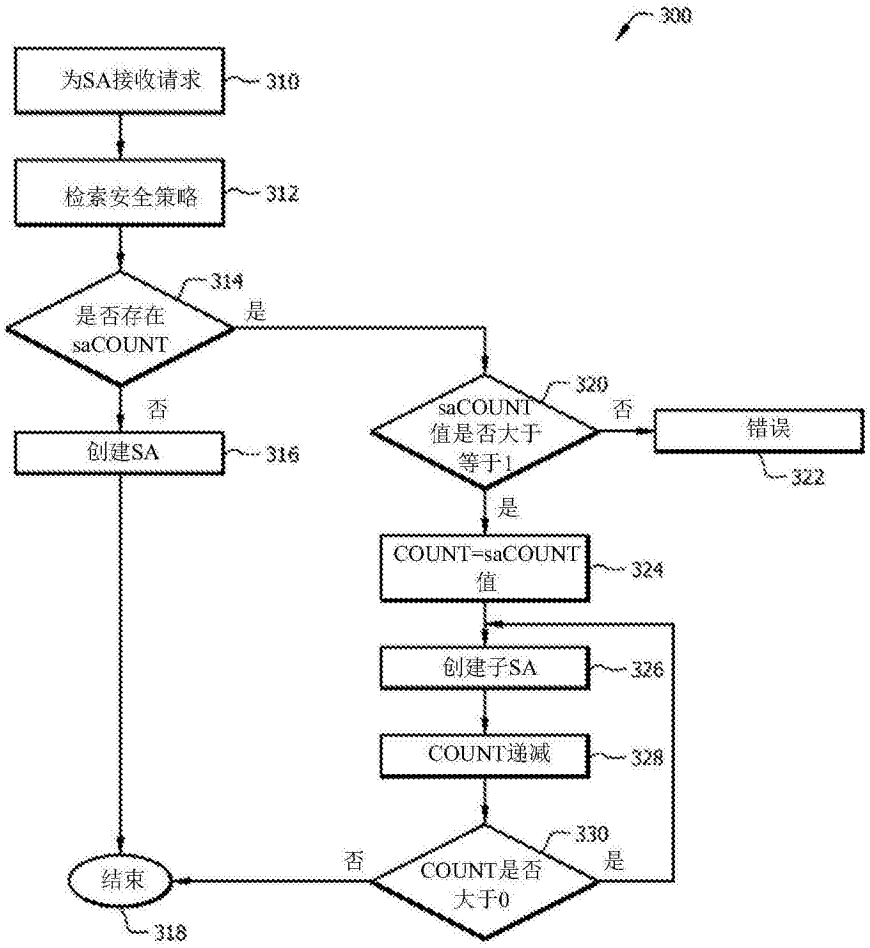

300
为SA接收请求
310
检索安全策略
312
是否存在saCOUNT
314
是
否
创建SA
316
saCOUNT值是否大于等于1
320
否
错误
322
是
COUNT=saCOUNT值
324
创建子SA
326
COUNT递减
328
COUNT是否大于0
330
否
是
结束
318

图3

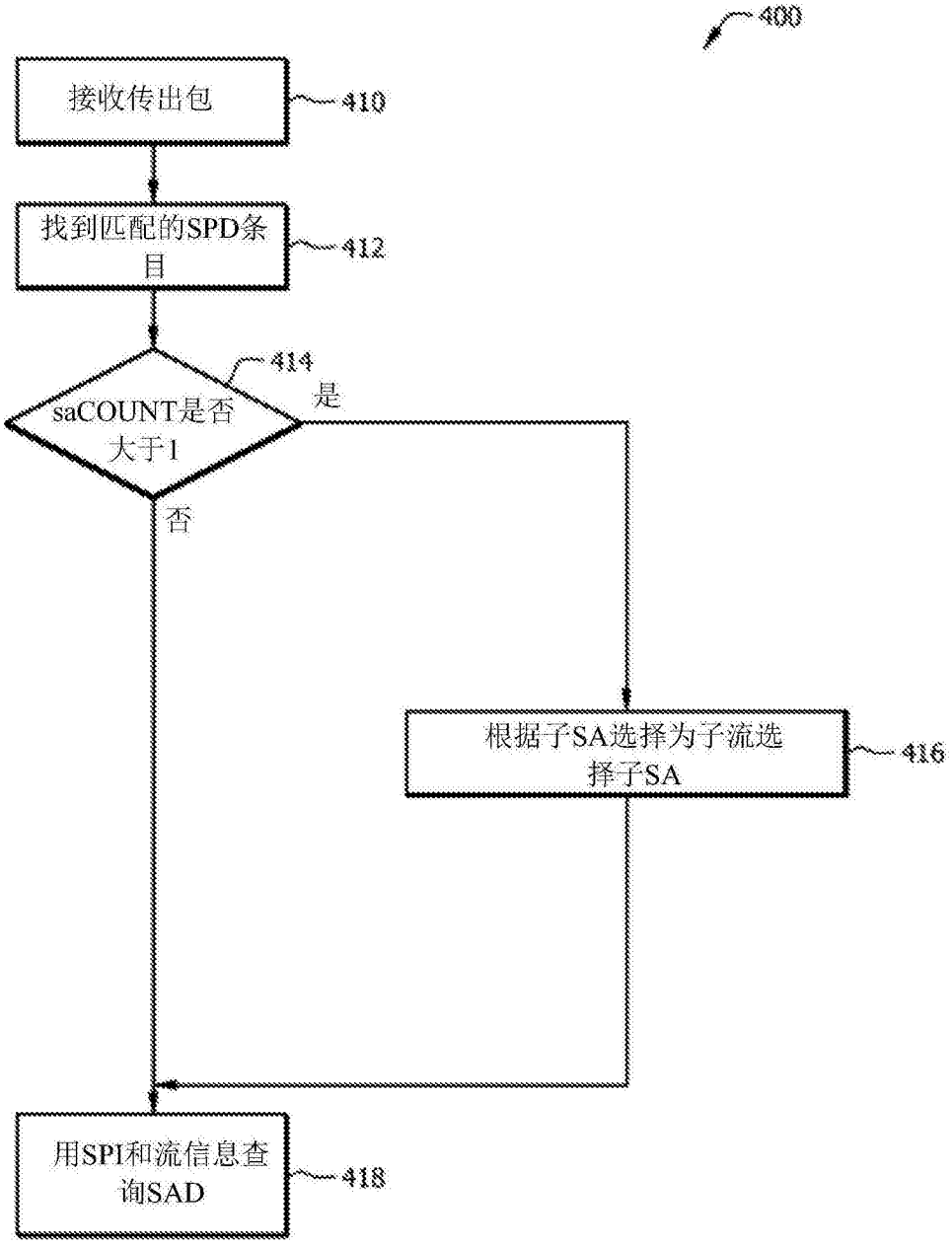

400
接收传出包
410
找到匹配的SPD条目
412
saCOUNT是否大于1
414
是
否
根据子SA选择为子流选择子SA
416
用SPI和流信息查询SAD
418

图4

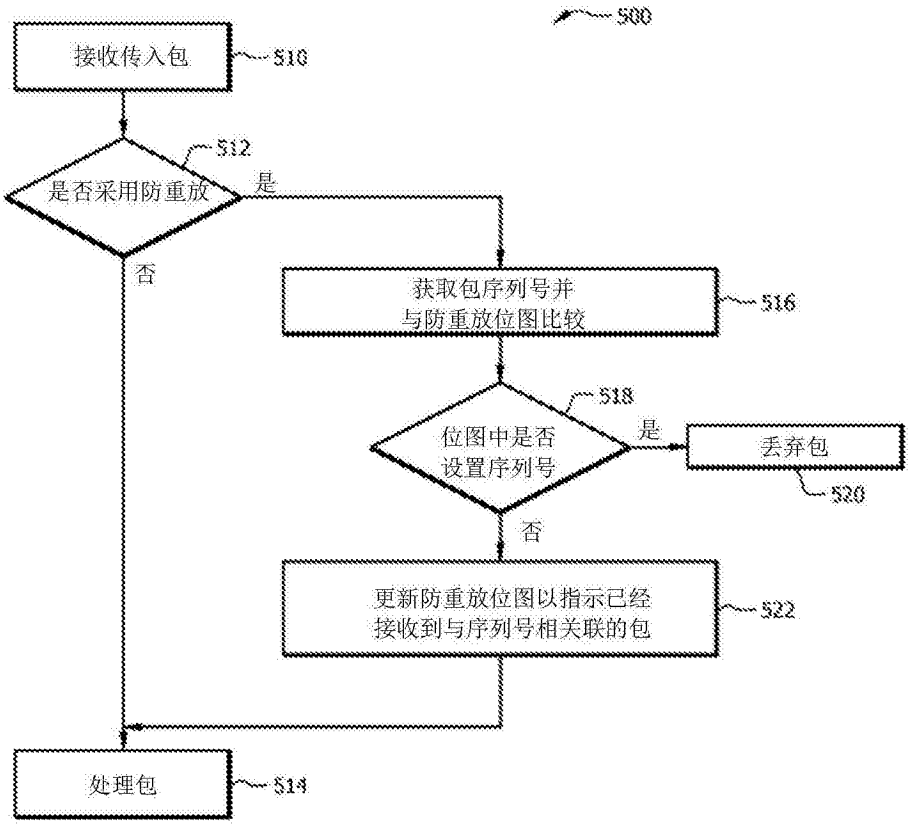

500
接收传入包
510
512
是否采用防重放
是
否
获取包序列号并
与防重放位图比较
516
518
位图中是否
设置序列号
是
丢弃包
520
否
更新防重放位图以指示已经
接收到与序列号相关联的包
522
处理包
514

图5

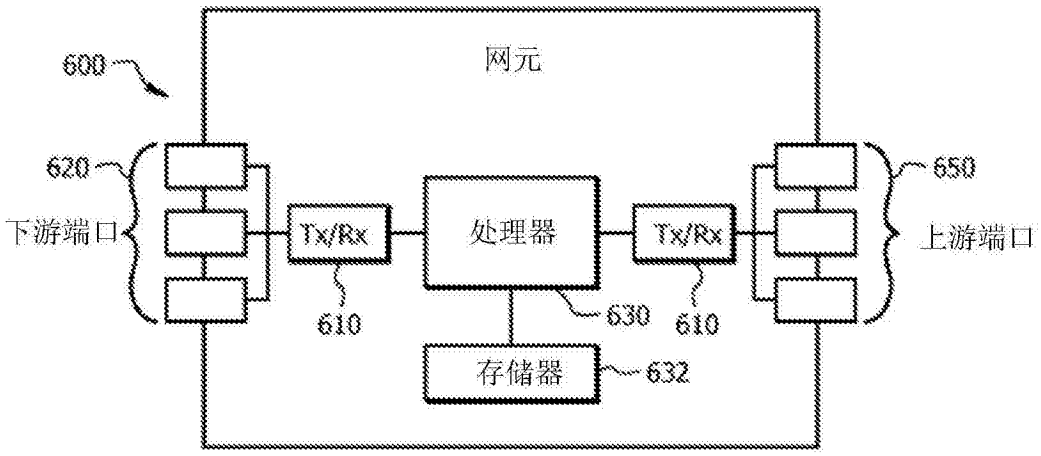

600
网元
620
下游端口
Tx/Rx
610
处理器
630
存储器
632
Tx/Rx
610
650
上游端口

图6