



(10) 授权公告号 CN 110537352 B

(45) 授权公告日 2022. 12. 09

(21) 申请号 201780089522.5

(22) 申请日 2017.04.13

(65) 同一申请的已公布的文献号
申请公布号 CN 110537352 A

(43) 申请公布日 2019.12.03

(85) PCT国际申请进入国家阶段日
2019.10.11

(86) PCT国际申请的申请数据
PCT/CN2017/080428 2017.04.13

(87) PCT国际申请的公布数据
W02018/188019 EN 2018.10.18

(73) 专利权人 诺基亚技术有限公司
地址 芬兰埃斯波

(72) 发明人 闫峥 卞姗姗

(74) 专利代理机构 北京市中咨律师事务所
11247

专利代理师 杨晓光

(51) Int.Cl.
H04L 9/40 (2022.01)
H04L 41/0893 (2022.01)
H04L 41/40 (2022.01)
H04L 43/08 (2022.01)
H04L 43/20 (2022.01)

审查员 周秋爽

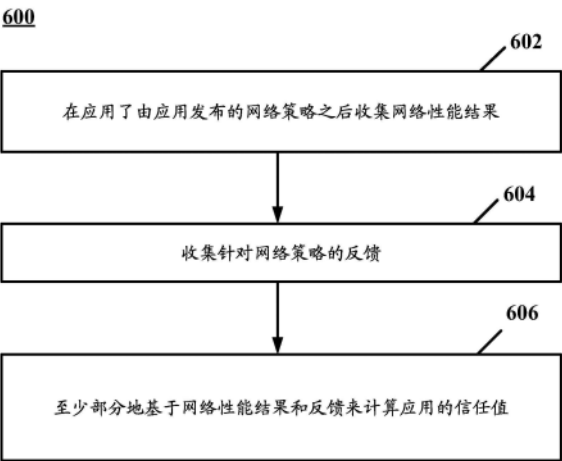
权利要求书4页 说明书14页 附图7页

(54) 发明名称

用于软件定义网络中的信任管理的装置、方法和非暂时性计算机可读介质

(57) 摘要

公开了用于软件定义网络中的信任管理的方法、装置、计算机程序产品和计算机可读介质。一种方法包括：在应用了由应用发布的网络策略之后，收集网络性能结果；收集针对所述网络策略的反馈；和至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值。



1. 一种用于软件定义网络中的信任管理的方法,包括:

在应用了由应用发布的网络策略之后,收集网络性能结果,其中,所述应用的身份由所述网络性能结果的提供者添加到所述网络性能结果中;

收集针对所述网络策略的反馈,其中如果所述网络策略对网络性能和/或安全性有良好的影响,则所述反馈是肯定的,否则所述反馈是否定的;和

至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值。

2. 根据权利要求1所述的方法,还包括:

确定至少一个网络性能监测器是否处于受信任状态,其中,所述网络性能结果由所述至少一个网络性能监测器监测;和

当网络性能监测器未处于受信任状态时,丢弃所述网络性能监测器的网络性能结果。

3. 根据权利要求2所述的方法,其中,所述至少一个网络性能监测器位于所述软件定义网络的数据平面中,并且由网络性能监测器装置管理,以及在所述网络性能监测器装置和所述至少一个网络性能监测器之间应用信任维持和控制协议。

4. 根据权利要求1-3中的任一项所述的方法,其中,所述网络性能结果由所述网络性能结果的提供者签名。

5. 根据权利要求1-3中任一项所述的方法,还包括:

从所述软件定义网络的至少一个控制平面接收所述应用的身份和所述网络策略的持续时间;和

通过将所述持续时间与网络性能监测的时间进行匹配,将所述应用的身份添加到所述网络性能结果中。

6. 根据权利要求1-3中的任一项所述的方法,其中,所述网络性能结果包括吞吐率、分组丢失概率和时间延迟中的至少一项。

7. 根据权利要求1-3中的任一项所述的方法,还包括:

对所述信任值进行签名;和

向所述应用和/或所述软件定义网络的至少一个控制平面提供签名的信任值。

8. 一种用于软件定义网络中的信任管理的方法,包括:

接收由应用发布的网络策略;

获取所述应用的信任值,其中,所述信任值由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算,其中如果所述网络策略对网络性能和/或安全性有良好的影响,则所述反馈是肯定的,否则所述反馈是否定的;

确定所述信任值是否高于阈值;

响应肯定的确定,检查所述网络策略是否与已应用的网络策略冲突;

当所述网络策略与所述已应用的网络策略冲突时,根据所述应用的优先级确定是否应用所述网络策略;或者,

当所述网络策略与所述已应用的网络策略不冲突时,应用所述网络策略。

9. 根据权利要求8所述的方法,还包括:

至少部分地基于所述信任值来计算所述应用的优先级。

10. 根据权利要求8或9所述的方法,其中,检查所述网络策略是否与已应用的网络策略冲突包括:

基于源IP地址、目的IP地址、源端口和目的端口,检查所述网络策略是否与已应用的网络策略冲突。

11.根据权利要求8-9中的任一项所述的方法,其中,基于所述应用的优先级来确定是否应用所述网络策略包括:

当所述应用的优先级高于已应用的网络策略的优先级时,用所述网络策略替换已应用的网络策略;

当所述应用的优先级低于已应用的网络策略的优先级时,拒绝所述网络策略;或者,

当所述应用的优先级等于已应用的网络策略的优先级时,在这种情况下,将已应用的网络策略和所述网络策略发送给网络管理员以做出最终决定,或者应用决定规则来自动设置网络策略。

12.根据权利要求8-9中的任一项所述的方法,其中,所述网络策略由所述应用签名,所述信任值由所述信任评估装置签名。

13.一种用于软件定义网络中的信任管理的装置,包括:

至少一个处理器;

至少一个存储器,其包括计算机程序代码,所述存储器和所述计算机程序代码被配置为与所述至少一个处理器一起工作,使所述装置:

在应用了由应用发布的网络策略之后,收集网络性能结果,其中,所述应用的身份由所述网络性能结果的提供者添加到所述网络性能结果中;

收集针对所述网络策略的反馈,其中如果所述网络策略对网络性能和/或安全性有良好的影响,则所述反馈是肯定的,否则所述反馈是否定的;和

至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值。

14.根据权利要求13所述的装置,其中,所述存储器和所述计算机程序代码还被配置为与所述至少一个处理器一起工作使所述装置:

确定至少一个网络性能监测器是否处于受信任状态,其中,所述网络性能结果由所述至少一个网络性能监测器监测;和

当网络性能监测器未处于受信任状态时,丢弃所述网络性能监测器的网络性能结果。

15.根据权利要求14所述的装置,其中,所述至少一个网络性能监测器位于所述软件定义网络的数据平面中,并且由网络性能监测器装置管理,以及在所述网络性能监测器装置和所述至少一个网络性能监测器之间应用信任维持和控制协议。

16.根据权利要求13-15中的任一项所述的装置,其中,所述网络性能结果由所述网络性能结果的提供者签名。

17.根据权利要求13-15中任一项所述的装置,其中,所述存储器和所述计算机程序代码还被配置为与所述至少一个处理器一起工作使所述装置:

从所述软件定义网络的至少一个控制平面接收所述应用的身份和所述网络策略的持续时间;和

通过将所述持续时间与网络性能监测的时间进行匹配,将所述应用的身份添加到所述网络性能结果中。

18.根据权利要求13-15中的任一项所述的装置,其中,所述网络性能结果包括吞吐率、分组丢失概率和时间延迟中的至少一项。

19. 根据权利要求13-15中任一项所述的装置,其中,所述存储器和所述计算机程序代码还被配置为与所述至少一个处理器一起工作使所述装置:

对所述信任值进行签名;和

向所述应用和/或所述软件定义网络的至少一个控制平面提供签名的信任值。

20. 一种用于软件定义网络中的信任管理的装置,包括:

至少一个处理器;

至少一个存储器,其包括计算机程序代码,所述存储器和所述计算机程序代码被配置为与所述至少一个处理器一起工作,使所述装置:

接收由应用发布的网络策略;

获取所述应用的信任值,其中,所述信任值由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算,其中如果所述网络策略对网络性能和/或安全性有良好的影响,则所述反馈是肯定的,否则所述反馈是否定的;

确定所述信任值是否高于阈值;

响应肯定的确定,检查所述网络策略是否与已应用的网络策略冲突;

当所述网络策略与所述已应用的网络策略冲突时,根据所述应用的优先级确定是否应用所述网络策略;或者,

当所述网络策略与所述已应用的网络策略不冲突时,应用所述网络策略。

21. 根据权利要求20所述的装置,其中,所述存储器和所述计算机程序代码被配置为与所述至少一个处理器一起工作,以使所述装置:

至少部分地基于所述信任值来计算所述应用的优先级。

22. 根据权利要求20或21所述的装置,其中,所述存储器和所述计算机程序代码还被配置为与所述至少一个处理器一起工作使所述装置:

基于源IP地址、目的IP地址、源端口和目的端口,检查所述网络策略是否与已应用的网络策略冲突。

23. 根据权利要求20-21中任一项所述的装置,其中,所述存储器和所述计算机程序代码被配置为与所述至少一个处理器一起工作使所述装置:

当所述应用的优先级高于已应用的网络策略的优先级时,用所述网络策略替换已应用的网络策略;

当所述应用的优先级低于已应用的网络策略的优先级时,拒绝所述网络策略;或者,

当所述应用的优先级等于已应用的网络策略的优先级时,在这种情况下,将已应用的网络策略和所述网络策略发送给网络管理员以做出最终决定,或者应用决定规则来自动设置网络策略。

24. 根据权利要求20-21中的任一项所述的装置,其中,所述网络策略由所述应用签名,所述信任值由所述信任评估装置签名。

25. 一种用于软件定义网络中的信任管理的装置,包括被配置为执行根据权利要求1-7中的任一项所述的方法的构件。

26. 一种非暂时性计算机可读介质,其上具有编码的语句和指令,以使处理器执行根据权利要求1-7中任一项所述的方法。

27. 一种用于软件定义网络中的信任管理的装置,包括被配置为执行根据权利要求8-

12中的任一项所述的方法的构件。

28.一种非暂时性计算机可读介质,其上具有编码的语句和指令以使处理器执行根据权利要求8-12中的任一项所述的方法。

用于软件定义网络中的信任管理的装置、方法和非暂时性计算机可读介质

技术领域

[0001] 本公开的实施例总体上涉及数据处理,并且更具体地,涉及软件定义网络中的信任管理。

背景技术

[0002] 软件定义网络(SDN)是一种新兴的网络范例,它使网络管理员能够非常快速地配置网络资源并调整网络范围的业务流以动态满足不断变化的需求。SDN的一个突出特点是,它从物理上将转发设备(称为数据平面)的转发功能与诸如控制器的控制元件(称为控制平面)分离。整个网络的管理可以依靠逻辑上集中的控制平面,而无需考虑底层设备的类型(例如,路由器、交换机、防火墙等)。这种新型的联网机制忽略了底层网络设备之间的差异,并通过应用编程接口(API)对新的网络功能进行编程,为运营商提供了一种非常简单的方式来管理网络。

[0003] 尽管有诸如集中控制和网络可编程性之类的许多高级属性,SDN也引入了许多安全威胁。SDN应用平面中的应用是通过北向接口直接和可编程地将其网络要求和期望的网络行为传达给控制平面的程序。通常,SDN系统中的控制器可能没有能力来自行区分应用的合格性、合法性和可信赖性。除此之外,设计不良的或错误的应用可能会无意地给SDN系统带来一系列新漏洞。因此,如何管理大量应用的信任成为一个紧迫的问题。

发明内容

[0004] 以简化形式提供本发明内容以介绍选择的构思,这些构思以下在详细描述中将被进一步描述。本发明内容并不旨在标识所要求保护的主题的关键特征或必要特征,也不旨在用于限制所要求保护的主题的范围。

[0005] 根据本公开的第一方面,提供了一种用于在软件定义网络中的信任管理的方法。所述方法可以包括:在应用了由应用发布的网络策略之后,收集网络性能结果;收集针对所述网络策略的反馈;至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值。

[0006] 根据本公开的第二方面,提供了一种用于在软件定义网络中的信任管理的装置。所述装置可以包括至少一个处理器;以及包括计算机程序代码的至少一个存储器,所述存储器和所述计算机程序代码被配置为与所述至少一个处理器一起工作,使所述装置:在应用了由应用发布的网络策略后,收集网络性能结果;收集针对所述网络策略的反馈;至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值。

[0007] 根据本公开的第三方面,提供了一种用于在软件定义网络中的信任管理的装置。所述装置可以包括:被配置为在应用了由应用发布的网络策略之后收集网络性能结果的构件;以及被配置为收集针对所述网络策略的反馈的构件;以及被配置为至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值的构件。

[0008] 根据本公开的第四方面,提供了一种计算机程序产品,该计算机程序产品体现在可由计算机读取的分发介质上并且包括程序指令,当所述程序指令被加载到计算机中时,所述程序指令执行以下操作:在应用了由应用发布的网络策略后,收集网络性能结果;收集针对所述网络策略的反馈;至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值。

[0009] 根据本公开的第五方面,提供了一种非暂时性的计算机可读介质,该非暂时性计算机可读介质在其上具有编码的语句和指令以使处理器执行以下操作:在应用了由应用发布的网络策略后,收集网络性能结果;收集针对所述网络策略的反馈;至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值。

[0010] 根据本公开的第六方面,提供了一种用于在软件定义网络中的信任管理的方法。所述方法可以包括:接收由应用发布的网络策略;获得所述应用的信任值,其中,所述信任值由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算;确定所述信任值是否高于阈值;响应肯定的确定,检查所述网络策略是否与已应用的网络策略冲突;如果所述网络策略与所述已应用的网络策略冲突,则根据所述应用的优先级确定是否应用所述网络策略;或者,如果所述网络策略与所述已应用的网络策略不冲突,则应用所述网络策略。

[0011] 根据本公开的第七方面,提供了一种用于在软件定义网络中的信任管理的装置。所述装置可以包括至少一个处理器;以及包括计算机程序代码的至少一个存储器,所述存储器和所述计算机程序代码被配置为与所述至少一个处理器一起工作,以使所述装置:接收由应用发布的网络策略;获得所述应用的信任值,其中,所述信任值由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算;确定所述信任值是否高于阈值;响应肯定的确定,检查所述网络策略是否与已应用的网络策略冲突;当所述网络策略与所述已应用的网络策略冲突时,根据所述应用的优先级确定是否应用所述网络策略;或者,当所述网络策略与所述已应用的网络策略不冲突时,应用所述网络策略。

[0012] 根据本公开的第八方面,提供了一种用于在软件定义网络中的信任管理的装置。所述装置可以包括:被配置为接收由应用发布的网络策略的构件;被配置为获得所述应用的信任值的构件,其中,所述信任值由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算;被配置为确定所述信任值是否高于阈值的构件;被配置为响应肯定的确定,检查所述网络策略是否与已应用的网络策略冲突的构件;被配置为当所述网络策略与所述已应用的网络策略冲突时,所述应用的优先级确定是否应用所述网络策略的构件;或者,被配置为当所述网络策略与所述已应用的网络策略不冲突时,应用所述网络策略的构件。

[0013] 根据本公开的第九方面,提供了一种计算机程序产品,该计算机程序产品体现在可由计算机读取的分发介质上并且包括程序指令,当所述程序指令被加载到计算机中时,所述程序指令执行以下操作:接收由应用发布的网络策略;获得所述应用的信任值,其中,所述信任值由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算;确定所述信任值是否高于阈值;响应肯定的确定,检查所述网络策略是否与已应用的网络策略冲突;当所述网络策略与所述已应用的网络策略冲突时,根据所述应用的优先级确定是否应用所述网络策略;或者,当所述网络策略与所述已应用的网络策略不冲突时,应

用所述网络策略。

[0014] 根据本公开的第十方面,提供了一种非暂时性的计算机可读介质,该非暂时性计算机可读介质在其上具有编码的语句和指令以使处理器执行以下操作:接收由应用发布的网络策略;获得所述应用的信任值,其中,所述信任值由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算;确定所述信任值是否高于阈值;响应肯定的确定,检查所述网络策略是否与已应用的网络策略冲突;当所述网络策略与所述已应用的网络策略冲突时,根据所述应用的优先级确定是否应用所述网络策略;或者,当所述网络策略与所述已应用的网络策略不冲突时,应用所述网络策略。

[0015] 通过以下结合附图对本申请的示例性实施例的详细描述,本公开的这些和其他目的、特征和优点将变得显而易见。

附图说明

[0016] 图1描绘了可以实现本公开的一些实施例的示意性系统架构;

[0017] 图2示出了根据本公开实施例的用于SDN中的信任管理的装置的简化框图;

[0018] 图3示出了根据本公开的另一实施例的用于SDN中的信任管理的装置的简化框图;

[0019] 图4示出了根据本公开的又一个实施例的用于SDN中的信任管理的装置的简化框图;

[0020] 图5示出了根据本公开的又一个实施例的用于SDN中的信任管理的装置的简化框图;

[0021] 图6是示出根据本公开的实施例的用于SDN中的信任管理的方法的流程图;

[0022] 图7是示出根据本公开的另一实施例的用于SDN中的信任管理的方法的流程图;

[0023] 图8是示出根据本公开的又一个实施例的用于SDN中的信任管理的方法的流程图;

[0024] 图9是示出根据本公开的又一实施例的用于SDN中的信任管理的方法的流程图。

具体实施方式

[0025] 出于说明的目的,在以下描述中阐述了细节,以便提供对所公开的实施例的透彻理解。然而,对于本领域技术人员而言显而易见的是,可以在没有这些具体细节的情况下或使用等效布置来实施实施例。

[0026] 图1描绘了示意性系统架构,其中可以实现本公开的一些实施例。如图1所示,系统架构100包括SDN系统106。注意,SDN系统可以采用任何合适的现有或将来的技术或协议,例如OpenFlow、OpenDaylight、网络虚拟化平台等。通常,SDN系统106可以包括三层:应用平面,控制平面和数据平面。

[0027] 应用平面可以包含多个SDN应用(APP) 108。SDN APP是通过北向接口(NBI) 124将其网络要求和期望的网络行为显式地、直接地和可编程地传达给SDN控制平面或控制器的程序。应用平面可以用于配置网络功能。网络策略或流规则可以在应用平面中生成并体现在控制平面中。

[0028] 控制平面或控制器可以基于选择的流规则或网络策略来生成数据转发命令,以经由南向接口126指令在数据平面中的数据转发。控制器是逻辑上集中的实体,其可以负责将来自SDN应用平面的需求转换到数据平面,并为SDN应用提供网络的抽象视图,其可以包括

统计信息和事件。控制平面可以制定协议,该协议用于更新诸如交换机、路由器和/或防火墙之类的数据平面设备的转发表。可以在控制平面中添加冲突检测(CD)模块/装置110,其用于检测新的网络策略或流规则是否与现有/应用的策略或流规则冲突。CD模块110可以基于从应用的信任值得出的优先级来决定可以选择并应用哪个流规则/网络策略。

[0029] 数据平面主要包括诸如路由器、交换机、防火墙等的转发设备112(硬件或软件或两者)。转发设备112可以基于由控制平面管理的流表(例如,控制平面提供的转发命令)来转发数据分组。数据平面可以转发数据流,收集网络信息,并将网络状态发送到控制平面。

[0030] 系统架构100还可以包括信任管理框架(TMF)130,其可以包含两个模块/装置:网络性能监测器(NPM)模块/装置104和信任评估(TE)模块/装置102。

[0031] NPM模块104可以包括多个探测器,其被配置为在由不同SDN应用发布的网络策略或流规则被执行和实现之后监测该网络策略或流规则的性能。探测器(硬件或软件或两者)可以位于网络中的数据平面的任何适当位置,并且被TMF 130信任以用于实现网络性能监测。在一个实施例中,NPM模块104可以应用信任维持和控制机制来管理探测器,以确保以如TMF所期望的可信赖的方式执行探测器的网络监测和相关的收集,例如,如以下文献所描述的协议:Z.Yan,P.Zhang,A.V.Vasilakos,“A Security and Trust Framework for Virtualized Networks and Software-Defined Networking”,Security and Communication Networks, Wiley,9(16),pp.3059-3069Nov.2016.Doi:10.1002/sec.1243和Z.Yan,P. Cofta,“A mechanism for trust sustainability among trusted computing platforms”,the First International Conference on Trust and Privacy in Digital Business(TrustBus'04),LNCS 3184,pp.11-19,Spain,September 2004,通过引用将其全部内容并入本文作为本申请的一部分。

[0032] 在应用流规则或网络策略之后,探测器可以按照吞吐率、丢包概率、时间延迟等来监测网络性能。这些监测结果可以与指示发布流规则或网络策略的应用的相应标签一起发送到TE模块102。

[0033] 通过收集以上监测结果以及来自控制平面和/或其他系统实体的反馈,TE模块102可以计算发布流规则或网络策略的应用的信任值。TE模块102可以将基于其评估的应用的信任值发布给控制平面,以帮助控制平面对由不同应用提供的流规则或网络策略的选择和决策。

[0034] 例如,在应用将其网络要求和期望的网络行为(即网络策略或流规则)传达给控制平面之前,它可以向TE模块102发送请求以获得该应用的信任值,其中TE模块102可以使用TE模块102的私钥对该信任值进行签名。然后,应用可以将其网络策略或流规则以及被证明的信任值发送到控制平面。

[0035] 作为另一实施例,如果控制平面从应用接收到流规则或网络策略,但是应用未附加其通过TE模块102被证明的信任值或该信任值未通过TE 模块102被证明,则控制平面可以向TE模块102发送请求以获得该应用的信任值,其中该信任值可以由TE模块102签名。

[0036] 另外,以上任何两个实体之间的通信可以是安全通信。网络性能结果可以由网络性能结果的提供者签名,例如,探测器收集的数据可以被其提供者签名,并且不能被其提供者否认。另外,流规则或网络策略可以由应用签名。例如,通过应用公钥密码系统,应用平面中的任何应用都可以向控制平面证实自己。该系统的身份管理可以基于公钥密码系统。系

统实体的公钥代表其唯一标识符。

[0037] 注意, TMF 130可以位于控制平面内或受信任的第三方中, 并由多个控制平面共享。此外, TE模块102和NPM 104可以集成到一个实体中, 也可以分布在不同的实体中并由它们管理。

[0038] 另外, SDN系统106可以包括多个控制平面, 每个控制平面可以管理网络的一部分, SDN APP可以向多个控制平面提供其流规则或网络策略。

[0039] TE模块102和NPM模块104可以以硬件、软件或其组合的形式实现, 包括但不限于服务器、台式计算机、膝上型计算机、云计算、互联网/网络节点、通信器、服务软件、或其任何组合。例如, TE模块102和 NPM模块104可以被部署为云服务。

[0040] 如图1所示, 链接114、116、118、120、122、124和126可以是安全通道。例如, 可以通过应用安全通信协议(例如, 传输层安全性(TLS)、安全套接字层(SSL)、OpenSSL、在TLS上的超文本传输协议(HTTP)、在SSL上的HTTP和HTTP安全(HTTPS)等)在系统架构100中的每两个参与方之间建立安全通道。

[0041] 图2示出了根据本公开实施例的用于SDN中的信任管理的装置200 的简化框图。装置200可以被实现为如图1所示的TE模块102。

[0042] 参考图2, 装置200可以包括收集元件202, 其被配置为在应用了由应用发布的网络策略之后收集网络性能结果。网络性能结果可以是转发设备的网络性能结果和/或整个网络的性能结果。在一个实施例中, 网络性能结果可以包括吞吐率、分组丢失概率、时间延迟等中的至少一个。

[0043] 例如, 收集元件202可以从位于SDN的数据平面中的一个或多个探测器收集网络性能结果。在一个实施例中, 如上所述, 探测器可以由NPM 104管理。在另一个实施例中, 网络性能结果可以由控制平面或控制器提供, 例如, 在应用了由应用发布的网络策略后, 控制器可以收集转发设备的网络性能结果或整个网络的性能结果。可以在预定义的持续时间内或直到应用另一个流规则或网络策略为止监测网络性能结果。通常, 可以在网络性能结果中添加应用的身份, 或者收集元件202可以识别发布链接到网络性能结果的底层流规则或网络策略的应用。另外, 可以在网络性能结果中添加时间戳以指示网络性能监测的时间长度。

[0044] 收集元件202可以进一步收集对网络策略的反馈。例如, 收集元件 202可以收集来自SDN的至少一个控制平面或任何其他实体的反馈。该反馈可以是在应用了网络策略之后网络策略对整个网络或单个转发设备的性能和/或安全性的影响的指示。例如, 如果网络策略对性能和/或安全性有良好的影响, 则反馈可以是肯定的, 否则反馈可以是否定的。作为示例, 反馈可以是分数, 并且反馈越正面, 则分数越高。

[0045] 在一个实施例中, 网络性能结果可以由网络性能结果的提供者签名。例如, 如果网络性能结果是由探测器提供的, 则探测器可以用其私钥对网络性能结果进行签名, 使得网络性能结果不能被其提供者否认, 并且装置 200可以检查网络性能结果是否被篡改了。

[0046] 在一个实施例中, 网络性能结果的提供者可以在网络性能结果中添加应用的身份。例如, 当NPM模块104指令探测器监测网络性能时, NPM 模块104可以向探测器通知应用的身份, 然后探测器可以在网络性能结果中添加应用的身份。在另一个实施例中, 控制平面可以将应用的身份嵌入到其被选择并应用于数据平面的流规则中, 然后探测器可以在监测期间知道应用的身份。

[0047] 所述装置可以进一步包括计算元件204,其被配置为至少部分地基于网络性能结果和反馈来计算应用的信任值。注意,当应用首次发布网络策略时,计算元件204可以设置应用的初始信任值。以下实施例给出了信任值的示例计算,但是在其他实施例中可以应用其他公式或算法。

[0048] $T_{i,c}$ 表示在时间c的应用i的信任值。 $T_{i,c}$ 可以由两部分贡献:在时间 c_j 时,来自控制平面j($j=1, \dots, J$)的反馈,其被表示为 $T_{fi,c}$,以及网络性能结果,其被表示为 $Tp_{i,c}$ 。计算元件204可以向与应用i具有交互的所有控制平面发送针对反馈的请求。在接收到该请求之后,控制平面j根据应用i在网络状态方面的统计记录,以诚实的方式发回其反馈 $te_{j,i}$ 。例如,如果应用i的流规则未引起任何网络性能或安全问题,则 $te_{j,i}$ 为肯定的,否则为否定的。假设计算元件204在时隙c总共接收到J个反馈。然后,计算元件204可以基于公式1)通过考虑时间影响(反馈越新,反馈越有价值)和J的影响值(J的值越大,评估越准确)来汇总所有反馈:

$$[0049] \quad T_{fi,c} = \frac{\theta(J)}{J} \sum_{j=1}^J te_{j,i} \times e^{-\frac{|c-c_j|}{\tau}}, \quad (1)$$

[0050] 其中 $\theta(J) = 1 - \exp\left(\frac{-J^2}{2(\sigma+\varepsilon)^2}\right)$ 是瑞利累积分布函数,用于建模J对信任评估的影响, $\varepsilon = -\frac{1}{J'}$, 其中参数J'是SDN系统中控制平面的总数。参数 τ 用于控制 $te_{j,i}$ 的衰减,因为最近的反馈可能对信任评估有更大的贡献。

[0051] 为了基于网络性能结果来计算 $Tp_{i,c}$,可以应用以下算法来准备计算。

[0052] 算法1:准备 $Tp_{i,c}$ 计算输入:网络吞吐率tr的监测结果;丢包概率lp;延时td;网络吞吐率的阈值 TH_tr;丢包概率的阈值TH_lp;延时的阈值TH_td。

[0053] $Po=0; Ne=0$

[0054] If $tr > TH_tr, Po++; \text{else } Ne++;$

[0055] If $lp > TH_lp, Po++; \text{else } Ne++;$

[0056] If $td < TH_td, Po++; \text{else } Ne++;$

[0057] 输出:Po和Ne。

[0058] 在时隙 c 处从所有探测器收集所有Po和Ne之后,计算元件204可以针对应用i($i=1, \dots, I$)检查附加到Po和Ne上的标签(即,应用的身份),然后通过组合来自探测器k的包含标签i的 Po_k 和 Ne_k ,使用公式2来计算 $Tp_{i,c}$ 。

$$[0059] \quad T_{pi,c} = \frac{\sum_{k=1}^K Po_{k,i}}{\sum_{k=1}^K Po_{k,i} + \sum_{k=1}^K Ne_{k,i} + r}, \quad r \geq 1$$

[0060] 其中r是确保 $0 \leq T_{pi,c} < 1$ 的参数,并且公式(2)始终有效。K是提供关于应用i的监测结果的探测器总数。

[0061] 最后,基于公式(3),可以将 $T_{fi,c}$ 和 $Tp_{i,c}$ 聚合在一起,并且还可以考虑前一时隙 c' 的过去信任值 $T_{i,c'}$ 。

$$[0062] \quad T_{i,c} = \alpha T_{i,c'} + \beta T_{fi,c} + \gamma T_{pi,c} \quad (3)$$

[0063] 其中 $\alpha + \beta + \gamma = 1$, 它们是加权参数。

[0064] 图3示出了根据本公开的另一实施例的用于SDN中的信任管理的装置的简化框图。装置300可以被实现为如图1所示的TE模块102。对于上面已经参考图2描述的一些部件, 为了简洁在此省略其描述。

[0065] 参考图3, 装置300可以包括收集元件302和计算元件304, 其中收集元件302可以被配置为在应用了由应用发布的网络策略之后收集网络性能结果并收集针对网络策略的反馈, 计算元件304被配置为至少部分地基于网络性能结果和反馈来计算应用的信任值。收集元件302和计算元件304 的功能分别类似于收集元件202和计算元件204的功能, 因此为了简洁在此省略其描述。

[0066] 装置300还可包括: 确定元件306, 被配置为确定至少一个网络性能监测器是否处于受信任状态, 其中, 所述网络性能结果由所述至少一个网络性能监测器监测; 丢弃元件308, 被配置为如果网络性能监测器不处于受信任状态, 则丢弃该网络性能监测器的网络性能结果。

[0067] 例如, 可以从位于SDN的数据平面中并且由诸如NPM模块104之类的网络性能监测器装置来管理的至少一个网络性能监测器收集网络性能结果, 确定元件306可以与网络性能监测器装置(例如NPM模块104) 进行检查以确定至少一个网络性能监测器(例如探测器)是否处于受信任状态, 并且如果网络性能监测器未处于受信任状态, 则丢弃元件308可以丢弃网络性能监测器的网络性能结果。

[0068] 在一个实施例中, 可以在NPM模块104和探测器之间应用信任维持和控制协议, 以确保每个探测器按预期工作。一旦探测器受到攻击或入侵, 就可以通知NPM模块104。因此, 确定元件306可以与NPM模块 104一起检查以确定探测器是否处于受信任状态。如果探测器处于受信任状态, 则可以在信任值计算中考虑该探测器提供的网络性能结果。否则, 探测器提供的网络性能结果可以被丢弃。以这种方式, 可以确保在信任值计算中仅使用可信的网络性能结果, 从而可以提高信任值计算的准确性。

[0069] 在一个实施例中, 网络性能结果的提供者(例如探测器)可能不知道应用的身份, 因此, 探测器可能不会将应用的身份添加到网络性能结果中。在这种情况下, 装置300可以自己将应用的身份添加到网络性能结果中。

[0070] 在该实施例中, 装置300还可以包括: 接收元件310, 被配置为从 SDN的至少一个控制平面接收应用的身份和网络策略的持续时间; 添加元件312, 被配置为通过将持续时间与网络性能监测的时间进行匹配, 将应用的身份添加到网络性能结果中。

[0071] 例如, 当诸如控制器之类的控制平面接收到网络策略时, 控制平面可以知道应用的身份。如果控制器选择并应用了网络策略, 则控制器可以周期性地将应用的身份和网络策略的持续时间发送给装置300。然后, 接收元件310可以接收应用的身份和网络策略的持续时间。添加元件312可以将持续时间与网络性能监测的时间进行匹配, 其中网络性能监测的时间可以被嵌入到网络性能结果中。以这种方式, 添加元件312可以识别网络性能结果, 并且将应用的身份添加到网络性能结果中。

[0072] 在一个实施例中, 装置300还可以包括: 签名元件314, 被配置为对信任值进行签名; 提供元件316, 被配置为将签名的信任值提供给应用和/或SDN的至少一个控制平面。通过使用签名的信任值, 应用和/或至少一个控制平面能够检测信任值是否已被篡改。例如,

当应用将网络策略发送到诸如控制器之类的控制平面时,应用可以附加由签名元件314签名的被证明的信任值。在另一个示例中,当应用不发送被证明的信任值或附加未被证明的信任值给控制器,控制器可以从签名元件314检索经被证明的信任值。在获得被证明的信任值之后,控制器可以验证签名。如果验证失败,则控制器可以拒绝该网络策略,否则控制器可以继续处理该网络策略。

[0073] 图4示出了根据本公开实施例的用于SDN中的信任管理的装置400 的简化框图。装置400可以被实现为控制器,控制器的模块或与控制器一起工作的独立装置。

[0074] 参考图4,装置400可以包括接收元件402,其被配置为接收由应用发布的网络策略。例如,当装置400被实现为控制器或其模块时,接收元件402可以通过北向接口从应用接收网络策略。如果装置400是独立设备,则接收元件402可以从控制器接收网络策略。另外,网络策略可以由应用签名。

[0075] 装置400还可包括:获取元件404,被配置为获取应用的信任值,其中,信任值由信任评估装置至少部分地基于网络性能结果和针对网络策略的反馈来计算。例如,如上所述,可以由装置200或300基于网络性能结果和针对网络策略的反馈来计算信任值。

[0076] 在一个实施例中,可以将信任值附加到由应用发布的网络策略。例如,装置200或300可以将信任值发送给应用,然后应用可以将信任值附加到网络策略,其中如上所述,可以由装置200或300对信任值进行签名。在这种情况下,获取元件404可以从网络策略获取信任值。

[0077] 在另一个实施例中,信任值可以不附加到网络策略。例如,应用仅将网络策略发送到控制器。在这种情况下,获取元件404可以从诸如装置 200或300的信任评估装置获取信任值。另外,如上所述,可以由装置200 或300对信任值进行签名。

[0078] 装置400还可以包括:确定元件406,被配置为确定信任值是否高于阈值。阈值可以是任何合适的值,例如它可以由运营商确定。注意,当应用首次发布网络策略时,可以由诸如装置200或300之类的信任评估装置来设置应用的初始信任值,其中,初始信任值可以高于阈值。通过使用该阈值,可以拒绝某些具有较低信任值的恶意应用、设计欠佳或错误的应用。响应于肯定的确定(即,信任值高于阈值),装置400可以进一步处理网络策略,否则可以拒绝网络策略。

[0079] 装置400还可包括检查元件408,其被配置为响应于信任值高于阈值来检查网络策略是否与已应用的网络策略冲突。检查元件408可以将任何合适的现有或将来的冲突检测技术用于网络策略。在一个实施例中,检查元件408可以基于源IP地址、目的IP地址、源端口和目的端口来检查网络策略是否与已应用的网络策略冲突。

[0080] 在一个实施例中,如果网络策略与已应用的网络策略冲突,则确定元件406可以基于应用的优先级来确定是否应用该网络策略。可以通过采用任何合适的方法来确定应用的优先级。例如,可以通过应用的类型来确定应用的优先级。作为示例,管理应用和安全应用可以具有比第三方应用更高的优先级。

[0081] 在一个实施例中,如果该应用的优先级高于已应用的网络策略的优先级,则可以将已应用的网络策略替换为该网络策略,其中,已应用的网络策略的优先级可以等于发布已应用的网络策略的应用的优先级。如果该应用的优先级低于已应用的网络策略的优先级,则该网络策略可能会被拒绝。如果该应用的优先级等于已应用的网络策略的优先级,则

在这种情况下可以将已应用的网络策略和该网络策略发送给网络管理员,以进行最终决策或应用决定规则来自动设置网络策略。

[0082] 在一个实施例中,装置400可以进一步包括应用元件410,其被配置为如果该网络策略与已应用的网络策略不冲突,则应用该网络策略。例如,应用元件410可以将网络策略转换成可以在数据平面中使用的任何合适的转发规则(多个)。

[0083] 图5示出了根据本公开的另一实施例的用于SDN中的信任管理的装置的简化框图。装置500可以被实现为控制器、控制器的模块或与控制器一起工作的独立装置。对于上面已经参考图4描述的一些部件,为了简洁,在此省略其描述。

[0084] 参考图5,装置500可以包括:接收元件502,被配置为接收由应用发布的网络策略;获取元件504,用于获取所述应用的信任度,其中,所述信任度由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算;确定元件506,用于确定所述信任值是否高于阈值;检查元件508,用于响应于肯定的确定,检查所述网络策略是否与已应用的网络策略冲突;如果所述网络策略与已应用的网络策略冲突,则确定元件506还用于基于所述应用的优先级,确定是否应用所述网络策略;或者,如果所述网络策略与所述已应用的网络策略不冲突,则应用元件510,用于应用该网络策略。接收元件502、获取元件504、确定元件506、检查元件508和应用元件510的功能分别类似于接收元件402、获取元件404、确定元件406、检查元件408和应用元件410的功能,因此为了简洁在此省略其描述。

[0085] 装置500还可以包括计算元件512,其被配置为至少部分地基于信任值来计算应用的优先级。例如,可以将应用 P_i 的优先级计算为

$$[0086] \quad P_i = F(T_i) \quad (3)$$

[0087] 其中 T_i 表示应用 i 的信任值。 T_i 的值越大, P_i 越高。值得注意的是, P_i 不仅受信任的影响,也可能受到其他因素的影响,因此函数 $F()$ 可以考虑其他输入,例如应用权限级别、重要性级别等,以便生成准确的优先级值。

[0088] 在相同的发明构思下,图6是示出根据本公开的实施例的用于SDN中的信任管理的方法的流程图。方法600可以由装置200或300执行。对于与先前实施例中描述的相同的部分或功能,为简洁起见省略其描述。

[0089] 如图6所示,方法600可以从步骤602开始。在步骤602,装置200或300可以在应用了由应用发布的网络策略之后收集网络性能结果。

[0090] 在步骤604,装置200或300可以收集针对网络策略的反馈。

[0091] 在步骤606,装置200或300可以至少部分地基于网络性能结果和反馈来计算应用的信任值。

[0092] 在相同的发明构思下,图7是示出根据本公开的另一实施例的用于SDN中的信任管理的方法的流程图。方法700可以由装置300执行。对于与先前实施例中描述的相同的部分或功能,为了简洁起见,省略其描述。

[0093] 如图7所示,方法700可以从步骤702开始。在步骤702,装置300可以在应用了由应用发布的网络策略之后收集网络性能结果。

[0094] 在步骤702-2,装置300可以确定至少一个网络性能监测器是否处于受信任状态,其中,网络性能结果由至少一个网络性能监测器监测。

[0095] 在步骤702-4,如果网络性能监测器不处于受信任状态,则装置300可以丢弃网络

性能监测器的网络性能结果。

[0096] 在步骤702-6,装置300可以从软件定义网络的至少一个控制平面接收应用的身份和网络策略的持续时间。

[0097] 在步骤702-8,装置300可以通过将持续时间与网络性能监测的时间进行匹配来将应用的身份添加到网络性能结果中。

[0098] 在步骤704,装置300可以收集针对网络策略的反馈。

[0099] 在步骤706,装置300可以至少部分地基于网络性能结果和反馈来计算应用的信任值。

[0100] 在步骤708,装置300可以对信任值进行签名。

[0101] 在步骤710,装置300可以将签名的信任值提供给应用和/或软件定义网络的至少一个控制平面。

[0102] 在一个实施例中,至少一个网络性能监测器位于软件定义网络的数据平面中并且由网络性能监测器装置管理,并且在网络性能监测器装置和至少一个网络性能监测器之间应用信任维持和控制协议。

[0103] 在一个实施例中,网络性能结果由网络性能结果的提供者签名。

[0104] 在一个实施例中,网络性能结果的提供者将应用的身份添加到网络性能结果中。

[0105] 在一个实施例中,网络性能结果包括吞吐率、分组丢失概率和时间延迟中的至少一个。

[0106] 在相同的发明构思下,图8是示出根据本公开的实施例的用于SDN 中的信任管理的方法的流程图。方法800可以由装置400或500执行。对于与先前实施例中描述的相同的部分或功能,为简洁起见省略其描述。

[0107] 如图8所示,方法800可以从步骤802开始。在步骤802,装置400 或500可以接收由应用发布的网络策略。

[0108] 在步骤804,装置400或500可以获取应用的信任值,其中该信任值由信任评估装置至少部分地基于网络性能结果和针对网络策略的反馈来计算。

[0109] 在步骤806,装置400或500可以确定信任值是否高于阈值。

[0110] 在步骤808,装置400或500可以响应于信任值高于阈值来检查网络策略是否与已应用的网络策略冲突。

[0111] 在步骤820,如果信任值不高于阈值,则装置400或500可以拒绝网络策略。

[0112] 在步骤810,如果网络策略与已应用的网络策略冲突,则装置400 或500可以基于应用的优先级来确定是否应用网络策略。

[0113] 在步骤812,如果网络策略与已应用的网络策略不冲突,则装置400 或500可以应用网络策略。

[0114] 在相同的发明构思下,图9是示出根据本公开的另一实施例的用于SDN中的信任管理的方法的流程图。方法900可以由装置500执行。对于与先前实施例中描述的相同的部分或功能,为了简洁,省略其描述。

[0115] 如图9所示,方法900可以从步骤902开始。在步骤902,装置500可以接收由应用发布的网络策略。

[0116] 在步骤904,装置500可以获取应用的信任值,其中信任值由信任评估装置至少部

分地基于网络性能结果和针对网络策略的反馈来计算。

[0117] 在步骤906,装置500可以确定信任值是否高于阈值。

[0118] 在步骤908,装置500可以响应于信任值高于阈值来检查网络策略是否与已应用的网络策略冲突。在一个实施例中,装置500可以基于源 IP地址、目的IP地址、源端口和目的端口来检查网络策略是否与已应用的网络策略冲突。

[0119] 在步骤920,如果信任值不高于阈值,则装置500可以拒绝网络策略。

[0120] 在步骤909,装置500可以至少部分地基于信任值来计算应用的优先级。

[0121] 在步骤910,如果网络策略与已应用的网络策略冲突,则装置500 可以基于应用的优先级来确定是否应用网络策略。

[0122] 在一个实施例中,如果该应用的优先级高于已应用的网络策略的优先级,则用该网络策略替换已应用的网络策略;如果该应用的优先级低于已应用的网络策略的优先级,则拒绝该网络策略;或者,如果该应用的优先级等于已应用的网络策略的优先级,则在这种情况下,将已应用的网络策略和该网络策略发送给网络管理员,以进行最终决策或应用决定规则来自动设置网络策略。

[0123] 在步骤912,如果网络策略与已应用的网络策略不冲突,则装置 500可以应用网络策略。

[0124] 在一个实施例中,网络策略由应用签名,并且信任值由信任评估装置签名。

[0125] 注意,如图2-5所示的装置200、300、400和500的任何组件可以被实现为硬件或软件模块。在软件模块的情况下,它们可以体现在有形的计算机可读可记录存储介质上。例如,所有软件模块(或其任何子集)可以在同一介质上,或者每个软件模块可以在不同介质上。软件模块可以例如在硬件处理器或芯片上运行。然后可以使用如上所述的在硬件处理器上执行的不同软件模块来执行方法步骤。

[0126] 根据本公开的一方面,提供了一种用于认证的装置。所述装置包括被配置为在应用了由应用发布的网络策略之后收集网络性能结果的构件;以及被配置为收集针对所述网络策略的反馈的构件;以及被配置为至少部分地基于所述网络性能结果和所述反馈来计算所述应用的信任值的构件。

[0127] 在一实施例中,该装置还包括:被配置为确定至少一个网络性能监测器是否处于受信任状态的构件,其中,网络性能结果由至少一个网络性能监测器来监测;以及被配置为如果网络性能监测器不处于受信任状态,则丢弃网络性能监测器的网络性能结果的构件。

[0128] 在一个实施例中,至少一个网络性能监测器位于软件定义网络的数据平面中并且由网络性能监测器装置管理,以及在网络性能监测器装置和至少一个网络性能监测器之间应用信任维持和控制协议。

[0129] 在一个实施例中,网络性能结果由网络性能结果的提供者签名。

[0130] 在一个实施例中,网络性能结果的提供者将应用的身份添加到网络性能结果中。

[0131] 在一个实施例中,该装置还包括:被配置为从软件定义网络的至少一个控制平面接收应用的身份和网络策略的持续时间的构件;以及被配置为通过将持续时间与网络性能监测的时间匹配来将应用的身份添加到网络性能结果中的构件。

[0132] 在一个实施例中,网络性能结果包括吞吐率、分组丢失概率和时间延迟中的至少一个。

[0133] 在一个实施例中,该装置还包括:被配置为对信任值进行签名的构件;以及被配置为向应用和/或软件定义网络的至少一个控制平面提供签名的信任值的构件。

[0134] 根据本公开的另一方面,提供了一种用于认证的装置。所述装置包括被配置为接收由应用发布的网络策略的构件;被配置为获取所述应用的信任值的构件,其中,所述信任值由信任评估装置至少部分地基于网络性能结果和针对所述网络策略的反馈来计算;被配置为确定所述信任值是否高于阈值的构件;被配置为响应肯定的确定,检查所述网络策略是否已与应用的网络策略冲突的构件;被配置为如果所述网络策略与所述已应用的网络策略冲突,则根据所述应用的优先级确定是否应用所述网络策略的构件;或者,被配置为如果所述网络策略与所述已应用的网络策略不冲突,则应用所述网络策略的构件。

[0135] 在一个实施例中,该装置还包括:被配置为至少部分地基于信任值来计算应用的优先级的构件。

[0136] 在一个实施例中,该装置还包括:被配置为基于源IP地址、目的IP地址、源端口和目的端口来检查网络策略是否已与应用的网络策略冲突的构件。

[0137] 在一个实施例中,如果该应用的优先级高于已应用的网络策略的优先级,则用网络策略替换已应用的网络策略;如果该应用的优先级低于已应用的网络策略的优先级,则拒绝该网络策略;或者,如果该应用的优先级等于已应用的网络策略的优先级,则在这种情况下,将已应用的网络策略和该网络策略发送给网络管理员以做出最终决定,或者应用决定规则来自动设置网络策略。

[0138] 在一个实施例中,网络策略由应用签名,并且信任值由信任评估装置签名。

[0139] 另外,本公开的一方面可以利用在计算设备上运行的软件。这样的实现可以采用例如处理器、存储器和例如由显示器和键盘形成的输入/输出接口。如本文所使用的,术语“处理器”旨在包括任何处理设备,例如包括CPU(中央处理单元)和/或其他形式的处理电路的处理设备。此外,术语“处理器”可以指不止一个单独的处理器。术语“存储器”旨在包括与处理器或CPU相关联的存储器,例如,随机存取存储器(RAM)、只读存储器(ROM)、固定存储设备(例如,硬盘驱动器)、可移动存储设备(例如软盘)、闪存等。处理器、存储器以及诸如显示器和键盘之类的输入/输出接口可以例如经由作为数据处理元件的一部分的总线互连。适当的互连(例如通过总线)也可以提供给网络接口,例如网卡,其可以提供与计算机网络进行接口;以及介质接口,例如软盘或CD-ROM驱动器,其可以提供与介质进行接口。

[0140] 因此,如本文所述,包括用于执行本公开的方法的指令或代码的计算机软件可以存储在相关联的存储设备(例如,ROM、固定或可移动存储器)中,并且在准备好被使用时,被部分或全部加载(例如,加载到RAM中)并由CPU执行。这样的软件可以包括但不限于固件、常驻软件、微代码等。

[0141] 如所指出的,本公开的方面可以采取计算机程序产品的形式,计算机程序产品被体现在其上体现有计算机可读程序代码的计算机可读介质中。而且,可以利用计算机可读介质的任何组合。所述计算机可读介质可以是计算机可读信号介质或计算机可读存储介质。计算机可读存储介质可以是例如但不限于电子,磁性,光学,电磁,红外或半导体系统、装置或设备,或前述的任何适当组合。计算机可读存储介质的更具体示例(非详尽列表)将包括以下:具有一根或多根电线的电连接、便携式计算机软盘、硬盘、RAM、ROM、可擦可编程只读存储器存储器(EPROM或闪存)、光纤、便携式光盘只读存储器(CD-ROM)、光学存储设备、

磁存储设备或上述的任意合适组合。在本文的上下文中,计算机可读存储介质可以是任何有形介质,其可以包含或存储供指令执行系统、装置或设备使用或与其结合使用的程序。

[0142] 用于执行本公开的各方面的操作的计算机程序代码可以以至少一种编程语言的任意组合来编写,所述编程语言包括诸如Java,Smalltalk, C++之类的面向对象的编程语言以及常规的过程编程语言,例如“C”编程语言或类似的编程语言。程序代码可以完全在用户计算机上、作为独立软件包而部分在用户计算机上、部分在用户计算机上并且部分在远程计算机上、或者完全在远程计算机或服务器上执行。

[0143] 本公开中描述的实施例具有以下优点:

[0144] 有效性:实施例可以解决应用平面中的应用与控制平面中的控制器之间的信任缺失。它提供了一种信任评估和管理机制以协助控制平面判断和选择应用提供的流规则或网络策略。

[0145] 细粒度的流规则选择:可以基于应用的信任值来计算应用的优先级。将其他影响因素包括在计算中也很灵活。因此,本公开的实施例可以支持细粒度的流规则选择。

[0146] 可扩展性:实施例可以支持多个控制平面以及大数据。应用ID被附加到由探测器收集的数据中,即使TE模块102收集了大量数据,也可以大大提高信任评估效率。

[0147] 可信赖性:通过应用信任维持和控制机制,以可信赖的方式执行网络性能监测。可以在TE模块102和NPM模块104之间对探测器提供的数据的可信性进行验证。在信任评估阶段,可以使用仅来自可信探测器的数据。当应用向控制平面提供流规则时,控制平面将验证应用的信任值。只有受信任的应用才有资格发布网络策略。网络策略的最终选择基于应用的信任值。最终可以选择并应用最值得信赖的应用的网络策略。

[0148] 附图中的流程图和框图示出了根据本公开的各种实施例的系统,方法和计算机程序产品的可能实现的架构、功能和操作。就这一点而言,流程图或框图中的每个框可以代表代码的模块、组件、段或部分,其包括至少一个用于实现指定的逻辑功能的可执行指令。还应注意,在一些替代实施方式中,方框中指出的功能可以不按图中指出的顺序发生。例如,取决于所涉及的功能,实际上可以基本上同时执行连续示出的两个框,或者有时可以以相反的顺序执行这些框。还应注意,框图和/或流程图说明的每个方框以及框图和/或流程图说明中的方框的组合可以由执行指定功能或动作的基于专用硬件的系统、或专用硬件和计算机指令的组合来实现。

[0149] 在任何情况下,应理解,本公开中示出的组件可以以各种形式的硬件、软件或其组合来实现,例如,专用集成电路(ASIC)、功能电路、具有相关存储器的经过适当编程的通用数字计算机等。给定本文提供的本公开的教导,相关领域的普通技术人员将能够考虑本公开的组件的其他实施方式。

[0150] 本文所使用的术语仅是出于描述特定实施例的目的,并不旨在限制本公开。如本文所使用的,单数形式“一”,“一个”和“该”也旨在包括复数形式,除非上下文另外明确指出。将理解的是,尽管这里可以使用术语第一,第二等来描述各种元件,但是这些元件不应受到这些术语的限制。这些术语仅用于区分一个元件和另一个元件。例如,在不脱离实施例的范围的情况下,第一元件可以被称为第二元件,并且类似地,第二元件可以被称为第一元件。还将理解的是,当在本说明书中使用时,术语“包括”,“包含”和/或“含有”规定了所述特征、整数、步骤、操作、元件和/或组件的存在,但是不排除存在或增加另一个特征、整

数、步骤、操作、元件、组件和/或其组合。

[0151] 已经出于说明的目的给出了各种实施例的描述,但是这些描述并不旨在是穷举的或限于所公开的实施例。在不脱离所描述的实施例的范围和精神的情况下,许多修改和变型对于本领域普通技术人员将是显而易见的。

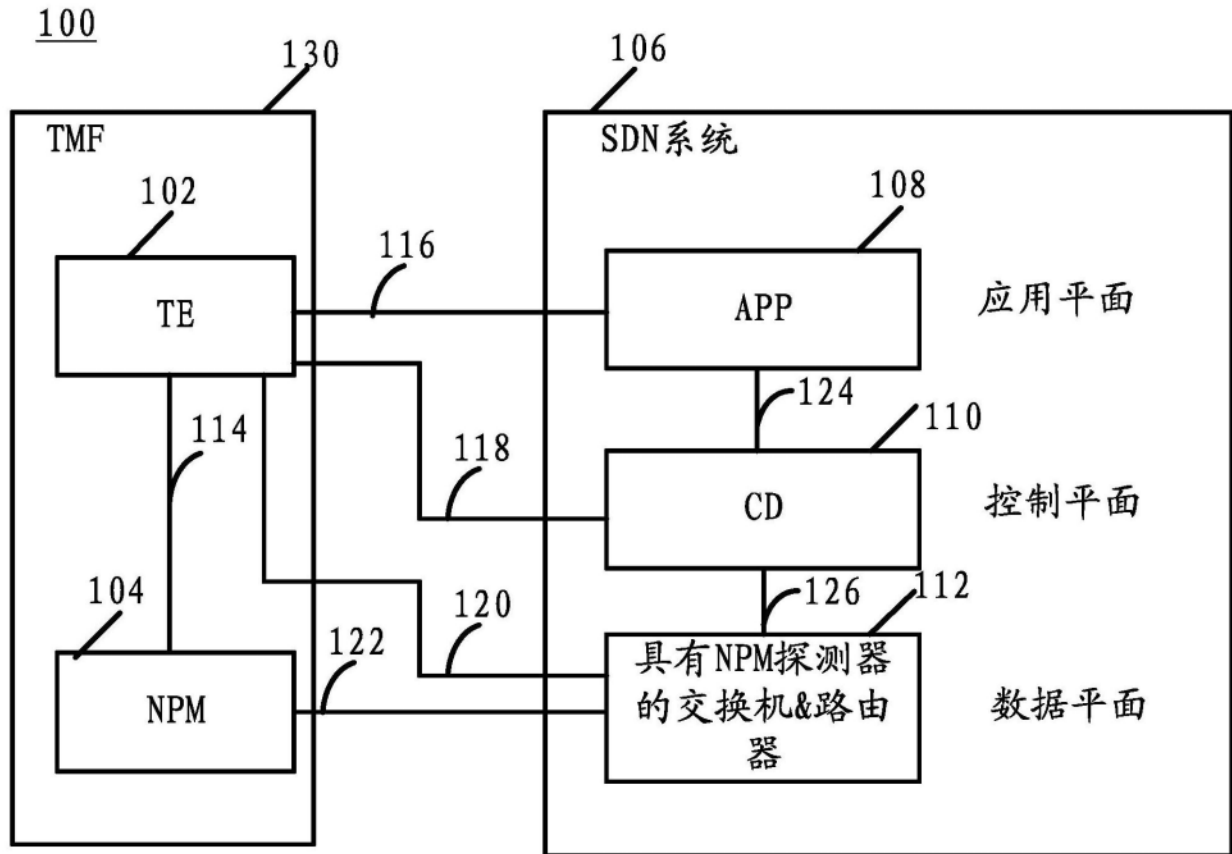


图1

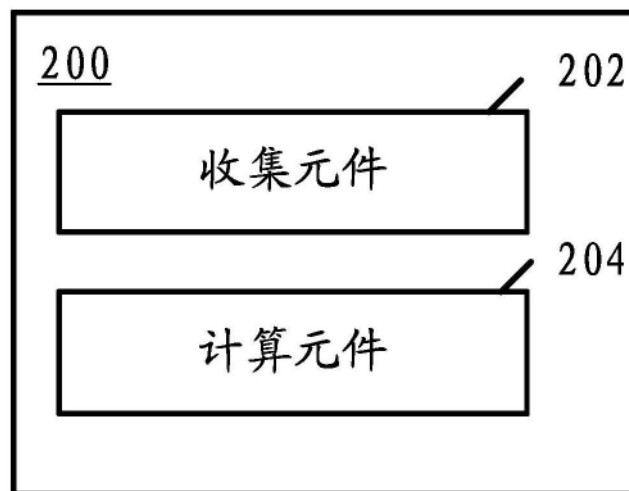


图2

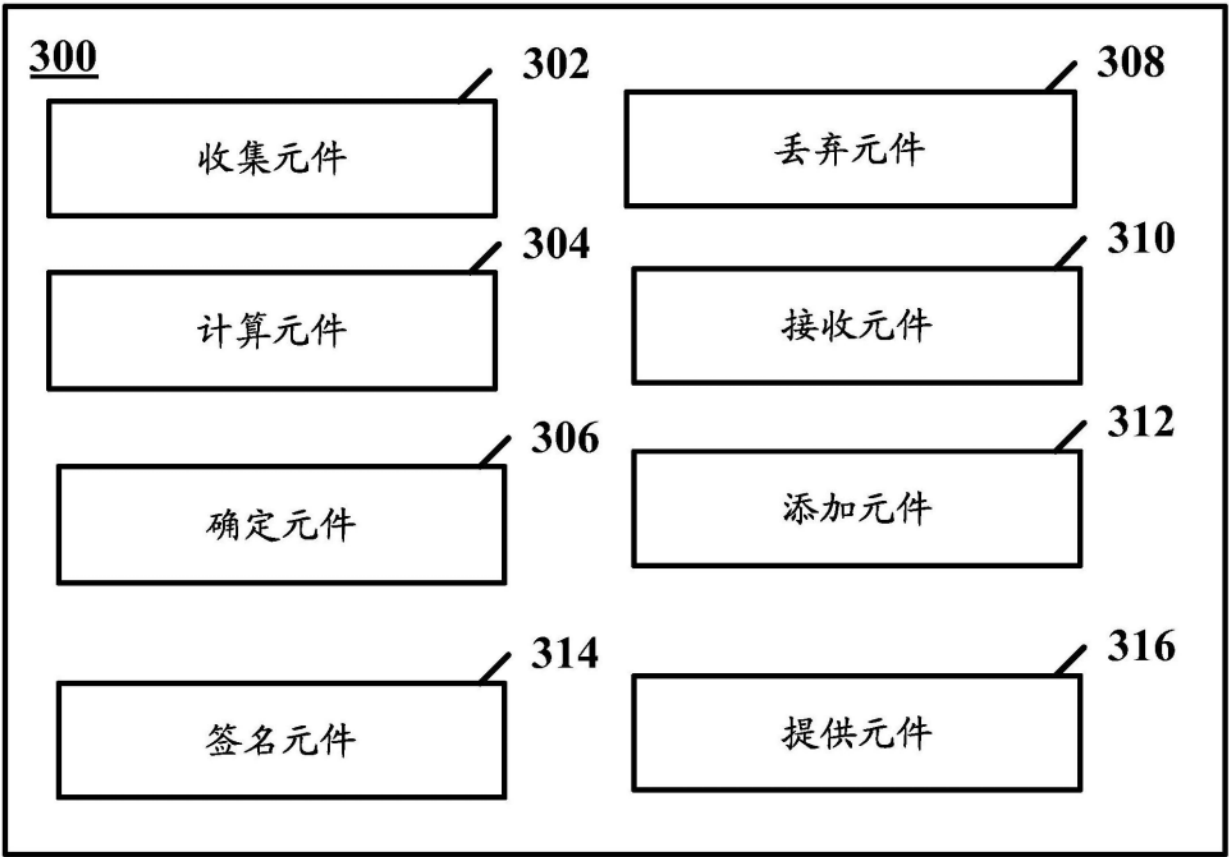


图3

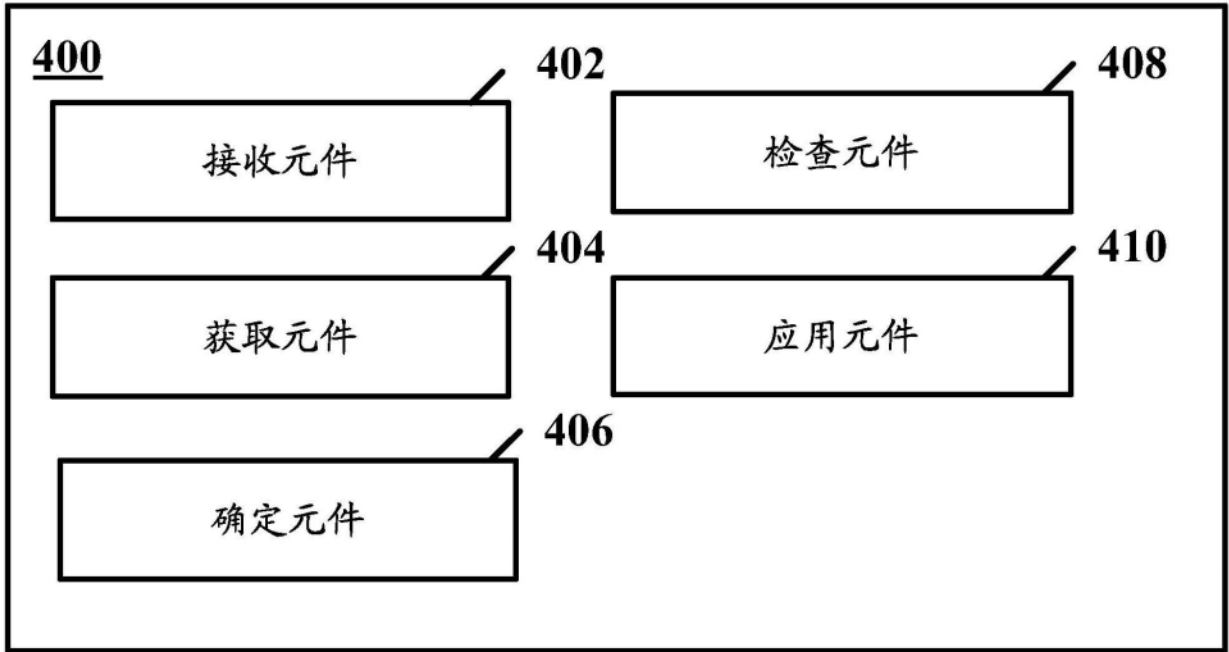


图4

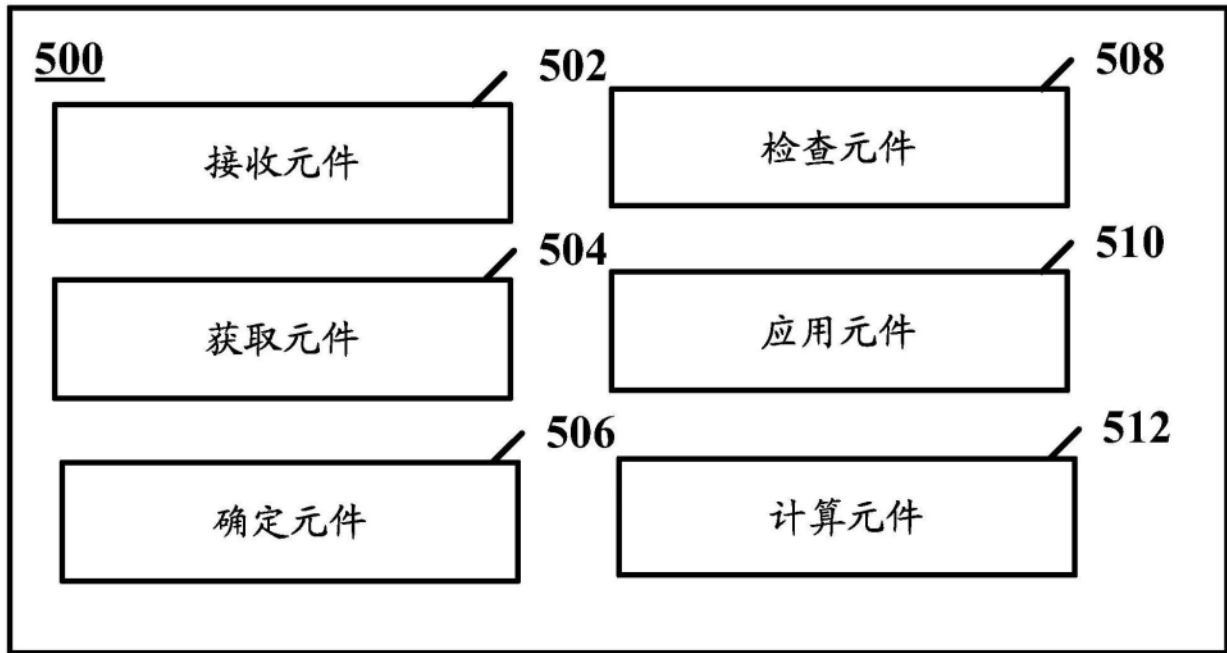


图5

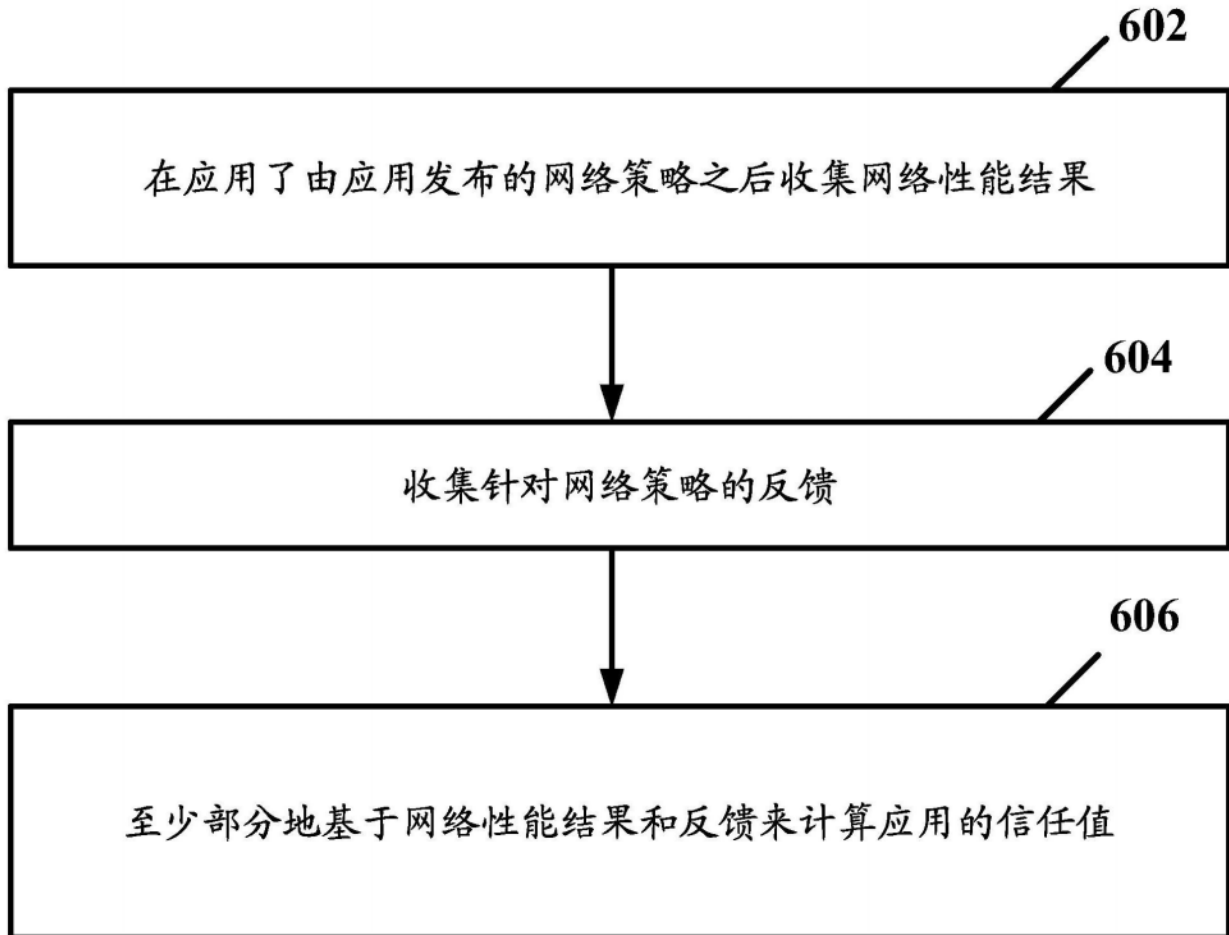
600

图6

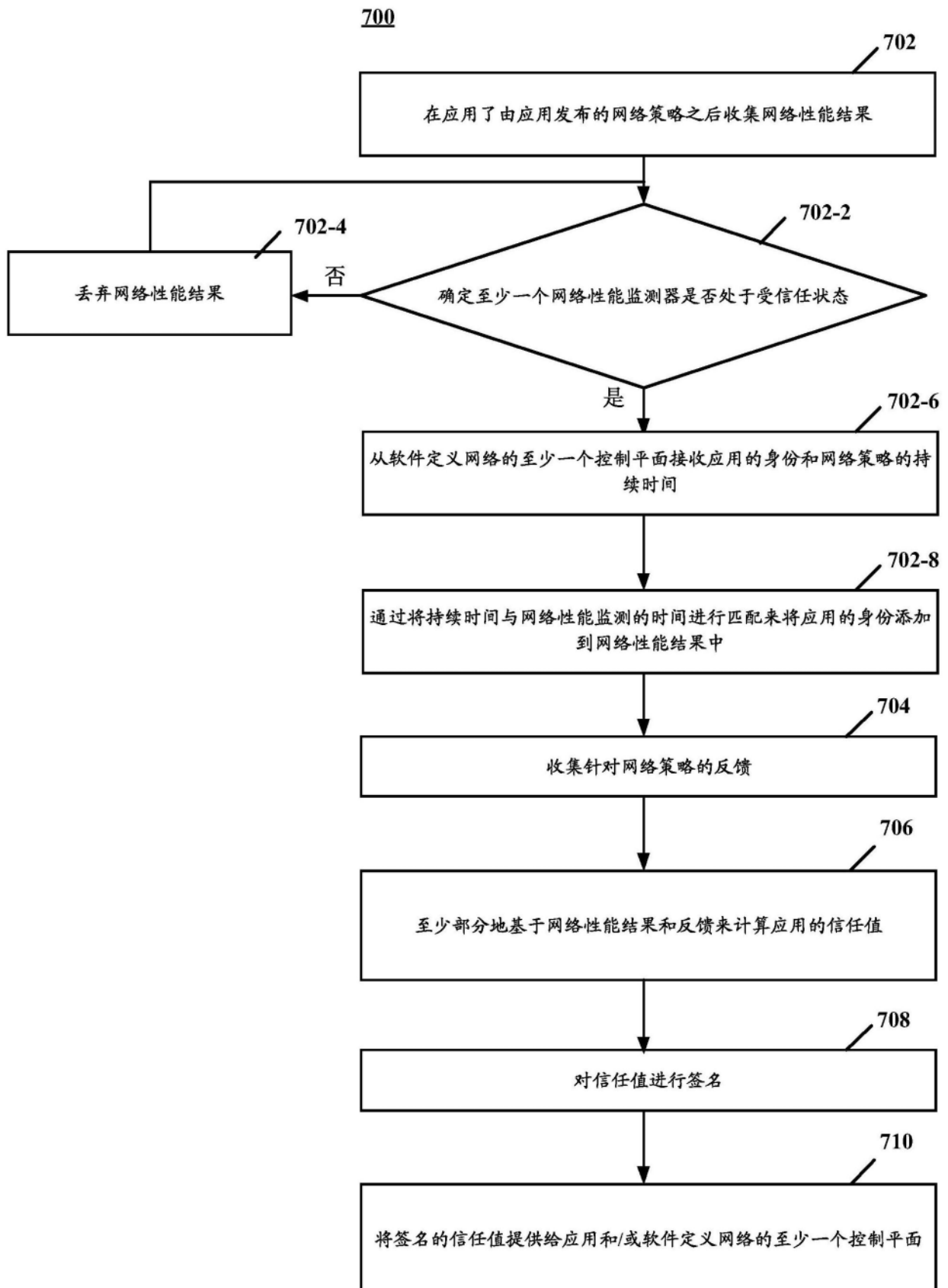


图7

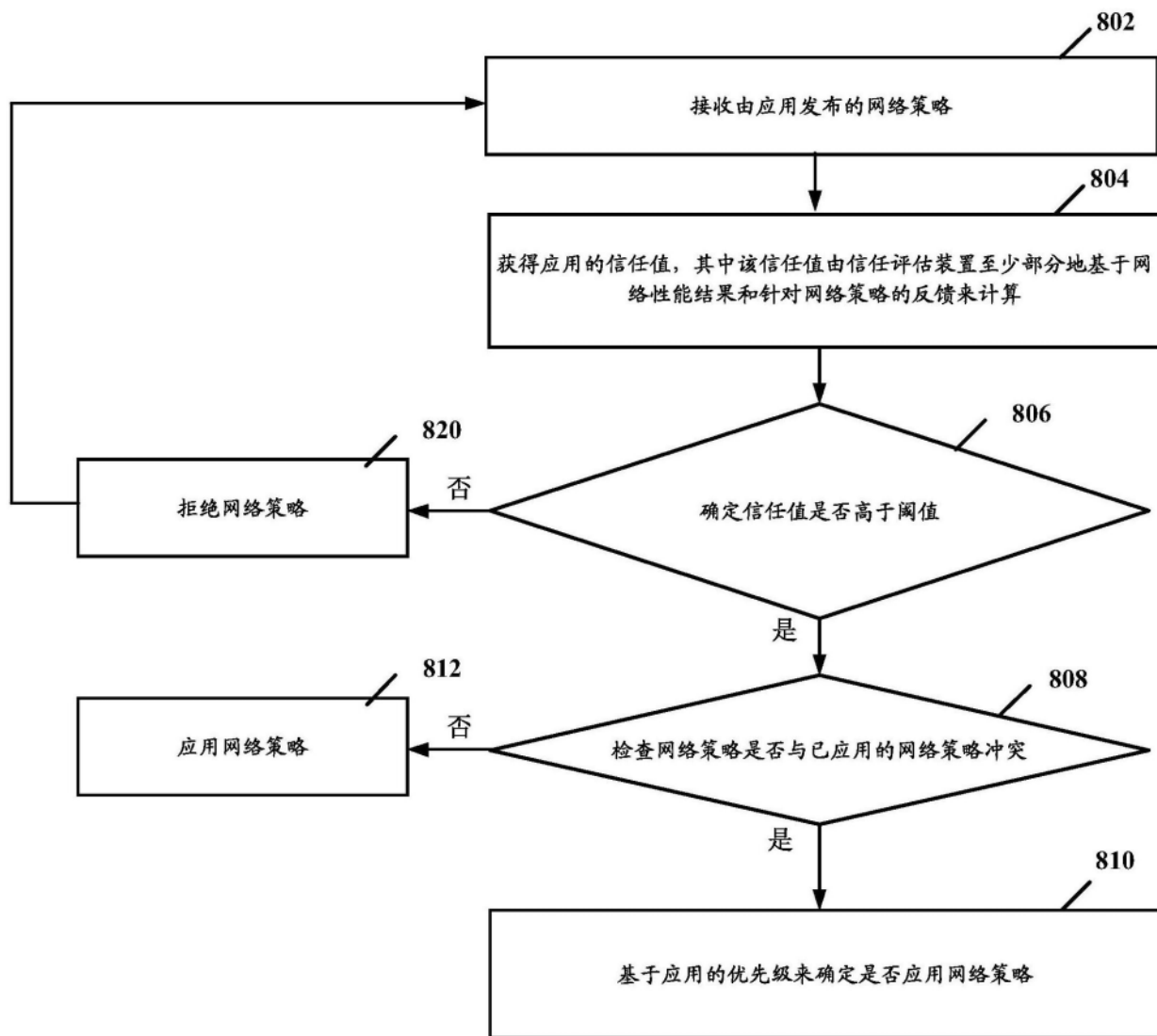
800

图8

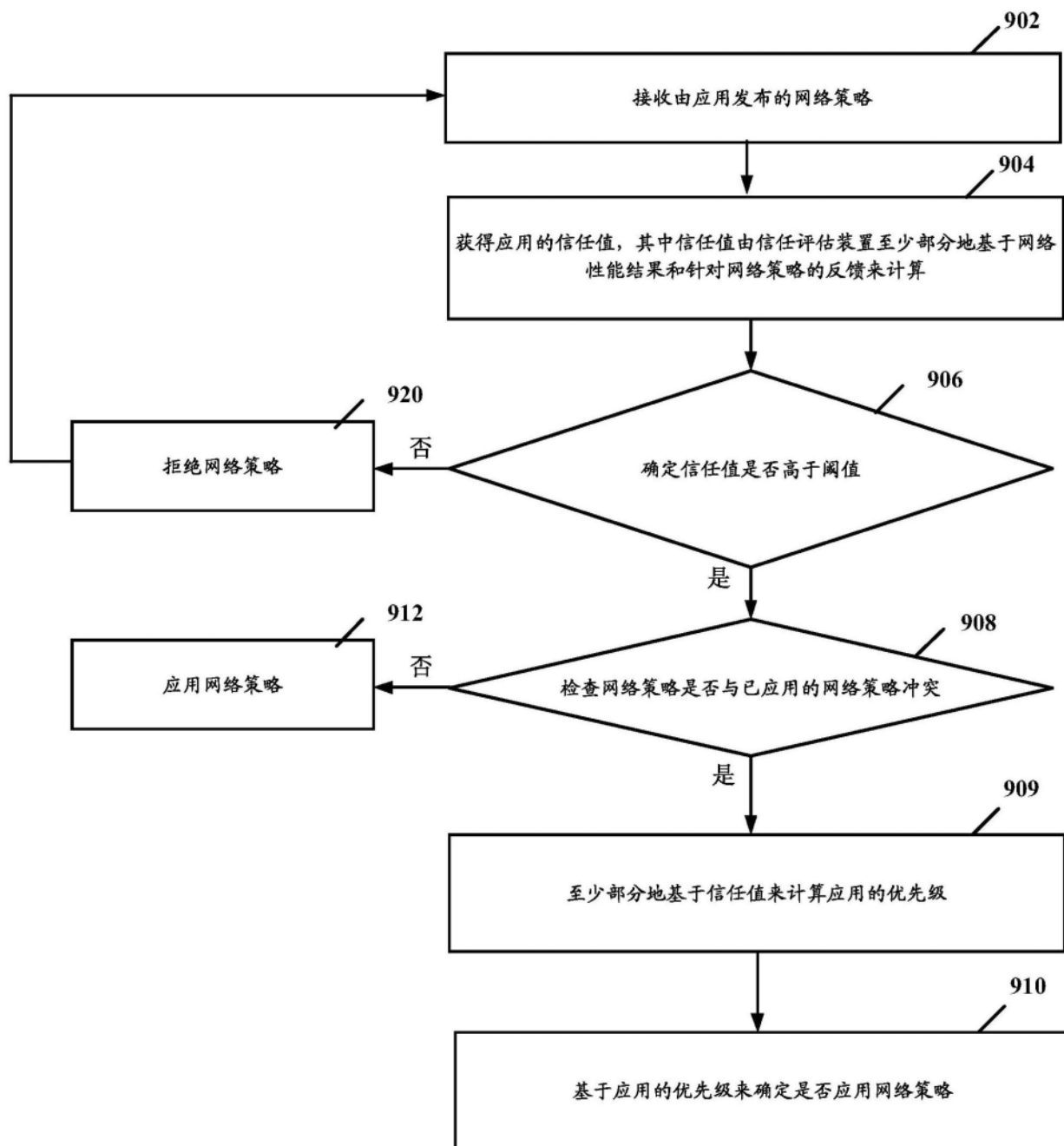
900

图9