(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 109768955 B
(45)授权公告日 2021.08.17

(21)申请号 201811330660.0

(22)申请日 2018.11.09

(65)同一申请的已公布的文献号
申请公布号 CN 109768955 A

(43)申请公布日 2019.05.17

(30)优先权数据
10-2017-0149532 2017.11.10 KR

(73)专利权人 高丽大学校产学协力团
地址 韩国首尔市城北区安岩路145高丽大学校(安岩洞五街)

(72)发明人 朴鎭雨 洪起元

(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
代理人 马爽 臧建明

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

(56)对比文件
US 2018234454 A1,2018.08.16
CN 104506531 A,2015.04.08
CN 105791205 A,2016.07.20
CN 107968785 A,2018.04.27

审查员 高伟

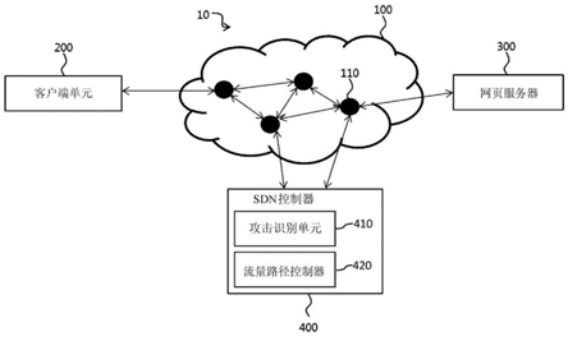
权利要求书2页 说明书13页 附图3页

(54)发明名称

基于软件定义网络防御分布式拒绝服务攻击的系统及方法

(57)摘要

提供一种基于软件定义网络防御分布式拒绝服务攻击的系统及其方法。根据本发明,当疑似攻击的HTTP请求消息到达网页服务器时,网页服务器将HTTP请求消息发送到位于网络中的软件定义网络控制器,且软件定义网络控制器而非为攻击目标的网页服务器确定分布式拒绝服务攻击且根据软件定义网络控制器的确定结果通过网络上的节点阻挡来自攻击者的流量。由此,将耗尽网页服务器的可用连接资源的疑似为分布式拒绝服务攻击的流量输入到软件定义网络控制器而非网页服务器。由此,可保护网页服务器免受分布式拒绝服务攻击且可确保对网页服务器的正常操作的维护。



CN 109768955 B

1.一种基于软件定义网络防御分布式拒绝服务攻击的方法,所述方法包括:

通过网页服务器将从客户端单元传输的不完整HTTP请求消息发送到软件定义网络控制器;

通过所述软件定义网络控制器将流量路径改变请求消息传输到一或多个软件定义网络节点,所述流量路径改变请求消息包含用于将所述不完整HTTP请求消息的目的地及随后HTTP消息的目的地从所述网页服务器改变为所述软件定义网络控制器的信息,其中所述随后HTTP消息紧跟在所述不完整HTTP请求消息之后且从所述客户端单元传输;

通过所述软件定义网络控制器确定从所述客户端单元传输的所述不完整HTTP请求消息是否是对所述网页服务器的攻击;

当所述不完整HTTP请求消息确认为正常HTTP请求消息时,通过所述软件定义网络控制器将恢复请求消息传输到所述一或多个软件定义网络节点,所述恢复请求消息包含用于将所述不完整HTTP请求消息的所述目的地及所述随后HTTP消息的所述目的地从所述软件定义网络控制器改变为所述网页服务器的信息,以便恢复所述客户端单元与所述网页服务器之间的信息传输路径;

当所述不完整HTTP请求消息确认为对所述网页服务器的所述攻击的消息时,通过所述软件定义网络控制器将丢弃请求消息传输到所述一或多个软件定义网络节点,所述丢弃请求消息包含在所述一或多个软件定义网络节点处丢弃所述不完整HTTP请求消息及所述随后HTTP消息的请求;以及

基于所述丢弃请求消息,通过所述一或多个软件定义网络节点丢弃所述不完整HTTP请求消息及所述随后HTTP消息。

2.根据权利要求1所述的基于软件定义网络防御分布式拒绝服务攻击的方法,还包括:

基于所述丢弃请求消息,通过所述一或多个软件定义网络节点将所述不完整HTTP请求消息及所述随后HTTP消息转发到所述网页服务器;以及

通过所述网页服务器接收所述不完整HTTP请求消息及所述随后HTTP消息。

3.根据权利要求1所述的基于软件定义网络防御分布式拒绝服务攻击的方法,其中所述丢弃请求消息包含所述客户端单元的源IP信息、目的地IP信息、源端口信息以及目的地端口信息中的至少一个。

4.一种基于软件定义网络防御分布式拒绝服务攻击的系统,所述系统包括:

软件定义网络;

网页服务器,配置成将不完整HTTP请求消息发送到软件定义网络控制器,所述不完整HTTP请求消息从客户端单元传输;

所述软件定义网络控制器,配置成

将流量路径改变请求消息传输到一或多个软件定义网络节点,所述流量路径改变请求消息包含用于将所述不完整HTTP请求消息的目的地及随后HTTP消息的目的地从所述网页服务器改变为所述软件定义网络控制器的信息,其中所述随后HTTP消息紧跟在所述不完整HTTP请求消息之后且从所述客户端单元传输,

确定从所述客户端单元传输的所述不完整HTTP请求消息是否是对所述网页服务器的攻击,

当所述不完整HTTP请求消息确认为正常HTTP请求消息时,将恢复请求消息传输到所述

一或多个软件定义网络节点,所述恢复请求消息包含用于将所述不完整HTTP请求消息的所述目的地及所述随后HTTP消息的所述目的地从所述软件定义网络控制器改变为所述网页服务器的信息,以便恢复所述客户端单元与所述网页服务器之间的信息传输路径,以及

当所述不完整HTTP请求消息确认为对所述网页服务器的所述攻击的消息所述攻击时,将丢弃请求消息传输到所述一或多个软件定义网络节点,所述丢弃请求消息包含丢弃所述不完整HTTP请求消息及所述随后HTTP消息的请求;以及

所述一或多个软件定义网络节点,配置成

基于所述流量路径改变请求消息将所述不完整HTTP请求消息及所述随后HTTP消息发送到所述软件定义网络控制器,以及

基于所述丢弃请求消息丢弃或阻挡所述不完整HTTP请求消息及所述随后HTTP消息。

5.根据权利要求4所述的基于软件定义网络防御分布式拒绝服务攻击的系统,其中所述网页服务器配置成在将所述不完整HTTP请求消息发送到所述软件定义网络控制器之后中断由所述客户端单元请求的所有任务或终止与所述客户端单元的连接。

6.根据权利要求4所述的基于软件定义网络防御分布式拒绝服务攻击的系统,其中所述软件定义网络控制器配置成

接收所述不完整HTTP请求消息及所述随后HTTP消息,以及

将针对所述不完整HTTP请求消息及所述随后HTTP消息的HTTP响应消息传输到所述客户端单元。

7.根据权利要求4所述的基于软件定义网络防御分布式拒绝服务攻击的系统,其中所述一或多个软件定义网络节点配置成基于所述恢复请求消息将所述不完整HTTP请求消息及所述随后HTTP消息转发到所述网页服务器,且所述网页服务器配置成通过经恢复路径接收所述不完整HTTP请求消息及所述随后HTTP消息,且将针对所述不完整HTTP请求消息及所述随后HTTP消息的HTTP响应消息传输到所述客户端单元。

基于软件定义网络防御分布式拒绝服务攻击的系统及方法

[0001] 相关申请案的交叉参考

[0002] 本申请基于且要求2017年11月10日在韩国知识产权局提交的第10-2017-0149532号韩国专利申请的优先权,所述申请的整个公开内容以引用的方式并入本文中。

技术领域

[0003] 本发明涉及一种基于软件定义网络(software-defined networking,SDN)使网页服务器抵御HTTP DDoS攻击的系统及其方法,且更确切地说涉及基于SDN防御DDoS攻击的系统及其方法,其中当疑似攻击的HTTP请求消息到达网页服务器时,网页服务器将疑似攻击的所述HTTP请求消息发送到位于网络中的SDN控制器,且所述SDN控制器而非为攻击目标的网页服务器确定所述HTTP请求信息是否是DDoS攻击,且根据确定结果通过网络上的节点(替代地,路由器)阻挡来自攻击者的流量。

背景技术

[0004] 分布式拒绝服务(distributed denial of service,DDoS)攻击是其中攻击者使用许多感染了恶意代码的僵尸PC来传输可使攻击目标系统超负荷或可占用大量连接资源以劣化目标系统的效能的大量流量,由此妨碍正常因特网服务的攻击。

[0005] 在过去,对网络/传输层的HTTP DDoS攻击(其产生大型或快速数据包),例如TCP/UDP/ICMP洪泛攻击,已经是主导的。

[0006] 因为这些攻击就体积及速度来说与由正常客户端产生的流量模式相比具有异常流量模式,所以各种基于网络的DDoS防御方法已经开发且应用,所述方法通过分析输入到例如交换机及路由器的网络装置的流量模式检测DDoS攻击且阻挡所检测到的攻击。

[0007] 然而,近年来,由于具有由正常客户端产生的类似业务模式的攻击流量已极大地增加,所以应用层DDoS攻击变得极难以准确地检测且使得预先存在的基于网络的DDoS保护技术无效。

[0008] 应用层HTTP DDoS攻击的典型实例为蜂猴(Slowloris)攻击及呈缓慢HTTP DDoS攻击形式的缓慢HTTP POST DDoS攻击,所述攻击滥用HTTP脆弱性且耗尽网页服务器的可用连接资源。缓慢HTTP DDoS攻击滥用HTTP脆弱性,其中通过传输不完整HTTP请求消息接收不完整HTTP请求消息的网页服务器需要维持连接直到HTTP请求消息完整为止。在此攻击中,攻击者在通过TCP三向信号交换建立与网页服务器的正常TCP连接作为攻击目标之后将不完整HTTP请求消息传输到网页服务器。接收不完整HTTP请求消息的网页服务器维持所述连接直到连续地传输所接收到的不完整HTTP请求消息的HTTP请求消息完整为止。然而,攻击者通过传输连续传输的不完整HTTP请求消息来长时间维持与网页服务器建立的连接。如果攻击者传输大量不完整HTTP请求消息且占用攻击目标网页服务器的大部分连接及信息处理资源,那么对应网页服务器的服务质量劣化。

[0009] 蜂猴攻击及缓慢HTTP POST DDoS攻击根据攻击者所传输的不完整HTTP请求消息的类型分类。在蜂猴攻击中,攻击者传输包含不完整HTTP报头的HTTP GET请求消息。在HTTP

消息中，报头与主体由新行字符“分隔，且在蜂猴攻击中，攻击者异常操纵HTTP消息以将具有HTTP报头而无新行字符的HTTP GET请求消息连续地传输到网页服务器。接收HTTP GET请求消息的网页服务器等待同时维持所述连接，直到接收用“终止的完整HTTP报头为止。攻击者每隔一定间隔将具有不完整HTTP报头的HTTP消息传输到网页服务器以长时间保持网页服务器的连接。因此，网页服务器占用可用的连接资源，且网页服务器处于无法提供到客户端的连接的状态中。

[0010] 缓慢POST DDoS攻击允许攻击者异常操纵HTTP POST请求消息且在很长时间段内将待传输的大量数据传输到网页服务器。HTTP POST请求消息的报头中的内容长度字段限定包含于HTTP POST请求消息的主体中的数据的大小，且网页服务器维持连接直到接收所有对应于所接收到的HTTP POST请求消息的内容长度字段值的数据为止。通过滥用此点，攻击者将HTTP POST请求消息中的内容长度字段值设定成极大值，且仅传输包含于实际传输的HTTP消息中的极小数据以维持网页服务器免于终止用于接收对应数据的连接。如果攻击者占用许多连接以达到网页服务器的最大数目连接，那么网页服务器将不能够向正常客户端提供连接，从而导致服务失败。

[0011] 目前，为了防御HTTP DDoS攻击，已经尝试通过设置网页服务器限制每特定传输IP地址的最大并行连接数目来防止攻击者占用网页服务器的可用连接资源。然而，如果攻击者利用多个僵尸PC，且每一僵尸PC维持少于网页服务器所允许的并行连接的最大数目的连接，那么攻击者可占用到网页服务器的大部分连接。因此，针对HTTP DDoS攻击的有效防御结果不可由所述方法预期。

[0012] 另外，网页服务器可设定计时器以用于接收HTTP请求消息来防御HTTP DDoS攻击。举例来说，当来自客户端的HTTP请求消息在阿帕奇(Apache)网页服务器的mod_reqtimeout模块的RequestReadTimeout指示符的特定时间内并不完整时，网页服务器有可能确定HTTP请求消息为DDoS攻击。然而，DDoS攻击可仅在由网页服务器设定的计时器期满之后确认，使得网页服务器的可用连接由攻击者占用直到网页服务器意识到攻击为止。同时，网页服务器可不再接受来自正常客户端的导致服务质量劣化的HTTP请求。

[0013] 到目前为止，对HTTP DDoS攻击的防御取决于服务器侧防御机构以通过网页服务器功能的适当设定检测及防御网页服务器中的攻击。然而，在服务器侧操作的DDoS防御机构在使网页服务器的效能劣化之前不能检测及阻挡攻击流量。另外，用于从攻击源到攻击目标系统的连接的网络资源被浪费。

[0014] 优选的HTTP DDoS防御机构为基于网络的DDoS防御机构，其检测网络装置(例如流量交换机或网络路由器)中的DDoS攻击，其中DDoS攻击流量经识别且在网络的中间路径处经阻挡而并不到达网页服务器。然而，HTTP DDoS攻击消息在例如交换机或路由器的网络装置处难以辨别，这是因为HTTP DDoS攻击流量就流量大小、模式以及速度来说非常类似于来自正常客户端的流量。

发明内容

[0015] 本发明的一个目的在于提供一种基于SDN使网页服务器抵御HTTP DDoS攻击的系统及其方法，其中当疑似攻击的HTTP请求消息到达网页服务器时，网页服务器将疑似攻击的HTTP请求消息发送到位于网络中的SDN控制器。SDN控制器而非为攻击目标的网页服务器

确定HTTP请求消息是否是DDoS攻击。当HTTP请求消息由SDN控制器确定为攻击流量时，SDN控制器操纵网络节点(替代地，路由器)来阻挡攻击流量，以使得攻击流量并不到达目标网页服务器。

[0016] 本发明的另一个目的在于提供一种基于SDN保护网页服务器的正常操作免受DDoS攻击的系统及其方法。在SDN控制器从网页服务器接收疑似HTTP请求消息之后，SDN控制器立即将流量路径改变请求消息传输到网络中的SDN节点以接收随后从可疑客户端单元而非网页服务器传输的HTTP请求消息。通过SDN控制器对对应HTTP请求消息是DDoS攻击还是正常网页服务的确定的结果，SDN控制器将流量路径改变请求消息传输到SDN节点以阻挡属于对应HTTP请求消息的后续流量或恢复正常网页服务的流量路径。

[0017] 本发明的示例性实施例提供一种基于SDN防御DDoS攻击的方法，所述方法包含：当从客户端单元传输的HTTP请求消息确定为疑似攻击的不完整HTTP请求消息时，通过网页服务器将HTTP请求消息发送到SDN控制器；通过SDN控制器将第一流量路径改变请求消息传输到一或多个SDN节点，所述第一流量路径改变请求消息包含用于将紧跟在从客户端单元传输到作为目的地的网页服务器的HTTP请求消息之后的HTTP消息的目的地从网页服务器改变为SDN控制器的信息；通过SDN控制器确定从客户端单元传输的不完整HTTP请求消息是否是攻击；当作为确认结果将HTTP请求消息确认为以攻击为目标的HTTP请求时，通过SDN控制器将第三流量路径改变请求消息传输到一或多个SDN节点以请求在一或多个SDN节点处丢弃从作为攻击者的客户端单元传输到作为目的地的网页服务器的消息；以及基于第三流量路径改变请求消息，通过一或多个SDN节点丢弃HTTP请求消息及紧跟在从客户端单元传输到作为目的地的网页服务器的HTTP请求消息之后的HTTP消息。

[0018] 方法可更包含：当疑似攻击的不完整HTTP请求消息确认为正常HTTP请求消息时，通过SDN控制器将第二流量路径改变请求消息传输到一或多个SDN节点，所述第二流量路径改变请求消息包含用于将紧跟在从客户端单元传输的HTTP请求消息之后的HTTP消息的目的地从SDN控制器改变为网页服务器的信息，以便恢复客户端单元与网页服务器之间的信息传输路径；基于第二流量路径改变请求消息，通过一或多个SDN节点将紧跟在从客户端单元传输到作为目的地的网页服务器的HTTP请求消息之后的HTTP消息转发到网页服务器；以及通过网页服务器接收紧跟在从客户端单元传输的HTTP请求消息之后的HTTP消息。

[0019] 第三流量路径改变请求消息可包含作为攻击者的客户端单元的源IP信息、目的地IP信息、源端口信息以及目的地端口信息中的至少一个。

[0020] 本发明的另一示例性实施例提供一种基于SDN防御DDoS攻击的系统，所述系统包含：SDN网络；客户端单元，其通过SDN网络将HTTP请求消息传输到作为目的地的网页服务器；网页服务器，其在从客户端单元传输的HTTP请求消息确定为疑似攻击的不完整HTTP请求消息时将HTTP请求消息发送到SDN控制器；SDN控制器，其将第一流量路径改变请求消息传输到一或多个SDN节点，所述第一流量路径改变请求消息包含用于将紧跟在从客户端单元传输到作为目的地的网页服务器的HTTP请求消息之后的HTTP消息的目的地从网页服务器改变为SDN控制器的信息，且当疑似攻击的不完整HTTP请求消息确认为以攻击为目标时，将第三流量路径改变请求消息传输到一或多个SDN节点以丢弃从作为攻击者的客户端单元传输到作为目的地的网页服务器的消息；以及一或多个SDN节点，其基于第三流量路径改变请求消息，丢弃或阻挡HTTP请求消息及紧跟在从客户端单元传输到作为目的地的网页服务

器的HTTP请求消息之后的HTTP消息。

[0021] 在将从客户端单元传输的疑似攻击的不完整HTTP请求消息发送到SDN控制器之后,网页服务器可中断由客户端单元请求的所有任务或终止与客户端单元的连接。

[0022] 一或多个SDN节点可基于第一流量路径改变请求消息将HTTP请求消息及紧跟在从客户端单元传输到作为目的地的网页服务器的HTTP请求消息之后的HTTP消息发送到SDN控制器,且SDN控制器可接收HTTP请求消息及紧跟在从客户端单元传输的HTTP请求消息之后的HTTP消息,且将针对HTTP请求消息及紧跟在所接收到的HTTP请求消息之后的HTTP消息的HTTP响应消息传输到客户端单元。

[0023] 在疑似攻击的不完整HTTP请求消息确认为正常HTTP请求消息时,SDN控制器可将第二流量路径改变请求消息传输到一或多个SDN节点,所述第二流量路径改变请求消息包含用于将紧跟在从客户端单元传输的HTTP请求消息之后的HTTP消息的目的地从SDN控制器改变为网页服务器的信息,以便恢复客户端单元与网页服务器之间的信息传输路径。

[0024] 一或多个SDN节点可基于第二流量路径改变请求消息将HTTP请求消息及紧跟在从客户端单元传输到作为目的地的网页服务器的HTTP请求消息之后的HTTP消息转发到网页服务器,且网页服务器可通过所恢复路径接收HTTP请求消息及紧跟在从客户端单元传输的HTTP请求消息之后的HTTP消息,且将针对HTTP请求消息及紧跟在所接收到的HTTP请求消息之后的HTTP消息的HTTP响应消息传输到客户端单元。

[0025] 根据本发明,当疑似攻击的HTTP请求消息到达网页服务器时,网页服务器将疑似攻击的HTTP请求消息传输到位于网络中的SDN控制器,且所述SDN控制器,而非为攻击目标的网页服务器,确定疑似攻击的HTTP请求消息是否是DDoS攻击,且通过网络上的节点(替代地,路由器)阻挡来自攻击者的流量。此外,将耗尽网页服务器的可用连接资源的疑似为DDoS攻击的流量输入到SDN控制器而非网页服务器,由此保护网页服务器免受DDoS攻击且确保对网页服务器的正常操作的维护。

[0026] 此外,当疑似攻击的HTTP请求消息到达网页服务器时,紧接在SDN控制器从网页服务器接收HTTP请求消息之后,SDN控制器将流量路径改变请求消息传输到SDN节点以接收随后从客户端单元而非网页服务器传输的HTTP消息,且根据对应HTTP请求消息是否是DDoS攻击的确定结果恢复流量路径或通过SDN节点阻挡对应流量,以使得来自所检测到的DDoS攻击者的流量在到达网页服务器之前被阻挡,由此防止连接到网页服务器的流量连接及网络路径中的占用带宽的浪费。

附图说明

[0027] 通过以下结合附图进行的详细描述将更加清楚地了解本发明的上文和其它方面、特征和其它优点,其中:

[0028] 图1是示出根据本发明的示例性实施例的基于SDN防御DDoS攻击的系统的配置的框图。

[0029] 图2和图3示出根据本发明的示例性实施例的基于SDN防御DDoS攻击的方法的流程图。

具体实施方式

[0030] 本发明中所使用的技术术语仅用于描述特定实施例，且并不意图限制本发明。此外，除非在本发明中另外限定，否则本发明中所使用的技术术语应解译为所属领域的技术人员通常理解的含义而不应解译为过度全面含义或过度简化含义。此外，当本发明中所使用的技术术语为并未准确地表达本发明的精神的错误技术术语时，应理解，所述技术术语被所属领域的技术人员可恰当地理解的技术术语取代。另外，本发明中所使用的一般术语应解译为限定在词典或情境中，而不应解译过度简化含义。

[0031] 此外，本发明中所使用的单数表达包含复数表达，除非在上下文中具有明确相反的含义。在本发明中，例如“包括”或“包含”的术语不应解译为必需包含本发明中揭示的所有各种组件或各种步骤，且应解译为可能并未包含其中的某一组件或一些步骤或可另外包含额外组件或步骤。

[0032] 此外，包含普通数字(例如第一及第二等等)的术语用于描述各种组件，但组件不受所述术语限制。上文术语仅用于区别一个组件与其它组件。举例来说，在不脱离本发明的范围的情况下，第一组件可被称为第二组件，且类似地，第二组件可被称为第一组件。

[0033] 下文中，将参考附图详细描述本发明的优选实施例，其中相同附图标号指代相同或类似元件，无论附图标号如何，且将省略其重复描述。

[0034] 此外，在以下描述中，可省略对已知相关联技术的详细解译以避免不必要地混淆本发明的主题。此外，应注意，附图仅用于容易地理解本发明的精神，且不应解译为本发明的精神受附图限制。

[0035] 图1是示出根据本发明的示例性实施例的基于SDN防御DDoS攻击的系统10的配置的框图。

[0036] 如图1中所示出，基于SDN防御DDoS攻击的系统10由SDN网络100、客户端单元200、网页服务器300以及SDN控制器400配置。图1中所示出的防御系统10的所有组件并非所需组件，且防御系统10可由比图1中所示出的组件更多的组件实施或还可由比其更少的组件实施。

[0037] SDN网络100由执行多个软件定义网络(software defined networking,SDN)功能的多个SDN节点110配置。

[0038] SDN节点110为在包含DDoS攻击者的客户端单元200与网页服务器300之间构成(替代地，形成)信息传输路径的选路系统。系统能够基于由SDN控制器作出的决策丢弃输入数据包。

[0039] 在本发明的示例性实施例中，主要描述SDN网络100，但本发明不限于此，且除了SDN网络100以外，包含DDoS攻击者的客户端单元200、网页服务器300以及SDN控制器400还可通过不同类型的通信网络(替代地，网络)彼此连接。

[0040] 此外，所述多个SDN节点110将从客户端单元200传输的HTTP请求消息转发到对应于目的地的网页服务器300。

[0041] 此外，所述多个SDN节点110响应于HTTP请求消息将从网页服务器300传输的针对HTTP请求消息的HTTP响应消息转发到客户端单元200。

[0042] 另外，多个(替代地，一或多个)SDN节点110分别接收从SDN控制器400传输的第一流量路径改变请求消息。在本文中，第一流量路径改变请求消息包含用于将紧跟在从包含

DDoS攻击者的客户端单元200传输到作为目的地的网页服务器300的HTTP请求消息之后的HTTP消息的目的地从网页服务器300改变为SDN控制器400的信息(例如,包含与SDN控制器400相关的目的地IP信息、与SDN控制器400相关的目的地端口信息等等)(替代地,用于改变SDN节点110的流量选路规则的信息)。

[0043] 此外,SDN节点110基于所接收到的第一流量路径改变请求消息将紧跟在从客户端单元200传输到作为目的地的网页服务器300的HTTP请求消息之后的HTTP消息(替代地,HTTP继续消息)传送(替代地,传输)到SDN控制器400。

[0044] 本发明中的所描述的HTTP请求消息指示从客户端单元200传输到作为目的地(替代地,接收单元)的网页服务器300的消息。在这种情况下,当HTTP请求消息分隔(替代地,划分)成多个消息且多个分隔的HTTP请求消息紧跟着传输到作为目的地的网页服务器300时,连续传输的HTTP请求消息表示为HTTP继续消息。此外,当HTTP请求消息分成多个消息时,如果最后一个部分的HTTP消息到达接收单元(替代地,目的地),那么对应HTTP请求消息可为一个完整的消息。此处,经传输直到接收单元中的HTTP请求消息完整为止的部分HTTP请求消息被称作不完整消息。

[0045] 此外,多个(替代地,一或多个)SDN节点110根据第一流量路径改变请求消息对紧跟在传输到SDN控制器400的HTTP请求消息之后的HTTP消息作出响应,以将针对紧跟在从SDN控制器400传输的HTTP请求消息之后的HTTP消息的HTTP响应消息传输到客户端单元200。

[0046] 另外,多个(替代地,一或多个)SDN节点110分别接收从SDN控制器400传输的第二流量路径改变请求消息。在本文中,第二流量路径改变请求消息包含用于将紧跟在客户端单元200传输的HTTP请求消息之后的HTTP消息的目的地从SDN控制器400改变为网页服务器300的信息,以使得客户端单元200与网页服务器300之间的信息传输路径经恢复以执行正常网络服务。

[0047] 此外,SDN节点110基于所接收到的第二流量路径改变请求消息将紧跟在从客户端单元200传输到作为目的地的网页服务器300的HTTP请求消息之后的HTTP消息(替代地,HTTP继续消息)传送(替代地,传输)到网页服务器300而非SDN控制器400。

[0048] 此外,多个(替代地,一或多个)SDN节点110根据第二流量路径改变请求消息对紧跟在传输到网页服务器300的HTTP请求消息之后的HTTP消息作出响应,以将针对紧跟在从网页服务器300传输的HTTP请求消息之后的HTTP消息的HTTP响应消息传输到客户端单元200。

[0049] 另外,多个(替代地,一或多个)SDN节点110分别接收从SDN控制器400传输的第三流量路径改变请求消息。在本文中,第三流量路径改变请求消息包含客户端单元200的源IP信息、目的地IP信息、源端口信息、目的地端口信息等等,所述客户端单元200是用于丢弃从作为攻击者的客户端单元200传输到作为目的地的网页服务器300的消息(替代地,数据包)的攻击者。

[0050] 此外,基于所接收到的第三流量路径改变请求消息,SDN节点110并未将紧跟在从客户端单元200传输到作为目的地的网页服务器300的HTTP请求消息之后的HTTP消息(替代地,用于攻击的HTTP请求消息/用于攻击的HTTP请求消息/用于攻击的缓慢HTTP请求消息)传输到SDN控制器400及网页服务器300,而是丢弃(替代地,删除/返回)所述HTTP消息。

[0051] 客户端单元200通过SDN网络100将信息(替代地,消息/数据包)传输到对应于目的地的网页服务器300。此时,客户端单元200可以是传输正常消息的终端或执行DDoS攻击的终端(替代地,攻击者)。

[0052] 此外,客户端单元200、网页服务器300以及SDN控制器400通过TCP三向信号交换方法等等彼此连接以执行用于请求、接受以及提供服务的程序。

[0053] 并且,客户端单元200将HTTP请求消息(替代地,缓慢HTTP请求消息/数据包)传输到作为目的地的网页服务器300。

[0054] 此外,客户端单元200响应于所传输的HTTP请求消息接收从网页服务器300传输的针对HTTP请求消息的响应消息(替代地,HTTP响应消息)。

[0055] 此外,当HTTP请求消息传输到SDN控制器400时,客户端单元200响应于所传输的HTTP请求消息接收从SDN控制器400传输的HTTP响应消息以维持因特网连接。

[0056] 并且,客户端单元200将HTTP消息连续地传输到网页服务器300直到对应于作为目的地的网页服务器300的HTTP请求消息完整为止。

[0057] 另外,客户端单元200响应于HTTP请求消息及连续传输的HTTP消息接收从网页服务器300或SDN控制器400传输的HTTP响应消息。

[0058] 网页服务器300通过SDN网络100接收从对应于源(替代地,出发)的客户端单元200传输的信息。

[0059] 并且,网页服务器300接收从通过SDN网络100(替代地,通信网络/网络)连接的客户端单元200传输的HTTP请求消息(替代地,缓慢HTTP请求消息/数据包)。

[0060] 并且,网页服务器300将针对所接收到的HTTP请求消息的响应消息(替代地,HTTP响应消息/响应信号/ACK信号)传输到传输所述HTTP请求消息的客户端单元200。

[0061] 此外,网页服务器300确定所接收到的HTTP请求消息是否可为疑似攻击的不完整HTTP请求消息。在这种情况下,网页服务器300可确定所接收到的HTTP请求消息是否是可能疑似攻击的不完整HTTP请求消息(替代地,用于攻击的HTTP请求消息)。举例来说,可通过比较Copen(其为到网页服务器300的消息输入连接的数目)与Cth(其为消息输入连接的阈值数目)进行确定。此处,除了比较消息输入连接的数目与连接的阈值数目的方法以外,用于确定所接收到的HTTP请求消息是否是疑似攻击的不完整HTTP请求消息的算法还可包含各种经开发或已知方法。

[0062] 作为确定结果,当所接收到的HTTP请求消息并不疑似攻击时,网页服务器300维持等待状态以用于接收除所接收到的HTTP请求消息以外的从客户端单元200另外(替代地,连续地)传输的HTTP消息(替代地,HTTP继续消息)。

[0063] 此外,作为确定结果,当所接收到的HTTP请求消息疑似攻击时,网页服务器300将所接收到的HTTP请求消息(替代地,疑似攻击的HTTP请求消息/缓慢HTTP请求消息/疑似攻击的缓慢HTTP请求消息)传输到SDN控制器400。

[0064] 此外,当网页服务器300由SDN控制器告知疑似攻击的不完整HTTP请求消息经确认为以攻击为目标时,网页服务器300终止(替代地,取消)与传输疑似攻击的HTTP请求消息的客户端单元200的连接(替代地,会话(session))。

[0065] 此外,网页服务器300响应于在所接收到的HTTP请求消息之后的HTTP消息将额外HTTP响应消息传输到客户端单元200。

[0066] SDN控制器400通过SDN网络100与客户端单元200、网页服务器300等等连接。

[0067] 此外，为了交换防御DDoS攻击所需的相关消息，SDN控制器400通过TCP三向信号交换方法等等与网页服务器300连接以执行用于请求、接受以及提供服务的程序。

[0068] 此外，SDN控制器400藉由使用SDN特性检测且阻挡网络中的DDoS攻击。在本文中，SDN隔开网络装置的控制平面与数据平面且在逻辑地集中的SDN控制器400中执行控制功能。

[0069] 另外，SDN控制器400管理属于计费区域的网络的整体信息，控制数据平面中的数据流，且为SDN应用提供网络抽象(network abstraction)。

[0070] 另外，SDN控制器400执行以下功能：使用SDN应用增强网络操作的效率，同时累积、管理且更新由SDN控制器400管理的网络的通识(替代地，信息/数据)。

[0071] 此外，SDN控制器400(替代地，攻击识别单元410)可藉由使用此类SDN的结构及特性检测DDoS攻击，且通过改变流选路规则阻挡攻击数据来抵抗缓慢HTTP DDoS攻击。

[0072] 因此，SDN控制器400收集SDN网络100的信息以重新配置预定信息传输路径。

[0073] 此外，SDN控制器400可由攻击识别单元410配置，所述攻击识别单元410用于确定HTTP请求消息(替代地，疑似攻击的HTTP请求消息/缓慢HTTP请求消息/疑似攻击的缓慢HTTP请求消息)是否是攻击。流量路径控制器420用于基于攻击识别单元410的确定结果控制(替代地，重新配置)流量路径。

[0074] 此外，SDN控制器400接收从网页服务器300传输的HTTP请求消息(替代地，疑似攻击的HTTP请求消息/缓慢HTTP请求消息/疑似攻击的缓慢HTTP请求消息)。

[0075] 此外，SDN控制器400将第一流量路径改变请求消息(替代地，路由改变消息)传输到一或多个SDN节点110，所述第一流量路径改变请求消息包含用于将紧跟在从客户端单元200传输到作为目的地的网页服务器300的HTTP请求消息之后的HTTP消息的目的地从网页服务器300改变为SDN控制器400的信息(例如，包含与SDN控制器400相关的目的地IP信息、与SDN控制器400相关的目的地端口信息等等)(替代地，用于改变SDN节点110的流量选路规则的信息)。

[0076] 此外，当数据流的目的地根据第一流量路径改变请求消息改变时，SDN控制器400而非网页服务器300接收紧跟在从客户端单元200传输的HTTP请求消息之后的HTTP消息。

[0077] 此外，SDN控制器400而非网页服务器300将针对紧跟在所接收到的HTTP请求消息之后的HTTP消息的HTTP响应消息传输到客户端单元200。

[0078] 另外，SDN控制器400确定(替代地，确认/识别/判断)所接收到的疑似攻击的不完整HTTP请求消息(替代地，疑似攻击的HTTP请求消息/缓慢HTTP请求消息/疑似攻击的缓慢HTTP请求消息)是否是攻击。在这种情况下，SDN控制器400可使用确定各种攻击的已知方法(替代地，方法)确定疑似攻击的不完整HTTP请求消息是否是攻击。

[0079] 此外，SDN控制器400还可确认所接收到的疑似攻击的不完整HTTP请求消息和/或连续地接收的HTTP消息(替代地，HTTP继续消息)是否是攻击。

[0080] 攻击识别单元410确认疑似攻击的不完整HTTP请求消息是否实际上是攻击，且还确认疑似攻击的不完整HTTP请求消息及紧接于所述HTTP请求消息接收到的一或多个HTTP消息是否是攻击。

[0081] 作为确认结果，当所接收到的疑似攻击的不完整HTTP请求消息确认为正常HTTP请

求消息时，SDN控制器400将第二流量路径改变请求消息(替代地，路由改变消息)传输到一或多个SDN节点110，所述第二流量路径改变请求消息包含用于将紧跟在从客户端单元200传输的HTTP请求消息之后的HTTP消息的目的地从SDN控制器400改变为网页服务器300的信息(替代地，改变SDN节点110的流量选路规则的信息)，以使得恢复客户端单元200与网页服务器300之间的信息传输路径以执行正常网络服务。

[0082] 此外，作为确认结果，当所接收到的疑似攻击的不完整HTTP请求消息确认为攻击的HTTP请求消息(替代地，缓慢HTTP请求消息)时，SDN控制器400将第三流量路径改变请求消息传输到一或多个SDN节点110，以便丢弃从客户端单元200朝向作为目的地的网页服务器300传输的消息(替代地，数据包)，所述第三流量路径改变请求消息包含作为攻击者的客户端单元200的源IP信息、目的地IP信息、源端口信息以及目的地端口信息(替代地，用于改变SDN节点110的流量选路规则的信息)。

[0083] 在本发明的示例性实施例中，仅描述通信网络是基于SDN的案例，但本发明不限于此。在使用各种通信方法的通信网络(替代地，网络)中，在通过形成于客户端单元200与网页服务器300之间的通信网络控制器(未示出)(例如，包含SDN控制器400等等)在网页服务器300中接收疑似攻击的消息的情况下，本发明还可通过具有第三设备配置，所述第三设备位于网络端处以接收疑似攻击的消息且将后续消息传输到网页服务器300或根据第三设备的疑似攻击的消息是否实际上为攻击的决策在网络端处丢弃后续消息。

[0084] 因此，当疑似攻击的HTTP请求消息到达网页服务器时，网页服务器将疑似攻击的HTTP请求消息发送到位于网络中的SDN控制器，且所述SDN控制器而非为攻击目标的网页服务器可确定疑似攻击的HTTP请求消息是否是DDoS攻击，且根据确定结果通过网络上的节点(替代地，路由器)阻挡来自攻击者的流量。

[0085] 此外，因此，当疑似攻击的HTTP请求消息到达网页服务器时，紧接在SDN控制器从网页服务器接收HTTP请求消息之后，SDN控制器将流量路径改变请求消息传输到SDN节点，以使得SDN控制器接收随后从客户端单元而非网页服务器传输的HTTP消息，且可取决于对应HTTP请求消息是DDoS攻击或不是DDoS攻击的确定结果恢复流量路径或通过SDN节点阻挡对应流量。

[0086] 下文中，将参考图1到图3详细描述根据本发明的基于SDN防御DDoS攻击的方法。

[0087] 图2和图3示出根据本发明的示例性实施例的基于SDN防御DDoS攻击的方法的流程图。

[0088] 首先，网页服务器300接收从通过SDN网络100(替代地，通信网络/网络)连接的客户端单元200传输的HTTP请求消息(替代地，缓慢HTTP请求消息/数据包)。

[0089] 并且，网页服务器300将针对所接收到的HTTP请求消息的响应消息(替代地，HTTP响应消息/响应信号/ACK信号)传输到传输所述HTTP请求消息的客户端单元200。

[0090] 此外，网页服务器300确定(替代地，确认/识别)所接收到的HTTP请求消息是否是疑似攻击的不完整HTTP请求消息。在这种情况下，网页服务器300可确定所接收到的HTTP请求消息是否是攻击的不完整HTTP请求消息(替代地，用于攻击的HTTP请求消息)。可通过已知方法或现有方法执行确定过程。确定的实例可为Copen比较，其中到网页服务器300的消息输入连接的数目与为消息输入连接的阈值数目的Cth相比较。本文中，除了比较消息输入连接的数目与消息输入连接的阈值数目的方法以外，用于确定所接收到的HTTP请求消息是

否是疑似攻击的不完整HTTP请求消息的算法还可包含各种已知方法。

[0091] 作为实例,网页服务器300经由包含于SDN网络100中的一或多个SDN节点110接收从客户端单元200传输的第一HTTP请求消息。

[0092] 此外,网页服务器300将第一HTTP响应消息传输到客户端单元200,所述第一HTTP响应消息是所接收到的第一HTTP请求消息的响应消息。

[0093] 此外,客户端单元200响应于第一HTTP请求消息接收从网页服务器300传输的第一HTTP响应消息。

[0094] 此外,网页服务器300可通过比较Copen(其为到网页服务器300的消息输入连接的数目)与Cth(其为消息输入连接的预定阈值数目)确定所接收到的第一HTTP请求消息是否是疑似攻击的不完整HTTP请求消息(步骤S210)。接着,网页服务器300中断与HTTP请求消息相关的所有任务。

[0095] 作为确定结果,当所接收到的HTTP请求消息并不是攻击时,网页服务器300保持在正常操作状态中以用于接收除所接收到的HTTP请求消息以外的从客户端单元200另外(替代地,连续地)传输的HTTP消息(替代地,HTTP继续消息)。

[0096] 作为实例,作为确定结果,当为到网页服务器300的消息输入连接的数目的Copen小于为输入连接的阈值数目的Cth时,网页服务器300保持在正常操作状态中以用于接收在第一HTTP请求消息之后从客户端单元200连续传输的HTTP消息(替代地,HTTP继续消息)(步骤S220)。此外,作为确定结果,当所接收到的HTTP请求消息疑似攻击时,网页服务器300将所接收到的HTTP请求消息(替代地,疑似攻击的HTTP请求消息/缓慢HTTP请求消息/疑似攻击的缓慢HTTP请求消息)发送到SDN控制器400。

[0097] 此外,网页服务器300中断(替代地,取消)由传输疑似攻击的HTTP请求消息的客户端单元200请求的所有任务(替代地,会话)。

[0098] 作为实例,作为确定结果,当为所述网页服务器300的消息输入连接的数目的Copen大于或等于为消息输入连接的阈值数目的Cth时,网页服务器300将所接收到的HTTP请求消息(替代地,疑似攻击的HTTP请求消息)发送到SDN控制器400且中断由来自客户端单元200的HTTP请求消息请求的任务(替代地,网页服务器300在将所接收到的HTTP请求消息发送到SDN控制器400之后终止与客户端单元200的连接)(步骤S230)。

[0099] 此后,SDN控制器400接收从网页服务器300发送的HTTP请求消息(替代地,疑似攻击的HTTP请求消息/缓慢HTTP请求消息/疑似攻击的缓慢HTTP请求消息)。

[0100] 此外,SDN控制器400将第一流量路径改变请求消息(替代地,路由改变消息)传输到一或多个SDN节点110,所述第一流量路径改变请求消息包含用于将紧跟在从客户端单元200传输到作为目的地的网页服务器300的HTTP请求消息之后的HTTP消息的目的地从网页服务器300改变为SDN控制器400的信息(例如,与SDN控制器400相关的目的地IP信息、与SDN控制器400相关的目的地端口信息等等)(替代地,用于改变SDN节点110的流量选路规则的信息)。

[0101] 作为实例,SDN控制器400接收从网页服务器300传输的HTTP请求消息(替代地,疑似攻击的HTTP请求消息)。

[0102] 另外,SDN控制器400将第一流量路径改变请求消息传输到包含于SDN网络100中的一或多个SDN节点110(替代地,位于客户端单元220与网页服务器300之间的一或多个节点

110)，所述第一流量路径改变请求消息包含用于将在HTTP请求消息之后从客户端单元200传输的HTTP继续消息的目的地从网页服务器300改变为SDN控制器400的信息(步骤S240)。

[0103] 此后，SDN节点110中的一或多个分别接收从SDN控制器400传输的第一流量路径改变请求消息。

[0104] 此外，SDN节点110基于所接收到的第一流量路径改变请求消息将紧跟在从客户端单元200传输到作为目的地的网页服务器300的所述HTTP请求消息之后的HTTP消息(替代地，HTTP继续消息)传送(替代地，传输)到SDN控制器400。

[0105] 此外，SDN控制器400接收紧跟在从客户端单元200传输的HTTP请求消息之后的HTTP消息。

[0106] 此外，SDN控制器400将针对紧跟在所接收到的HTTP请求消息之后的HTTP消息的HTTP响应消息传输到客户端单元200。

[0107] 作为实例，一或多个SDN节点110分别接收从SDN控制器400传输的第一流量路径改变请求消息。

[0108] 此外，一或多个SDN节点110中的每一个根据所接收到的第一流量路径改变请求消息将紧跟从客户端单元200到作为目的地的网页服务器300的HTTP请求消息传输的HTTP继续消息转发到SDN控制器400而非网页服务器300。

[0109] 此外，SDN控制器400通过一或多个SDN节点110接收紧跟来自客户端单元200的HTTP请求消息传输的HTTP继续消息，所述SDN控制器400通过第一流量路径改变请求消息重新配置，且将针对所接收到的HTTP继续消息的HTTP响应消息传输到客户端单元200(步骤S250)。

[0110] 此后，SDN控制器400确认(替代地，确定/识别/判断)所接收到的不完整HTTP请求消息是否是攻击(替代地，疑似攻击的HTTP请求消息/缓慢HTTP请求消息/疑似攻击的缓慢HTTP请求消息)。在这种情况下，SDN控制器400可通过使用确定各种攻击的已知或现有方法确认不完整HTTP请求消息为攻击。

[0111] 作为实例，SDN控制器400确认所接收到的HTTP请求消息是否是攻击(步骤S260)。

[0112] 作为确认结果，当所接收到的疑似攻击的不完整HTTP请求消息确认为正常HTTP请求消息时，SDN控制器400将第二流量路径改变请求消息(替代地，路由改变消息)传输到一或多个SDN节点110，所述第二流量路径改变请求消息包含用于将紧跟在从客户端单元200传输的所述HTTP请求消息之后的HTTP消息的目的地从SDN控制器400改变为网页服务器300的信息(替代地，改变SDN节点110的流量选路规则的信息)，以使得恢复客户端单元200与网页服务器300之间的信息传输路径以执行正常网络服务。

[0113] 作为实例，作为确认结果，当所接收到的第一HTTP请求消息确认为正常HTTP请求消息，以便将客户端单元200与网页服务器300之间的信息传输路径恢复到正常状态时，SDN控制器400将第二流量路径改变请求消息传输到包含于SDN网络100中的一或多个SDN节点110(替代地，位于客户端单元200与网页服务器300之间的一或多个SDN节点110)，所述第二流量路径改变请求消息包含将在HTTP请求消息之后从客户端单元200连续传输的继续消息的目的地从SDN控制器400改变为网页服务器300的信息(步骤S270)。

[0114] 此后，SDN节点110中的一或多个分别接收从SDN控制器400传输的第二流量路径改变请求消息。

[0115] 此外,SDN节点110基于所接收到的第二流量路径改变请求消息将紧跟在从客户端单元200传输到作为目的地的网页服务器300的HTTP请求消息之后的HTTP消息转发(替代地,传输)到网页服务器300而非SDN控制器400。

[0116] 此外,网页服务器300接收紧跟在从客户端单元200传输的HTTP请求消息之后的HTTP消息。

[0117] 此外,网页服务器300响应于所接收的紧跟的HTTP消息将额外HTTP响应消息传输到客户端单元200。

[0118] 作为实例,SDN节点110中的一或多个分别接收从SDN控制器400传输的第二流量路径改变请求消息。

[0119] 此外,一或多个SDN节点110中的每一个基于所接收到的第二流量路径改变请求消息将紧跟从客户端单元200到作为目的地的网页服务器300的HTTP请求消息传输的HTTP继续消息转发到网页服务器300而非SDN控制器400。

[0120] 此外,在一或多个SDN节点110接收第二流量路径改变请求消息之后,网页服务器300通过一或多个SDN节点110接收紧跟来自客户端单元200的HTTP请求消息传输的HTTP继续消息(步骤S280)。

[0121] 此外,作为确认结果,当所接收到的疑似攻击的不完整HTTP请求消息确认为以攻击为目标的HTTP请求消息(替代地,缓慢HTTP请求消息)时,SDN控制器400将第三流量路径改变请求消息传输到一或多个SDN节点110,以便丢弃从作为攻击者的客户端单元200传输到作为目的地的网页服务器300的消息(替代地,数据包),所述第三流量路径改变请求消息包含作为攻击者的客户端单元200的源IP信息、目的地IP信息、源端口信息以及目的地端口信息(替代地,用于改变SDN节点110的流量选路规则的信息)。

[0122] 作为实例,作为确认结果,当所接收到的HTTP请求消息确认为用于攻击的HTTP请求消息时,SDN控制器400将第三流量路径改变请求消息传输到一或多个SDN节点110(替代地,位于客户端单元200与网页服务器300之间的一或多个SDN节点110),以便丢弃从作为攻击者的客户端单元200传输到作为目的地的网页服务器300的HTTP继续消息,所述第三流量路径改变请求消息包含作为攻击者的客户端单元200的源IP信息、目的地IP信息、源端口信息、目的地端口信息等等(步骤S290)。

[0123] 此后,SDN节点110中的一或多个分别接收从SDN控制器400传输的第三流量路径改变请求消息。

[0124] 此外,基于所接收到的第三流量路径改变请求消息,SDN节点110并未将紧跟在从客户端单元200传输到目的地的HTTP请求消息之后的HTTP消息(替代地,用于攻击的HTTP请求消息/用于攻击的缓慢HTTP请求消息)转发到SDN控制器400及网页服务器300,而是丢弃(替代地,删除)所述HTTP消息。

[0125] 作为实例,SDN节点110中的一或多个分别接收从SDN控制器400传输的第三流量路径改变请求消息。

[0126] 此外,一或多个SDN节点110当中的至少一个SDN节点110基于所接收到的第三流量路径改变请求消息丢弃紧跟从客户端单元200到作为目的地的网页服务器的HTTP请求消息传输的HTTP继续消息(步骤S300)。

[0127] 在本发明的示例性实施例中,如上文所描述,当疑似攻击的HTTP请求消息到达网

页服务器时，网页服务器将疑似攻击的HTTP请求消息发送到位于网络中的SDN控制器，且SDN控制器而非为攻击目标的网页服务器确定DDoS攻击且根据确定结果通过网络上的节点(替代地，路由器)阻挡来自攻击者的流量，以输入疑似为DDoS攻击的通过传输不完整HTTP消息耗尽网页服务器的可用连接资源的流量，由此保护网页服务器免受DDoS攻击且确保对网页服务器的正常操作的维护。

[0128] 此外，在本发明的示例性实施例中，如上文所描述，当疑似攻击的HTTP请求消息到达网页服务器时，紧接在SDN控制器从网页服务器接收HTTP请求消息之后，SDN控制器将流量路径改变请求消息传输到SDN节点以接收从客户端单元而非网页服务器连续地传输的HTTP消息且恢复流量路径或根据确定对应HTTP请求消息是否是攻击的结果通过SDN节点阻挡对应流量，以在到达网页服务器之前从网络装置阻挡来自所检测到的DDoS攻击者的流量，由此防止流量的递送，以使得可避免浪费网络路径中的占用带宽。

[0129] 上文，尽管通过例如具体组件等特定事项、实施例以及附图描述本发明，但其仅为了辅助对本发明的整体理解而提供。因此，本发明不限于所述实施例。因此，本发明中公开的实施例并不用于限制而是描述本发明的技术精神，且本发明的技术精神的范围不受所述实施例限制。本发明的范围应通过所附权利要求解译，且其等效范围中的所有技术精神应解译为被本发明的权利要求涵盖。

[0130] 根据本发明，当疑似攻击的HTTP请求消息到达网页服务器时，网页服务器将疑似攻击的HTTP请求消息发送到位于网络中的SDN控制器，且SDN控制器而非为攻击目标的网页服务器确定DDoS攻击且根据确定结果通过网络上的节点(替代地，路由器)阻挡疑似DDoS攻击的流量，由此保护网页服务器免受DDoS攻击且确保对网页服务器的正常操作的维护，所述DDoS攻击通过传输来自攻击者的不完整HTTP消息耗尽网页服务器的可用连接资源。因此，本发明可广泛用于DDoS攻击防范领域、网络管理领域、分布式服务器领域等等。

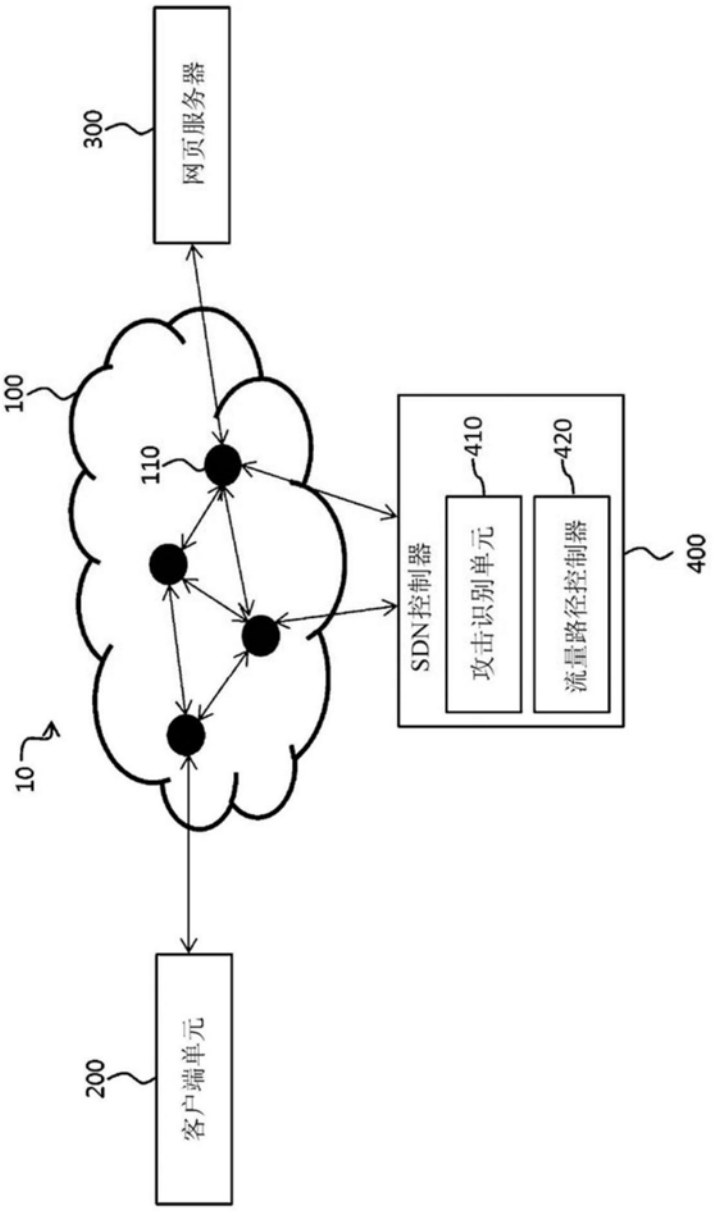

300
网页服务器
100
110
SDN控制器
410
攻击识别单元
420
流量路径控制器
400
10
200
客户端单元

图1

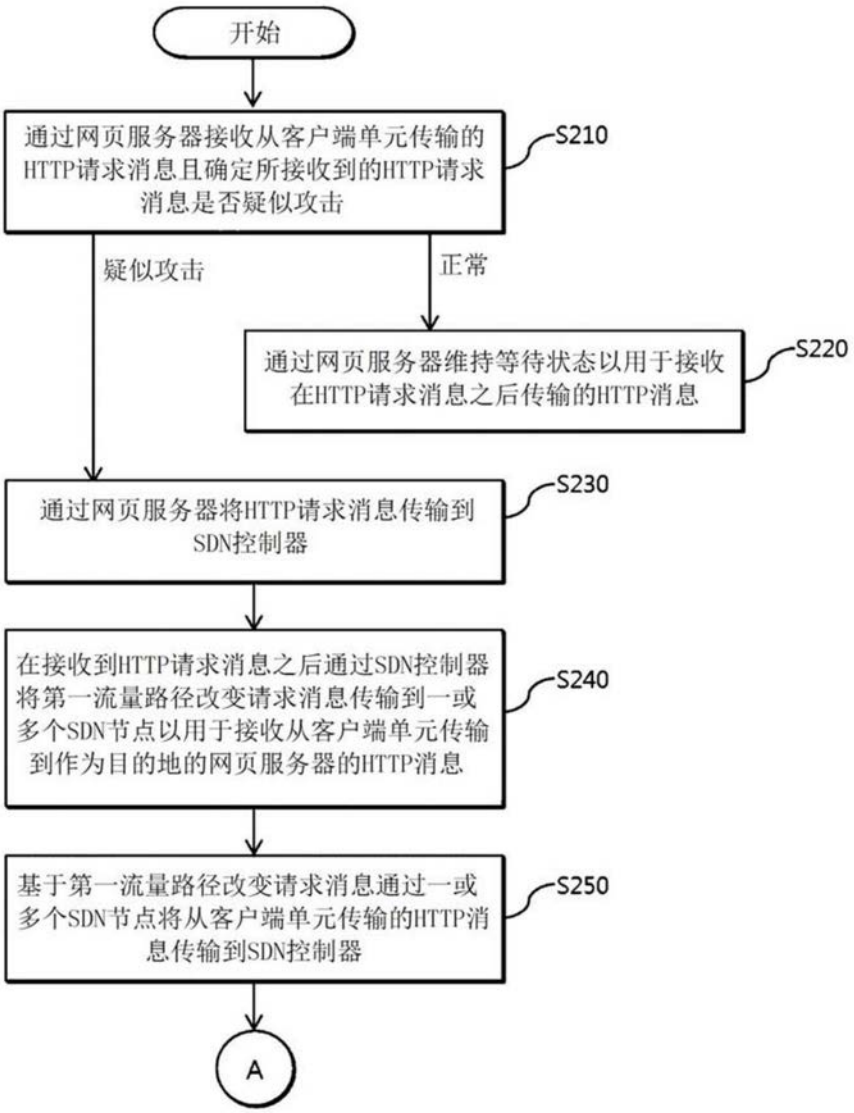

开始
通过网页服务器接收从客户端单元传输的HTTP请求消息且确定所接收到的HTTP请求消息是否疑似攻击
S210
疑似攻击
正常
通过网页服务器维持等待状态以用于接收在HTTP请求消息之后传输的HTTP消息
S220
通过网页服务器将HTTP请求消息传输到SDN控制器
S230
在接收到HTTP请求消息之后通过SDN控制器将第一流量路径改变请求消息传输到一或多个SDN节点以用于接收从客户端单元传输到作为目的地的网页服务器的HTTP消息
S240
基于第一流量路径改变请求消息通过一或多个SDN节点将从客户端单元传输的HTTP消息传输到SDN控制器
S250
A

图2

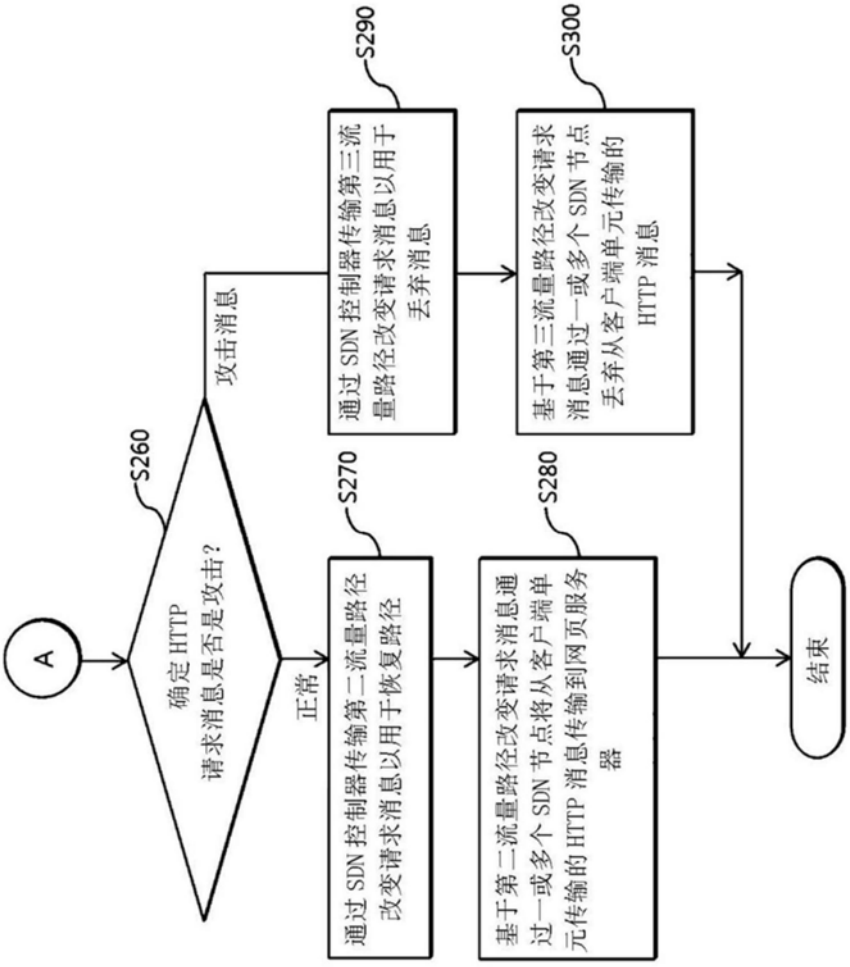

A
确定 HTTP
请求消息是否是攻击?
S260
攻击消息
正常
通过 SDN 控制器传输第三流量路径改变请求消息以用于丢弃消息
S290
基于第三流量路径改变请求消息,通过一或多个 SDN 节点丢弃从客户端单元传输的 HTTP 消息
S300
通过 SDN 控制器传输第二流量路径改变请求消息以用于恢复路径
S270
基于第二流量路径改变请求消息,通过一或多个 SDN 节点将从客户端单元传输的 HTTP 消息传输到网页服务器
S280
结束

图3