(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2016 年 11 月 10 日 (10.11.2016)

WIPO | PCT

(10) 国际公布号
WO 2016/177131 A1

(51) 国际专利分类号:
H04L 29/06 (2006.01) *H04L 29/12* (2006.01)

(21) 国际申请号: PCT/CN2016/076649

(22) 国际申请日: 2016 年 3 月 17 日 (17.03.2016)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201510504850.X 2015 年 8 月 17 日 (17.08.2015) CN

(71) 申请人: 中兴通讯股份有限公司 (ZTE CORPORATION) [CN/CN]; 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(72) 发明人: 周广腾 (ZHOU, Guangteng); 中国广东省深圳市南山区高新技术产业园科技南路中兴通讯大厦, Guangdong 518057 (CN)。

(74) 代理人: 北京康信知识产权代理有限责任公司 (KANGXIN PARTNERS, P.C.); 中国北京市海淀区知春路甲 48 号盈都大厦 A 座 16 层, Beijing 100098 (CN)。

(81) 指定国 (除另有指明，要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明，要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

[见续页]

(54) Title: METHOD, APPARATUS, AND SYSTEM FOR PREVENTING DOS ATTACKS

(54) 发明名称 : 防止 DOS 攻击方法、装置和系统

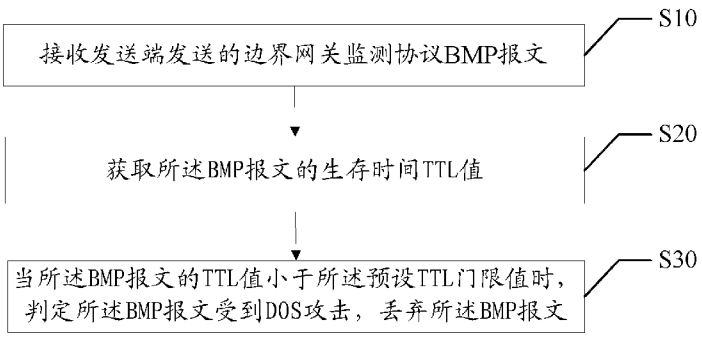

图 1

S10 Receive a border gateway monitoring protocol BMP packet sent by a sending terminal
S20 Acquire the time-to-live TTL value of the BMP packet
S30 When the TTL value of the BMP packet is less than a preset TTL threshold value, determine that the BMP packet has suffered a DOS attack, and drop the BMP packet

(57) Abstract: Disclosed in the present invention is a method for preventing DOS attacks, the method comprising the following steps: receiving a border gateway monitoring protocol BMP packet sent by a sending terminal; acquiring the time-to-live TTL value of the BMP packet; and when the TTL value of the BMP packet is less than a preset TTL threshold value, determining that the BMP packet has suffered a DOS attack, and dropping the BMP packet. Also disclosed in the present invention are an apparatus and system for preventing BMP packet DOS attacks. The present invention prevents IP spoofing DOS attacks by means of TTL values.

(57) 摘要: 本发明公开了一种防止 DOS 攻击方法，该方法包括步骤：接收发送端发送的边界网关监测协议 BMP 报文；获取所述 BMP 报文的生存时间 TTL 值；当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文。本发明还公开了一种 BMP 报文防止 DOS 攻击装置和系统。本发明实现了通过 TTL 值来防止受到伪装 IP 的 DOS 攻击。

WO 2016/177131 A1

本国际公布:

— 包括国际检索报告(条约第 21 条(3))。

— 在修改权利要求的期限届满之前进行，在收到该修改后将重新公布(细则 48.2(h))。

— 根据申请人的请求，在条约第 21 条(2)(a)所规定的期限届满之前进行。

防止 DOS 攻击方法、装置和系统

技术领域

本发明涉及通信领域，尤其涉及一种防止 DOS 攻击方法、装置和系统。

背景技术

拒绝服务（Denial of Service，DOS）攻击是一种通过发送大量数据包使得计算机或者网络无法提供正常服务的攻击形式。它可能在短时间内耗尽所有可用的网络资源或者被攻击对象的系统资源，使得合法的用户无法通过或被处理，从而阻碍网络中的正常通信，给被攻击者乃至网络带来巨大的危害。

BMP（BGP Monitoring Protocol draft-ietf-grow-bmp-07，BGP 协议 draft-ietf-grow-bmp-07 监测）定义了设备之间建立链接和报文交互处理的方法，在对设备间报文交互处理过程。大部分控制协议对等进程都建立在相邻或者直连的路由器之间，在路由器之间进行报文交互处理过程中，攻击者会模拟真实的 BMP 报文，对节点发送报文。当设备的接口板接收到这些报文后，直接送到控制层面的 BMP 协议处理，而不去辨别这些报文的“合法性”，不去辨别这些报文是否为 DOS 攻击报文，所述设备因为处理这些“合法”报文，即处理受到伪装 IP（Internet Protocol，因特网互联协议）的 DOS 攻击的报文，会导致系统异常繁忙，CPU（Central Processing Unit，中央处理器）占用率高。

发明内容

本发明实施例的主要目的在于提供一种防止 DOS 攻击方法、装置和装置，解决防止受到伪装 IP 的 DOS 攻击的技术问题。

为实现上述目的，本发明实施例提供的一种防止 DOS 攻击方法，包括步骤：

接收发送端发送的边界网关监测协议 BMP 报文；

获取所述 BMP 报文的生存时间 TTL 值；

当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文。

在本发明实施例中，所述获取所述 BMP 报文的 TTL 值的步骤之后，还包括：

当所述 BMP 报文的 TTL 值大于或等于所述预设 TTL 门限值时，判定所述 BMP 报文为正常 BMP 报文，继续对所述 BMP 报文进行处理。

在本发明实施例中，所述接收发送端发送的 BMP 报文的步骤之前，还包括：

根据通用 TTL 安全保护机制设置所述预设 TTL 门限值。

在本发明实施例中，所述根据通用 TTL 安全保护机制设置所述预设 TTL 门限值的步骤之前，还包括：

通过网络通讯协议与发送端建立链接。

此外，为实现上述目的，本发明还提供一种防止 DOS 攻击装置，所述装置包括：

接收模块，设置为接收发送端发送的边界网关监测协议 BMP 报文；

获取模块，设置为获取所述 BMP 报文的生存时间 TTL 值；

判定模块，设置为当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文。

在本发明实施例中，所述判定模块，还设置为当所述 BMP 报文的 TTL 值大于或等于所述预设 TTL 门限值时，判定所述 BMP 报文为正常 BMP 报文，继续对所述 BMP 报文进行处理。

在本发明实施例中，所述防止 DOS 攻击装置还包括：

设置模块，设置为根据通用 TTL 安全保护机制设置所述预设 TTL 门限值。

在本发明实施例中，所述防止 DOS 攻击装置还包括：

建立模块，设置为通过网络通讯协议与发送端建立链接。

此外，为实现上述目的，本发明还提供一种防止 DOS 攻击系统，所述系统发送端和接收端：

所述接收端，设置为接收发送端发送的边界网关监测协议 BMP 报文；

所述接收端，还设置为获取所述 BMP 报文的生存时间 TTL 值；

所述接收端，还设置为当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文；

所述发送端，设置为向所述接收端发送边界网关监测协议 BMP 报文。

在本发明实施例中，所述接收端，还设置为当所述 BMP 报文的 TTL 值大于或等于所述预设 TTL 门限值时，判定所述 BMP 报文为正常 BMP 报文，继续对所述 BMP 报文进行处理；

所述接收端，还设置为根据通用 TTL 安全保护机制设置所述预设 TTL 门限值；

所述发送端，还设置为当向所述接收端发送 BMP 报文时，将所述 BMP 报文的 TTL 值修改成 TTL 的最大值 255。

在本发明实施例中，还提供了一种计算机存储介质，该计算机存储介质可以存储有执行指令，该执行指令用于执行上述实施例中的防止 DOS 攻击方法。

本发明实施例通过获取所接收到的BMP报文的TTL值，当所述接收到的BMP报文的TTL值小于预设 TTL 门限值时，将所述 BMP 报文丢弃，实现通过 TTL 值来防止受到伪装 IP 的 DOS 攻击。

附图说明

图 1 为本发明防止 DOS 攻击方法较佳实施例的流程示意图；

图 2 为本发明防止 DOS 攻击装置较佳实施例的功能模块示意图；

图 3 为本发明防止 DOS 攻击系统较佳实施例的功能模块示意图。

本发明目的的实现、功能特点及优点将结合实施例，参照附图做进一步说明。

具体实施方式

应当理解，此处所描述的具体实施例仅仅用以解释本发明，并不用于限定本发明。

本发明实施例的主要解决方案是：接收发送端发送的边界网关监测协议 BMP 报文；获取所述 BMP 报文的生存时间 TTL 值；当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文。通过获取所接收到的 BMP 报文的 TTL 值，当所述接收到的 BMP 报文的 TTL 值小于预设 TTL 门限值时，将所述 BMP 报文丢弃，实现通过 TTL 值来防止受到伪装 IP 的 DOS 攻击。

由于现有的技术无法通过更改 TTL 值来防止受到拒绝服务攻击，从而浪费 CPU 资源。

基于上述问题，本发明提供一种防止 DOS 攻击方法。

参照图 1，图 1 为本发明防止 DOS 攻击方法第一实施例的流程示意图。

在本实施例中，所述防止 DOS 攻击方法包括：

步骤 S10，接收发送端发送的边界网关监测协议 BMP 报文；

接收端和发送端通过 TCP/IP 协议建立链接。所述 TCP/IP 协议是 Internet 最基本的协议，是 Internet 国际互联网的基础，由网络层的 IP 协议和传输层的 TCP 协议组成。所述接收端还可以通过 IPX/SPX（Internetwork Packet Exchange/Sequences Packet Exchange，分组交换/顺序交换）协议等与所述发送端建立链接。在所述 IPX/SPX 中，IPX 主要实现网络设备之间连接的建立维持和终止；SPX 协议是 IPX 的辅助协议，主要实现发出信息的分组、跟踪分组传输，保证信息完整无缺的传输。

所述接收端接收所述发送端发送的 BMP 数据报文，所述接收端和所述发送端都配置了GTSM（Generalized TTL Security Mechanism，通用 TTL 安全保护机制）。所述 GTSM 是一种通过检查 IP 报文头中的 TTL 值是否在一个预先定义好的特定范围内，从而实现对 IP 上的业务进行保护的机制。所述 GTSM 主要用于保护建立在 TCP/IP（Transmission Control Protocol/Internet Protocol，传输控制协议/因特网互联协议，又名网络通讯协议）基础上的控制层面协议免受 DOS 攻击。例如，攻击者模拟真实的通讯协议，对一台设备不断发送报文，导致设备因处理这些“合法（攻击报文）”而使系统异常繁忙，CPU 占用率过高。所述发送端发送的 BMP 数据报文的 TTL 值是经过其数据层面修改的。所述 TTL 值是指定 IP 数据包在被路由器丢弃之前允许通过的最大网段数量，TTL 的作用是限制 IP 数据包在计算机网络中的存在时间，所述 TTL 的最大值是 255，TTL 字段由 IP 数据包的发送者设置，在所述 IP 数据包从源目的的整个转发路径上，每经过一个转发路径上的路由器，所述转发路径上的路由器都会修改这个 TTL 值，具体做法是将所述 TTL 值减 1，然后再把所述 IP 数据包转发出去。因此，在本发明实施例中，所述发送端将要发送给接收端的 BMP 数据报文的 TTL 值修改成 255。所述发送端优选为网关设备，如路由器，具有三层交换功能的网络交换机等，所述接收端包括但不限于服务器等能提供计算服务的设备，优选地，所述发送端为路由器，所述接收端为服务器。即所述服务器和所述路由器通过 TCP/IP 协议建立链接。所述服务器和所述路由器都配置了 GTSM。当所述路由器要向所述服务器发送 BMP 数据报文时，所述路由器将要发送给服务器的 BMP 数据报文的 TTL 值修改成 255。所述服务器接收所述路由器发送的 BMP 数据报文。

步骤 S20，获取所述 BMP 报文的生存时间 TTL 值；

当所述接收端接收到所述发送端发送的 BMP 数据报文时，通过其数据层面获取所述 BMP 数据报文的 TTL 值。如所述服务器接收所述路由器发送的 BMP 数据报文时，通过其数据层面获取所述 BMP 数据报文的 TTL 值。

步骤 S30，当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文。

当所述接收端接收的 BMP 数据报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 数据报文受到 DOS 攻击，为非法的 BMP 数据报文，所述接收端就会丢弃所述非法的 BMP 数据报文，不会继续向数据层面的上层传递所述非法的 BMP 数据报文。优选地，所述预设 TTL 门限值为所述接收端通过配置的 GTSM 设置。所述接收端通过其配置的 GTSM，根据所述接收端和所述发送端之间的网络拓扑结构设置所述预设 TTL 门限值，所述网络拓扑结构是指用传输介质互连各种设备的物理布局，指构成网络的成员间特定的物理的，即真实的、或者逻辑的，即虚拟的排列方式。如当所述接收端和所述发送端之间的网络中的转发路径上有 10 个路由器，则将所述预设 TTL 门限值设置为 245。因为所述发送端发送的 BMP 数据报文的 TTL 值每经过一个转发路径上的路由器，所述 TTL 值就会减 1，当所述 BMP 数据报文经过转发路径上的 10 个路由器时，所述 BMP 数据报文的 TTL 值减小至 245，因此将所述预设 TTL 门限值设置为 245，即所述接收端接收的 BMP 数据报文的 TTL 值的范围应该在 245 到 255 之间。

所述接收端在接收所述发送端发送的 BMP 数据报文时，会同时接收其它设备发送的受到

DOS 攻击的 BMP 数据报文，而所述其它设备发送的的受到 DOS 攻击的 BMP 数据报文的 TTL 值一般都为 64 或 100 等，并不会达到 255，所以当所述发送端发送的 BMP 数据报文和所述其它设备发送的受到 DOS 攻击的 BMP 数据报文都经过同样个数转发路径上的路由器时，所述其它设备发送的受到 DOS 攻击的 BMP 数据报文的 TTL 值会小于预设 TTL 门限值。如当所述预设 TTL 门限值为 245 时，则当所述接收端接收的 BMP 数据报文的 TTL 值小于 245 时，则判定所述接收端接收的 BMP 数据报文为非法的 BMP 数据报文，丢弃所述非法的 BMP 数据报文。如当所述服务器和所述路由器之间存在 10 个转发 BMP 数据报文的路由器时，当所述服务器接收到所述路由器发送的 BMP 数据报文的 TTL 值小于 245 时，表示所述服务器接收的 BMP 数据报文为非法的 BMP 数据报文，所述服务器会将所述 BMP 数据报文丢弃。

当所述接收端接收的 BMP 数据报文的 TTL 值大于或者等于所述预设 TTL 门限值时，判定所述 BMP 数据报文未受到 DOS 攻击，为正常的 BMP 数据报文，并将所述正常的 BMP 数据报文继续向数据层面的上层传递，如向控制层面传递，即继续对所述正常的 BMP 数据报文进行处理。如当所述预设 TTL 门限值为 245 时，则当所述服务器接收的 BMP 数据报文的 TTL 值大于或者等于 245 时，则判定所述服务器接收的 BMP 数据报文为正常的 BMP 数据报文，继续对所述正常的 BMP 数据报文进行处理。

本实施例通过获取所接收到的 BMP 报文的 TTL 值，当所述接收到的 BMP 报文的 TTL 值小于预设 TTL 门限值时，将所述 BMP 报文丢弃，实现通过 TTL 值来防止受到伪装 IP 的 DOS 攻击，降低设备的 CPU 占用率，提高设备的使用寿命。

本发明进一步提供一种防止 DOS 攻击装置。

参照图 2，图 2 为本发明防止 DOS 攻击装置较佳实施例的功能模块示意图。

在本实施例中，所述防止 DOS 攻击装置包括：

接收模块 10，设置为接收发送端发送的边界网关监测协议 BMP 报文；

接收端和发送端通过 TCP/IP 协议建立链接。所述 TCP/IP 协议是 Internet 最基本的协议，是 Internet 国际互联网的基础，由网络层的 IP 协议和传输层的 TCP 协议组成。所述接收端还可以通过 IPX/SPX 协议等与所述发送端建立链接。在所述 IPX/SPX 中，IPX 主要实现网络设备之间连接的建立维持和终止；SPX 协议是 IPX 的辅助协议，主要实现发出信息的分组、跟踪分组传输，保证信息完整无缺的传输。

所述接收端接收所述发送端发送的 BMP 数据报文，所述接收端和所述发送端都配置了 GTSM。所述发送端发送的 BMP 数据报文的 TTL 值是经过其数据层面修改的。所述 TTL 值是指定 IP 数据包在被路由器丢弃之前允许通过的最大网段数量，TTL 的作用是限制 IP 数据包在计算机网络中的存在时间，所述 TTL 的最大值是 255，TTL 字段由 IP 数据包的发送者设置，在所述 IP 数据包从源目的的整个转发路径上，每经过一个转发路径上的路由器，所述转发路径上的路由器都会修改这个 TTL 值，具体做法是将所述 TTL 值减 1，然后再把所述 IP 数据包

转发出去。因此，优选地，所述发送端将要发送给接收端的 BMP 数据报文的 TTL 值修改成 255。所述发送端优选为网关设备，如路由器，具有三层交换功能的网络交换机等，所述接收端包括但不限于服务器等能提供计算服务的设备，优选地，所述发送端为路由器，所述接收端为服务器。即所述服务器和所述路由器通过 TCP/IP 协议建立链接。所述服务器和所述路由器都配置了 GTSM。当所述路由器要向所述服务器发送 BMP 数据报文时，所述路由器将要发送给服务器的 BMP 数据报文的 TTL 值修改成 255。所述服务器接收所述路由器发送的 BMP 数据报文。

获取模块 20，设置为获取所述 BMP 报文的生存时间 TTL 值；

当所述接收端接收到所述发送端发送的 BMP 数据报文时，通过其数据层面获取所述 BMP 数据报文的 TTL 值。如所述服务器接收所述路由器发送的 BMP 数据报文时，通过其数据层面获取所述 BMP 数据报文的 TTL 值。

判定模块 30，设置为当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文。

当所述接收端接收的 BMP 数据报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 数据报文受到 DOS 攻击，为非法的 BMP 数据报文，所述接收端就会丢弃所述非法的 BMP 数据报文，不会继续向数据层面的上层传递所述非法的 BMP 数据报文。优选地，所述预设 TTL 门限值为所述接收端通过配置的 GTSM 设置。所述接收端通过其配置的 GTSM，根据所述接收端和所述发送端之间的网络拓扑结构设置所述预设 TTL 门限值，所述网络拓扑结构是指用传输介质互连各种设备的物理布局，指构成网络的成员间特定的物理的，即真实的、或者逻辑的，即虚拟的排列方式。如当所述接收端和所述发送端之间的网络中的转发路径上有 10 个路由器，则将所述预设 TTL 门限值设置为 245。因为所述发送端发送的 BMP 数据报文的 TTL 值每经过一个转发路径上的路由器，所述 TTL 值就会减 1，当所述 BMP 数据报文经过转发路径上的 10 个路由器时，所述 BMP 数据报文的 TTL 值减小至 245，因此将所述预设 TTL 门限值设置为 245，即所述接收端接收的 BMP 数据报文的 TTL 值的范围应该在 245 到 255 之间。

所述接收端在接收所述发送端发送的 BMP 数据报文时，会同时接收其它设备发送的受到 DOS 攻击的 BMP 数据报文，而所述其它设备发送的的受到 DOS 攻击的 BMP 数据报文的 TTL 值一般都为 64 或 100 等，并不会达到 255，所以当所述发送端发送的 BMP 数据报文和所述其它设备发送的受到 DOS 攻击的 BMP 数据报文都经过同样个数转发路径上的路由器时，所述其它设备发送的受到 DOS 攻击的 BMP 数据报文的 TTL 值会小于预设 TTL 门限值。如当所述预设 TTL 门限值为 245 时，则当所述接收端接收的 BMP 数据报文的 TTL 值小于 245 时，则判定所述接收端接收的 BMP 数据报文为非法的 BMP 数据报文，丢弃所述非法的 BMP 数据报文。如当所述服务器和所述路由器之间存在 10 个转发 BMP 数据报文的路由器时，当所述服务器接收到所述路由器发送的 BMP 数据报文的 TTL 值小于 245 时，表示所述服务器接收的 BMP 数据报文为非法的 BMP 数据报文，所述服务器会将所述 BMP 数据报文丢弃。

当所述接收端接收的 BMP 数据报文的 TTL 值大于或者等于所述预设 TTL 门限值时，判

定所述 BMP 数据报文未受到 DOS 攻击，为正常的 BMP 数据报文，并将所述正常的 BMP 数据报文继续向数据层面的上层传递，如向控制层面传递，即继续对所述正常的 BMP 数据报文进行处理。如当所述预设 TTL 门限值为 245 时，则当所述服务器接收的 BMP 数据报文的 TTL 值大于或者等于 245 时，则判定所述服务器接收的 BMP 数据报文为正常的 BMP 数据报文，继续对所述正常的 BMP 数据报文进行处理。

本实施例通过获取所接收到的 BMP 报文的 TTL 值，当所述接收到的 BMP 报文的 TTL 值小于预设 TTL 门限值时，将所述 BMP 报文丢弃，实现通过 TTL 值来防止受到伪装 IP 的 DOS 攻击，降低设备的 CPU 占用率，提高设备的使用寿命。

本发明进一步提供一种防止 DOS 攻击系统。

参照图 3，图 3 为本发明防止 DOS 攻击系统较佳实施例的功能模块示意图。

在本实施例中，所述防止 DOS 攻击系统发送端 110 和接收端 220：

所述接收端 220，设置为接收发送端发送的边界网关监测协议 BMP 报文；

所述发送端 110，设置为向所述接收端发送边界网关监测协议 BMP 报文。

在本实施例中，所述发送端 110 优选为路由器，所述接收端 220 优选为服务器。

所述服务器和所述路由器通过 TCP/IP 协议建立链接。所述 TCP/IP 协议是 Internet 最基本的协议，是 Internet 国际互联网的基础，由网络层的 IP 协议和传输层的 TCP 协议组成。所述服务器还可以通过 IPX/SPX 协议等与所述路由器建立链接。在所述 IPX/SPX 中，IPX 主要实现网络设备之间连接的建立维持和终止；SPX 协议是 IPX 的辅助协议，主要实现发出信息的分组、跟踪分组传输，保证信息完整无缺的传输。

所述路由器发送 BMP 数据报文给所述服务器，所述服务器接收所述路由器发送的 BMP 数据报文。优选地，所述服务器和所述路由器都配置了 GTSM。

所述发送端 220，还设置为当向所述接收端发送 BMP 报文时，将所述 BMP 报文的 TTL 值修改成 TTL 的最大值 255。

所述路由器发送的 BMP 数据报文的 TTL 值是经过其数据层面修改的。所述 TTL 值时指定 IP 数据包在被路由器丢弃之前允许通过的最大网段数量，TTL 的作用是限制 IP 数据包在计算机网络中的存在时间，所述 TTL 的最大值是 255，TTL 字段由 IP 数据包的发送者设置，在所述 IP 数据包从源目的的整个转发路径上，每经过一个转发路径上的路由器，所述转发路径上的路由器都会修改这个 TTL 值，具体做法是将所述 TTL 值减 1，然后再把所述 IP 数据包转发出去。因此，优选地，所述路由器将要发送给服务器的 BMP 数据报文的 TTL 值修改成 255。

所述接收端 220，还设置为获取所述 BMP 报文的生存时间 TTL 值；

当所述服务器接收到所述路由器发送的BMP数据报文时，通过其数据层面获取所述BMP数据报文的TTL值。

所述接收端220，还设置为当所述BMP报文的TTL值小于所述预设TTL门限值时，判定所述BMP报文受到DOS攻击，丢弃所述BMP报文；

当所述服务器接收的BMP数据报文的TTL值小于所述预设TTL门限值时，判定所述BMP数据报文受到DOS攻击，为非法的BMP数据报文，所述服务器就会丢弃所述非法的BMP数据报文，不会继续向数据层面的上层传递所述非法的BMP数据报文。

所述接收端220，还设置为根据通用TTL安全保护机制设置所述预设TTL门限值；

优选地，所述预设TTL门限值为所述服务器通过配置的GTSM设置。所述服务器通过其配置的GTSM，根据所述服务器和所述路由器之间的网络拓扑结构设置所述预设TTL门限值，所述网络拓扑结构是指用传输介质互连各种设备的物理布局，指构成网络的成员间特定的物理的，即真实的、或者逻辑的，即虚拟的排列方式。如当所述服务器和所述路由器之间的网络中的转发路径上有10个路由器，则将所述预设TTL门限值设置为245。因为所述路由器发送的BMP数据报文的TTL值每经过一个转发路径上的路由器，所述TTL值就会减1，当所述BMP数据报文经过转发路径上的10个路由器时，所述BMP数据报文的TTL值减小至245，因此将所述预设TTL门限值设置为245，即所述服务器接收的BMP数据报文的TTL值的范围应该在245到255之间。

所述服务器在接收所述路由器发送的BMP数据报文时，会同时接收其它设备发送的受到DOS攻击的BMP数据报文，而所述其它设备发送的的受到DOS攻击的BMP数据报文的TTL值一般都为64或100等，并不会达到255，所以当所述路由器发送的BMP数据报文和所述其它设备发送的受到DOS攻击的BMP数据报文都经过同样个数转发路径上的路由器时，所述其它设备发送的受到DOS攻击的BMP数据报文的TTL值会小于预设TTL门限值。如当所述预设TTL门限值为245时，则当所述服务器接收的BMP数据报文的TTL值小于245时，则判定所述服务器接收的BMP数据报文为非法的BMP数据报文，丢弃所述非法的BMP数据报文。

所述接收端220，还设置为当所述BMP报文的TTL值大于或等于所述预设TTL门限值时，判定所述BMP报文为正常BMP报文，继续对所述BMP报文进行处理；

若所述服务器接收的BMP数据报文的TTL值大于或者等于所述预设TTL门限值，则判定所述BMP数据报文未受到DOS攻击，为正常的BMP数据报文，并将所述正常的BMP数据报文继续向数据层面的上层传递，如向控制层面传递，即继续对所述正常的BMP数据报文进行处理。如当所述预设TTL门限值为245时，则当所述服务器接收的BMP数据报文的TTL值大于或者等于245时，则判定所述服务器接收的BMP数据报文为正常的BMP数据报文，继续对所述正常的BMP数据报文进行处理。

需要说明的是，在本文中，术语“包括”、“包含”或者其任何其他变体意在涵盖非排他性的包含，从而使得包括一系列要素的过程、方法、物品或者装置不仅包括那些要素，而且还包括没有明确列出的其他要素，或者是还包括为这种过程、方法、物品或者装置所固有的要素。在没有更多限制的情况下，由语句“包括一个……”限定的要素，并不排除在包括该要素的过程、方法、物品或者装置中还存在另外的相同要素。

上述本发明实施例序号仅仅为了描述，不代表实施例的优劣。

通过以上的实施方式的描述，本领域的技术人员可以清楚地了解到上述实施例方法可借助软件加必需的通用硬件平台的方式来实现，当然也可以通过硬件，但很多情况下前者是更佳的实施方式。基于这样的理解，本发明的技术方案本质上或者说对现有技术做出贡献的部分可以以软件产品的形式体现出来，该计算机软件产品存储在一个存储介质（如 ROM/RAM、磁碟、光盘）中，包括若干指令用以使得一台终端设备（可以是手机，计算机，服务器，空调器，或者网络设备等）执行本发明各个实施例所述的方法。

以上仅为本发明的优选实施例，并非因此限制本发明的专利范围，凡是利用本发明说明书及附图内容所作的等效结构或等效流程变换，或直接或间接运用在其他相关的技术领域，均同理包括在本发明的专利保护范围内。

工业实用性

本发明实施例提供的上述技术方案，可以应用于 DOS 攻击过程中，通过获取所接收到的 BMP 报文的 TTL 值，当所述接收到的 BMP 报文的 TTL 值小于预设 TTL 门限值时，将所述 BMP 报文丢弃，实现通过 TTL 值来防止受到伪装 IP 的 DOS 攻击。

权 利 要 求 书

1、一种防止拒绝服务 DOS 攻击方法，所述防止 DOS 攻击方法包括以下步骤.

接收发送端发送的边界网关监测协议 BMP 报文；

获取所述 BMP 报文的生存时间 TTL 值；

当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文。

2、如权利要求 1 所述的防止 DOS 攻击方法，其中，所述获取所述 BMP 报文的 TTL 值的步骤之后，还包括：

当所述 BMP 报文的 TTL 值大于或等于所述预设 TTL 门限值时，判定所述 BMP 报文为正常 BMP 报文，继续对所述 BMP 报文进行处理。

3、如权利要求 1 或 2 所述的防止 DOS 攻击方法，其中，所述接收发送端发送的 BMP 报文的步骤之前，还包括：

根据通用 TTL 安全保护机制设置所述预设 TTL 门限值。

4、如权利要求 3 所述的防止 DOS 攻击方法，其中，所述根据通用 TTL 安全保护机制设置所述预设 TTL 门限值的步骤之前，还包括：

通过网络通讯协议与发送端建立链接。

5、一种防止拒绝服务 DOS 攻击装置，所述防止 DOS 攻击装置包括：

接收模块，设置为接收发送端发送的边界网关监测协议 BMP 报文；

获取模块，设置为获取所述 BMP 报文的生存时间 TTL 值；

判定模块，设置为当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文。

6、 如权利要求 5 所述的防止 DOS 攻击装置，其中，所述判定模块，还设置为当所述 BMP 报文的TTL值大于或等于所述预设TTL门限值时，判定所述BMP报文为正常BMP报文，继续对所述 BMP 报文进行处理。

7. 如权利要求 5 或 6 所述的 BMP 报文防止 DOS 攻击装置，其中，所述防止 DOS 攻击装置还包括：

设置模块，设置为根据通用 TTL 安全保护机制设置所述预设 TTL 门限值。

8、 如权利要求 7 所述的 BMP 报文防止 DOS 攻击装置，其中，所述防止 DOS 攻击装置还包括：

建立模块，设置为通过网络通讯协议与发送端建立链接。

9、 一种防止拒绝服务 DOS 攻击系统，所述防止 DOS 攻击系统包括发送端和接收端：

所述接收端，设置为接收发送端发送的边界网关监测协议 BMP 报文；

所述接收端，还设置为获取所述 BMP 报文的生存时间 TTL 值；

所述接收端，还设置为当所述 BMP 报文的 TTL 值小于所述预设 TTL 门限值时，判定所述 BMP 报文受到 DOS 攻击，丢弃所述 BMP 报文；

所述发送端，设置为向所述接收端发送边界网关监测协议 BMP 报文。

10、如权利要求 9 所述的防止 DOS 攻击系统，其中，所述接收端，还设置为当所述 BMP 报文的 TTL 值大于或等于所述预设 TTL 门限值时，判定所述 BMP 报文为正常 BMP 报文，继续对所述 BMP 报文进行处理；

所述接收端，还设置为根据通用 TTL 安全保护机制设置所述预设 TTL 门限值；

所述发送端，还设置为当向所述接收端发送 BMP 报文时，将所述 BMP 报文的 TTL 值修改成 TTL 的最大值 255。

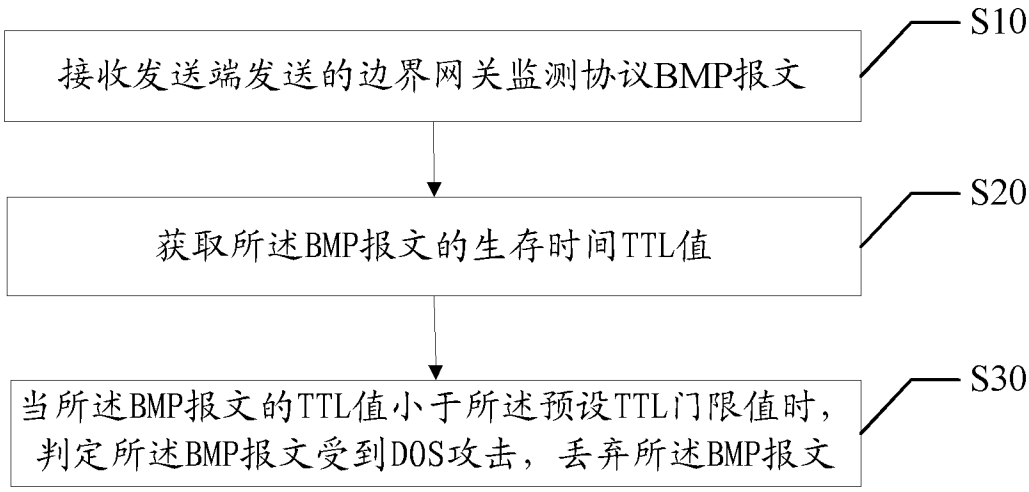
接收发送端发送的边界网关监测协议BMP报文
S10
获取所述BMP报文的生存时间TTL值
S20
当所述BMP报文的TTL值小于所述预设TTL门限值时，判定所述BMP报文受到DOS攻击，丢弃所述BMP报文
S30

图 1

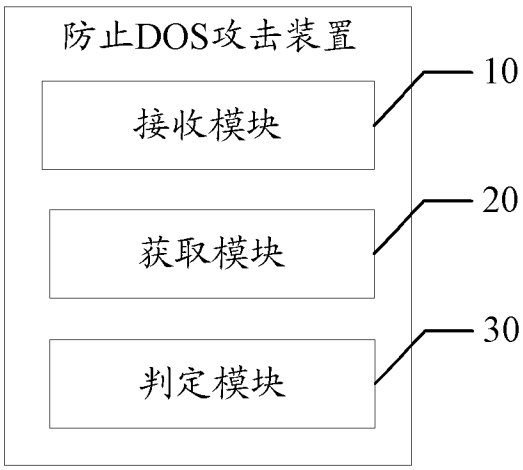
防止DOS攻击装置
接收模块
10
获取模块
20
判定模块
30

图 2

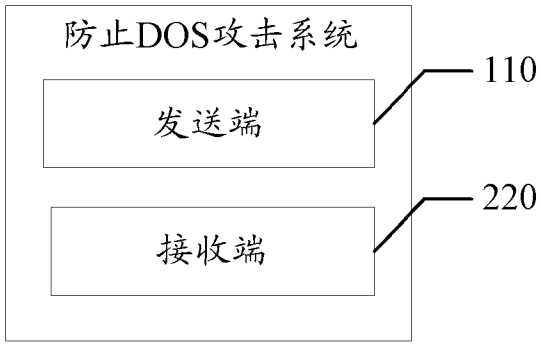

图 3

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2016/076649

A. CLASSIFICATION OF SUBJECT MATTER

H04L 29/06 (2006.01) i; H04L 29/12 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L; H04W; H04Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNABS, CNTXT, CNKI, VEN: Denial of Service, DOS, attack, packet, TTL, Time To Live

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	CN 101674312 A (ZTE CORP.), 17 March 2010 (17.03.2010), claims 1-7, description, page 3, 2nd line from the bottom to page 5, line 21, and page 6, paragraph 2	1-10
A	CN 104348749 A (HUBEI YUHENG TECHNOLOGY CO., LTD.), 11 February 2015 (11.02.2015), the whole document	1-10
A	CN 104125242 A (BEIJING UNIONREAD INFORMATION TECHNOLOGY LTD.), 29 October 2014 (29.10.2014), the whole document	1-10
A	JP 2006345347 A (MATSUSHITA ELECTRIC IND CO., LTD.), 21 December 2006 (21.12.2006), the whole document	1-10

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 May 2016 (20.05.2016)	**27 May 2016 (27.05.2016)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **SUN, Yufang** Telephone No.: (86-10) **62089367**

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2016/076649

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101674312 A	17 March 2010	CN 101674312 B	19 December 2012
CN 104348749 A	11 February 2015	None	
CN 104125242 A	29 October 2014	CN 104125242 B	13 May 2015
JP 2006345347 A	21 December 2006	None	

国际检索报告

国际申请号 PCT/CN2016/076649

A. 主题的分类

H04L 29/06(2006.01)i; H04L 29/12(2006.01)i

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

H04L; H04W; H04Q

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNABS,CNTXT,CNKI,VEN:拒绝服务，攻击，报文，生存时间，Denial of Service, DOS,attack, packet,TTL,Time To Live

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
X	CN 101674312 A (中兴通讯股份有限公司) 2010年 3月 17日 (2010-03-17) 权利要求1-7，说明书第3页倒数第2行到第5页第21行，说明书第6页第2段	1-10
A	CN 104348749 A (湖北誉恒科技有限公司) 2015年 2月 11日 (2015-02-11) 全文	1-10
A	CN 104125242 A (北京阅联信息技术有限公司) 2014年 10月 29日 (2014-10-29) 全文	1-10
A	JP 2006345347 A (MATSUSHITA ELECTRIC IND CO LTD) 2006年 12月 21日 (2006-12-21) 全文	1-10

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2016年 5月 20日	2016年 5月 27日

ISA/CN的名称和邮寄地址	受权官员
中华人民共和国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088	孙玉芳
传真号 (86-10)62019451	电话号码 (86-10)62089367

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2016/076649

检索报告引用的专利文件			公布日 (年/月/日)	同族专利			公布日 (年/月/日)
CN	101674312	A	2010年 3月 17日	CN	101674312	B	2012年 12月 19日
CN	104348749	A	2015年 2月 11日		无		
CN	104125242	A	2014年 10月 29日	CN	104125242	B	2015年 5月 13日
JP	2006345347	A	2006年 12月 21日		无		