**MiddlePolice: Fine-Grained Endpoint-Driven In-Network Traffic Control for Proactive DDoS Attack Mitigation（MiddlePolice:用于主动DDOS攻击缓解的细粒度端点驱动的网内流量控制）**

**1.文章内容属于计算机网络的哪一层；**

应用层与传输层

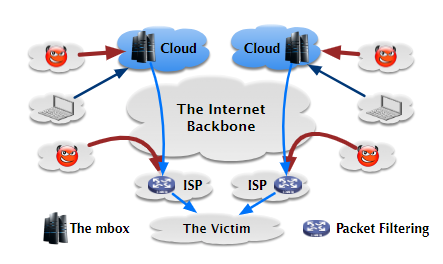
目前的DDOS攻击主要分为两个大类，分别为Layer 4和Layer 7，也叫做第四层攻击和第七层攻击。

Layer 4 DDOS攻击主要是发生在传输层，而传输层的功能主要是一些网络协议，所以像TCP/ACK攻击，DNS反射型攻击之类的都是在Layer 4这一层。因为它是属于协议类型攻击，那么就会需要大量的资源（IP和流量），所以这一层攻击也常在僵尸网络DDOS攻击里面出现，而这类攻击的攻击对象主要是个人电脑，web服务器等网络设备。

Layer 7 DDOS攻击主要是发生在应用层，比如某一个错误的指令导致系统死机或者下线。像JOOMLA攻击，GET攻击之类的就属于Layer 7攻击。这里有个误区，大部分人认为Layer 7攻击只可以发生在web服务器上，其实不然，它也可以用作在个人手机，电脑上等。

**2.文章解决了什么问题，是如何解决的；**

本文介绍了一种将dos-protection-as-service解决方案的部署能力与基于目的地的网络能力系统控制相结合的中间件。通过允许从目的地到提供者的反馈，MiddlePolice可以有效地执行目的地选择的控制策略，而不需要来自无关方的部署。



中间的受警察保护的受害者将其通信重定向到mboxes。每个mbox负责管理遍历的交通，以执行受害者选择的交通控制策略。交通警察依赖于中间警察生成的功能的反馈循环来消除下游路径上的部署需求。当受害者将其IP地址保密时，一个部署mbox就可以保护从mbox到受害者的整个下游路径。对于IP地址暴露的受害者，攻击者可以通过将mbox和直接攻击流量传递给受害者。同样的漏洞能力也适用于现有的基于云的ddos预防系统。为了解决这个问题，中间警察设计了一个包过滤机制，该机制依赖于商品路由器或交换机上的ACL来消除不经过任何mbox的流量。只要每个瓶颈链路都受到上游过滤器的保护，就可以防止旁路攻击。

**Middle Police’s traffic policing algorithm**

(i)探测从每个mbox到受害者的可用下游带宽

估计下游带宽的根本挑战是，中间警察不需要在下游链路部署。这样的挑战是双向的:过高的估计将导致下游洪水泛滥，使交通管理变得毫无用处，而过低的估计将浪费下游的容量，影响网络性能。

为了解决高估问题，中间警察依赖于可接受性反馈机制，让发送者自我报告他们成功地向受害者发送了多少包。具体地说，在数据包到达时，mbox会在数据包中标记一个不可伪造的功能。当数据包被发送到受害者时，部署在受害者上的中间警察的能力处理模块(CHM)将携带的能力返回给mbox。如果在足够长的时间间隔(与mbox和受害者之间的RTT相比)之后，该功能没有返回到mbox, mbox将认为数据包丢失。因此，反馈使mbox能够推断每个发送方的包丢失率(以下简称LLR)。然后，mbox将下游容量估计为从所有发送方接收到的数据包数与在下游路径上丢失的数据包数之差。由于该方法是基于向受害者发送的交通量来进行估计的，因此解决了过估计问题。

为了防止低估，mbox将来自每个发送方的包分类为特权包和最优包。具体地说，mbox为每个发送方维护一个速率窗口WR，以确定每个周期(下称检测周期)中允许发送方使用的特权包的数量。WR的计算是基于上述下游容量估计以及受害者选择的策略。发送到wr之外的包被分类为“最佳工作包”。mbox将所有特权包转发给受害者，而对于best-effort包的转发决策受制于一个短期的包丢失率(以下简称SLR)。SLR在RTT粒度上反映了下游包丢失率(拥塞)。也就是说，如果在到达一个best-effort包时下游没有阻塞，mbox将转发该包。因此，即使下游容量(以及WR)被低估，只要下游路径不拥挤，mbox仍然可以进一步发送数据包。公平的制度。每个mbox根据受害者选择的共享策略在其发送方之间分配其带宽估计。

(ii)为发送者分配带宽，以执行受害人所选择的交通管制政策。

**PACKET FILTERING**

（i）过滤原语：

每个mbox将它的遍历包封装到UDP包中，并使用UDP源端口和目标端口(总共32位)来携带一个身份验证器，这是它们的box和过滤点之间共享的秘密。因此，使用随机端口号的500Gbps攻击(Ar-bor Networks观察到的最大攻击)将减少到∼100 bps，因为正确猜测的概率是 2\*\* （-32）。共享密钥可以基于密码安全的伪随机数生成器定期协商。我们不依赖UDP源地址过滤，以避免源欺骗。

（ii)packet 过滤点:

部署的过滤点应该有足够的带宽，以便旁路攻击流量不会在过滤之前造成包丢失。过滤机制应该部署在DDoS攻击导致的每个瓶颈链接上，或者上游。对于具有高带宽连接的受害服务器，如果瓶颈链接是受害者网络中的内部链接，那么受害者可以在其网络的入站点部署过滤器。如果瓶颈链接是连接受害者与其ISP的链接，受害者可以与ISP合作，在商业上合理的条件下，在ISP的网络中更深地部署过滤器，以便旁通流量无法到达受害者的网络。

**3.与其他方法相比，文章有哪些创新点？是否存在不足；**

解决DDos 攻击的一种实用方法是将所有目标流量(例如通过 DNS 或 BGP )重定向到一个第三方的、DDoS-protection-as-a-service提供商(例如CloudFlare)，该提供商配备了良好的过滤机制，在将剩余的良性流量传递到目标之前删除攻击流量。这种方法很有吸引力，因为它们不需要修改现有的网络基础设施，并且可以扩展以处理非常大的攻击。然而，这些基于云的系统使用专有的攻击检测算法和过滤算法，因此它们无法强制执行客户所需的业务或应用程序驱动。其次，由于客户不知道刷洗算法，误报可能导致实际客户在不知不觉中流失给受害者。最后，现有的基于云的系统假设所有发送给受害者的通信都将首先路由到它们的基础设施，这一假设可能会被聪明的攻击者所违反。

另一种本地方法基于网络功能的概念，其中源发送速率由接收方同意以网络强制执行的功能的形式确定。虽然第三方清理服务和网络功能都可以有效地减少不堪重负的目的地的不必要流量，但DDoS-protection-as-a-service解决方案将所有调度决策(例如公平、优先级和攻击识别)外包给了提供者，而基于能力的解决方案则需要对现有基础设施进行大量修改才能运行。这些基于功能的系统并非没有挑战，而且大多数都面临着重大的部署障碍。需要跨不同自治系统的密钥管理和路由器升级。或者，有些方法要求客户端修改他们的网络堆栈，以插入定制的packet headers，这造成了额外的部署障碍.

从技术上讲，Middle Police将基于云的解决方案的部署能力与基于功能的系统的基于目的地的控制相结合。实现这一目标的关键思想是将监控功能从Internet核心转移到云基础设施。每个潜在的DDoS受害者服务器使用MiddlePolice的防御选择一个或多个云提供商，并使用DNS将其流量定向到由其选择的云提供商部署的交警单位(称为mbox)。每个mbox通过一个自生成功能的反馈循环来评估其到受害者的路径状态，并对发送给受害者的流量进行管理，以实现细粒度的流量控制。此外，Middle Police还包括一种过滤几乎所有试图绕过它们的流量的机制，只使用在普通路由器上已经存在的 ACL 配置。MiddlePolice还可以实现ARROW针对关键流量的特殊通行证，并为高级客户提供优先级服务。

Middle Police 的特点：

* 易于部署和扩展；
* 目的地驱动的传输控制策略；
* 修复旁路漏洞（解决暴露IP地址问题，防止流量绕过云基础设施，直接传给受害服务器）

不足：无法解决局域网内DDoS攻击，以及ARP欺骗和攻击

**4、若存在不足，请给出解决方案。**

* **双绑措施**是在路由器和终端上都进行IP-MAC绑定的措施，它可以对ARP欺骗的两边，伪造网关和截获数据，都具有约束的作用。这是从ARP欺骗原理上进行的防范措施，也是最普遍应用的办法。它对付最普通的ARP欺骗是有效的。
* **ARP个人防火墙**是通过在终端电脑上对网关进行绑定，保证不受网络中假网关的影响，从而保护自身数据不被窃取的措施。
* **VLAN和交换机端口绑定**通过划分VLAN和交换机端口绑定，以图防范ARP，也是常用的防范方法。做法是细致地划分VLAN，减小广播域的范围，使ARP在小范围内起作用，而不至于发生大面积影响。同时，一些网管交换机具有MAC地址学习的功能，学习完成后，再关闭这个功能，就可以把对应的MAC和端口进行绑定，避免了病毒利用ARP攻击篡改自身地址。也就是说，把ARP攻击中被截获数据的风险解除了。
* **PPPoE**网络下面给每一个用户分配一个帐号、密码，上网时必须通过PPPoE认证，这种方法也是防范ARP措施的一种。PPPoE拨号方式对封包进行了二次封装，使其具备了不受ARP欺骗影响的使用效果。