文章编号：1005-8451（2011）11-0011-03

身份与位置分离映射网络中的DDoS研究

张栋纯，刘 颖，高德云
（北京交通大学 电子信息工程学院，北京 100044）

摘 要：身份与位置分离映射网络将IP地址的双重属性分离，解决了传统网络中的许多问题，同时，也对DDoS（Distributed Denial of Service，分布式拒绝服务）攻击有很大的缓解作用。本文将传统网络和身份与位置分离映射网络中的DDoS攻击流量进行了定量对比分析，证明了身份与位置分离映射网络对DDoS攻击具有很好的缓解作用。

关键词：DDoS攻击；身份与位置分离映射网络；攻击流量
中图分类号：TP393 文献标识码：A

Research on DDoS in Mapping Network of Identity and Location Identifier Separating

ZHANG Dong-chun, LIU Ying, GAO De-yun
(School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: The Mapping Network of Identity and Location Identifier Separating could separate the dual attributes of the IP address to solve many problems in traditional network. It could also mitigate the effect of DDoS(Distributed Denial of Service) attack. In this paper, by analysing and comparing the attack traffic in both of the traditional network and the Mapping Network of Identity and Location Identifier Separating, it was proved that the Mapping Network of Identity and Location Identifier Separating could play a good role in the mitigation of DDoS attack.

Key words: DDoS attack; Mapping Network of Identity and Location Identifier Separating; attack traffic

近年来，互联网的诸多问题日益显现，如路由可扩展问题、移动性支持能力差、安全性问题等。IP地址的身份与位置双重属性是引发这些问题的原因之一[2]。身份与位置分离映射网络能够彻底解决IP地址的双重属性问题，其中，2007年我国启动的“973”项目“一体化可信网络与普适服务体系基础研究”中提出的一体化网络[3]就属于身份与位置分离映射网络。在身份与位置分离映射网络中，使用主机地址（IPha）代表终端的身份信息，路由地址（IPra）代表终端的位置信息。终端进行通信时，仅使用主机地址进行通信，终端用户只知道自己的身份，而不知道拓扑位置。

文献[1]给出的近几年DDoS攻击的流量增长数据表明，DDoS攻击对互联网正常运作造成的危害日益严重。DDoS的攻击者通过控制大量“僵尸主机”（被攻击者入侵过或可间接利用的主机），向受害主机发送大量看似合法的网络包，从而造成网络阻塞或服务器资源耗尽，使合法用户无法正常访问服务器的网络资源。身份与位置分离映射网络将IP地址的双重属性分离，对传统网络中的DDoS攻击有很大的缓解作用。

1 DDoS攻击分析

DDoS攻击广义地分为软件漏洞利用型和流量攻击型两类，本文将重点对流量型的DDoS攻击进行分析，用受攻击主机接收到的攻击流量来度量DDoS的攻击效果。

1.1 分析假设

为了分析证明身份与位置分离映射网络对DDoS攻击的缓解作用，作出如下假设：

（1）对传统网络和身份与位置分离映射网络，采用相同的拓扑结构进行分析，如图1。

图中T为攻击主机，攻击的目标主机是主机B，即攻击者T控制网络中的其他主机作为“僵尸主机”，对主机B发起DDoS攻击。

收稿日期：2011-01-24
基金项目：国家自然科学基金（60833002）；中央高校基本科研业务费专项资金资助（2011JBM016，2011JBM012）。
作者简介：张栋纯，在读硕士研究生；刘 颖，讲师。

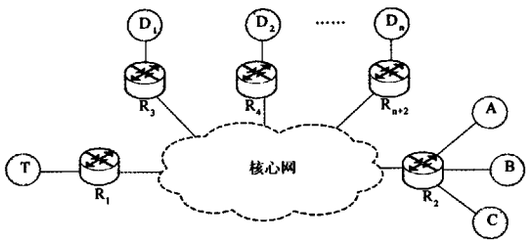

图1 网络拓扑结构

（2）所有“僵尸主机”与目标主机之间，都有一条可达链路，其中，位于目标主机本地网络内部的链路，由于有较高的带宽，能够通过的流量较大，而外地链路能够通过的流量较小[4]。这里假设外地链路最大流量为b(Mbps)，本地链路的最大流量为cb(Mbps，c>1)。目标主机通常是服务器，对链路带宽的要求较高，因此假设与目标主机直连的链路最大流量为一个较大值T(Mbps)。设传统网络下攻击者制造的最大攻击流量为F_1，在身份与位置分离映射网络下制造的最大攻击流量为F_2。

（3）攻击者的能力有限，只能控制网络中的部分主机发起攻击，设受控主机的数量为k。攻击者为了造成最大程度的损害，会控制“僵尸主机”对目标主机造成尽可能大的攻击流量。

1.2 传统网络分析

在传统网络中，攻击者可以根据一个终端的IP地址同时获得该终端的身份信息和拓扑位置信息，且由于本地链路能够通过的流量较大，因此攻击者将有针对性地选取距离目标主机近的主机进行控制（主机A和C），以产生最大的流量。依据假设，DDoS攻击者能够制造的最大攻击流量为

$$F_1=\begin{cases}(k-2)\,b+2\,c\,b\,,\ [(k-2)\,b+2\,c\,b]<T\\ T\,,\ [(k-2)\,b+2\,c\,b]\geqslant T\end{cases}\qquad(1)$$

1.3 身份与位置分离映射网络分析

在身份与位置分离映射网络中，由于攻击者仅能获知终端的身份信息，而无法获取终端的拓扑位置信息，因此只能随机选取网络中的主机进行控制，发起攻击。依据假设，DDoS攻击者能够制造的最大攻击流量有3种可能情形：（1）随机选取的主机全部在目标主机B的外地链路，设该情况最大攻击流量为$F_{2,1}$，发生的概率为$P_{2,1}$；（2）随机选取的主机仅有一台在目标主机B的本地链路，设该情况最大攻击流量为$F_{2,2}$，发生的概率为$P_{2,2}$；（3）随机选取的主机恰好有两台在目标主机B的本地链路，设该情况最大攻击流量为$F_{2,3}$，发生的概率为$P_{2,3}$。

综合以上3种情形，在身份与位置分离映射网络下，DDoS攻击者能够制造的平均最大攻击流量为：

$$\begin{aligned}F_2&=F_{2,1}\,P_{2,1}+F_{2,2}\,P_{2,2}+F_{2,3}\,P_{2,3}\\&=\begin{cases}k\,b\,\dfrac{(n-k+2)\,(n-k+1)}{(n+2)\,(n+1)}+[(k-1)\,b+c\,b]\,\dfrac{2\,k\,(n-k+2)}{(n+2)\,(n+1)}\\ \quad+[(k-2)\,b+2\,c\,b]\,\dfrac{k\,(k-1)}{(n+2)\,(n+1)}=f',\ f'<T\\ T\ ,\ f'\geqslant T\end{cases}\end{aligned}\qquad(2)$$

1.4 对比分析及结论

比较2种网络下DDoS攻击者能够制造的最大攻击流量，即F_1与F_2的大小。设c=10，b=1(Mbps)，T=50(Mbps)。

首先，考虑攻击者能力固定，即“僵尸主机”数量k固定的情况下，随着网络拓扑的扩大，即随着n的增大，攻击者制造的攻击流量对比。假设k=3，F_1和F_2的值变化如图2。

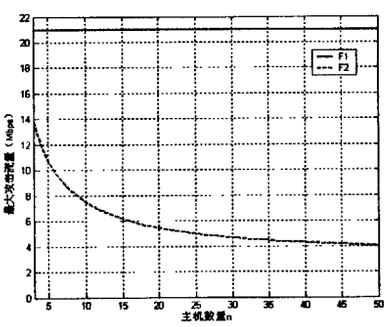

图2 攻击流量随主机总数的变化情况

从图中可以看出，随着n的增加，F_1不改变，而F_2不断减小，且F_2始终小于F_1。并且随着n的增大，F_2逐渐接近于3（Mbps），这个值是当“僵尸主机”全部位于目标主机B的外地链路时产生的攻击流量值。

可见，随着网络规模的增大，DDoS攻击者在身份与位置分离映射网络中制造的攻击流量将逐渐降低，并趋向一个固定的值，在传统网络中的攻击流量不会变化。并且身份与位置分离映射网络中的最大攻击流量始终小于传统网络，因此身份与标识分离映射网络对于DDoS攻击有明显的缓解作用。

考虑另外一种情况，当网络中的主机数量一

定，即n固定，攻击者的能力逐渐增加，即攻击者控制用于DDoS攻击的僵尸主机数量k增加，得到的结果如下。

当n=100，随着k的增加，F_1和F_2的变化如图3。

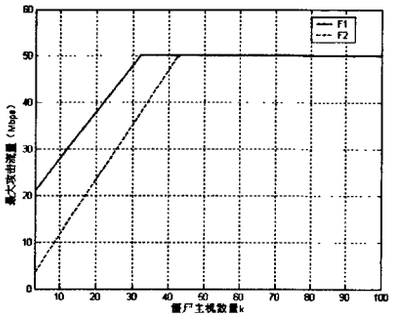

图3　攻击流量随僵尸主机数量的变化情况

图3中，在n不变的情况下，随着k的增加，F_1和F_2都不断增加，但是F_2始终小于等于F_1。F_1和F_2的差值逐渐减小，当攻击者能够制造的攻击流量达到T时，$F_1=F_2=T$，二者相等。当k较小时，F_1与F_2的差值较大。

这说明在2种网络中，随着攻击者能够控制的主机数量增加，DDoS攻击对目标主机的攻击流量都会逐渐增大。但是身份与位置分离映射网络中的攻击流量始终不超过传统网络。当攻击者能够控制的主机数量较少时，身份与位置分离映射网络中的攻击流量与传统网络中的攻击流量相比，相差较多，这说明身份与位置分离映射网络对DDoS攻击的缓解作用在攻击者能力不强的情况下尤为明显。同时，在身份与位置分离映射网络中，要达到与传统网络相同的攻击流量，攻击者需要控制更多的主机，才能达到目的。

2　结束语

身份与位置分离映射网络能够解决传统互联网存在的诸多问题，本文分析了它对DDoS攻击的缓解作用。随着对身份与位置分离映射网络研究的不断深入，其相对于传统互联网的优势将愈发明显，是未来网络的发展方向，有着广阔的发展及应用前景。

参考文献：

[1] Jose N. DDoS Attack Evolution [J]. Network Security, 2008 (7): 7-10.

[2] David C, Robert B, Aaron F, Venkata P. FARA: Reorganizing the Addressing Architecture. Proc. Proceedings of the ACM SIGCOMM workshop on Future Directions in Network Architecture (FDNA)[C]. Karlsruhe, Germany, August 2003, pp. 313-321.

[3] 张宏科，苏　伟. 新网络体系基础研究——一体化网络与普适服务[J]. 电子学报，2007，35（4）：593-598.

[4] Wu-chun F, Hurwitz, J, Newman H. Optimizing 10-Gigabit Ethernet for Networks of Workstations, Clusters, and Grids: A Case Study. Proceedings of the 2003 ACM/IEEE conference on Supercomputing[C]. November 2003, pp. 50.

责任编辑　陈　蓉

（上接P10）

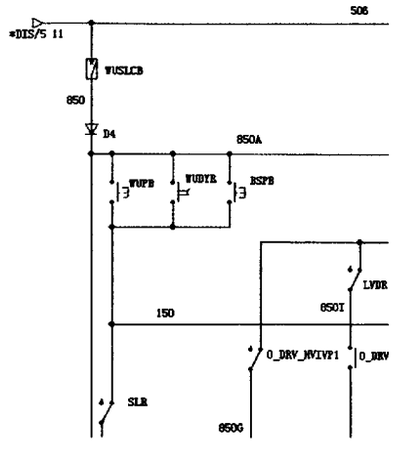

图3　经设置传入状态部分效果图

4　结束语

经测试应用，该平台能够快速便捷的输入大量城轨列车电路原理图，可适用于不同型号的列车，具有较强的可扩展性和可移植性。平台不仅能够用于列车电路原理教学，还可以用于电路设计和电路逻辑验证等仿真。

参考文献：

[1] 和青芳. 计算机图形学原理及算法教程[M]. 北京：清华大学出版社，2005.

责任编辑　陈　蓉