用活动IP表和ICMP报文防御IP欺骗DDoS攻击

陈 伟，罗绪成，秦志光

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】介绍了分布式拒绝服务攻击的原理；分析了四种具有代表性的防御方法；提出一种针对IP欺骗DDoS攻击的防御方法，在自治系统边界，利用活动IP记录表对进入自治系统的数据包进行处理，来自活动IP的网络流直接通过；没有活动记录的IP数据包被自治系统边界路由器或邻近边界的路由器丢弃，并发送网间控制报文协议(ICMP)超时差错报文通报源节点，IP不活动的IP欺骗DDoS攻击数据包不能到达受害节点；被丢弃的合法数据包由其源节点上层协议或应用进行重传。

关 键 词 活动IP; DDoS; IP欺骗
中图分类号 TP393.08 文献标识码 A

IP Spoofing DDoS Defense Using Active IP Record and ICMP Message

CHEN Wei，LUO Xu-cheng，QIN Zhi-guang

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract This paper describes the principle of Distributed Denial of Service (DDoS) attack. Several representative defense methods are analyzed to against it. A defense method against IP spoofing DDoS attack is proposed. An active IP record table is used to detect all IP packets passing through the border of autonomy system in this method. Packets of the source IP address which are not active will be discarded by the border routers or routers near the border in the autonomy system, according to the Internet Control Message Protocol (ICMP) protocol, timeout ICMP messages will be sent to the source IP hosts, and thus, IP spoofed packets will be discarded, because their source IP usually are not active. Although some legal packets will also be discarded, the retransmission will be triggered by the timeout ICMP messages immediately.

Key words active IP; distributed denial of service; IP spoofing

分布式拒绝服务攻击(DDoS)是目前最流行的一种网络攻击方式，其原理简单，易于实现，攻击破坏力极强，对当前网络的安全构成了很大的威胁[1]。

DDoS攻击者通常分布于Internet中的大量安全防御级别较低的节点作为攻击傀儡机，组成多级的DDoS攻击僵尸网络，通过向僵尸网络发送远程控制命令，协同大量的傀儡机直接或间接向其攻击目标发送大量的网络分组。这些网络分组在受害端汇聚成压倒性的网络流量，耗尽受害者的网络带宽或系统资源，从而造成对合法用户的拒绝服务[1]。

DDoS攻击通常运用IP欺骗技术对攻击源地址进行伪装，增大了攻击破坏力，同时也增加了依据数据包源地址进行攻击溯源以及安全审计、取证的难度。

DDoS攻击的防御一直是一个难点，近年来，研究人员在该领域展开深入的研究，提出了许多防御方法，仍然没有找到很好的解决办法。

1 相关工作

本文分析了四种具有代表性的DDoS防御方法，包括入口过滤、源回溯、回推等。

1.1 入口过滤

入口过滤[2]在ISP边界路由器实施，对从ISP网络进入Internet的数据包进行检测过滤，拦截具有非法源IP地址的数据包，主要针对源IP欺骗DDoS攻击。ISP网络边界路由器检查数据包源IP地址是否属于ISP网络所辖网络地址范围，丢弃源IP不属于该ISP网络的数据包。

入口过滤在攻击源端实施，是对IP欺骗DDoS攻击最简单、有效的防御方法。但该防御方法在客户

收稿时间：2007－09－07
基金项目：电子信息产业发展基金重点招议标项目(信部运[2005]555)
作者简介：陈 伟(1978－)，男，博士生，主要从事信息安全方面的研究；罗绪成(1974－)，男，博士生，主要从事分布式系统信息安全、对等计算、网络安全等方面的研究；秦志光(1956－)，男，教授，博士生导师，主要从事网络计算、信息安全等方面的研究.

网络自身的路由器上实施，在牺牲路由器部分资源、影响路由转发效率的同时，却不能给ISP带来直接的利益，也不能直接对ISP网络的安全提供防护；而且需要在全网范围内大规模实施，因此入口过滤一直没有得到有效的推广和实施。

1.2 源回溯

源回溯[3]是在数据包传输过程中，由路由器或其他网络组件记录或标记所经过的全部或部分节点。接受方根据记录的节点信息重构数据包的近似传输路径，源回溯需要通信子网、ISP 的支持和协作。

源回溯的方法有很多，一些需要较长的路径回溯时间，另一些则会产生额外的数据流，从而加重网络的负载。而且数据包传输节点也可能被攻击者控制，破坏路径回溯。另外，使用源回溯得到的攻击路径处理DDoS攻击也存在各ISP协作以及响应时间等问题。

1.3 路由回推

路由回推[4]基于拥塞控制的思想，当某条链路流量达到该链路拥塞阈值时，路由器丢弃数据包，同时检查造成其拥塞的入口链路，并通知这些链路的上游路由器，要求其对网络流量进行相应的限制。上游路由器以同样的方式进行流量限制，并回推给上游路由器。

1.4 基于路由跳数的过滤

基于路由跳数的过滤[5]是位于受害端的DDoS攻击防御方案，数据包从源端到目的端(Tome to Live，TTL)值的变化反应了数据包从源地址到目的地址所经过的路由跳数。而经IP欺骗后的数据包TTL值变化所反应的路由跳数一般与伪造的源IP到目的IP的路由跳数不一致，因此可以作为检验数据包源IP是否经过伪造的依据。该防御方法需要维护一张较大源IP、TTL值表，在进行防御时表的查询匹配需要消耗不少的系统资源。另外，资深攻击者在进行IP欺骗时，可将伪造IP匹配的TTL作为数据包TTL，从而躲避了该防御方法。

2 使用活动IP记录和ICMP报文的IP欺骗DDoS防御方法

本文提出了一种适用于自治系统边界的IP欺骗DDoS攻击防御方法，保障网络和系统在遭到IP欺骗DDoS攻击时仍能正常提供网络服务。该方法基于大量DDoS攻击都采用源IP欺骗的事实[6]，定义了一个活动IP记录表[7]。活动IP是其真实性得到确认的IP，非活动IP则是真实性还没得到确认的IP，IP欺骗攻击所使用的源IP就是非活动IP。

该DDoS防御方法不依赖于攻击检测，利用活动IP表在自治系统边界，对进入其中的网络流进行限制，优先让来自活动IP的网络流通过；而对来自非活动IP的网络流并不是简单地丢弃，而是减小其TTL值，使其被后面的边界或邻近边界的路由器丢弃。根据TCP/IP协议，路由器丢弃TTL超时数据包的同时，发送ICMP数据包超时差错报文，通知源节点[8]。若源节点是真实的，其上层协议或应用会对该数据包进行重传；重传后的数据包IP被加入活动IP表，从而承认其真实性。活动IP表仅暂时延缓了其网络流的传输，后续的网络流将被优先通过；而IP欺骗产生的IP由于不可达，因此欺骗流量被永久地丢弃。

2.1 防御架构

防御架构的实施位于受害端与中间网络之间的受害网络边界——自治系统边界[9]，此时攻击流量已经汇聚到了一定规模，利于进行攻击的检测；而且在此处可以将防御任务分配到有限的多点[10]，避免出现网络流量瓶颈的同时，又提供了一定的防御缓冲，对以网络带宽为攻击目标的DDoS攻击能起到一定的防御效果[11]。

若自治系统与Internet主干网络之间通过多条链路进行连接，则该方法可以同时在这多条链路的边界实施防御，分解攻击防御的压力。同时，该方法的多个防御节点彼此独立，不需要各个防御节点进行协作，因此不会引入实现复杂性。

2.2 活动IP表

活动IP表将IP在数据包源地址中出现的频度作为该IP是否活动的准则，与自治系统建立连接，或请求建立连接的IP被判定为活动IP加入活动IP表；而IP欺骗通常随机产生IP，出现的频度较低，因此被判定为非活动IP。

活动IP表的大小用于设定防御网关所能承受的最大网络流量，可以由网络管理员手动设定，也可以在没有攻击的情况下，由程序根据通过的网络流量曲线自学习获得。

DDoS防御网关收到数据包以后，将数据包源IP用于活动IP表查询，命中则直接放行数据包；没有命中的数据包被标记后放行。标记即对其TTL字段修改，随机改为一个较小的值为 0～n，n根据自治系统的大小而定，确保数据包在到达受害主机之前被丢弃。

活动IP表记录与系统已建立连接的IP和正在请

求建立连接的IP，因此它由连接IP表和请求IP表两部分构成，如图 1 所示。

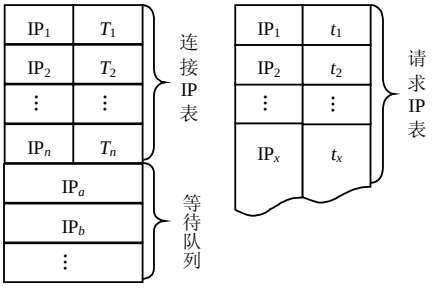

图1　活动IP表

2.2.1　连接IP表

连接IP表中的IP与系统已建立连接，为真实IP地址。每个IP都对应一个时间值，表示该IP的预计存活时间T，在该时间内来自该IP的每个数据包将被放行，同时刷新IP的预计存活时间。

2.2.2　请求IP表

请求IP表用于记录正在请求与自治系统建立连接的IP。当防御网关收到来自连接IP表以外IP的数据包时，为该IP在请求IP表中建立一个表项。这些IP地址的真实性或活动性还有待进一步的考证。同样，该表中每一IP表项也对应一个时间值——等待证实时间，在该时间内有来自该IP地址的数据包到达，或来自该IP的数据包达到某个数值，则说明该IP为真实IP，该IP被移至连接IP表中。如果连接IP表满，则放入等待队列中排队；若等待证实时间超时，没有收到来自该IP的数据包，则说明该IP不活动，将被从请求IP表中移除。

2.3　防御流程

用活动IP表和ICMP报文防御IP欺骗DDoS攻击流程如图 2 所示。初始时活动IP表为空，在连接IP表未满的情况下，数据包到达以后不进行活动IP表匹配而直接通过，同时将数据包源IP记录到连接IP表中。

连接IP表满后，数据包到达后首先进行源IP的连接IP表匹配，命中后放行数据包，并刷新预计存活时间；未命中则进行请求IP表匹配。命中后检查连接IP表是否未满，未满则移至其中；否则放入连接IP表等待队列，同时放行该数据包。当连接IP表有表项超时移除时，将等待队列首项移至其中。若查询请求IP表未命中，则该数据包为非活动IP数据包，将其源IP插入请求IP表，同时修改其TTL进行标记，并放行。

经标记后的非活动IP数据包在自治系统中路由转发至TTL为 0 后，路由器将其丢弃，并发送ICMP生命期超时差错报文通告源节点。

真实源节点收到ICMP差错报文，由上层协议或应用进行响应，重传的数据包将命中请求IP表，同时该IP会被标记了连接IP。

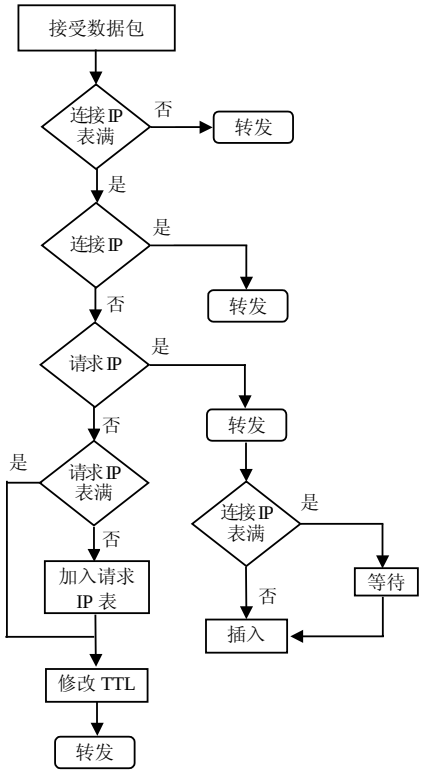

图2　DDoS攻击防御流程

3　结 束 语

DDoS攻击是目前网络安全的一大威胁，由于攻击数据包没有明显的特征，使标识攻击流量很困难，因而很难从网络流量中准确地过滤攻击流量。另外大多数的DDoS攻击都采用IP欺骗技术，增强了攻击效果，藏匿了攻击形迹，增大了攻击防御以及安全审计、取证的难度，同时解除攻击者被法律制裁的后顾之忧，进一步刺激了攻击者进行攻击、破坏的欲望。

本文跳出传统DDoS防御方法溯源或在受害端实施检测响应的思路，提出了一种结合活动IP连接记录和ICMP报文的DDoS攻击防御方法，以高速硬件网络处理设备为DDoS攻击防御网关，部署在用户自治网络的边界入口路由器之前，在DDoS发生时，依据活动网络连接记录优先让活动网络连接的数据流通过。通过修改TTL值，让身后的边界或邻近边界的路由器丢弃非活动连接的数据包，并发送ICMP差错报文通报源节点。丢弃IP欺骗数据包的同时，

仅延缓合法用户数据包的传送，从而保障了网络和系统正常服务的能力。

多台 DDoS 防御网关可在用户自治系统边界的多条入口链路独立、并行地处理网络流，横向分摊了攻击防御压力。将数据包 TTL 修改为较小随机值，并将丢包的任务随机分配给边界路由器或邻近边界的若干路由器，纵向分解了路由器丢包压力，保障了网络流处理速率，避免了单点失效。

参 考 文 献

[1] CERT Advisory. Denial of service[C/OL]. http://www.cert.org/tech tips/denial of service.html, 1999-05-16.
[2] MIRKOVIC J, REIHER P. A taxonomy of DDoS attack and DDoS defense mechanisms[J]. SIGCOMM Computer Communication, 2004, 34(2): 39-53.
[3] ALJIFRI H. IP traceback: a new denial-of-service deterrent[J]. Security & Privacy Magazine, 2003, 1(2): 24-31.
[4] IOANNIDIS J, BELLOVIN S. Implementing pushback: router-based defense against DOS attacks[C]//In Proceedings of the Network and Distributed System Security Symposium (NDSS). San Diego, USA: [s.n.], 2002.
[5] JIN C, WANG H, SHIN K G. Hop-count filtering: An effective defense against spoofed DDoS traffic[C]//In Proceedings of the 10th ACM Conference on Computer and Communications Security. New York, USA: ACM Press, 2003.
[6] PERRIG A, SONG D, YAAR A. StackPi: a new defense mechanism against IP spoofing and DDoS attacks[R]. CMU, 2002.
[7] CHALLITA A, HASSAN M E, MAALOUF S, et al. A survey of DDoS defense mechanisms[C]//In 3rd FEA Student Conference Proceeding. Beirut, USA: America University, 2004.
[8] POSTEL J. Internet control message protocol[EB/OL]. http://www.ietf.org/rfc/, 1981-09-01.
[9] HANDLEY M, GREENHALGH A. Steps towards a DOS resistant internet architecture[C]//In ACM SIGCOMM Workshop on Future Directions in Network Architecture (FDNA). New York, USA: ACM Press, 2004.
[10] KEROMYTIS A D, MISRA V, RUBENSTEIN D. SOS: an architecture for mitigating DDoS attacks, selected areas in communications[J]. IEEE Journal, 2004, 22(1): 176-188.
[11] AKELLA A, BHARAMBE A, REITER M, et al. Detecting DDoS attacks on ISP networks[C]//In Proceedings of ACM SIGMOD/PODS Workshop on Management and Processing of Data Streams (MPDS) FCRC. San Diego, USA: ACM Press, 2003.

编 辑 黄 莘

(上接第1178页)

[19] RANASINGHE D, ENGELS D, COLE P. Security and privacy: modest proposals for low-cost RFID systems [DB/OL]. http://www.m-lab.ch/auto-id/SwissRe Workshop/papers/SecurityAndPrivacy-ModestProposalsForLowCost RFIDsystems.pdf, 2004-10-15.
[20] KATZ J, SHIN J S. Parallel and concurrent security of the HB and HB+ protocols[C]//Advances in Cryptology, EUROCRYPT'06. [S.l.]: Eurocrypt, 2006.
[21] PIRAMUTHU S. HB and related lightweight authentication protocols for secure RFID tag/reader authentication[C]//In Collaborative Electronic Commerce Technology and Research. Basel, Switzerland: [s.n], 2006.
[22] CLAUDE C, GILDAS A. Noisy tags: A pretty good key exchange protocol for RFID tags[C]//The IFIP Conference in Smart Card Research and Advanced Application. Spain: [s.n], 2006.
[23] NATARAJAN V, BALASUBRAMANIAN A, MISHRA S, et al. Sridhar, security for energy constrained RFID system[C]//The Fourth IEEE Workshop on Automatic Identification Advanced Technologies(AutoID'05). [S.l.]: IEEE, 2005: 181-186.
[24] MIKKO L, STAAKE T, FLORIAN M, et al. From identification to authentication, a review of RFID product authentication techniques[DB/OL]. http://events.iaik. tugraz.at/RFIDSec06/Program/papers/010%20-%20Product%20Authentication%20Techniques.pdf, 2006-10-22.

编 辑 黄 莘