

基于自治系统的 DDoS 攻击防御技术研究

胡 滨, 代昆玉, 涂孝颖

(贵州大学 计算机科学与信息学院, 贵州 贵阳 550025)

摘 要: DDos 攻击是危害巨大且难以防御的一种网络攻击方式, 基于自治系统路由器上流量认证的防御技术, 可有效地抵御这种攻击, 但其也存在一些不足. 由此对一些尚不完善的地方进行了改进, 提出了基于自治系统的两级认证体制, 满足了数据传输效率与安全性的要求, 并通过引入数据传输速率与当前剩余生存周期的关系, 扩展了其防御攻击的范围, 实现了不但可以抵御洪水 DDos 攻击, 还可以抵御半开式连接 DDos 攻击.

关键词: DDos 攻击防御; 自治系统; 流量认证

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)07-0053-04

Research for DDos Attacks Defense Based on Autonomous System

HU Bin, DAI Kun-yu, TU Xiao-ying

(College of Computer and Information, Guizhou University, Guiyang 550025, China)

Abstract: DDos attack is a widespread use of attack which difficult to defend, based on autonomous system router traffic authentication technologies can effectively resist such attacks. We proposed to improve the autonomous system of two certification systems according to some of these technology shortcomings, to meet the data transmission efficiency and security requirements. Through the introduction of state of the current data transfer rate and life cycle of the relationship to expand the scope of its defensive attack, such as flood DDos attacks, semi-open connections DDos attacks.

Key words: DDos attack defense; autonomous system; certified traffic

1 引言

DDoS(分布式拒绝服务)攻击通过在很短时间段内, 多个傀儡机向被攻击目标机发送大量数据包, 阻塞网络带宽, 耗尽其系统资源, 迫使被攻击目标机中断服务^[1]. 此类攻击与网络访问时的瞬间拥挤很相像, 导致难以提炼 DDos 攻击的行为特征. DDos 攻击是当前因特网最有破坏性的一种攻击方式, 如何防御这种攻击成为了网络安全研究的热点问题, 虽然已经有各种防御的方法, 但都存在着种种的问题, 需要进一步完善.

基于因特网自治系统路由器上流量认证技术的 DDos 防御技术, 是目前被业界认为对 DDos 攻击有效的防御技术, 并被 NGN 安全机制所考虑. 这种基于流量的防御技术可有效防御普通的 DDos 攻击,

但是仍存在问题, 例如数据传输效率低等^[2]. 本文针对此技术的一些不足, 提出了一种改进的方法, 即在路由器上实施两级认证体制, 可满足数据传输效率和安全性的需要, 并且通过对数据包存活周期的调整, 将原方法只能抵御普通洪水攻击扩展到可抵御半开式连接攻击. 实验表明改进后的算法提高了传输效率, 能增强抵御 DDos 攻击的能力.

2 基于自治系统流量认证 DDos 防御技术

基于因特网自治系统路由器上流量认证技术的 DDos 防御方法, 其认证的原理是源主机向目的主机进行传输数据前, 首先向路由器请求发送许可证, 在取得许可证后, 再进行数据的传输, 许可证有一定的存活周期, 对传输的数据量有一定的要求^[3]. 在传输的过程中, 所经过的路由器都要对许可证进行

收稿日期: 2009-08-13; 修回日期: 2009-10-13

基金项目: 贵大自青基合字(2009)028 号

检查,并在数据包的包头添加一个认证信息.最终,目标主机将所有的认证信息数组反馈给源主机,从而实现源主机通过路由器的认证,向目标主机进行数据的传输.此过程中许可证的申请如图 1 所示.

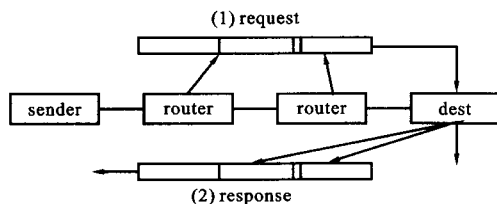


图 1 许可证申请过程

一个许可证只适用于一对传输的主机,许可证的是由密钥、时间标识及建立连接的相关信息组成的,其格式如图 2 所示.在许可证中包含数据发送包大小 N 及数据包发送时间 T 之间的比例关系,通过对这个比例关系的控制,可较好地控制发送的时间及数据大小.许可证的包头依据其申请的各个不同过程,由普通包头、特定包头及更新包头等构成.

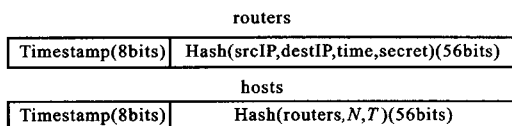


图 2 许可证数据包格式

从许可证的数据包格式可知,其存储空间较大,但 TCP/IP 数据包头部空间有限,需要在网络层包头及传输层包头间再插入一层来进行相关数据的存储^[4].因而这种设计方法存在以下不足,一是如何有效提高许可证的传输效率,二是如何有效抵御半开式连接攻击.

3 算法改进

3.1 自治系统的两级认证体制

为解决上述认证数据包的长度过大问题,提高传输效率,在原算法基础上引入粗颗粒基于自治系统的认证机制,即在自治域中,首个接收到申请认证包的边界路由器负责此次认证包的产生,其申请过程如图 3 所示.源端在向目的端发送的认证申请包,需要穿过三个自治域,每一个自治域上边界路由器(图粗线圆圈表示)在将接收到的请求包头中,插入本次的认证信息,从而有效减少认证的数据包长度.

假设单个自治域中有 n 个路由器,域中路径长度是 l ,认证数据包长度是 c ,那么减少的认证负载为: $S = cl(n-1)/n$.若 $n=3, l=9, c=6$,则每个包的大小能减少 54Bytes,明显增加了数据传输的效率.

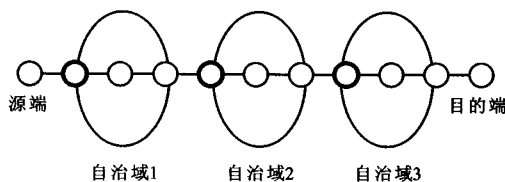


图 3 基于自治系统的许可证申请过程

原算法认证体制的认证包长度固定,不能根据安全性需求灵活调整,本文对原算法进行了改进,引入两种认证数据包:一是第一级认证,数据包 8 字节,二是第二级认证,数据包长 4 字节.这两级认证的特点是,第一级认证安全性高,但传输效率稍低,而第二级认证恰恰相反.这种设计可以满足不同安全性及传输效率的需求.其认证数据包格式如图 4 所示.

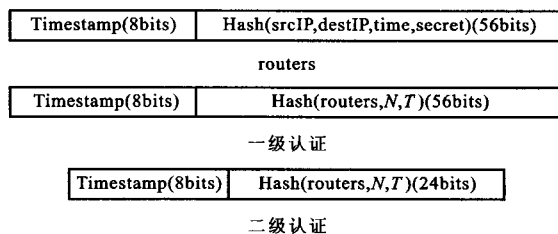


图 4 一级认证和二级认证数据包格式

认证数据包生成过程如下:

源端向目的端发送申请数据包时,每一自治域的边界路由器形成初始认证包,长度为 8Bytes.发送到目的端后,目的端根据申请数据包的安全性进行评估,安全性主要参考数据包的历史安全信息.通过概率 $\gamma (0 \leq \gamma \leq 1)$ 形成第一级认证,概率 $(1-\gamma)$ 形成第二级认证,最后形成一个认证数据链反馈给源端.

当 $\gamma=1$ 时,都使用第一级认证;当 $\gamma=0$ 时,都使用第二级认证.当 γ 值高时,则认证安全性较高,传输效率降低;当 γ 值低时,则认证结果相反,安全性低,传输效率高.

若认证数据包的密钥被破译概率为 P ,那么安全性 S 则是 $1-P$,从源端到目的端的认证数据包的安全性可以表示为

$$p = p_1^\gamma p_2^{1-\gamma}, 0 \leq \gamma \leq 1 \quad (1)$$

式中, p_1 为第一级认证被破译概率, p_2 为第二级认证被破译概率,全程路径是 n .

由式(1)计算,当 $p_1 \ll p_2, \gamma$ 由 1 减少时, p 值仍然较大,即稍微降低安全性,数据传输效率不会明显下降,仍然可以满足要求.

如第一级认证包长 a Bytes, 第二级认证包长 b Bytes, 认证包头长 d Bytes, 认证标记长 e Bytes, 负

载为 m Bytes,由式(1)可推导出,基于自治系统的总传输效率是

$$p = \frac{mn}{\gamma al + (1 - \gamma)bl + dn + mn + en}, 0 \leq \gamma \leq 1 \quad (2)$$

3.2 基于生存周期上限的流量认证体制

对拥有许可证的源端发起的洪水攻击,在原算法依据引入细颗粒的体制来解决,可依靠单个许可证允许传输的数据量 N 与允许传输时间 T 之间的比例关系实现.其主要原理是对发送速率大于 N/T 值的源端进行控制,小于该值的进行通过^[5].具体过程是:首先路由器检查接收的数据包是否合法,即是否拥有许可证;然后检查此许可证是否超时,如果时间超过 T ,则进行丢弃;对该许可证设置相应的状态,设置其生存周期为 $L * T/N$,同时在该状态中许可证所允许传输的数据量加上 L .

原算法的许可证的体制可以有效抵御一般的洪水攻击,这是由于洪水攻击时总是尽最大程度地发送数据包,只要对 N 和 T 的最大限度进行控制,就可捕捉到检测对象的异常状态^[6].但是,对于半开式连接攻击,原算法仅凭简单的设置上限并不能有效地抵御其攻击,这是因为对 N 和 T 只设置了上限,不能体现 T 时间内的速率,但半开式连接攻击是在瞬间的流量突发,有时并不会超过 N 和 T 的上限.

本文引入数据传输速率与状态当前剩余生存周期的关系来实现抵御半开式连接的攻击.依靠此关系,能够通过剩余生存周期体现传输量的近期速率,即通过设置生存周期最大值来检测突发情况,如图5所示.通过设置生存周期上限 t_{tl_up} ,当状态更新时,达到了该生存周期最大值,就采取应对措施,准确地捕捉到异常.

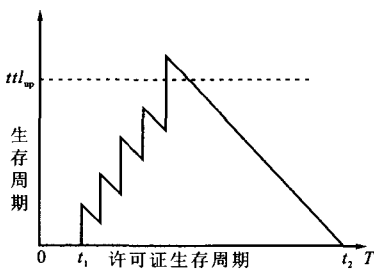


图5 生存周期上限示意图

在图5中,假定 t_1 到 t_2 有突发流量,在这段时间内的有许可证的流量平均速率为 v ,其表达式为

$$v(t_2 - t_1) = (t_{tl_up} + t_2 - t_1) * N/T \quad (3)$$

在式(3)中,两边均是 $(t_2 - t_1)$ 内传输的数据流量,于是可得

$$t_{tl_up} = (vT/N - 1)(t_2 - t_1)$$

对于半开式连接攻击来说,其速率最低是被攻击链路带宽 C ,即 $v \geq C$,于是

$$t_{tl_up} \geq (CT/N - 1)(t_2 - t_1)$$

通过上式可以得到 t_{tl_up} 的最小值.当 t_{tl_up} 设置的较低时,相应的检测时间 $(t_2 - t_1)$ 就会变短,但不能低于一定的阈值,否则正常的访问流量突发会被错误当做 DDoS 攻击行为.半开式连接攻击一个重要特征是攻击会持续比较长的时间,而正常的访问突发通常时间较短.因此可通过设置较长的检测时间来区别上述两种行为.同时, t_{tl_up} 也不能设置的太大,因为半开式连接 DDoS 攻击持续时间通常有限,过大的 t_{tl_up} 值将导致无法判断异常的攻击行为.

当检测到异常的 DDoS 攻击行为后,不能采用简单的抛弃手段,这是因为抛弃有可能把源端的正常流量或因误警把正常流量丢失掉^[7].只要半开式连接攻击平均流量不超过链路带宽的所能承受的范围,就可考虑通过系统缓存对目的端实施防护,并采取负载均衡的办法将数据量进行分流.

4 实验结果

为了验证本改进算法对半开式连接攻击的有效性,选取了一个典型的因特网拓扑进行实验,其拓扑结构如图6所示.图中共有了四个自治域,目的端在自治域1中,正常的源端在自治域2中,攻击者在自治域3中,各个自治域之间可以互连互通.

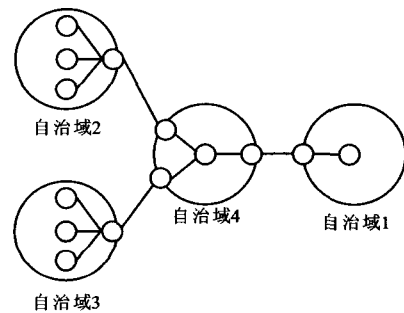


图6 实验网络环境结构图

在自治系统中,设定所有的自治域都支持认证.当自治域2中合法的源端与自治域1中的目标端进行文件传输操作时,自治域3中攻击者向自治域1中目标端开始了单机的半开式连接拒绝服务攻击.通过实验可知,原算法致使合法用户与目标端的通信遭到了阻塞,而改进后的算法,自治域中的路由器检测到了攻击行为,通过负载均衡机制,带宽很快得到了恢复,如图7所示.

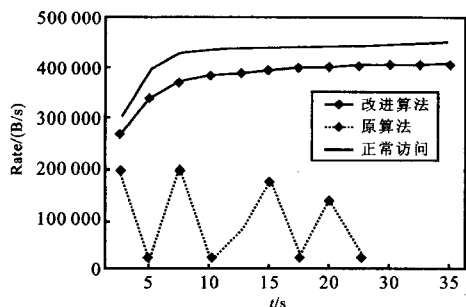


图7 实验结果

5 结束语

DDoS 攻击是当前因特网主要的攻击方式,随着网络环境的日益复杂,传统的防御方法对其检测防御的效率不高.基于因特网自治系统路由器上流量认证技术的 DDoS 检测防御方法,是一种对其攻击进行检测防御的技术,能在网络骨干传输节点上对攻击行为实施有效的控制.本文在其基础上对原算法的一些不足进行了改进和完善,引入了两级认证体制,满足数据传输效率和安全性的要求,并同时扩展了检测防御的攻击范围,解决了原算法不能防御半开式连接攻击的问题,实验表明该方法对 DDoS 的检测防御具有一定的实用性和可用性.

参考文献:

- [1] 张明猛,赵天福. DDOS 攻击检测技术研究[J]. 计算机与信息技术,2007(4):58-61.
- [2] 孙知信,姜举良,焦琳. DDoS 攻击检测和防御模型[J].

软件学报,2007,18(9):2245-2258.

- [3] Kim Y, Lau W C, Chuah M C, et al. Packet score: statistics-based overload control against distributed denial-of-service attacks[J]. IEEE Transactions Dependable and Secure Computing, 2006, 3(2): 141-155.
- [4] Jian Kang, Yuan Zhang, Jiu Bin Ju. Classifying DDoS attacks by hierarchical clustering based on similarity[C]// Proceeding of Fifth International Conference on Machine Learning and Cybernetics. Dalian, 2006.
- [5] Yaar A, Perrig A, Song D. StackPi: new packet marking and filtering mechanisms for DDoS and IP spoofing Defense [J]. IEEE Journal on Selected Areas in Communications, 2006, 24(10): 1853-1863.
- [6] Khan, Traora. Queue-based analysis of DoS attacks[C]// Proc of IEEE Information Assurance workshop. Japan, 2005: 266-273.
- [7] Sun H, Zhaung Y, Chao H J. A principal components analysis-based robust DDoS defense system[C]// IEEE International Conference Communications. Scotland, 2008: 1663-1669.

作者简介:

胡滨 男, (1977-), 硕士, 讲师, 布依族. 研究方向为计算机网络安全.

代昆玉 女, (1979-), 硕士, 讲师, 土家族. 研究方向为数据挖掘、网络安全.

涂孝颖 男, (1977-), 硕士, 讲师, 土家族. 研究方向为计算机网络安全.

(上接第 52 页)

- [2] 尚勇, 吴顺君, 项海格. 并行延时 LMS 算法[J]. 中国科学: E 辑, 2002, 32(4): 523-529.
- [3] 李博, 李哲英, 刘媛媛. 流水线 ADC 功耗优化算法及其硬件实现[J]. 微电子学与计算机, 2008, 25(4): 131-135.
- [4] 周珍, 郭立. 固定延迟的流水线双精度浮点除法电路[J]. 微电子学与计算机, 2008, 25(5): 84-87.
- [5] Dai I Kim, De P, Wilde. Performance analysis of signed self-orthogonalizing adaptive lattice filter [J]. IEEE Transactions on circuits and systems: analog and digital signal processing, 2000, 47(9): 1227-1237.

- [6] Haibing Qi. Analysis and application of gradient adaptive lattice filtering algorithm[C]// International conference on computer and electrical engineering 2008. Phuket, IEEE CS, 2008: 744-747.

- [7] Keshab K Parhi. VLSI digital signal processing systems: design and implementation[M]. New York: John Wiley and Sons, 1999.

作者简介:

齐海兵 男, (1969-), 博士研究生, 高级工程师. 研究方向为光、电信号与信息处理、光电器件等.