基于增强权证的无状态过滤机制

金 光[①②] 杨建刚[①] 魏 蔚[①] 董亚波[①]
[①](浙江大学计算机科学与技术学院 杭州 310027)
[②](宁波大学信息科学与工程学院 宁波 315211)

摘 要：该文针对拒绝服务攻击的防御技术，着重分析了新涌现的权证技术，包括基本思想、无状态过滤和通信量验证体系。探讨了权证能否引发新的攻击和对网络传输性能的影响，针对已有方案的一些技术缺陷提出了改进对策，包括：用通知保护权证请求，多级别权证，动态的权证分配。理论估算和仿真试验表明，这些方法能更好地兼顾安全性和效率性，性能明显优于原方案，提高了权证技术的可行性。

关键词：网络安全；拒绝服务攻击；无状态过滤；权证
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1009-5896(2008)10-2490-04

Stateless Filtering Based on Enhanced Capabilities

Jin Guang[①②] Yang Jian-gang[①] Wei Wei[①] Dong Ya-bo[①]
[①](*College of Computer Science and Technology*, *Zhejiang University*, *Hangzhou* 310027, *China*)
[②](*College of Information Science and Engineering*, *Ningbo University*, *Ningbo* 315211, *China*)

Abstract: Major defensive mechanisms against DoS attacks in the Internet are reviewed. Especially the most recent capabilities techniques, such as basic concepts, stateless flow filtering and the Traffic Validation Architecture (TVA), are analyzed deeply. The related discussions about the shortcomings of current capabilities techniques, such as potential Denial-of-Capability (DoC) attacks, decrement of transmission efficiency, are given in detail. Some improvement methods are provided. They include protecting capabilities requests with notifications, bi-level capabilities, flexible and dynamical capabilities assignment, etc. These methods enhance the robustness and efficiency of capabilities. Theoretical evaluations and simulations show that the improvements outperform original schemes and are more practical in the Internet.

Key words: Network security; DoS attacks; Stateless filtering; Capabilities

1 引言

拒绝服务(Denial of Service, DoS)攻击严重威胁因特网的安全。防御 DoS 攻击已成为网络安全研究领域的主要方向之一。虽然已涌现了许多防御技术方案[1]，但限于现有的因特网架构，均未能从根本上解决问题。着眼于下一代安全因特网(Next Generation Secure Internet，NGSI)[2]，一些学者提出其设计应当具有最低的信赖需求、最少的网络元素状态等特点。最近引起关注的权证(capability)[3]方案初步体现了 NGSI 的一些特点，值得深入研究。

1.1 DoS 攻击的防御技术

DoS 防御技术分为检测、预防、响应、容忍消除等 4 类[1]。检测主要基于统计分析等技术，包括异常和误用检测[4]。预防则强调排除伪造包，如入口过滤[5]等。响应如定位攻击源或入口即路径追溯[6]。容忍消除主要涉及过滤技术，如在上游路由器处实施反馈限流[7]。

以上技术各有特点，但均面临一个难题：面对大规模攻击中多达 10 万台以上的傀儡攻击机，均会因处理能力不足而严重影响路由器 TCAM 内存和转发包的效率，使其不堪重负。

1.2 无状态过滤和权证技术

传统过滤技术依赖于状态，允许或拒绝某些用事先规定的特征，如目标地址或端口等来表征的特定数据流通过。考虑到路由器资源有限，NGSI[2]明确提出网络元素应具最少的状态数量。

基于此，为从根本上革新网络的安全体系架构，最近出现了无状态过滤和权证的思想。权证[8]类似令牌，表示源站 S 得到目标机 D 许可用于发送的一次性凭证(注：为强调其申请、颁发、携带和核查，建议译成“权证”较合适)。将资源控制权赋予 D 和中间链路，并由它们作出许可决定。权证由 D 发布且包含于每个包中，在网络中生效并接受沿路各路由器的核查。

无状态流过滤器(Stateless Internet Flow Filtering, SIFF)[9]提出了首个具体的权证方案。S 先和 D 建立连接以获得授权。S 先送出权证请求包，沿路各路由器在包中依序插入各自的特征标记，D 收到后将完整的标记序列即权证回传 S。S 随后将该权证附于所发送数据包中，以接受沿路各

2007-03-28 收到，2007-12-17 改回
浙江省自然科学基金(Y106023)和宁波市自然科学基金(2006A610014)资助课题

路由器核查并优先通过。更完善的是通信流验证体系(Traffic Validation Architecture，TVA)[3]，TVA 在 IP 层和 TCP 层之间插入填充层存放权证信息。整个通信过程也分两个阶段，对应两种包：权证请求(Request To Send, RTS)包和授权数据包。前者用于建立 S 和 D 的授权连接，后者用于正常数据传输。

TVA 中各路由器生成自身预权证并置入 RTS 包，预权证含路由器本地时间戳和 hash 值。D 收到 RTS 包后，处理预权证并分配有效期 T 和通信量上限 N 以生成权证并回传 S。此后 S 可发送授权包，各路由器将检查其是否同时满足授权、限时和限量的要求。RTS 包本身为非授权包，非授权通信被严格限流(仅限 5%带宽)。

权证技术面临以下关键环节：(1)权证能否抵御已有的 DoS 攻击？(2)如何避免权证引发新的 DoS 攻击？(3)权证是否对网络传输性能有较大影响？(4)权证是否会破坏因特网的开放性？

本文将在深入分析 TVA 的基础上提出改进方案(Enhanced TVA，ETVA)。

2　提高权证体系的安全性

2.1 TVA 的安全措施

TVA 的安全性有相对全面的安排，充分考虑了攻击者伪造或猜测权证、勾结型攻击等可能性。目前看，大部分措施的效果良好。最薄弱之处是权证申请环节，有可能引发拒绝权证请求(Denial of Capability, DoC)[10]攻击：攻击者发送大量 RTS 包来淹没非授权信道(5%带宽)，已获权证的老用户继续使用授权信道不受影响，而新用户的 RTS 包将必须与攻击包竞争非授权信道。路由器因无法区分而随机丢弃，用户则需反复发送 RTS 包并经较长时间才能得到权证。

相应理论分析如下。设攻击者发送大量 RTS 包泛滥非授权信道，导致链路拥塞。设路径中 n 个路由器遭受同样丢包率 σ，则合法 RTS 能通过的概率为 $P_1=(1-\sigma)^n$。设 S 共重复发送 m 次 RTS 包，则一个包能全部通过并获得所有预权证到达 D 的概率为

$$P_2=1-(1-(1-\sigma)^n)^m \tag{1}$$

设 σ=0.9，n=3，m=100，则 P_2=0.095。即重复 100 次也仅有极低的概率获得权证，这将难以忍受。

TVA 推荐公平队列法[3]：AS 边界入口路由器对 RTS 包插入一个标识，以供下游路由器用来对包公平排队。出发点是有限队列数量不会影响路由器运行，且伪造标识的影响无法跨越 AS。但该机制被批评又回到了对数据包限流的旧有模式[10]。本文的仿真试验表明：如攻击包和合法包从同一边界进入，即共享同一标识，则基于标识的公平队列法基本无效。如攻击者位于 AS 内部，则恶意 RTS 包可包含随机伪造标识而造成 DoC 攻击。

2.2　使用主动通知抵御 DoC 攻击

本文建议，路由器非授权信道遭遇 RTS 包过载时须丢包，同时需对该包源地址发出通知：明确告知其丢包是因限流所致，通知附带时间戳 t 和标记 γ。γ 计算如下：

$$\gamma=\mathrm{Hash}(\mathrm{srcIP},\ \mathrm{routerIP},\ t,\ \mathrm{secret}) \tag{2}$$

S 收到通知后立即再发送含 γ 和 t 的增强权证请求包(Enhanced RTS, ERTS)。这里 secret 由路由器控制，且随 t 变化。无效和过期 ERTS 包将被识别和丢弃，从而削弱了攻击者泛滥发送 ERTS 包的可能影响。这种通知机制是路由器和客户机进行网络层交互以进行认证。主动通知和动态调高优先级的机制将使合法请求脱颖而出。

收到 ERTS 包后，路由器检验其 γ 和 t，如合格则用授权信道转发，转发过程采用基于源地址的公平排队。如因拥塞而被丢弃，新通知将再次被发送给 S。TVA 中分配给授权信道 95%的带宽，在 ETVA 中授权包和 ERTS 包共享此 95%带宽，为避免浪费带宽，ERTS 包仅限于 0~5%带宽。

攻击者也可能试图泛滥发送 ERTS 包，但显然伪造源地址不会收到通知，也无法发出有效 ERTS 包。具真实源地址的傀儡机可发送 ERTS 包，但此类傀儡机的数量将是有限的。即使同一傀儡机用真实地址泛滥发送 ERTS 包，基于源的公平排队将使攻击效果极为有限。公平排队机制中还要对每个源的列队长度进行限制，这样即使同一个攻击者发送大量具真实源地址的恶意 ERTS 包，也无法形成有效的 DoC 攻击。

3　改进权证体系的数据传输效率

3.1 权证对数据传输的影响

同其它安全措施一样，权证对正常数据传输会造成影响，主要如下：权证需沿路核查运算；路由改变需重新申请权证；权证自身占用额外带宽；频繁换发权证影响数据高速传输应用。本文着重分析后 2 条。

TVA 中预权证长 64bit，权证头部信息长 96bit。因特网路径长一般小于 30 跳，以平均 15 跳计，权证长达 96+15.64=1056bit 即 132byte，对于 1500byte 的长 IP 包而言，增加约 8.8%的负载开销；而对于仅 40byte 的 TCP 控制包，增加开销高达 330%。此外 TVA 中对权证采用单一有效期 T 和通信量 N，即将到期或过量时，须换发新权证。对于合法数据传输应用而言，频繁换发权证会影响传输效率。

3.2 ETVA 的改进原则

权证的大小和结构统一是为了核查的标准化和无状态化。在此前提下适当调整权证大小和种类可解决单一化的缺陷。建议将单一权证改进为多级别、多用途和灵活性的动态机制。多级别指权证具不同大小，对应不同传输效率和转发时间；多用途指不同具体应用可持有不同权证，以在安全和效率上更好地符合应用要求；灵活分配指 D 根据具体资源和安全状况等综合考虑来颁发不同权证。ETVA 体现一个安全原则：老用户的可信度更大。对初次申请设定较小的 T 和 N 值，对反复申请的用户则给予较大值，即 S 对权证的申请更新次数越多，有效值越大。

3.3 两级权证和灵活的分配机制

本文将路由器生成的预权证增为两种，原有 64bit 称长预权证(LC)，新增 32bit 短预权证(SC)，见图 1。显然，LC 安全性好，但 SC 传输效率更高。

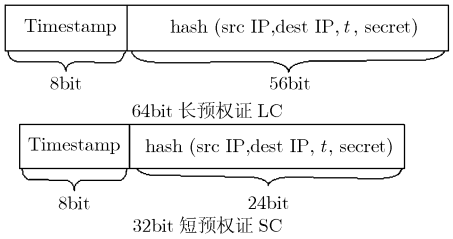

图 1 长预权证和短预权证的格式

路由器在 RTS 包中插入两种预权证。D 收到时，根据实际状况判断并颁发不同权证。请求包中如仅含 1 个预权证，即路径中仅 1 个路由器，则取长权证 LC。如请求包中含 n>1 个预权证，即路径长 n，则取 LC_1，LC_n 及中间全部 SC_i, $2 \le i \le n-1$。S 得到的权证见图 2。

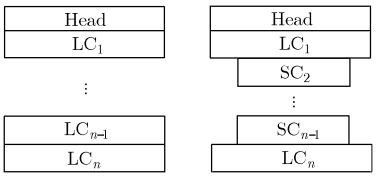

图 2 授权包中的权证结构

设 LC 长 a bit，SC 长 b bit，权证头部长 c bit，数据包其它内容为 x bit，则 TVA 和 ETVA 中数据包的传输负载效率分别为

$$\lambda_{\mathrm{TVA}} = \frac{x}{an + c + x} \tag{3}$$

$$\lambda_{\mathrm{ETVA}} = \frac{x}{b(n-2) + 2a + c + x},\ n > 1 \tag{4}$$

3.4 有效期和通信量限制的动态策略

ETVA 中，首个 RTS 包将获得最初设定的 $N_{\min}$ 和 $T_{\min}$，而当 S 请求更新权证时，D 为该权证赋予更大 N 和 T 值。可取值如下：

$$N = N_{\min} + k \cdot \alpha N_{\min} \tag{5}$$

$$T = T_{\min} + k \cdot \beta T_{\min} \tag{6}$$

式中 k 是权证更新次数，α 和 β 是各自的增长系数，由 D 自行选择。如取 1，即每次新增 1 个 $N_{\min}$ 或 $T_{\min}$。

经过 k 次更新，可得

$$N' = N_{\min}(k+1)\left(1 + \alpha k/2\right) \tag{7}$$

$$T' = T_{\min}(k+1)\left(1 + \beta k/2\right) \tag{8}$$

各自的扩大倍率分别是：

$$\delta = (k+1)(1 + \alpha k/2) \tag{9}$$

$$\theta = (k+1)(1 + \beta k/2) \tag{10}$$

为避免让路由器记录状态，传输速率 v 会小于 N/T，即 T 会先于 N 到期，所以更关注有效期内的实际传输量。分别计算如下：

$$S_{\mathrm{TVA}} = vT_{\min}(k+1) \tag{11}$$

$$S_{\mathrm{ETVA}} = vT_{\min}(k+1)(1 + \beta k/2) \tag{12}$$

4 仿真结果和分析

本文在 NS2 网络仿真环境中进行了分析测试，结果表明，ETVA 能获得良好效果。

为更好地予以比较，本文使用文献[3]的拓扑结构作为 DoC 攻击场景，见图 3。路由器瓶颈链路为 10Mbps，授权和非授权信道分别使用 9.5Mbps 和 0.5Mbps。每个客户通过一个稍修改的 TCP 协议发送一个 20kB 的文件给目标。权证请求用 TCP/SYN 包捎带，超时为 1s，最多 8 次重试即放弃。攻击场景分为：(1)假设攻击包与合法包通过同一边界入口进入 AS，即拥有同一标识；(2)假设攻击者位于 AS 内，RTS 包中标识为随机产生。

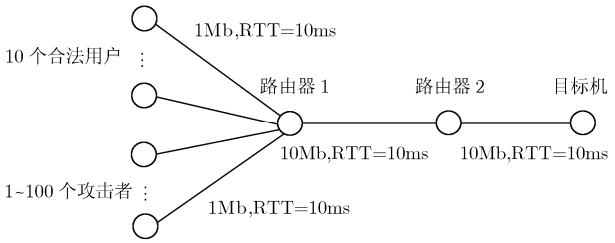

图 3 DoC 攻击下的仿真试验拓扑

如图 4 和图 5 所示，TVA 的能力被严重削弱，仅少量攻击者即可完全抑制合法权证请求，但即使攻击者增至 100，ETVA 仍表现良好。

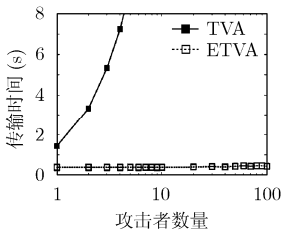

图 4 DoC 攻击场景 (1)的仿真试验结果

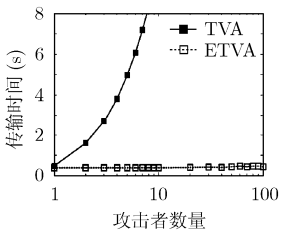

图 5 DoC 攻击场景 (2)的仿真试验结果

图 6 给出了权证大小和路径长度的关系，其中头部信息 c=96bit，TVA 中 a=64bit，ETVA 中 b=32bit，可看出 ETVA 中权证尺寸处于相对较低的水平。图 7 是当有效负载 x=1kbyte 时 ETVA 和 TVA 的传输效率比较，可看出路径越长，ETVA 的优势越明显。图 8 给出了路径长度固定为 15 跳时的传输效率比较。图 9 则给出了数据传输量与权证更新次数的关系：更新次数较多时，ETVA 具有更大的通信量。

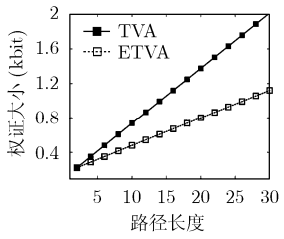

图 6 权证大小和路径长度的关系

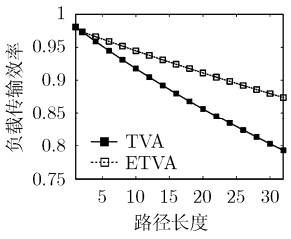

图 7 授权包在不同度路径的传输效率

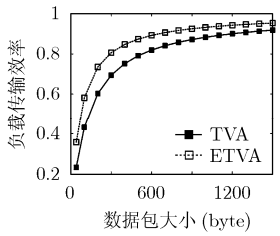

图 8 权证对包有效负载的传输效率影响

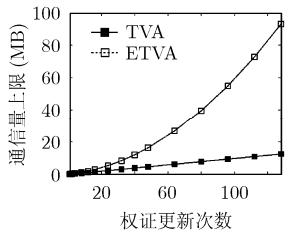

图 9 通信量限制和权证更新次数的关系

5　结束语

针对以 TVA 为代表的权证技术，着重分析了权证请求的安全性和传输效率上的不足，并提出相应改进措施，仿真试验表明改进效果较好。今后我们将继续深入研究权证体系和 NGSI。

参 考 文 献

[1] Douligeris C and Mitrokotsa A. DDoS attacks and defense mechanism: classification and state-of-the-art. *Computer Networks*, 2004, 44(3): 643–666.

[2] Bellovin S, Clark D, Perrig A, and Song D. A clean-slate design for the next-generation secure Internet. National Science Foundation Workshop on Next-Generation Secure Internet, Pittsburgh, PA, 2005.

[3] Yang X, Wetherall D, and Anderson T. A DoS limiting architecture. Proc. ACM Sigcomm, Philadelphia, PA, 2005: 241–252.

[4] 田俊峰, 张喆, 赵卫东. 基于误用和异常技术相结合的入侵检测系统的设计与研究. 电子与信息学报, 2006, 28(11): 2162–2166.
Tian Jun-feng, Zhang Zhe, and Zhao Wei-dong. The design and research of intrusion detection system based on misuse and anomaly. *Journal of Electronics & Information Technology*, 2006, 28(11): 2162–2166.

[5] Ferguson P and Senie D. RFC2827, Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. Los Angeles, 2000.

[6] Gao Z and Ansari N. Tracing cyber attacks from the practical perspective. *IEEE Communications Magazine*, 2005, 43(5): 123–131.

[7] 梁丰, Yau D. 利用路由器自适应限流防御分布拒绝服务攻击 (英文). 软件学报, 2002, 13(7): 1220–1227.
Liang Feng and Yau D. Using adaptive router throttles against distributed Denial-of-Service attacks. *Journal of Software*, 2002, 13(7): 1220–1227.

[8] Anderson T, Roscoe T, and Wetherall D. Preventing Internet Denial-of-Service with capabilities. Proc. ACM HotNets, Cambridge, MA, 2003.

[9] Yaar A, Perrig A, and Song D. SIFF: A stateless Internet flow filter to mitigate DDoS flooding attacks. Proc. IEEE Symposium on Security and Privacy, Oakland, CA, 2004: 130–143.

[10] Argyraki K and Cheriton D. Network capabilities: the good, the bad and the ugly. Proc. ACM HotNets, College Park, MD, 2005.

金　光：　男，1972 年生，博士生，副教授，研究方向为网络安全.
杨建刚：　男，1959 年生，教授，博士生导师，研究方向为计算智能和网络安全.
魏　蔚：　男，1983 年生，博士生，研究方向为网络安全.
董亚波：　男，1974 年生，博士，副教授，研究方向为网络安全.