doi:10.3969/j.issn.1000-436x.2013.09.016

面向自治域的 DoS 攻击流抑制模型

江先亮[1,3]，金光[2,3]，杨建刚[1]，何加铭[2,3]

(1. 浙江大学 计算机科学与技术学院, 浙江 杭州 310027；2. 宁波大学 信息科学与工程学院, 浙江 宁波 315211；
3. 浙江省移动网络应用技术重点实验室，浙江 宁波 315211)

摘 要：针对因特网上的 DoS 攻击，结合下一代安全因特网架构，分析了现有权证方案在申请、授权和解授权等方面的问题。兼顾网络拥塞反馈机制，结合多级主动队列、信誉计算等思想，提出了一种面向自治域的 DoS 攻击流抑制模型，并进一步分析其有效性。通过在 NS2 上利用权威的 CAIDA 真实拓扑数据集，对权证授权时间和授权通信量、平均权证获取时间、不同方案的文件传输时间进行对比分析和评价，结果表明本方案能有效降低平均权证获取时间，提高文件传输效率，使权证方案更具可行性和顽健性。

关键词：网络安全；拒绝服务攻击；自治域；网络拥塞；权证

中图分类号：TP393 **文献标识码**：A **文章编号**：1000-436X(2013)09-0132-10

AS-level model for restraining DoS attacks

JIANG Xian-liang[1,3], JIN Guang[2,3], YANG Jian-gang[1], HE Jia-ming[2,3]

(1. College of Computer Science and Technology, Zhejiang University, Hangzhou 310027, China; 2. College of Information Science and Engineering, Ningbo University, Ningbo 315211, China; 3. Mobile Network Application Technology Key Laboratory of Zhejiang Province, Ningbo 315211, China)

Abstract: Combined with the next generation security architecture, a novel AS-level defense scheme was proposed to restrain DoS attacks in the Internet. And the deficiencies of previous capability schemes were analyzed in detail, especially on requesting/withdrawing authorization of capabilities. The scheme takes account of a congestion feedback mechanism, a combination with multi-level active queue management, and the credit computation. Then a further analysis on the scheme's effectiveness was presented. Several experiments with NS2 and CAIDA's topology datasets were performed to evaluate the authorizing time and traffic, the average requesting time and common file transfer time of different schemes. The results show that this scheme can effectively reduce the average requesting time of capabilities, improve common file transfer efficiency, and enhance the feasibility and robustness.

Key words: network security; denial-of-service attack; autonomous system; network congestion; capabilities

1 引言

因特网的巨大成功和不断发展，动力在于它的开放性。新的网络应用能轻易加入到网络中，能在任何时候发送任何东西给任何人，而不需要网络管理者或接收方的允许。正因为如此，现有网络架构对于诸如 DoS 等的恶意攻击总是措手不及[1]，很难进行有效阻止和限制。但如果在网络中加入过多的限制，保证网络足够安全，则会降低网络的开放性，不利于新应用的加入和网络的发展。作者认为，如何权衡该矛盾，设计一个能抑制 DoS 攻击的因特网开放架构具有重要的意义。

收稿日期：2012-07-06；**修回日期**：2012-12-15

基金项目：国家科技重大专项基金资助项目(2011ZX03002-004-02)；浙江省移动网科技创新团队基金资助项目(2010R50009)；浙江省自然科学基金资助项目(LY12F02013)；宁波市自然科学基金资助项目(2012A610014)；宁波市移动网络应用技术创新团队基金资助项目(2011B81002)

Foundation Items: This Research was Supported in Part by Major Projects of National Science and Technology (2011ZX03002-004-02)；Zhejiang Provincial Technology Innovation Team (2010R50009); The Natural Science Foundation of Zhejiang Province (LY12F02013); The Natural Science Foundation of Ningbo (2012A610014); Ningbo Municipal Technology Innovation Team (2011B81002)

2　相关研究

DoS 攻击防御技术的研究[2]主要有两大主线：规则和标记。规则以防火墙、入侵检测等传统技术为主，它们不对数据分组做任何改变，仅依据规则对分组进行检测[3,4]和过滤。与规则不同，标记则采用了一定的技术手段，利用数据分组携带标记信息，并在关键路由器或受害主机上进行检测和过滤。

典型的标记技术有概率分组标记(PPM)[5]、确定分组标记(DPM)[6]和路径标识(Pi)[7,8]等，它们主要基于 IPv4，适当修改后也可应用于 IPv6。然而，它们也都存在一定程度的不足。如对于 PPM，其路径重构开销过大，且重构出路径时最佳防御期已过。DPM 在跨域的情况下很难部署，虽然能定位攻击源的接入路由器地址，但需不同域间的配合。Pi 类方案可快速进行过滤，但是不能将防御推进到攻击流的上游，防御能力和效果有限。为此，文献[9]提出融合部署方案，综合考虑了 DPM 和 Pi 的优点。

为实现更为智能和彻底的防御，Anderson 等[10]提出目标端授权的攻击防御策略，即权证技术。权证类似于令牌，强调申请、许可、携带和校验，为一次性使用的许可，由目标主机授权且含于数据分组中。权证的出现满足 NGSI 对于网络元素应具有最少状态的设想[11~13]，增强了过滤攻击分组的能力，减少了过滤时需要的状态信息。

截至目前，卡内基梅隆大学的 Perrig 和杜克大学的 Yang 分别领导的研究小组在权证研究上相继取得了显著进展。Perrig 等首次提出 SIFF[14]，强调发送方在发送数据前，需要先发送请求分组向接收者申请权证，沿路节点在请求分组中插入特定标记(预权证)，目标主机如接受请求，则生成权证并回传。发送方可用该权证进行数据发送，沿途节点核查携带权证的数据分组，匹配则转发，否则丢弃。Yang 等进一步提出了较完整的通信流检验体系(TVA, traffic validation architecture)[15]，有效地降低了路由器处理权证所需的计算资源和存储需求，实现可递增部署等特性。Shue 等[16]针对权证申请，提出了建立廉价网络权证的思想。然而权证引发了研究者的分歧，如 Argyraki 等[17]对权证技术进行了综合分析，客观评价了其优势和不足。但是，无可置疑的是权证思想在抗攻击方面的优越性，它能有效地抵抗已有或潜在的伪造攻击和洪泛攻击。

本文的研究内容以权证为基础，兼顾拥塞反馈，面向自治域一级提出 DoS 攻击流抑制模型(MRDA, model for restraining DoS attack)。后面先对 MRDA 设计中出现的一些问题进行了假设，接下来介绍了 MRDA 思想和关键结构，随后描述了详细设计和实现部分，并给出了基于 NS2 平台的仿真实验和分析讨论。

3　MRDA 假设和目标

3.1　安全威胁形式

实际情形中，虽然路由器和主机都可能受攻击和控制，但用户管理的设备比网络设备更易被攻击和控制。MRDA 的设计更多信任网络中受管理的设备，将 AS 看作一个独立的信任单元。若 AS 中某一设备被攻击和控制，则该 AS 不可信任，可能修改或丢弃其转发的数据分组。然而，网络攻击是多样化的，MRDA 不能应对所有类型的攻击，它主要针对以下两大类攻击时更为有效。

1) 目标洪泛攻击。攻击者发送大量洪泛攻击分组到受害者，消耗其计算和通信资源，造成受害者无法为合法用户提供正常服务。

2) 链路洪泛攻击。攻击者向网络注入大量攻击分组造成链路拥塞，以破坏瓶颈链路的合法通信。有多种情形：①攻击分组的目标端过于分散；②攻击数据分组的 TTL 值在到达受害者之前已减至 0；③目标端未部署防御系统；④目标端是协同攻击者。

3.2　前提假设

MRDA 针对的攻击形式有限，考虑防御措施失效，如某些条件不满足，应不影响原有网络的整体性能。

1) MRDA 主要针对网络层资源和带宽耗尽型 DoS 攻击，对其他类型或层次的攻击不一定有效。

2) 攻击者能力强，能构建实施洪泛攻击或协同洪泛攻击，且攻击者较为狡猾。

3) 受害者有能力检测攻击，具备通过内容检测等技术获知数据分组是否为攻击分组。

4) 轻量级密钥交换和信息加密，能在实现过程中满足线速度的处理要求。

5) 安全的域内通信，借助已有手段阻止源地址欺骗和信息篡改，保证域内服务器或路由器通信的可靠性。

6) 网络设备可更新。

4 MRDA 思想和关键结构

4.1 MRDA 思想

MRDA 汲取了已有权证技术方案(特别是 TVA)的优点，采用了 Stopit[18]和 NetFence[19]中的源端过滤思想，缓解了网络中攻击分组泛滥对链路、路由器和服务器的资源消耗。

图 1 给出了 MRDA 的结构，其可被设计成类似于 DNS 或电子邮件的基础服务设施，其中，虚线环为 AS 的范围。假设 S_1(S_1 和后续涉及的符号含义如表 1 所示)欲发送数据给 D_2，首先向本地 S_{IQS} 申请去往 D_2 的权证，获授权后即可发送数据给 D_2。携带权证的数据分组经中间路由器的验证，最终到达 D_2。D_2 如检测到携带权证的数据分组为恶意，则经 D_{IQS} 向 S_{IQS} 发送拦截请求，明确拦截流<*Ticket*, S_1, D_2>，同时指出拦截时间长度 T_{block}。MRDA 利用权证标记的不可伪造性(潜在可能伪造的时间远大于密钥更新时间)，消除了地址伪造攻击，对于拦截请求则采用了三元组。如果中间路由器发生拥塞，则其产生聚合前缀(源 AS)，经信息查询服务器(IQS, information query server)告知源 AS 出口路由器限速 T_{limit} 时长，拥塞路由器利用优先级方式进行队列管理。

MRDA 中每个 AS 都有一个 IQS，主要负责申请(向目标主机)、管理和授权(向本地主机)权证，管理域内主机，处理限速请求和拦截请求。在处理限速请求和拦截请求时，IQS 直接将请求发给源端 S_{IQS}，同时考虑高效，在一个大的 AS 中可采用多台服务器提供均衡的 IQS 服务。

在 MRDA 中，IQS 需要知道其他 AS 的 IQS 地址，并发送拦截请求。为解决这一问题，MRDA 采用了 Stopit[18]中给出的方法，利用 BGP 协议广播 IQS 的地址，其他 AS 可从 BGP 路由信息中学习到 IQS 的地址。

4.2 MRDA 关键结构

4.2.1 信息查询服务器

IQS 是 MRDA 中的核心和关键部分之一，如前所述，它主要完成权证的申请、管理和授权，管理域内的主机，并协助其他 AS 的 IQS 进行协同防御。IQS 可在已有 DNS 基础上进行功能扩展来实现，抑或作为新增的类似于 DNS 的基础设施进行建设。

4.2.2 AS 接入和出口路由器

MRDA 以 AS 为单位进行网络部署，主要在边界路由器上进行升级，在 AS 内则由相应 IQS 对地址伪造进行过滤，同时接受域内攻击的响应和措施部署。边界路由器分为两类，即边缘接入路由器和 AS 出口路由器。接入路由器位于边缘网络的接入点，可部署拦截请求，对异常流进行过滤。出口路由器位于 AS 之间，对下游的拥塞进行处理，部署下游的限流请求。

4.2.3 数据分组头扩展层

MRDA 采用了权证标记进行攻击的防御，需在数据分组中携带权证，接受中间路由器的验证。与 TVA 不同，MRDA 是以 AS 为单位进行权证申请，并由 IQS 授权给域内主机，因而权证格式不同于 TVA。此外，MRDA 还进行攻击拦截和拥塞限流，因而需要数据分组能够携带拦截请求和限流请求。

表 1 MRDA 符号注释

符号	注解
S_i	源 AS 主机
D_i	目标 AS 主机
S_{IQS}	源 AS 信息查找服务器
D_{IQS}	目标 AS 信息查找服务器
Ticket	数据分组携带的权证标记
T_{block}	请求拦截时间
T_{maxb}	最大允许拦截时间
T_{limit}	请求限流时间
T_{maxl}	最大允许限流时间

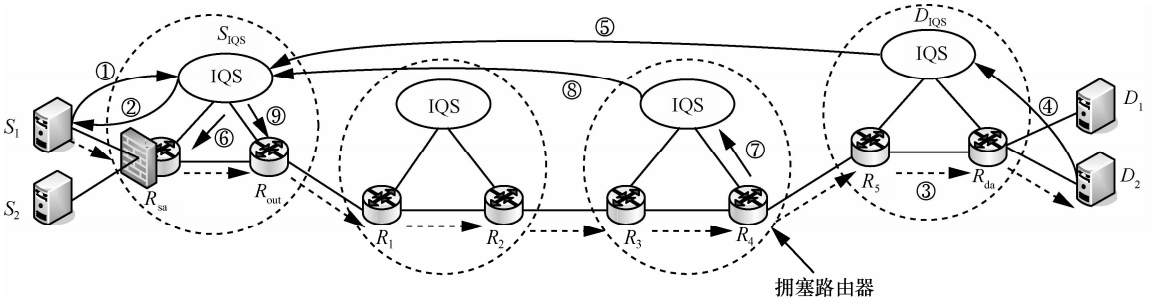


图 1 MRDA 结构示意

4.3　交互过程

MRDA 具有闭环控制的特点，参与者彼此能认证和识别对方，接收者可对源 AS 的数据传输进行控制，在保证安全性的前提下尽可能降低通信开销。MRDA 对拥塞控制进行了考虑，设计了通告和限流机制。如图 1 中的执行过程每一步都用序号进行标注，其中，数据传输为①→②→③，攻击拦截为④→⑤→⑥，拥塞限流为⑦→⑧→⑨。

① S_1 向 S_{IQS} 请求权证，申请发送数据给 D_2，S_{IQS} 收到请求后对其进行验证，如果合法则开始构建权证。构建权证过程中，如没有 D_2 授权的权证则需向 D_2 进行权证申请，然后利用申请到的权证构建授权给 S_1 的权证。

② S_{IQS} 将构建的权证返回给 S_1，S_1 收到权证后则可以发送携带权证的数据。

③ S_1 发送含有合法权证的数据分组，沿途路由器对数据分组进行验证，合法则放行，否则降级传输(降级为普通数据分组，在普通队列竞争传输)。

④ D_2 检测到接收的数据分组(携带权证)是恶意的，如使用流量检测技术[20,21]，则向 D_{IQS} 发送拦截请求，要求其通知 S_{IQS} 进行拦截，拦截的时长为 T_{block}(最大为 T_{maxb})，实验中采用经验值。

⑤ D_{IQS} 接受 D_2 的拦截请求，并向 S_{IQS} 发送拦截请求，S_{IQS} 对请求进行验证，如合法则通知 R_{sa} 部署拦截规则。

⑥ S_{IQS} 通知 R_{sa} 进行拦截，R_{sa} 接受并对来自于 S_1 的数据流进行拦截。

⑦ 路由器 R_4 发现拥塞，对数据流进行地址前缀聚合，获取流量较大的前缀地址(假设地址前缀属于 S_{IQS} 所在的 AS)，然后向域内的 IQS 发送限流请求，时长为 T_{limit}(最大为 T_{maxl})。

⑧ R_4 所在域的 IQS 向 S_{IQS} 发送限流请求。

⑨ S_{IQS} 通知 R_{out} 部署限流规则，R_{out} 接受并降低 AS 外出流量。

5　MRDA 详细设计与实现

5.1　权证请求和授权

权证强调申请、授权、携带和验证，为短期通信凭证，在 TVA[15]中得到了较好的设计。初始通信时，未获得权证的发送者需先获得接收者授权的权证，然后携带权证进行数据发送，接受中间路由器的校验，最终将数据分组传递到接收端。

对于权证的请求和授权，应如何实现？已有研究[15]认为可考虑 2 种方式：1) 利用专门请求分组申请权证，该方式占用较多路由器开销和处理时间，但能获得较好的实时性；2) 利用 TCP SYN/ACK，在数据部分携带权证请求和授权信息，该方式能节省网络资源，但实时性不是很理想。结合这 2 种方式的特点，MRDA 对于权证请求和授权以 TCP SYN/ACK 为主，同时在网络性能不好或实时性要求较高时采用专门请求和授权数据分组。

MRDA 在权证申请和授权上做了精心设计，放弃了 TVA 中采用的端对端模式，改用两级申请模式，即源主机向本地 IQS 申请、本地 IQS 向目标主机申请。采用该模式主要考虑以下 2 点：

1) 端对端的请求占用的网络通信资源较大；

2) 端对端的申请占用对端处理资源较多。

图 2 所示为源主机向本地 IQS 服务器申请权证。源主机发送一个权证请求分组，服务器收到请求分组后对其进行验证并构建和授权权证(假定 IQS 有到目标端的权证)。授权时涉及授权通信量(N')和时间(T')的计算，如式(1)所示。

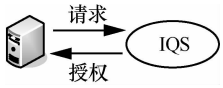


图 2　源主机向本地 IQS 请求权证

$$\begin{cases} N' = N'_{\min} + k\alpha N' \\ T' = T'_{\min} + k\beta T' \end{cases} \tag{1}$$

其中，$N'_{\min}$ 和 $T'_{\min}$ 为初始授权通信量和时间，单位分别为 Mbit 和 s；N' 和 T' 为经 k 次更新后的授权通信量和时间，单位同 $N'_{\min}$ 和 $T'_{\min}$，上限分别为 $N'_{\max}$ 和 $T'_{\max}$；k 为更新次数，取值为正整数；α 和 β 为控制系数。为减少中间路由器的存储状态，源端的发送速率应小于 N'/T'。

图 3 为源端 IQS 向目标主机申请权证。源端 IQS 采用专门或附带的方式向目标主机发送请求包，沿途路由器向转发的数据分组中插入预权证和更新拥塞标识，更新规则为 min(当前路由器拥塞度量，上游路由器拥塞度量)。目标主机收到请求后，先提取拥塞标识并更新对源 IQS 的信誉评估值(如式(2)所示)，产生综合评价值(如式(3)所示)，决定是否授权权证。如果授权则计算授权通信量(N)和时间(T)(如式(4)所示)，并构建权证回传给源 IQS。

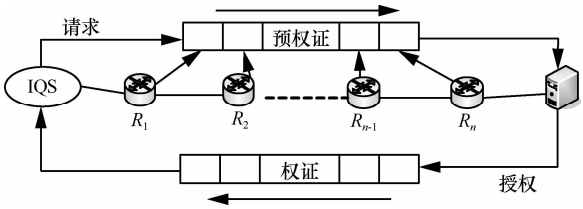


图 3 源 IQS 向目标主机请求权证

$$P=\begin{cases}(1-\eta t)P+(-1)^{\rho}\dfrac{P}{\lambda}\\(1-\eta t)P\end{cases} \tag{2}$$

式(2)中，当前信誉值 $P\geqslant 0$；η、ρ 和 λ 为控制系数，其中，$\eta<1$，ρ 取值为 0 或 1(发现恶意取 1，否则取 0)，λ 取正整数。

$$Au=\begin{cases}P, & P<C\\C, & P>C\end{cases} \tag{3}$$

其中，Au 取信誉值和拥塞值中的最小值，提高网络通信效率；拥塞度量值 $C\geqslant 0$。

$$\begin{aligned}N&=N_{\min}+l\delta N\cdot Au\\T&=T_{\min}+l\theta T\cdot Au\end{aligned} \tag{4}$$

其中，$N_{\min}$ 和 $T_{\min}$ 为初始授权通信量和时间，单位分别为 Gbit 和 m；N 和 T 为经 l 次更新后的授权通信量和时间，单位同 $N_{\min}$ 和 $T_{\min}$，上限分别为 $N_{\max}$ 和 $T_{\max}$；l 为更新次数，取值为正整数；δ 和 θ 为控制系数。

图 4 为预权证和权证格式，也可采用文献[22]的增强型权证方案，进一步权衡通信效率和安全。

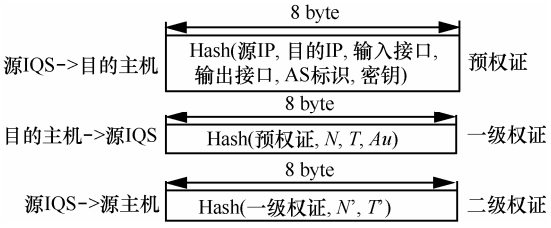


图 4 预权证和权证格式

5.2 数据分组携带权证

针对请求权证如何在数据分组中携带 TVA[15] 提出 3 种可选形式：新增头部、IP 选项和填充层。MRDA 采用了填充层的方式携带权证(如图 5 所示)，处于 IP 层和上层协议之间，便于网络层处理。

图 5 权证信息在数据分组中的位置

填充层的数据结构简述如下，图 6 给出了公共头部的字段格式，并描述了源主机与源 IQS 间的权证申请所需填充层的数据结构，其中数字所用的单位为 bit(以下均同)。

图 6 公共头部及源主机请求权证结构

图 7 所示为源 IQS 与目标主机的权证请求和授权的填充层结构。该结构主要包含请求时需填充的信息和授权时携带的信息，其中 Au 由式(3)导出，拥塞标识为式(3)中的 C 值。

图 7 源 IQS 请求权证结构

图 8 所示为填充层中携带的权证及其相关信息，包含了公共头部、授权 N' 和 T'、授权 N 和 T，以及 *nonce* (可设为 64 bit 随机数，为防止伪造，可以取 128 bit 或 256 bit，甚至更大)。

公共头部(16)	指针(8)	数量(8)
N(16)	*T*(16)	
N'(16)	*T*'(16)	
nonce(64)		
Au(32)		
权证1(64)		
…		
权证*n*(64)		

图 8　数据分组携带权证结构

5.3　路由器验证权证

携带权证的数据分组经中间路由器转发时，如何进行验证？MRDA 对首次出现的数据分组重新计算散列(如式(5)所示)，并匹配数据分组中携带的权证。为减少路由器存储的状态，将数据分组携带的 *nonce* 记录在缓存中，简化后继匹配，只在 T' 超时(在队列控制中要求传输速率不大于 N'/T'，因而判断 T' 即可)时将其丢弃。对验证失败的权证，可能有 2 种情况，即伪造或路由失效，MRDA 不进行区分，仅将其作为普通数据分组做降级处理。

$$\text{hash}(\text{hash}(\text{hash}(\text{源}IP,\text{目的}IP,\text{输入接口,输出接口,}AS\text{标识,密钥})N,T,Au),N',T') \tag{5}$$

5.4　路由节点失效处理

为提高 MRDA 的顽健性，设计时需考虑路由失效和改变(如路由器故障或重启)的情况，数据分组能否正常传输。该过程主要表现为分组到达路由器后，发现路由器缓存中无相关权证状态(未建立状态或因缓存状态或密钥丢失)，以至于无法验证。

该情况一般较少(现有网络的路由相对较稳定)，但仍需考虑，以降低对网络正常通信的影响。MRDA 采用对合法分组降级的方式来解决。发生路由失效时，新的路由节点(原本不在该路径上)将合法分组降为一般数据分组(未携带权证的数据分组)在剩路径中传输，并改变公共头部的类型字段为降级，以表明后续数据分组传输为降级传输，不需进行验证。同时，路由器对数据分组降级后，将通过 IQS 反馈该信息给源 IQS，让其停止授权该权证。目标主机收到降级的合法分组时，将返回降级反馈分组，提示发送者重新申请权证。

5.5　瓶颈链路拥塞处理

瓶颈链路的影响对网络来说不可忽视，为此需要对瓶颈链路的拥塞进行控制。图 9 为路由器队列管理示意，分为 3 种类型：请求队列、合法分组队列和普通分组队列。请求队列主要用于容纳通过链路的请求分组，其占整个队列的 0%~5%(依据请求状况动态变化)；合法分组队列为携带合法权证的数据分组所经过的队列，占整个队列的 90%~95%；普通分组队列为降级数据分组和未携带权证的数据分组经过的队列，占整个队列的 5%。从队列分配可看出，若洪泛攻击发生，攻击分组只占用普通队列(从路由器验证可知，权证伪造攻击分组和路由失效分组同时都不能被成功验证，因而全被降级处理)，而不会影响其他队列，因而将攻击限制在带宽的 5%以下，保证了正常的网络通信。

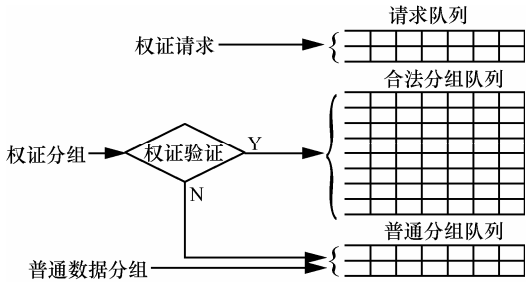


图 9　路由器队列管理示意

此外，在处理大流量造成的拥塞时，MRDA 采用限流反馈机制。下游路由器产生拥塞时，利用 IQS 之间的协作，通知源 AS 的出口路由器限流。

5.6　密钥更新

在 MRDA 中，每条流的权证是否可以一直保持不变？回答是否定的。原因是攻击者可能通过暴力破解的形式，获得权证信息，并利用其进行洪泛攻击。为阻止攻击者对权证的伪造攻击，需要对某些信息进行改变，以使攻击无效。与 TVA 和 SIFF 类似，路由器通过不断改变密钥，以达到抵抗攻击的能力。同时，对于 IQS 之间，路由器与 IQS 之间的数据传输采用了加密方式，以防止窃听和篡改等威胁。式(6)为 MRDA 采用的 D-H 密钥交换过程[23]。

$$\begin{aligned} K &= (Y_{\text{B}})^{X_{\text{A}}} \bmod q \\ &= (\alpha^{X_{\text{B}}} \bmod q)^{X_{\text{A}}} \bmod q \\ &= (\alpha^{X_{\text{B}}})^{X_{\text{A}}} \bmod q \\ &= (\alpha^{X_{\text{A}}})^{X_{\text{B}}} \bmod q \\ &= (\alpha^{X_{\text{A}}} \bmod q)^{X_{\text{B}}} \bmod q \\ &= (Y_{\text{A}})^{X_{\text{B}}} \bmod q \end{aligned} \tag{6}$$

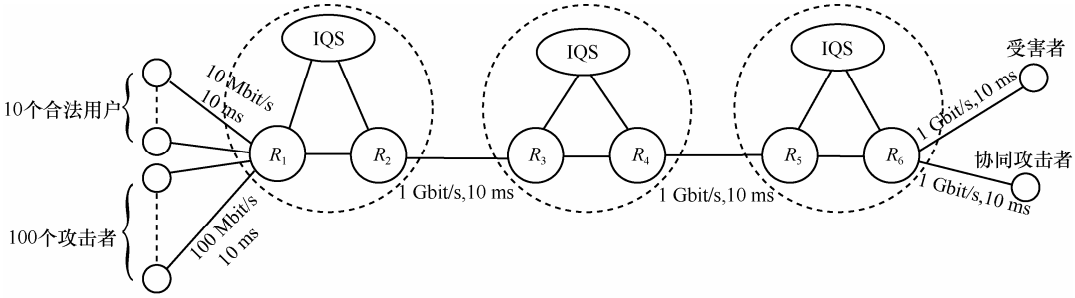


图 10　MRDA 仿真拓扑示意

6　仿真实验评估与分析

6.1　实验数据和仿真拓扑

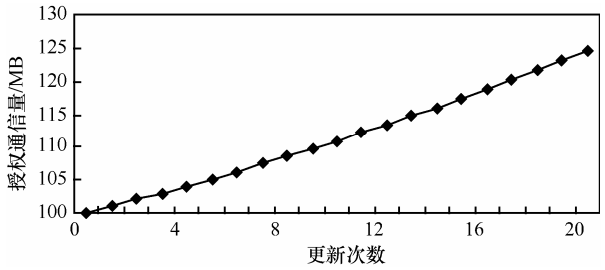
为有效评估 MRDA，仿真实验采用了权威的 CAIDA[24]提供的大规模真实因特网拓扑数据集。原数据集多达数百万条拓扑记录。作者选择 Skitter 中的 HR20030507SR 数据集，删除重复后，随机选择了 10 000 条路径作为仿真实验数据，并在 NS2 下构建如图 10 的仿真拓扑。其中，R_1~R_6 为路由节点，IQS 为不同域的信息查询服务器节点，实验数据集跨不同的自治域，且每条路径的最后一跳相同。为逼近真实网络，依据真实的数据集生成权证，并进行申请、授权、携带和验证操作。

仿真拓扑中，合法用户数为 10，接入带宽 10 Mbit/s，延迟为 10 ms。攻击者数为 100，攻击模式为 Flooding DoS，接入带宽为 100 Mbit/s，延迟为 10 ms。所有域间链路的带宽为 1 Gbit/s(实际中可能要大许多)，延迟为 10 ms，受害者的接入带宽为 1 Gbit/s，延迟为 10 ms。仿真开始时，合法用户发送 10 MB 数据文件到受害者，瓶颈链路队列结构如图 9 所示，攻击者的攻击类型包含协同攻击和异常攻击，尽可能使受害者服务降低甚至产生拒绝服务。

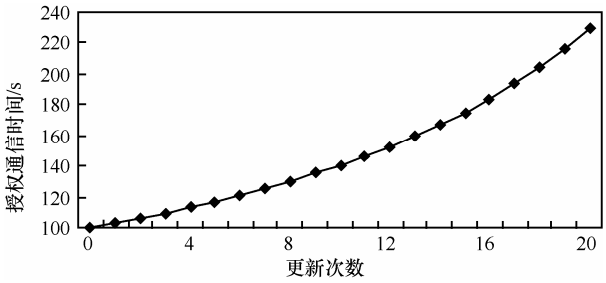
6.2　实验结果

首先来看权证授权的有效性。图 11 给出了源 IQS 和目标机授权权证的通信量和通信时间与更新次数的关系，随着更新次数(合法)不断增加，授权通信量呈曲线增长趋势，总体符合预期的要求。

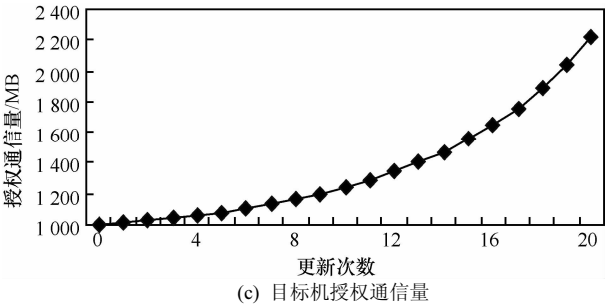
其次来看 10 MB 文件在不同方案下的传输表现。图 12 给出 SIFF[14]、PUSHBACK[25]、TVA[15]和 MRDA 传输同样大小文件，在不同攻击者数量情况下的时间对比。可看出，MRDA 模型能在攻击者数量增加的情况下，保持文件传输时间基本不变，具有更好的文件传输稳定性。



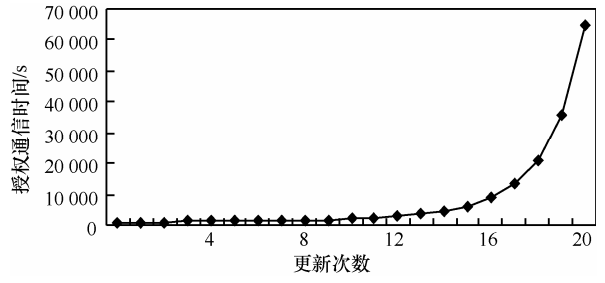
(a) 本地 IQS 授权通信量



(b) 本地 IQS 授权通信时间



(c) 目标机授权通信量



(d) 目标机授权通信时间

图 11　MRDA 中权证授权通信量和通信时间变化

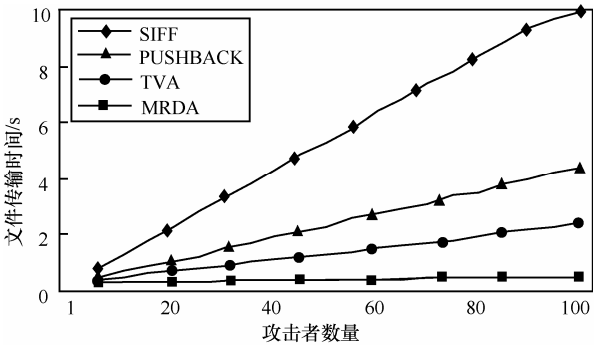


图 12　MRDA 与已有方案在文件传输场景下对比

最后来看权证请求时间。图 13 比较了 TVA[15] 中权证请求时间与 MRDA 的权证请求时间，可以看出 MRDA 的权证请求时间相比 TVA[15]有较大改善，除首次申请时间较长，并且在合法者请求越多时其平均请求时间越短。

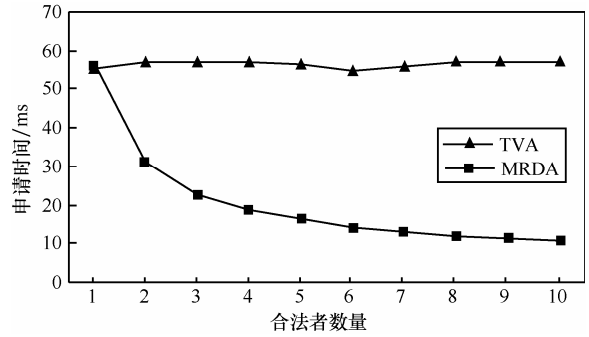


图 13　MRDA 与 TVA 的平均权证请求时间对比

此外，表 2 对不同的标记类 DoS 防御方案进行了对比，可以看出，本文方案相对于 TVA 的计算和通信开销有所降低，主要原因为本文方案采用了两级权证机制。对于顽健性而言，能与 TVA 相当，好于其他方案。

6.3　分析和讨论

6.3.1　可部署性和扩展性

MRDA 的设计目标是面向自治域(AS)实现增量部署，同时激励早期部署，需要更新路由器和主机，并构建 IQS 服务器。每个 AS 可独自部署 IQS 服务器，并从中获得好处，同时仅需要更新边界路由器(接入路由器和出口路由器)以支持权证产生与验证、过滤请求产生与处理和限流请求产生与处理。一个部署了 MRDA 的 AS 能阻止攻击流进入网络，验证所有的数据流，同时部署了 MRDA 的中间 AS 或目标 AS 能发现伪造权证攻击或接收方检测出异常攻击，并通知源 AS 进行过滤。

一个中间传输的 AS 仅需验证转发数据分组的合法性，丢弃非法分组，保证合法通信，因而需要升级边界路由器的部分功能，利用数据分组头部携带的信息在路由器上实现拥塞控制，保证合法分组的通信。

对于未部署 MRDA 的 AS，同样保证其正常通信，但只能让其以一般数据分组的形式穿过传输网络，实现该目标主要依靠路由器的队列管理，它构建了一般数据分组的队列，占用带宽较少(因为未部署 MRDA 的 AS 产生的数据分组可能为非法的)。

MRDA 适用于 IPv6，在 IP 分组头部除包含固定的字段外，具有灵活的扩展头部，而本文方案可在 IP 分组的扩展头部携带权证信息，因而可以很容易从 IPv4 升级到 IPv6 版本。此外，MRDA 可进一步设计成支持双协议的模式，根据 IP 分组头部字段进行自动识别和进行相应处理。

6.3.2　安全性和效率

MRDA 的安全性主要体现在 3 个方面：1) 权

表 2　　**不同的基于标记的 DoS 防御方案对比总结**

方案	属性						
	网络架构	防御阶段	防御层次	计算	通信	复杂性	顽健性
PPM[5]	IPv4	响应	网络层	高	低	低	低
DPM[6]	IPv4	响应	网络层	中	低	低	中
Pi[7,8]	IPv4	响应	网络层	中	低	低	低
SIFF[14]	IPv4/NGSI	预防和响应	网络层	中	中	低	中
TVA[15]	NGSI	预防和响应	网络层和应用层	高	高	中	高
StopIt[18]	NGSI	检测和响应	网络层和应用层	低	高	高	中
NetFence[19]	NGSI	检测和响应	网络层	低	低	中	中
BINC[16]	NGSI	预防	应用层	低	低	中	低
本文方案	NGSI	预防和响应	网络层和应用层	中	中	低	高

证标记的安全，该特性通过 64 bit 权证和动态密钥来实现；2) 过滤和限流机制，能在受伪造权证攻击、异常攻击中及时响应并消除，极大地降低攻击造成的危害，限流机制的采用，能提高网络通信的效率，降低由于分组丢失而造成的重传所带来的通信压力；3) 抵抗针对自身的攻击。因有部分攻击可能会对系统本身进行攻击，破坏其防御能力(例如 DoC 攻击[17])。MRDA 具有自我抵抗能力，对域内的请求采用验证方式，同时在高负载时利用客户端猜谜[26]降低其被域内主机的请求洪泛，保证 IQS 的安全性。在中间链路上，请求信道也受到了保护，以 AS 为单位的请求能将请求数量控制在一定范围内(截至 2011 年底，因特网上的 AS 数量约在 50 000 个[27]左右，实际在用数量变化不大)。

MRDA 的效率主要体现在其对现有网络传输性能影响较小，概括起来包括 3 个方面：1) 权证本身对数据传输信道的占用应尽量小，因而在 MRDA 中的权证长度采用变长[22]，其依据对源 AS 的信任决定，同时要能抵抗伪造权证伪造攻击；2) 授予权证通信的时间(T)和通信量(N)不宜过小，因而在 MRDA 采用两级授权，即接收方对源 IQS 的授权和源 IQS 对域内主机的授权，这两类授权中的 N 和 T 各不相同，前者较大，可持续的通信时间较长，通信量以 Gbit 计；后者则较小，通信时间以秒计，通信量以 Mbit 计；3) 对中间传输队列进行动态控制，这可提高链路的利用率。例如 RTS 队列在 0%~5% 间波动，假设主干带宽为 40 Gbit/s，此时仅按 5% 分配则需 2 Gbit/s 的带宽保留给 RTS，而此时 RTS 需要的带宽仅 200 Mbit/s，这将造成 90%的带宽浪费。而动态队列管理可将该部分带宽用于数据通信。

6.3.3 攻击限制性能

攻击限制主要体现在两方面。一是对域内攻击的限制，主要由 IQS 对域内主机管理实现，每个在域内进行传输数据的主机都是真实可信的，地址不能伪造。当域内其他主机受到本域内主机的(洪泛)攻击时，将向 IQS 进行请求过滤，本文未给出具体实现细节，作者假设其是可控制的。二是对 AS 间的攻击限制能力，主要采用 3 个机制：①权证标记；②攻击拦截；③传输限流。权证的使用在 TVA、Passport 和 SIFF 等都有讨论和使用，其可抗拒大规模的洪泛攻击，接收者能控制发送者的数据发送，能实现较好的攻击限制。然而，其应对狡猾攻击的(如利用合法权证的策略洪泛)存在不足，因而采用过滤机制，由接收者对发送者进行过滤，并在后续权证授权时将其视为次级用户。此外，为防止协同攻击造成的拥塞，MRDA 采用传输限速机制，由 IQS 间的协作限制大流量 AS 的出口速率。

7 结束语

本文针对 DoS 防御技术，分析已有权证方案的问题，面向 AS 设计和实现了 DoS 攻击流抑制模型。NS2 上的仿真对比实验显示，MRDA 具有较好的性能，同时对现有网络通信传输的影响较小。

参考文献：

[1] Arbor networks. worldwide infrastructure security report[EB/OL]. http://www.arbornetworks.com/en/research.html, 2012.

[2] PENG T, LECKIE C, RAMAMOHANARAO K. Survey of network-based defense mechanisms countering the DoS and DDoS problems[J]. ACM Computing Surveys, 2007, 39(1):1-42.

[3] 张永铮, 肖军, 云晓春等. DDoS 攻击检测和控制[J]. 软件学报, 2012, 23(8):2258-2072.
ZHANG Y Z, XIAO J, YUN X C, *et al*. DDoS attacks detection and control mechanisms[J]. Journal of Software, 2012, 23(8):2258-2072.

[4] 王进, 阳小龙, 隆克平. 基于大偏差统计模型的 Http-Flood DDoS 检测机制及性能分析[J]. 软件学报, 2012, 23(5):1272-1280.
WANG J, YANG X L, LONG K P. Http-flood DDoS detection scheme based on large deviation and performance analysis[J]. Journal of Software, 2012, 23(5):1272-1280.

[5] GOODRICH M T. Probabilistic packet marking for large-scale IP traceback[J]. IEEE/ACM Transactions on Networking, 2008, 16(1): 15-24.

[6] BELENKY A, ANSARI N. On deterministic packet marking[J]. Computer Networks, 2007, 51(10):2677-2700.

[7] YAAR A, PERRIG A, SONG D. Pi: a path identification mechanism to defend against DDoS attacks[A]. Proceedings of IEEE Symposium on Security and Privacy[C]. 2003.

[8] 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.

[9] 金光, 张飞, 钱江波等. 融合路径追溯和标识过滤的 DDoS 攻击防御方案[J]. 通信学报, 2011, 32(2):61-67.
JIN G, ZHANG F, QIAN J B, *et al*. DDoS defense with IP traceback and path identification[J]. Journal on Communications, 2011, 32(2):61-67.

[10] ANDERSON T, ROSCOE T, WETHERALL D. Preventing internet denial-of-service with capabilities[J]. ACM SIGCOMM Computer Communications Review, 2004, 34(1):39-44.

[11] BELLOVIN S M, CLARK D, PERRIG A, *et al*. A clean-slate design for the next-generation secure internet[A]. Proceedings of National Science Foundation Workshop on Next-Generation Secure Internet[C]. 2005.

[12] 吴建平, 吴茜, 徐恪. 下一代互联网体系结构基础研究及探索[J]. 计算机学报, 2008, 31(9):1536-1548.
WU J P, WU Q, XU K. Research and exploration of next-generation Internet architecture[J]. Chinese Journal of Computers, 2008, 31(9):1536-1548.

[13] 林闯, 雷蕾. 下一代互联网体系结构研究[J]. 计算机学报, 2007, 30(5): 693-711.
LIN C, LEI L. Research on next generation Internet architecture[J]. Chinese Journal of Computers, 2007, 30(5):693-711.

[14] YAAR A, PERRIG A, SONG D. SIFF: a stateless internet flow filter to mitigate DDoS flooding attacks[A]. Proceedings of IEEE Symposium on Security and Privacy[C]. 2004.

[15] YANG X, WETHERALL D, ANDERSON T. TVA: a DoS-limiting network architecture[J]. IEEE/ACM Transactions on Networking, 2008, 16(6):1267-1280.

[16] SHUE C A, KALAFUT A J, ALLMAN M, *et al*. On building inexpensive network capabilities[J]. ACM SIGCOMM Computer Communication Review, 2012, 42(2):73-79.

[17] ARGYRAKI K, CHERITON D. Network capabilities: the good, the bad and the ugly[A]. Proceedings of ACM HotNets IV[C]. 2005.

[18] LIU X, YANG X, LU Y. To filter or to authorize: network-layer DoS defense against multimillion-node botnets[A]. Proceedings of ACM SIGCOMM[C]. 2008.

[19] LIU X, YANG X, XIA Y. NetFence: preventing Internet denial of service from inside out[A]. Proceedings of ACM SIGCOMM[C]. 2010.

[20] 孙红杰, 方滨兴, 张宏莉. 基于链路特征的 DDoS 攻击检测方法[J]. 通信学报, 2007, 28(2):88-93.
SUN H J, FANG B X, ZHANG H L. DDoS attacks detection based on link character[J]. Journal on Communications, 2007, 28(2):88-93.

[21] 臧天宇, 云晓春, 张永铮等. 基于通信特征和 D-S 证据理论分析僵尸网络相似度[J]. 通信学报, 2011, 32(4):66-76.
ZANG T Y, YUN X C, ZHANG Y Z, *et al*. Botnet's similarity analysis based on communication features and D-S evidence theory[J]. Journal on Communications, 2011, 32(4):66-76.

[22] 金光, 杨建刚, 魏蔚等. 基于增强权证的无状态过滤机制[J]. 电子与信息学报, 2008, 30(10):2490-2493.
JIN G, YANG J G, WEI W, *et al*. Stateless filtering based on enhanced capabilities[J]. Journal of Electronics & Information Technology, 2008, 30(10):2490-2493.

[23] RESCORLA E. Diffie-hellman key agreement method[EB/OL]. http://tools.ietf.org/html/rfc2631, 1999.

[24] CAIDA[EB/OL]. http://www.caida.org, 2011.

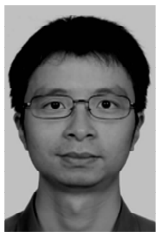
[25] MAHAJAN R, BELLOVIN S M, FLOYD S, *et al*. Controlling high bandwidth aggregates in the network[J]. ACM Computer Communication Review, 2002, 32(3):62-73.

[26] PARNO B, PERRIG A, WENDLANDT D, *et al*. Portcullis: protecting connection setup from denial-of-capability attacks[A]. ACM SIGCOMM[C]. 2007.

[27] BGP routing table analysis reports[EB/OL]. http://www.cidr-report.org/as2.0/#General_Status, 2011.

作者简介：

江先亮（1986-），男，安徽黄山人，浙江大学博士生，主要研究方向为无线网络和网络安全。



金光（1972-），男，浙江台州人，博士，宁波大学教授，主要研究方向为网络安全与无线网络。

杨建刚（1959-），男，四川西昌人，博士，浙江大学教授、博士生导师，主要研究方向为计算智能和网络安全。

何加铭（1949-），男，浙江绍兴人，博士，宁波大学教授，主要研究方向为无线通信和移动互联网应用。