基于路由器代理的分布式湮没检测系统

朱文涛 李津生 洪佩琳
(中国科学技术大学电子工程与信息科学系 合肥 230027)

摘 要 TCP 同步湮没是最常见也是最重要的拒绝服务攻击,研究其防范措施对保障网络安全具有重要意义.为弥补状态检测防火墙和基于服务器方案等传统对策的不足,湮没检测系统 FDS 在叶节点路由器上监控 TCP 控制分组,根据"SYN-FIN 匹配对"协议特性对本地统计信息进行分析以检测攻击.为保护大规模网络,该文将基于代理的分布式入侵检测理论与湮没攻击检测结合,给出了面向硬件的简化系统 SFDS.以 SFDS 作为集成在路由器网络接口的检测代理,提出了一种高性能的分布式湮没检测系统并论述了其全局判决机理.

关键词 同步湮没;湮没检测系统;路由器;代理;分布式入侵检测
中图法分类号 TP393

A Router-Agent-Based Distributed Flooding Detection System

ZHU Wen-Tao LI Jin-Sheng HONG Pei-Lin
(*Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei* 230027)

Abstract TCP SYN flood is one of the most common and most important denial of service attacks. Research against SYN flood is of great value to network security. Traditional countermeasures such as stateful inspection firewalls and other server-based solutions have been proved limited and not very efficient. We present a novel approach based on the Flooding Detection System (FDS), which is installed at the leaf routers. Based on the protocol behavior of TCP SYN-FIN pairs, the FDS detects attacks by monitoring TCP control packets and analyzing the local statistical information. To protect large scale network, we first associate the agent-based distributed intrusion detection with detecting SYN flood attacks. A Simplified Flooding Detection System (SFDS) is then proposed and its algorithm is proved to be hardware-oriented. By integrating the SFDSs as detection agents into network interfaces of the routers, we propose a high-performance distributed flooding detection system and its global decision mechanism is illustrated.

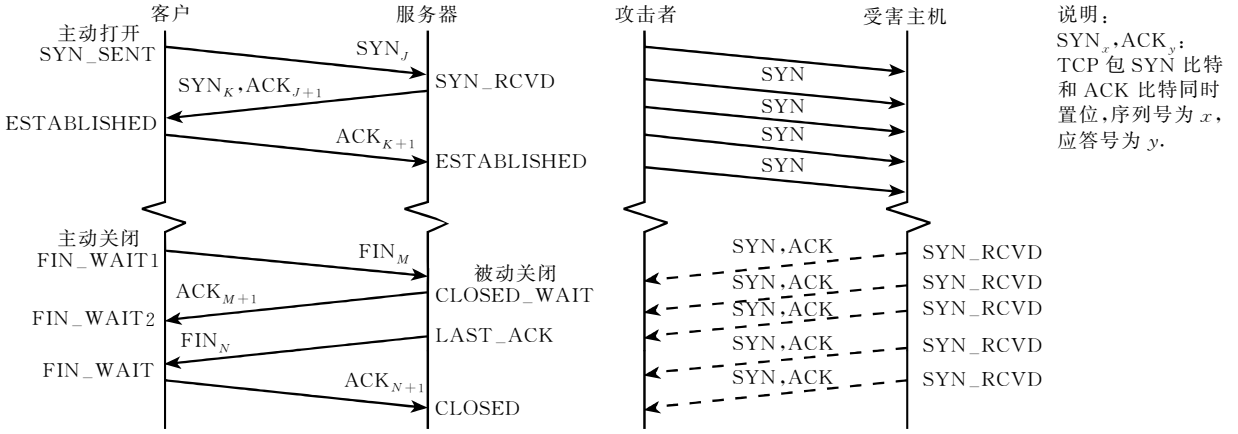
Keywords SYN flood; flooding detection system; router; agent; distributed intrusion detection

1 引 言

自 20 世纪 90 年代以来,拒绝服务攻击(DoS)一直是网络攻击的重要手段,其中以 TCP 同步湮没(SYN flood)为代表.SYN flood 出现于 1996 年,攻击者向目标主机的 TCP 侦听端口高速发送连接请求包(SYN 比特置位,下称 SYN 包),却又不按三次握手规程完成连接(参见图 1),从而使待连接队列饱和,不能接受新连接请求[1].攻击程序通常使用伪

收稿日期:2002-07-23;修改稿收到日期:2003-03-26.本课题得到国家自然科学基金项目"面向大规模网络的分布式入侵检测和预警模型"资助(90104030).**朱文涛**,男,1979 年生,博士研究生,主要研究方向为通信协议与网络安全. E-mail: wtzhu@263.net. **李津生**,男,1937 年生,教授,博士生导师,主要研究领域为信息通信与下一代因特网. **洪佩琳**,女,1961 年生,教授,博士生导师,主要研究领域为策略控制和信息安全.

造的源 IP 地址发动 SYN flood 以隐藏自身①,使受害主机及包过滤防火墙难以区分合法客户的连接请求和攻击者伪造的连接请求,危害非常大.



(a) 正常 TCP 连接的建立(三次握手)及拆除过程(主动关闭)　(b) 攻击者高速发送大量 SYN 包但不完成三次握手,SYN/ACK 包有去无回

图 1　正常 TCP 连接的建立过程及 SYN flood 攻击原理

为防范 SYN flood 攻击,典型的解决方案是启用状态检测防火墙[2],它由包过滤防火墙演进而来,通过监视客户与服务器的通信,维护表征当前连接的状态表,通过关联分析以判断 TCP 包是否合法.有的状态检测防火墙能代替服务器向客户回送连接响应,待三次握手完成再把连接导向真正的服务器,起到代理的作用.这类系统的缺点是必须为所有连接都维护相关信息,如源和目的地址、源和目的端口、当前状态,甚至 TCP 最大段长度 MSS[3] 等,需耗费大量存储空间.IPv6 取代 IPv4 是发展必然[4],届时线性状态表规模几乎要翻两番,检索深度亦显著增大.在高强度 DoS 攻击下,防火墙自身也难以避免资源耗尽的局面[2].

另一类解决方案则基于服务器本身,包括 SYN cache 和 SYN cookie 技术.SYN cache[5] 对 TCP 协议的实现稍加修改,用哈希表代替线性表来保存半连接信息,减少了 TCP 待连接队列的存储空间开销.SYN cache 仅仅是部分改善了服务器抗 SYN flood 攻击的能力.SYN cookie② 则根本不维护任何半连接信息,它要求 TCP 软件对收到的 SYN 包应答特殊的 SYN/ACK 包,其应答号由源和目的地址、源和目的端口、连接发起序列号按加密算法求出.当客户方对此 SYN/ACK 包应答以 ACK 包时,服务器检查其应答号以判断是否为对先前 SYN/ACK 包的确认,如正确则直接进入连接建立状态,从而跳过半开连接状态,避免 SYN flood 攻击.SYN cookie 的缺点在于 TCP 协商选项被全部丢弃,例如 MSS 和时戳[3] 等,从而对 TCP 性能有不可忽视的影响.另外,由于 SYN cookie 在连接建立起来之前根本不保存相关状态,因而 TCP 超时重发/出错重传的特点被摒弃,这直接影响到 TCP 面向连接的可靠传输特性.最后,SYN cookie 还额外引入了易被 ACK flood 攻击的脆弱性[5].

2　同步湮没检测系统 FDS

状态检测防火墙和基于服务器本身的解决方案都具有如下共同缺点:(1)攻击者通常用伪造源 IP 地址发动 SYN flood,Internet 路由具有非对称性,路由器只对目的地址寻址而不作源地址控制,也不维护出入 IP 分组的状态信息,所以很难查出真正攻击源;(2)已有解决方案或者消耗存储空间维护状态信息,或者需要处理器进行连接相关计算,无攻击情况下这些开销造成资源浪费,高强度攻击下防护系统自身又难以胜任;(3)连接建立时间不可避免地延长,甚至 TCP 实现规范被部分地破坏,从而影响到网络传输的性能.所以,研究 SYN flood 对抗措施具有重要意义,需引入新的机制弥补已有方案的不足.下面就介绍专门针对 SYN flood 攻击的入侵检测系统(Intrusion Detection System,IDS),即湮没检测系统 FDS[6].

FDS 的基本思想是在叶节点路由器(leaf rout-

① 伪造的源地址(记为 A)应满足对攻击目标(记为 B)而言网络不可达,否则当 A 收到 B 的 SYN/ACK 包时,按 TCP 协议,A 会被动响应以 RST 包通知 B 有错误发生.这样 B 就会拆除半连接,攻击也就不会起效果.

② 见 http://cr.yp.to/syncookies.html

er)上统计 TCP 控制分组的数量,使用特定算法来判决是否出现 SYN flood 攻击.按照入侵检测系统的分类[7],FDS 通过寻找与正常流量模式的偏离来检测攻击,故属于异常检测(anomaly detection);两个 FDS 分别监控网络进出流量,不针对特定操作系统和应用软件,所以又属于基于网络的入侵检测系统(NIDS).但是,FDS 突破了 NIDS 必须基于网段嗅听的技术路线,能以独立模块的形式植入叶节点路由器,使特定功能的入侵检测成为路由器的副产品.从 SYN flood 应对措施来看,FDS 是继状态检测防火墙和基于服务器方案之后的新型机制——基于路由器的解决方案.

在正常的 TCP 连接建立和拆除过程中,SYN 包和 FIN 包分别标识连接的开始和结束(参见图 1),这里 SYN 包统指仅有 SYN 比特置位的 TCP 包(在客户方看来是连接的开始)和 SYN、ACK 两比特同时置位的 TCP 包(在服务器看来是连接的开始),下同.RST 包亦可拆除 TCP 连接,所以和 SYN 包、FIN 包合称 TCP 控制分组(control packets)[6],是 FDS 统计的对象,如图 2 所示.相应地,SYN、FIN、RST 三个状态比特均为 0 的就称作 TCP 数据分组.

根据 TCP 协议,RST 包可以被动产生,例如在一个关闭的端口上收到数据(记作 $RST_{passive}$);也可以主动产生,例如强行拆除已有连接(记作 RST_{active}).由于对 FDS 而言,$RST_{passive}$ 不与 SYN 关联,故被认为是背景噪声,而 RST_{active} 则相当于特殊的 FIN 包.这样,正常 TCP 连接总可用 SYN-FIN 匹配对来描绘,包括(SYN,FIN)对、(SYN/ACK,FIN)对、(SYN,RST_{active})对三种具体形式.由于 FDS 无法区分两类 RST 包,通常取总个数的 75% 作为 RST_{active} 个数[6].

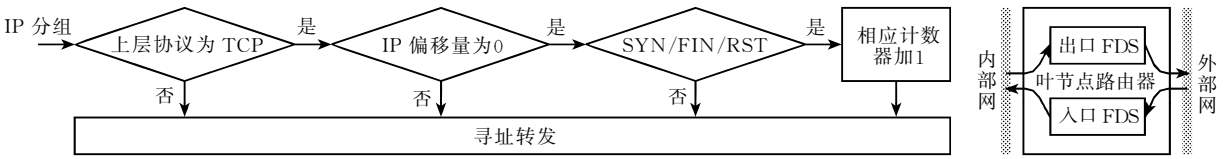


图 2　FDS 的工作示意图

同步湮没检测器由部署在叶节点路由器内的两个 FDS 组成(见图 2),每个 FDS 包含三个计数器,统计每个 t_0 时段内 TCP 控制分组个数;当某一方向流量与正常 SYN-FIN 统计模式明显偏离时就认为该方向出现 SYN flood 攻击.根据对 Internet 业务的统计,t_0 取为 20s;FIN 包总是迟于相应的 SYN 包出现,为使它们按连接关联,对每个 t_0 时段,FIN 包统计时间要延迟 $t_d=10$s.t_0 与 t_d 均可调,且 FDS 检测算法对两者的具体数值并不敏感[6].

定义 $\Delta_n=SYN(n)-FIN(n)$,$X_n=\Delta_n/F(n)$,其中 Δ_n 是在第 n 个时段内 SYN 包个数与 FIN 包个数之差,X_n 是 Δ_n 与 FIN 包均值估计 $F(n)$ 之比,且不再与具体网络或业务相关.FDS 将 $\{X_n\}$ 看作一随机过程,运用鲁棒性好的 non-parametric CUSUM 算法进行在线分析来检测湮没攻击.

FDS 具有明显的优点.出口 FDS(见图 2)监测内部网外出流量,能揭示攻击源的范围,不受伪造源地址欺骗;FDS 不维护连接状态,不进行相关计算,因而存储器/处理器开销特别小,本身对 SYN flood 具有免疫力;现今路由器多数都支持 IP 分组分类和区分 QoS/CoS[4],FDS 能方便植入其中,湮没检测也不破坏 TCP 协议及其性能.这样,FDS 就基本解决了本节开头指出的三大难题.另外,就入侵检测而言,特定网络业务中大量连接并发建立的 SYN burst 现象(如 Web 浏览器打开包含大量图片链接的页面时会对每个链接单独发起新 TCP 连接)常使一些 IDS 产生虚警,FDS 以 SYN-FIN 匹配对为理论依据,有效避免了误报①.

现今入侵检测(包括 DoS 攻击检测)需解决的主要问题之一是高速化,检测逻辑应尽量简单高效并便于硬件实现.另一方面,拓展检测视野、提高系统容错性亦是发展趋势.本文提出一种分布式湮没检测系统,并给出一种从 FDS 发展而来的湮没检测代理的实现方案.

3　分布式湮没检测系统

3.1　DIDS 的基本原理

传统的基于主机或基于网络的 IDS 局限于单一架构,缺乏对异构系统及大规模网络的监测能力,

① 如同其它 IDS 一样,FDS 也不可能做到完美无缺.例如它不进行状态维护,图 2 中检查 TCP 包时只从第一个 IP 分片查看 TCP 头标,若黑客强行分片使 TCP 头标位于第二个 IP 分片中(是一种碎片攻击),则可逃避检测.

不同 IDS 之间也不能协同工作,故难以对不断发展的网络提供安全保障.叶节点路由器内的两个 FDS 虽然可升级为通过共享存储器协作,但仍属于局部检测.为保护大范围异构网络,需发展分布式入侵检测系统 DIDS[7]以克服传统 IDS 在大规模网络环境下的局限性,做到从不同子网发生的攻击来判断整体网络可能存在的风险,从而实时检测和预警.本文将分布式入侵检测系统框架与湮没攻击检测结合,提出由遍布网络的多个代理(agent)组成的分布式湮没检测系统.这些代理从 FDS 改进而来,并部署于所有路由器(不仅限于叶节点路由器)的网络接口上,它们将安全事件向分析中心汇报以进行全局网络监控.

使用分布式系统检测 SYN flood 需要作以下假设:①攻击出现的概率较低,两次攻击发生的时间间隔足够长;②网络稳定,路由表变化缓慢,在短时间内从特定源地址到特定目的地址的 IP 分组具有固定路径.条件①保证分析中心不会将两次攻击混淆为一个事件,且与代理间不至于频繁通信,条件②保证能有效检测出攻击源和攻击目标,并能识别协同攻击等形式.据美国网络安全服务商 Riptech 的调查报告,受网络攻击最频繁的公司平均每 6 个月遭受 700 次安全事件①.这样一般而言,一台网络服务器平均每天受到的 SYN flood 攻击至多 4 次.典型的 SYN flood 持续时间约为 10min,对于通常的园区网和城域网,路由器的寻路转发表在这期间大都变化很小,所以上述两个条件一般都能满足,而分布式湮没检测系统的代理就部署在这些路由器的网络接口上.

3.2 检测代理——面向硬件的 SFDS

FDS 作为检测代理存在一些不利因素:CUSUM 检测算法中$\{X_n\}$为一浮点数序列,硬件化时对芯片要求高,算法亦略显复杂.本文给出一简化的只涉及定点计算的替代系统,称之为 SFDS(Simplified Flooding Detection System).如图 3 所示,在 t_c 时刻 SYN 包计数器值保存为 syn_c后清零,在 t_c+t_d 时刻 FIN 包和 RST 包计数器值保存为 fin_c和 rst_c 后清零,此时(t_c+t_d时刻)进行计算判决:若 syn_c小于门限值 syn_{min}则无操作,否则令 $fin_c=fin_c+rst_c\times3/4$ 为计入 RST_{active}后当前时段的 FIN 包个数,若 syn_c/fin_c 大于门限 p/q 则向分析中心报警.SFDS 仍取 $t_0=20$,$t_d=10$.对一台不受保护的主机要发起有效湮没,所需最小攻击速率的典型值是每秒 500 个 SYN 包②,考虑到 N 个湮没源协同攻击的情况(如分布式 DoS),应取 $syn_{min}=500\times t_0/N$,通常 N 不会太大,如取 $N=25$,则有 $syn_{min}=400$.p/q 是 SFDS 容忍的最高 SYN-FIN 比,当 $syn_c\times q>fin_c\times p$,则认为当前方向上出现 SYN flood 攻击.

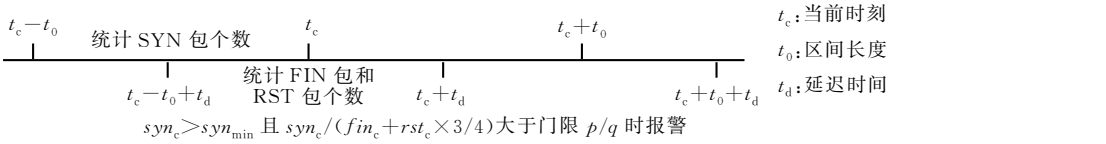


图 3 SFDS 检测过程与判决原理

需要指出的是,FDS 部署在叶节点路由器内,两套 FDS 判决算法略有不同,而 SFDS 部署在全体路由器的所有网络接口上(每个接口各两个③),仅当 syn_c大于 syn_{min}时才检查 SYN-FIN 比,且 p/q 值允许依情况设定.例如,作者对园区网内某路由器进行了 24 小时×31 天的连续监测,统计结果表明仅个别 SYN-FIN 比显著高于 1.75,而低于 1.75 的比值呈密集分布;1.75=7/4,故此情况下 p 取 7 而 q 应取 4.

SFDS 采用的定点算法非常简单而又高效,其检测逻辑基于硬件上极易实现的计数单元.对百兆以太网,t_0时段内最多发送的 SYN 包个数为 $t_0\times100\times10^6/(64\times8)=3906250<2^{22}$(64×8 比特是最短以太帧长[8]),取 SYN/FIN/RST 计数器各占 22 比特,每个路由器接口(一进一出两个 SFDS)共需要 $22\times3\times2=132$ 比特存储空间,这样用 FPGA 实现 SFDS 的话根本不需要片外存储器.此外,SFDS 算法既适用于 IPv4 网络又适用于 IPv6 网络,而相比之下,状态检测中仅维护一对 IPv6 地址就需要 256

① 见 http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report.20020128.pdf

② SFDS 只作为分布式检测的代理且判决门限可调.系统的整体性能对实际攻击中的具体速率并不敏感.

③ 现今多数路由器都提供 telnet 等服务供远程管理,所以同样存在被 SYN flood 攻击的可能.FDS 只检查路由器在两个方向上转发的流量,而 SFDS 检查每个网络接口(如百兆以太网线路卡)上的进出流量,这样一个叶节点路由器实际要包含 4 个 SFDS,故能额外检测针对路由器本身的 SYN flood 攻击.进一步,把 SFDS 以硬件模块的形式集成到二层/三层交换机的各个端口,就能准确检测到攻击源;而相比之下,FDS 只能揭示攻击源所在的子网.根据 DIDS 的策略设置,分析中心可直接向交换机下达指示,阻塞攻击源所在端口.

比特的存储单元.

3.3　分布式检测与中心判决

集成在路由器接口上的 SFDS 在本文提出的分布式检测系统中担任 agent 角色.分布式湮没检测系统的特点是分析中心能从来自 agent 的汇报中总体把握网络局势,即使个别 agent 出现误报或漏报,分析中心也能从全局的高度进行修正.对于 SYN flood,分布式湮没检测系统不仅能准确刻画出从攻击源到目标的有向路径,而且能识别出协同攻击等辅助形式.以图 4 为例,部署在路由器 A,B,C,E,F 上的 10 个 agent 在短时间内都向分析中心报告检测到的攻击行为,分析中心根据事先输入的网络拓扑结构判断出这是一次来自子网 a 和 b 向子网 e 内一台或多台主机发起的协同攻击,而子网 c 或 d 并未参与,攻击目标也不位于子网 g 内;另一方面,由于叶节点路由器 F 上 agent 所报告的事件得不到相关情况的支持,故被认为是虚警从而加以忽略①.

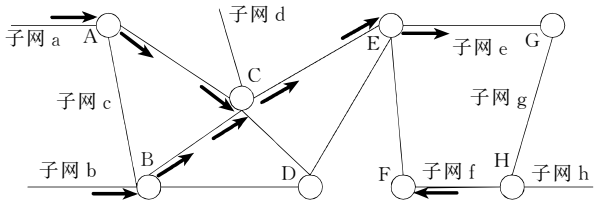


图 4　分布式湮没检测系统工作原理

分布式湮没检测系统由分析中心和遍布全网的检测代理组成,这些代理集成在路由器的所有网络接口上,并可以作为独立的电路模块执行面向硬件的 SFDS 检测算法.路由器本身不要求执行对称路由检查或进行网络源地址控制.整体系统不但能检测单点攻击,还能检测分布式的协同攻击,且中心判决具有较低的虚警率和漏警率.在网络安全形势不断严峻的今天,该方案不失为一种高性能的入侵检测系统.

4　结束语

本文分析了一种典型的 DoS 攻击——TCP 同步湮没,讨论了基于状态检测防火墙和基于服务器本身的对策,以及这些解决方案存在的缺点.FDS 是一种新的基于路由器的 SYN flood 检测手段,它以 TCP 连接的 SYN-FIN 匹配对为理论基础,通过对网络流量中的 TCP 控制分组进行统计分析来发现偏离常态的攻击行为.本文进一步提出了一种简化的便于硬件实现的 SFDS,并以其作为集成在路由器网络接口上的检测代理,提出了一种面向大规模网络的分布式湮没检测系统.

作者在一台安装 Mandrake Linux 8.2 的高档微机上完成了 SFDS 的软件实现(以百兆以太网卡作为路由器网络接口,基于 Linux 内核计数器实现 SFDS),其工作流程如图 5 所示.使用基于 libnet 编写的 SYN flood 程序作攻击测试,SFDS 取 $syn_{\min}=400$,$p=7$,$q=4$.当攻击速率大于每秒 20 个 SYN 包时系统即报警,且软件 SFDS 在每秒 2×10^5 个包(此速率已超百兆以太网理论上限)的考验下仍能正常工作,据此推断由硬件实现的 SFDS 将会有更好的检测性能.综上所述,本文提出的以 SFDS 为代理的分布式入侵检测系统具有较强的实用意义,对发展其它形式的拒绝服务攻击(尤其是分布式拒绝服务攻击)的检测系统亦有很高的研究价值.

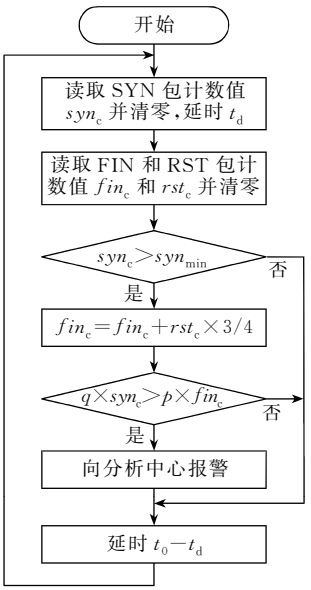


图 5　软件 SFDS 流程图

参　考　文　献

1　Stevens W. Unix Network Programming. Volume 1: Networking APIs: Sockets and XTI. 2nd Edition. Beijing: Tsinghua University Press, 1999(in Chinese)
(UNIX 网络编程(第 2 版)第 1 卷:套接口 API 和 X/Open 传输接口 API. 北京:清华大学出版社, 1999)

2　Noureldien N A, Osman I M. A stateful inspection module architecture. In: Proceedings of TENCON 2000, Kuala Lumpur, Malaysia, 2000.259～265

① 一种可能是路由器 F 自身受到来自子网 f 的攻击,见前一脚注.另外,路由器 G 也可能在受到远程攻击.

3 Postel J. Transmission Control Protocol. RFC 0793, 1981

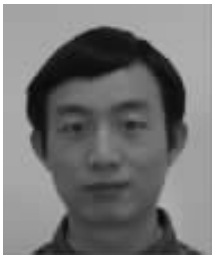
4 Li Jin-Sheng, Hong Pei-Lin. Network Technology of the Next Generation Internet. Beijing: People's Post & Telecom Press, 2001(in Chinese)
(李津生, 洪佩琳. 下一代 Internet 的网络技术. 北京: 人民邮电出版社, 2001)

5 Lemon J. Resisting SYN flood DoS attacks with a SYN cache. In: Proceedings of USENIX BSDCon 2002, San Francisco, California, USA, 2002. 89～98

6 Wang H, Zhang D, Shin K G. Detecting SYN flooding attacks. In: Proceedings of Infocom 2002, New York, USA, 2002. 1530～1539

7 Balasubramaniyan J S, Garcia-Fernandez J O, Isacoff D, Spafford E, Zamboni D. An architecture for intrusion detection using autonomous agents. In: Proceedings of Computer Security Applications Conference, Phoenix, Arizona, USA, 1998. 13～24

8 Tanenbaum A S. Computer Networks. 3rd Edition. Beijing: Tsinghua University Press, 1998(in Chinese)
(Tanenbaum A S. 计算机网络(第 3 版). 北京: 清华大学出版社, 1998)



ZHU Wen-Tao, born in 1979, Ph. D. candidate. His research interests include communication protocols and network security.

LI Jin-Sheng, born in 1937, professor and Ph. D. supervisor. His research interests include information communication and the next generation Internet.

HONG Pei-Lin, born in 1961, professor and Ph. D. supervisor. Her research interests include policy control and information security.