

DDoS 攻击检测综述^{*}

严 芬^{1,2}, 王佳佳¹, 赵金凤¹, 殷新春¹

(1. 扬州大学 信息工程学院 计算机科学与工程系, 江苏 扬州 225009; 2. 南京大学 计算机软件新技术国家重点实验室, 南京 210093)

摘 要: 结合 DDoS 攻击检测方法的最新研究情况, 对 DDoS 攻击检测技术进行系统分析和研究, 对不同检测方法进行比较, 讨论了当前该领域存在的问题及今后研究的方向。

关键词: 分布式拒绝服务; 攻击检测

中图分类号: TP393 文献标志码: A 文章编号: 1001-3695(2008)04-0966-04

Survey of detection on DDoS attack

YAN Fen^{1,2}, WANG Jia-jia¹, ZHAO Jin-feng¹, YIN Xin-chun¹

(1. Dept. of Computer Science & Engineering, College of Information Engineering, Yangzhou University, Yangzhou Jiangsu 225009, China;
2. State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210093, China)

Abstract: This paper combined with the latest research on DDoS attack detection methods, carried on system analysis and research to the DDoS attack detection technique, and compared different methods with each other. Finally, discussed the existing problems and the future direction in this field.
Key words: DDoS(distributed denial of service); attack detection

0 引言

DoS(denial of service, 拒绝服务)攻击是对网络服务有效性的一种破坏,使受害主机或网络不能及时接收并处理外界请求,或无法及时回应外界请求,从而不能提供给合法用户正常的服务,形成拒绝服务。DDoS攻击就是利用足够数量的傀儡机产生数目巨大的攻击数据包对一个或多个目标实施 DoS 攻击,耗尽受害端的资源,使受害主机丧失提供正常网络服务的能力。DDoS攻击已经是当前网络安全最严重的威胁之一,是对网络可用性的挑战。反弹攻击和 IP 源地址伪造技术的使用使得攻击更加难以察觉。就目前的网络状况而言,世界的每一个角落都有可能受到 DDoS 攻击,但是只要能够尽可能检测到这种攻击并且作出反应,损失就能够减到最小程度。因此,DDoS攻击检测方法的研究一直受到关注。

1 DDoS 攻击的研究现状

DDoS攻击的研究主要在预防、检测、响应追踪三个方面。

防范 DDoS攻击的第一道防线就是攻击预防。预防的目的是在攻击尚未发生时采取措施,阻止攻击者发起 DDoS 攻击进而危害网络。在 DDoS 攻击的预防研究方面,目前研究最多的还是提高 TCP/IP 协议的质量,如延长缓冲队列的长度和减少超时时间。目前,SYN cookie 技术已经讨论完善,并在 UNIX 系统中得到了应用。另外,加强事先防范以及采取更严密的措

施来加固系统也是必要的,主要的安全措施包括避免 FUD (fear, uncertainty and doubt)、加强中间环节的网络安全、加强与网络服务提供商的合作、优化路由及网络结构、优化对外提供服务的主机、保护主机不被入侵、审核系统规则、使用密码检查。

仅仅预防攻击是不够的,当攻击真的发生时需要进行响应。响应追踪的目的是消除或缓解攻击,尽量减小攻击对网络造成的危害。响应追踪研究又可以分为攻击发生时追踪和攻击发生后追踪。攻击发生后追踪的主要方法包括路由器产生 ICMP 追踪消息法、分组标记法、数据包日志记录法;攻击发生时追踪的主要方法包括基于 IPSec 的动态安全关联追踪法、链路测试法和逐跳追踪法等。

为了尽快响应攻击,就需要尽快地检测出攻击的存在。在检测研究方面,目前已有很多种方法以及不同的分类。本文将对 DDoS 攻击的检测进行详细的分析和系统的研究。

2 DDoS 攻击检测方法

- 2.1 按检测模式分类的检测方法
- 2.1.1 基于误用的 DDoS 检测

基于误用的 DDoS 攻击检测是指事先收集已有 DDoS 攻击的各种特征,然后将当前网络中数据包的特征和各种攻击特征相互比较,如果特征匹配则发现 DDoS 攻击。基于误用方法依赖于攻击特征的选取,一般用于检测利用漏洞型的 DDoS 攻

收稿日期: 2007-03-28; 修回日期: 2007-06-28 基金项目: 国家“863”计划资助项目(2003AA142010); 江苏省高技术研究计划资助项目(BG2004030)

作者简介: 严芬(1978-),女,江苏泰州人,博士研究生,主要研究方向为网络与信息安全(yufen@sina.com);王佳佳(1981-),女,硕士研究生,主要研究方向为网络安全;赵金凤(1982-),女,硕士研究生,主要研究方向为安全评估;殷新春(1962-),男,教授,博士,主要研究方向为密码学与信息安全、并行与分布式计算。

击。基于误用的 DDoS 检测主要是利用了特征匹配、模型推理、状态转换和专家系统的方法。

特征匹配主要是利用各种 DDoS 的特征进行检测。例如 Trinoo 攻击的特征有: a) 傀儡机在安装攻击工具时可能输出以下一行代码“rcp IP 地址: leaf /usr/sbin/rpc. listen”; b) 傀儡机的 contab 文件被修改, 因此只要时常检查 contab 文件就可以检测到主机是否被 Trinoo 攻击入侵; c) 特定端口开放, 常见的如 UDP 27655 端口等。只要将已知攻击的特征输入特征库就可以迅速地检测出攻击是否存在, 如 ping of death, teardrop 等。目前这方面已有较为成熟的产品, 如 Snort。

模型推理也是利用 DDoS 攻击的特征进行检测。将已知 DDoS 的各种特征作为基础建立一个攻击特征库, 对包含这些特征的行为进行监视, 并判断出网络中是否出现已知攻击。文献[1] 利用模型推理的原理和人工神经网络能够在有限、不完全和非线性的数据资源的条件下检测出攻击的特点, 提出了一种利用神经网络的分析特长来进行误用检测的方法。

状态转换将 DDoS 攻击看成被系统监测的一系列系统状态转换和相对应的条件, 攻击事件与系统状态不要求一一对应。文献[2] 中将 Petri 网用于入侵检测, 类似于利用状态转换分析图检测 DDoS 攻击的方法。

专家系统将专家关于 DDoS 攻击检测的知识转换成特征库中的特征与规则, 是知识检测中运用最多的一种方法。检测系统一旦认为网络中出现了与专家系统中攻击发生的条件相匹配的现象, 就判定发生了攻击。文献[3] 就是利用专家系统提出了一种新的检测方法。

2. 1. 2 基于异常的 DDoS 检测

基于异常的 DDoS 攻击检测是指通过监视系统审计记录上系统使用的异常情况, 可以检测出违反安全的事件。目前, 大多数的 DDoS 攻击检测都属于异常检测。基于异常的 DDoS 检测取决于检测模型的建立, 不同的模型对应着不同的检测方式, 主要包括统计检测、模式预测、人工智能检测、机器学习检测四种方法。

统计检测是应用最早也是应用最多的一种方法。当 DDoS 攻击发生时, 网络中会出现流量突增并超过正常工作时极限流量的现象。很多 DDoS 攻击检测手段是用统计的方法计算出网络正常工作时流量的阈值, 然后与当前网络流量进行比较, 如果当前网络流量超过了阈值则说明可能发生了 DDoS 攻击。文献[4] 利用变化点检测的方法在线、快速地检测出 DDoS 攻击的发生; 文献[5] 通过统计的方法用马尔可夫链模型表示网络正常行为的文件, 将其与当前网络行为比较来检测攻击; 文献[6] 采用熵和卡方检验的方法分别给出了一种检测攻击的模型; 文献[7] 基于大规模网络流量的自相似特性, 采用相似度的分析方法发现 DDoS 攻击时产生的流量异常; 文献[8] 提出了一种基于流连接密度(FCD) 的 DDoS 攻击检测方法。

模式预测就是通过分析攻击发生前必然发生的一些现象来判断是否发生了 DDoS 攻击。DDoS 攻击的发生不是毫无预兆的, 例如每次攻击发生前夕, 攻击者要解析受害者的主机名, 因此网络中就会出现大量的地址解析请求, 如果解析后发现同一个主机名称出现过多的话, 则可能发生攻击。还可以通过特

定攻击发生时会产生一些特定格式的数据包来判断攻击的类型, 例如 TFN2K 攻击时会发送一些数据段只包含文字和数字字符的数据包, 其他一些攻击则发送数据段只包含二进制字符串和 high-bit 字符的数据包。文献[9] 给出了基于时间的推理方法, 利用时间规则来识别网络正常模式特征, 并能够通过归纳学习产生规则集, 从而具有预测性。

基于人工智能的检测方法主要包括数据挖掘、人工神经网络和模糊理论等。DMDoS^[10] 就是利用数据挖掘中的关联算法和聚类算法分布处理数据来达到检测 DDoS 攻击的目的。人工神经网络检测不仅可以用于误用检测而且可以用于异常检测。在异常检测中主要是采用正常的网络数据来训练神经网络模型, 经过适当训练后, 该模型即可通过本身的性质辨识出网络是否受到了攻击。文献[11] 利用小波神经网络结合遗传算法设计了一种检测 DDoS 的工具; 文献[12] 提出了基于模糊理论的检测方法, 该方法要求并行检测网络中的正常信号和异常信号, 并用模糊理论对检测结果进行计算, 再通过与动态阈值的比较判断 DDoS 攻击对当前网络危害的程度。

使用机器学习的方法实现 DDoS 攻击的检测也是可行的。文献[13] 提出了基于机器学习的入侵检测系统, 将遗传算法和贝叶斯分类算法结合使用, 使得检测规则可以自动生成。

2. 1. 3 混合模式 DDoS 检测

混合模式 DDoS 攻击检测是将误用 DDoS 攻击检测和异常 DDoS 攻击检测两种方式混合使用。通常使用数据挖掘的方法, 由异常检测发现攻击, 从发现的攻击中摘录特征放入误用模式特征库中, 再利用误用检测的方法来检测 DDoS 攻击。但实际效果根据具体情况的不同也有差异。

2. 1. 4 分析

基于误用的 DDoS 检测是建立负面行为模型, 误报率低, 但存在检测率不高的问题。误用检测模型往往依赖于具体的环境, 可移植性和可扩展性较差。由于必须将所有已知的攻击规则输入知识库, 模型的维护开销较大, 需要不断更新知识库且只能检测已知攻击。另外, 对攻击特征的提取也存在一定的困难。

基于异常的 DDoS 检测是建立正面行为模型, 检测率很高, 但误报率也很高。异常检测模型最大的优点是可以检测出未知攻击。

现有研究结果说明了没有一种 DDoS 攻击检测方式对于所有的 DDoS 攻击都有效。基于误用的 DDoS 检测必须与基于异常的 DDoS 检测联合使用才能达到理想的效果。混合模式 DDoS 检测能够对误用检测和异常检测的缺陷产生互补作用, 达到高检测率的同时也能保持低误报率。因此, 几乎目前所有的 DDoS 攻击检测产品都包含有误用检测模块和异常检测模块。

2. 2 按算法部署位置分类的检测方法

2. 2. 1 源端检测

源端 DDoS 攻击检测指的是将检测算法布置在发出攻击数据包的主机所处网络的边界路由器上。将 DDoS 攻击检测系统部署在源端, 可以使得攻击数据流在进入网络之前被阻止。文献[14] 通过在整个源端网络中发现进出的数据流与正常网络模型的异常来检测 DDoS 攻击; 文献[15] 采用了基于历

史记录的源 IP 地址过滤的方法,在源端网络边界路由器上过滤以较高频率出现的 IP 地址的数据包,阻止内部可能的攻击源;文献[16]通过在源端网络边界路由器上部署出口过滤机制来过滤源 IP 地址被伪造的攻击报文;在文献[17,18]提出的攻击源端检测 DDoS 攻击的方法中,均用到了基于变化点的快速检测方法。

2.2.2 中间网络检测

中间网络 DDoS 攻击检测是指将攻击检测算法部署在整个网络上,包括路由器、交换机或其他网络设备。

在中间网络进行检测,通常是在核心路由器上部署分布式的 DDoS 防御检测系统。文献[8]首先在核心路由器上以时间间隔 t 对网络流 F 进行采样;然后分别计算出(源地址、目的地址、目的端口)相同的数据包的集合,得到以上三元组相同的数据包 a 随时间变化的序列;当时间间隔很大时计算该序列的自相关系数 $r_k = \frac{\sum_{i=1}^{N-k} (a_i - \bar{a})(a_{i+k} - \bar{a})}{\sqrt{\sum_{i=1}^N (a_i - \bar{a})^2}}$ 。其中: $a_i(i=1,2,\dots,k)$ 为 k 个 t 时间内 a 的序列; \bar{a} 为 a 的数学期望; r_k 即为自相关系数。如果自相关系数不为 0,则说明发生了 DDoS 攻击。文献[19]提出了在边界路由器检测 SYN flooding 攻击的方法。

2.2.3 目的端检测

目的端 DDoS 攻击检测是指将攻击检测算法部署在被攻击的主机和相关网络设备上。目前应用得最多的攻击检测都是在目的端(即受害端)进行的。

文献[20]提出了一种 HCF 方法,利用数据包从源端到达目的端所需要的跳数是不可改变的,将网络中特定服务器作为目的端,建立一张源地址和跳数相对应的表。通过查表可以区别出正常数据包和源地址经过伪造的数据包,其理论依据是源地址经过伪造的数据包和源地址正常的数据包报头中的 TTL 值是不同的。文献[21]提出了使用 SYN cache 和 SYN cookies 来抵抗 SYN flooding 攻击的方法,用 SYN cache 和 SYN cookies 代替目的主机建立 SYN 连接,在连接完成后再转交给目的主机。这样可以避免攻击者利用三次握手原理进行 SYN 攻击;文献[22]提出了往返时间级拥塞窗口算法的连续动态模型。使用拥塞控制算法根据目的端网络拥塞反馈信号估计可用带宽,分组速率能快速收敛并能长期保持在可用带宽附近。

2.2.4 分析

源端检测是最为理想的一种方法,能够在受害端受到攻击之前阻止攻击的发生,将攻击对网络的威胁降到最低,但对检测系统的要求较高,源地址被伪造的数据包很容易在源端检测出来。但是要求所有的网络服务提供商都安装源端检测算法显然不切实际,而且源端攻击包流量小,不易检测。

中间网络检测比源端检测具有更好的可实施性和更低的覆盖要求。但也存在边界网关的修改、路由器的负载、缺乏网间合作等问题。

目的端 DDoS 攻击检测是最容易的,因为目的端的攻击数据流量最大,并且最注重于对 DDoS 的防范。缺点是如果上游网络链接被阻塞的话,目的端不管做什么也于事无补。

2.3 其他检测方法和相关研究

随着无线网络的发展,出现了专门针对无线网络的 DDoS

攻击。无线网络和有线网络的环境是不同的,检测的手段也不同。特别强调服务质量的无线网络如何检测和应对 DDoS 分布式拒绝服务攻击成为当前的一个敏感点。文献[23]对无线网络中 DDoS 攻击进行了分析和分类,并从 RTS/CTS 包的检测、单个用户访问的频率、重传时间和响应阶段等方面用标记的方式进行检测。

随着网络安全技术的发展,产生了主动检测 DDoS 攻击的技术,如利用蜜罐、蜜网进行 DDoS 攻击特征提取,帮助进行 DDoS 攻击检测。蜜罐是故意接受攻击的目标,进出蜜罐的几乎全是攻击流量,因此,察觉攻击和发现未知攻击的特征就会容易很多。蜜网是指另外采用了技术的蜜罐,能够以合理的方式记录下黑客的行动,同时尽量减小或排除对因特网上其他系统造成的风险。文献[24]利用虚拟蜜罐技术提出了一种框架,可以应用于 DDoS 检测技术。还可以使用安全协议进行加密或认证、检测并抵御 DDoS 攻击。文献[25]认为 DDoS 防御的重点应该是攻击发生后如何保证正常服务的性能和质量。他们提出一种基于信息安全服务建设的思想,利用 IPSec 建立安全通道,用安全通道两端的访问控制列表区分开合法用户数据流和攻击流,过滤掉攻击用户的非法数据流。

DDoS 的根本解决办法是在整个 Internet 中建立一个全球范围的防御系统,因此一些检测方法在源端、中间网络和目的端均部署了防御点。

2.4 DDoS 攻击检测系统的体系结构

DDoS 攻击检测系统的体系结构大致可以分为三种:基于主机(host-based)型、基于网络(network-based)型和基于移动代理(agent-based)型。基于主机型的 DDoS 攻击检测系统是指该检测系统能够在主机上运行,如文献[22]提出了一种可以配置在主机上的拥塞控制算法,能够反馈主机可用带宽。真正的 DDoS 攻击发生时,受害主机自身的性能、处理能力和各方面的开销都很大,在这种超负荷的情况下受害主机再运行 DDoS 攻击检测系统有一定的困难。因此,仅依靠主机型的检测是不够的。基于网络型的 DDoS 攻击检测系统起到一定的作用,如文献[8]通过在网络中对流量状态的比较判断攻击。随着 DDoS 攻击的复杂化和大型化,检测系统也需要分布式相互协作,要求具有自适应性、可扩展性等,因此出现了基于移动代理型的 DDoS 攻击检测系统,如文献[26]就是利用若干个相互独立的 agent 分布进行检测,然后将检测结果发送到检测中心。

3 DDoS 攻击检测方法的分析

检测率、误报率、漏报率、检测攻击需要的时间、算法的复杂程度、建立检测模型的难易程度和检测模型的维护开销都是评价 DDoS 攻击检测系统的因素。本文选择了这七项技术指标对几种主要的 DDoS 攻击检测算法进行了比较,如表 1 所示。

除了检测算法本身的性能外,DDoS 攻击检测算法部署的位置对于检测的效率也有很大的影响。表 2 从检测率、误报率、漏报率、算法部署的难易程度,以及算法部署在相应位置时所需要花费的路由器开销、网络开销和管理开销这七个方面对算法部署的位置进行了分析比较。

表 1 DDoS 攻击检测技术比较

| DDoS 检测技术 | 指 标 | | | | | | |
|--------------|-----|-----|-----|------|-------|------|------|
| | 检测率 | 误报率 | 漏报率 | 收敛时间 | 算法复杂度 | 建模难易 | 维护开销 |
| 特征匹配 | 相当高 | 相当低 | 高 | 实时 | 低 | 较易 | 较大 |
| 模型推理 | 较高 | 较低 | 较高 | 较快 | 较高 | 难 | 较大 |
| 状态转换 | 较低 | 较低 | 较高 | 快 | 较低 | 较易 | 较小 |
| 专家系统 | 较低 | 较低 | 较高 | 较慢 | 较高 | 难 | 较大 |
| 统计 | 较高 | 低 | 较低 | 较快 | 较低 | 较易 | 较小 |
| 模式预测 | 较高 | 较低 | 低 | 较慢 | 高 | 较难 | 较小 |
| 系统调用 | 较低 | 相当低 | 高 | 快 | 低 | 较易 | 较小 |
| 数据挖掘 | 较高 | 较低 | 较低 | 较慢 | 较高 | 较易 | 较大 |
| 神经网络 | 较高 | 较低 | 较低 | 较快 | 较低 | 较易 | 较小 |
| 模糊理论 | 较高 | 较低 | 较低 | 快 | 低 | 较难 | 较小 |
| 机器学习 | 较低 | 低 | 较高 | 快 | 较低 | 较难 | 较小 |

表 2 DDoS 攻击检测算法部署位置比较

| 部署 位置 | 指 标 | | | | | | |
|----------|-----|-----|-----|------|-----------|-------------|------|
| | 检测率 | 误报率 | 漏报率 | 部署难易 | 路由器 开销 | 正常报文 存活率 | 管理开销 |
| 源端 | 较低 | 较低 | 较高 | 难 | 较小 | 大 | 较小 |
| 中间网络 | 较高 | 较低 | 较低 | 难 | 较小 | 较大 | 大 |
| 目的端 | 高 | 较高 | 低 | 易 | 大 | 小 | 较小 |

4 结束语

为了避免 DDoS 造成灾难性的后果, 尽早识别攻击并采取相应的对策是十分重要的。DDoS 攻击检测系统的主要作用在于: a) 监视并检测网络安全状况; b) 识别 DDoS 攻击行为和攻击者; c) 为以后防御 DDoS 攻击提供重要的信息。因此, DDoS 攻击检测是必要的。

本文系统地研究了现有 DDoS 攻击检测的方法, 并从不同的方面对它们进行了分析和比较。随着网络的发展, DDoS 攻击也日益呈现出复杂性、多变性、范围广、追踪难等特征。但是每一种 DDoS 攻击检测方法只在有限的工作条件和处理范围内有作用, 缺乏通用高效的检测方案。今后要做的工作主要包括: a) 提高源端检测的效率, 降低源端检测的时空复杂度; b) 掌握网络中可控网络设备的数据传输情况, 在攻击尚未成熟前准确预警; c) 在攻击被检测出来后及时准确地过滤攻击包。

此外, 当前检测系统所面临的高效检测、实时监测、高速网络中的攻击检测、特征模式的确认、攻击标准化描述语言等问题都有待于进一步研究。

参考文献:

[1] ANNADY J. Artificial neural networks for misuse detection[C] // Proc of National Information System Security Conference. Arlington: [s. n.], 1998: 443- 456.

[2] 严芬, 黄皓, 殷新春. 基于 CTPN 的复合攻击检测方法研究[J]. 计算机学报, 2006, 29(8) : 1383-1391.

[3] TAMARU A, GILHAM F, JAGANNATHAN R, *et al.* A real-time intrusion detection expert system(IDES) [R]. Menlo Park, CA: Computer Science Laboratory, 1992.

[4] 何慧, 张宏莉, 张伟哲, 等. 一种基于相似度的 DDoS 攻击检测方法[J]. 通信学报, 2004, 25(7) : 176-184.

[5] YE Nong. A markov chain model of temporal behavior for anomaly de-tection[C] //Proc of IEEE Workshop on Information Assurance and Security United States Military Academy. New York: West Point, 2000.

[6] FEINSTEIN L, SCHNACKENBERG D, BALUPARI R, *et al.* Statis-tical approaches to DDoS attack detection and response[C] //Proc of DARPA Information Survivability Conf and Exposition. Washington

DC: [s. n.], 2003.

[7] 郝志宇, 云晓春, 张宏莉, 等. 基于相似度的 DDoS 异常检测系统[J]. 计算机工程与应用, 2004, 40(35) : 122-124, 225.

[8] 孙钦东, 张德运, 高鹏. 基于时间序列分析的分布式拒绝服务攻击检测[J]. 计算机学报, 2005, 28(5) : 767- 773.

[9] VIGNA G, KEMMERER R A. NetSTAT: a network-based intrusion detection system[J]. Journal of Computer Security, 1999, 7(1) : 37- 71.

[10] 高能, 冯登国, 向继. 一种基于数据挖掘的拒绝服务攻击检测技术[J]. 计算机学报, 2006, 29(6) : 944- 951.

[11] 蒋平. 基于小波神经网络的 DDoS 攻击检测及防范[J]. 计算机工程与应用, 2006, 42(3) : 116-119.

[12] 张彦波, 李明. 基于模糊理论的分布式拒绝服务攻击检测[J]. 计-算机应用, 2005, 25(12) : 2751- 2752.

[13] 王旭仁, 许椿生. 基于机器学习的入侵检测系统研究[J]. 计算机工程, 2006, 32(14) : 107-108, 153.

[14] MIRKOVIC J, PIRER G. Attacking DDoS at the source[C] //Proc of the 10th IEEE International Conference on Network Procotols. Paris: [s. n.], 2002: 312- 321.

[15] TAO Peng, LECKIE C, RAMAMOHANARAO K. Protection from distributed denial of service attacks using history-based IP filtering [C] //Proc of IEEE Intemational Conference on Communications. Anchorage: [s. n.], 2003: 482- 486.

[16] SANS Institute. Egress filtering v0. 2[EB/ OL]. (2000-02). <http://www.sans.org/y2k/egress.htm>.

[17] 陈伟, 何炎祥, 彭文灵, 等. 一种轻量级的拒绝服务攻击检测方法[J]. 计算机学报, 2006, 29(8) : 1392-1400.

[18] 林白, 李鸥, 赵桦. 基于源端网络的 SYN flooding 攻击双粒度检测[J]. 计算机工程, 2005, 31(10) : 132-134.

[19] WANG H, ZHANG D, SHIN K G. Detecting SYN flooding attacks [C] //Proc of Annual Joint Conference of the IEEE Computer Society and Communications Society (INFOCOM). New York: [s. n.], 2002: 1530-1539.

[20] JIN Cheng, WANG Hai-ning, SHIN K G. Hop-count filtering: an ef-fective defense against spoofed DDoS traffic[C] //Proc of the 10th ACM Conference on Computer and Communications Security. New York: ACM Press, 2003: 30- 41.

[21] LEMON J. Resisting SYN flood DoS attacks with a SYN cache[C] // Proc of BSD Conference. Berkeley: USENIX Association, 2002: 13- 20.

[22] 邵立松, 张鹤颖, 窦文华. 基于窗口的端到端拥塞控制: 网络稳定性与效率[J]. 计算机学报, 2006, 29(3) : 353- 360.

[23] REN Wei, JIN Hai, LIU Teng-hong. Congestion targeted reduction of quality of service DDoS attacking and defense scheme in mobile Ad hoc networks[C] //Proc of the 7th IEEE International Symposium on Multimedia. Washington DC: [s. n.], 2005.

[24] PROVOS N. A virtual honeypot framework[C] //Proc of the 13th USENIX Security Symposium. Berkeley: USENIX Association, 2004.

[25] CHEN H G, CHOW R. A new perspective in defending against DDoS [C] //Proc of the 10th IEEE Int 'l Workshop on Future Trends of Distributed Computing Systems. Los Alamitos: [s. n.], 2004: 186- 190.

[26] FOO S Y, ARRADONDO M. Mobile agents for computer intrusion detection[C] //Proc of the 36th Southeastern Symposium on System Theory. Atlanta: [s. n.], 2004: 517- 521.