信息安全技术丛书

基于信号处理的低速率拒绝服务攻击的检测技术

吴志军　岳　猛　著

科学出版社

信息安全技术丛书

基于信号处理的低速率拒绝服务攻击的检测技术

吴志军　岳　猛　著

科学出版社

北　京

内 容 简 介

针对低速率拒绝服务（LDoS）攻击具有平均流量低（占用较小的共享带宽）的特点，本书在时域采用数据包统计的方法分析 LDoS 攻击流量的特性，在频域采用频谱分布统计的方法研究 LDoS 攻击的特征，采用经典的数字信号处理技术对网络流量数据进行采样和处理，完成 LDoS 攻击的特性分析、特征检测和流量过滤等关键技术的研究。全书共 9 章，包括：（1）LDoS 攻击的时域流量建模；（2）LDoS 攻击性能的研究；（3）基于互相关的 LDDoS 攻击时间同步和流量汇聚方法；（4）LDoS 攻击的时频域特征及其检测方法；（5）基于卡尔曼滤波一步预测技术的 LDoS 攻击检测方法；（6）基于 Duffing 振子的 LDoS 攻击检测方法；（7）基于漏值多点数字平均的 LDoS 攻击检测方法；（8）基于信号互相关的 LDoS 攻击检测方法；（9）基于数字滤波器的 LDoS 攻击过滤方法。

全书内容由浅入深，涵盖了 LDoS 的知识，为读者更深入地掌握 LDoS 检测和防御技术提供了参考。本书可作为网络安全研究领域科研人员和网络设计工程人员的参考书。

图书在版编目 (CIP) 数据

基于信号处理的低速率拒绝服务攻击的检测技术 / 吴志军，岳猛著. —北京：科学出版社，2015.6
（信息安全技术丛书）
ISBN 978-7-03-044750-0

Ⅰ. ①基… Ⅱ. ①吴…②岳… Ⅲ. ①计算机网络－安全技术
Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2015)第 124341 号

责任编辑：陈 静 王迎春 / 责任校对：郭瑞芝
责任印制：张 倩 / 封面设计：迷底书装

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

三河市骏走印刷有限公司 印刷

科学出版社发行 各地新华书店经销

*

2015 年 6 月第 一 版 开本：720×1 000 1/16
2015 年 6 月第一次印刷 印张：11 1/4
字数：224 000

定价：58.00 元

（如有印装质量问题，我社负责调换）

序

长期以来，分布式拒绝服务（distributed denial of service，DDoS）攻击是大规模网络和网络数据中心（internet data center，IDC）的最大安全威胁之一。对于在线企业，特别是电信运营商数据中心网络来说，它的出现无疑是一场灾难。由 DDoS 攻击给电信运营商等造成的经济损失每年高达数百亿美元，而且造成的危害越来越大。但到目前为止，国内外尚未研究出一种有效的方法来抵御 DDoS 攻击，传统的防护方法有心无力。因此，如何有效地防御 DDoS 攻击，保护目标（主机或者服务器）不被攻击是信息安全领域研究的一个热点。

目前，大数据和云计算的发展面临许多关键性问题，其中最关键的问题就是信息安全。随着大数据和云计算的不断普及，其面临的信息安全问题日趋严重，已成为制约其发展的重要因素。信息化的发展历程表明信息系统的建设和发展之后必须经历信息安全保障的过程，信息技术的重大变革将直接影响信息安全领域的发展进程。在大数据和云计算面临的安全挑战中，承载平台遭受攻击的问题非常突出。大数据和云计算平台由于其用户、信息资源高度集中，容易成为黑客攻击的目标，由 DDoS 攻击造成的后果和破坏性将明显超过传统的企业网应用环境。随着越来越多的公司使用虚拟化数据中心和云服务，企业基础设施中的新弱点也逐渐暴露出来。与此同时，DDoS 攻击正在从数据暴力泛滥方式转向更有针对性的方式——向信息系统或网络应用平台基础设施发起攻击。因此，研究有效的检测和防御低速率拒绝服务（low-rate DoS，LDoS）攻击的方法具有重要意义。

吴志军教授长期从事 DDoS 攻击的检测和防御研究，在大规模网络安全防护方面进行了大量理论研究和应用实践，掌握了网络防护的系统理论和技术，积累了丰富的基础知识和实际经验。该书深入浅出地介绍了 DDoS 攻击的原理和特点，讲解了检测和防御 LDoS 攻击的基础知识，并结合具体方法说明在实际网络中检测和防御 DDoS 攻击的方法。该书内容是吴志军教授带领的课题组十几年的研究成果，部分思想已经在国内外著名期刊上发表，得到了国内外专家的认可和好评，对相关网络管理单位开展防御 DDoS 攻击的工作具有很好的借鉴意义。

网络防御和攻击是一场持久的博弈。随着大数据时代的到来以及云计算的普及，网络攻防也进入一个新的时期，应不断丰富网络安全的理论和实践。因此，防御 DDoS 攻击是一项长期而艰巨的任务。希望该书能够使广大读者从中受益，并为读者努力探索、刻苦研究检测和防御 DDoS 攻击的新方法提供帮助。

杨义先

2015 年 1 月

前　言

目前，网络安全已经成为国际上的焦点，针对国家政府机关、企事业单位和重要信息部门的攻击事件层出不穷。“棱镜门”事件的主角斯诺登爆料，美国经常入侵和攻击中国的主干网络，包括入侵清华大学主干网，网络安全形势日益严峻。另外，以营利为目的的网络攻击者形成了一条“黑色产业链”，有计划地攻击特定目标获取巨额经济利益，网络进入了软绑架勒索时代。国家计算机网络应急技术处理协调中心的一份研究报告显示，黑客攻击已经形成了一条隐蔽的产业链，目前我国网络安全黑色产业链产值已超过 2.38 亿元，造成的损失超过 76 亿元，已经成为不可忽视的地下经济力量。

根据美国计算机安全研究所（computer security institute，CSI）和美国联邦调查局（federal bureau of investigation，FBI）的调查结果，网络攻击采用的主要手段是分布式拒绝服务（DDoS）攻击。由于 DDoS 攻击的行为自然、单一，攻击渠道正常、合法，所以 DDoS 攻击十分难以防范和追踪。根据 CSI/FBI 每年的统计结果可知，1998 年开始出现 DDoS 攻击，2003 年达到顶峰，之后进入黑色产业链时代。全球许多著名的网站（如 Yahoo、CNN、Buy、eBay、亚马逊、微软、网易、百度、谷歌等）均为受害者。统计表明，历史上 DDoS 攻击一年造成的最高损失达到 65643300 美元。

随着 DDoS 攻击技术的不断更新，新型 DDoS 攻击方式层出不穷。近年来，出现了一种新型的拒绝服务攻击，称为低速率分布式拒绝服务（low-rate DDoS，LDDoS）/低速率拒绝服务（LDoS）攻击。LDoS 攻击的平均流量很小，只有正常流量的 10%～20%（形象地称为地鼠攻击），它利用传输控制协议（transmission control protocol，TCP）超时重传机制的漏洞，周期性地发送短脉冲（又被称为脉冲攻击），使得攻击流可以周期性地占用网络带宽，导致合法的 TCP 流总是认为网络的负担很重，造成所有受其影响的 TCP 流进入超时重传状态，最终使得受害主机的吞吐量大幅度降低（也被称为降质（reduction of quality，RoQ）攻击）。LDoS 攻击具有流量小、隐蔽性强的特点，传统 DDoS 攻击的检测机制对它无能为力，可使受害机器长时间遭受攻击而不被察觉。LDoS 攻击所表现出的破坏性对大规模网络具有极大的危害性。目前，入侵检测手段采用的方法为时序机制，即在设定的检测时间内对攻击包的个数进行统计，根据统计流量的大小判定是否存在攻击。由于 LDoS 攻击脉冲的持续时间很短，远小于现有检测方法设定的平均检测时间，而且 LDoS 攻击的平均流量很小，因此，现有检测手段对于 LDoS 攻击无能为力，原因是平均共享的带宽并不是非常大。在分布式情况下，成倍的傀儡机发起攻击可以通过降低最高速率或者延长攻击周期来进一步降低单个通信量的速率，导致检测更加困难。

1. 目标

本书针对 LDoS 攻击具有平均流量低（占用较小的共享带宽）的特点，在时域采用数据包统计的方法分析 LDoS 攻击流量的特性；在频域采用频谱分布统计的方法研究 LDoS 攻击的特征，采用经典的数字信号处理技术将网络流量数据当成信号采样和处理，进行 LDoS 攻击的特征提取、攻击检测和流量过滤等关键技术的研究。

LDoS 攻击具有隐蔽性强和破坏力大的特点，因此成为黑色产业链经营者获取经济利益的主要手段之一，社会影响极其恶劣。本书的研究成果有助于阻断黑色产业链经营者利用 LDoS 攻击作为营利手段，从而减少国家的经济损失并降低社会负面影响。

2. 内容安排

全书共 9 章，内容如下。

第 1 章从 LDoS 攻击的漏洞利用机制开始，研究了 LDoS 攻击的产生原理，建立了 LDoS 攻击的时域流量模型。

第 2 章研究 LDoS 攻击的性能，在搭建的真实网络实验环境中针对 Web 和 FTP 两种情况进行了网络吞吐量和刷新延迟的研究。

第 3 章研究基于互相关的 LDDoS 时间同步和流量汇聚的方法。采用互相关算法，根据 LDDoS 攻击脉冲之间的时序关系，确定最优的攻击方式。

第 4 章研究 LDoS 攻击的时频域特征及其检测方法，采用缓存队列占有率统计的方法来提取 LDoS 攻击的特征；采用时间窗统计的手段，对到达的数据分组进行统计分析，准确判断 LDoS 攻击脉冲的突变时刻，即判定某个时刻是否有流量突变出现。

第 5 章研究利用卡尔曼滤波一步预测技术，针对建立的 LDoS 攻击流量矩阵模型采用卡尔曼滤波算法进行预测和估算，基于上一状态预测现在的状态。

第 6 章研究基于混沌理论，采用 Duffing 振子利用混沌相位的变化从正常网络流量中检测 LDoS 攻击流量。

第 7 章研究利用小信号检测理论，采用漏值多点数字平均方法检测 LDoS 攻击，并估计其攻击周期和脉宽。

第 8 章研究基于信号互相关的 LDoS 攻击检测方法，采用基于循环卷积的互相关算法来计算攻击脉冲经过不同传输通道在特定的攻击目标端的精确时间，利用无周期单脉冲预测技术估计 LDoS 攻击的周期参数，提取 LDoS 攻击的脉冲持续时间的相关性特征。

第 9 章研究在频域设计数字滤波器，根据正常 TCP 和 LDoS 攻击在频域中的频谱分布，滤除 LDoS 攻击流量的频谱，实现 LDoS 攻击流量的过滤。

3. 本书特色

本书主要有以下两个特点。

（1）将信号处理理论和技术应用到网络流量数据处理中。在时域进行 LDoS 攻击流量的统计分析，在频域进行 LDoS 攻击流量的处理。

（2）在频域进行 LDoS 攻击检测和过滤。采用滤波器预测技术、混沌理论和小信号处理理论检测 LDoS 攻击，以及采用滤波器技术在频域过滤 LDoS 攻击流量。

本书的主要创新点如下。

（1）提出基于相关的 LDoS 攻击时间同步和流量汇聚的方法。

（2）提出基于卡尔曼滤波的 LDoS 攻击检测方法。

（3）提出基于小信号理论采用基于漏值多点数字平均技术的 LDoS 攻击检测方法。

（4）提出基于混沌 Duffing 振子的 LDoS 攻击的检测方法。

（5）提出基于数字滤波器的 LDoS 攻击流量的过滤方法。

4. 阅读建议

建议在阅读本书时先从拒绝服务（denial of service，DoS）攻击的概念和原理入手，逐步掌握 DDoS 攻击的特点；然后熟悉在时域和频域对网络流量分析的基本方法，揭示网络流量在攻击出现时的异常；最后通过网络流量分析，采用各种信号处理方法进行攻击检测，进而采取过滤措施抵御攻击。

本书是中国民航大学电子信息工程学院航空电信网及信息安全研究实验室的教师和研究生多年的研究和开发成果。本书内容是在师生共同发表的学术论文、撰写的技术报告和申请的发明专利的基础上整理而成的。其中，吴志军作为主编负责全书的内容安排和结构设计，并编写第 1 章、第 2 章、第 4 章、第 7 章、第 9 章内容；岳猛负责编写第 3 章、第 5 章、第 6 章和第 8 章内容。另外，参与本书研究工作的人员包括张东、刘颖、裴宝松、刘星辰、谢科、李光、张力园和闫长灿等，张力园和闫长灿在本书的整理、编辑和校正等方面做了大量艰苦的工作，在此对他们表示衷心的感谢。王彩云、沈丹丹、尹盼盼、沙永鹏等为本书的校对付出了时间和劳动，在此致谢。本书的研究得到了北京邮电大学信息安全中心的杨义先教授和武汉大学计算机学院的何炎祥教授的指正，在此表示衷心的感谢。

本书的撰写得到了国家自然科学基金面上项目（No.61170328，No.U1333116）、天津市应用基础与前沿技术研究计划（自然科学基金重点项目，No.12JCZDJC20900）、2013 年民航科技引导资金项目（No.MHRD20130217）、中央高校基本科研业务费（No.3122013P007，No.3122013D007，No.3122013D003），以及中国民航大学科研建设平台项目（2014—2016）的资助，在此表示衷心的感谢。

本书是一本针对低速率拒绝服务攻击的研究著作，对研究大规模网络抵御 DDoS 攻击的技术人员具有一定的借鉴意义和参考价值。本书可作为网络安全研究领域科研

人员和网络设计工程人员的参考书。全书内容由浅入深，涵盖了大型网络安全管理和设计人员需要掌握的知识，也为读者更深入地掌握 DDoS 检测和防御技术，从事网络安全保护研究方面的工作提供了参考。

由于作者水平有限，书中难免存在不足之处，恳请广大读者批评指正。

作　者

2015 年 1 月

目　录

第 1 章　低速率拒绝服务攻击原理与模型

长期以来，拒绝服务（denial of service，DoS）攻击是大型网络主要的安全威胁之一，造成了巨大的经济损失[1]。随着 DoS 攻击技术的演变，出现了一种新型的 DoS 攻击，称为低速率拒绝服务（low-rate denial of service，LDoS）攻击[2]。

2001 年，在 Internet2 Abilene 骨干网络上第一次检测到 LDoS 攻击方式[3]，它是一种周期性的脉冲（pulse）攻击。由于该攻击在时域（time domain）上平均速率很低，具有攻击流量占用带宽小的特点，所以 Kuzmanovic 和 Knightly[4]形象地将其称为“地鼠”拒绝服务（shrew DoS）攻击；而该攻击的信号形式为周期性脉冲，Iwanari 等[5]又将其称为“脉冲”攻击；LDoS 攻击的最终目的是降低被攻击目标的服务质量，Guirguis 等[6]将其称为“降质”（reduction of quality，RoQ）攻击。

LDoS 与传统的泛洪拒绝服务（flood denial of service，FDoS）攻击不同，LDoS 攻击以降低系统的服务质量为目的，攻击者不需要长期维持高速率的攻击流，而是利用网络协议或者应用服务自适应机制的漏洞，周期性地发送脉冲式的攻击流。由于攻击流只在特定的短时间内发送，而同一周期其他时间段内不发送任何流量，所以 LDoS 攻击的平均攻击速率比较低，甚至低于合法用户的平均流量[7]。LDoS 攻击可以被认为是对传统 DoS 攻击的改进形式，这种低速率的特性使其更加隐蔽，不容易被检测和防范[8]。

1.1　引　　言

随着互联网技术及应用的飞速发展与普及，我国网民数量急剧增长，《第 34 次中国互联网络发展状况统计报告》[9]显示，截至 2014 年 6 月，中国网民规模达 6.32 亿人，较 2013 年年底增加了 1442 万人，互联网普及率为 46.9%。然而随之而来的网络安全形势日益严峻，病毒、木马、黑客频繁行动，频频发生的网络恶意攻击导致财产损失的情况让众多互联网用户对网络信息安全缺乏信心，这一切无疑对正在迅速发展的互联网产业产生了严重影响。

1.1.1　背景

经济利益已经成为攻击、病毒等恶意程序制造者最大的驱动力。恶意程序制造者已经不再以炫耀自己的技术为目的，也不再“单打独斗”，而是结成了团伙，进而形成一整条黑色产业链。从事此类恶意行为的成本很低，收益很大，但调查处理的成本很高，这是其愈演愈烈的根本原因之一[10]。

DoS 攻击利用多台已经被攻击者所控制的机器对某一台单机发起攻击，在带宽有限的情况下，被攻击的主机很容易失去反应能力。作为一种分布、协作的大规模攻击方式，DoS 攻击主要瞄准比较大的站点，如商业公司、搜索引擎和政府部门的站点。2000 年以来，全球许多著名的网站，如 Yahoo、CNN、Buy、eBay 等，包括新浪网（中国）相继遭到 DoS 攻击；俄罗斯黑手党在敲诈某银行和赌场未遂后，实施 DoS 攻击导致一家中型电信运营商全部掉线。Arbor Networks 宣告 2014 年上半年是容量耗尽、DoS 攻击最频繁的时期。因此，DoS 攻击被认为是互联网服务提供商（Internet Service Provider，ISP）目前最大的运营危害[11]。近来国内安全站点黑客基地也因受到攻击而经常不能提供 Web 服务。2004 年 10 月 17 日，国内某著名公司因遭受低速洪水攻击而使得大多数用户不能登录其即时聊天系统；2006 年 10 月 17 日，国内多家网站受到 LDoS 攻击。LDoS 攻击包穿透电信的多层路由过滤和各个公司的入侵检测系统，直达服务器，造成多家国内大型网站停止服务[2, 12]。严峻的网络安全形势说明网络进入了软绑架勒索时代，DoS 会造成严重的经济损失和恶劣的社会影响，所以检测和防御 DoS 攻击刻不容缓。

DoS 攻击犯罪有两个明显不同于传统犯罪的特点：①犯罪现场的不确定性，带来了电子证据的法律效力及有关损失的评估难题；②立法执法跟不上形势，很难了解犯罪行为造成的破坏价值。如果这种攻击被用于攻击基础网络，那么带来的损失不可估量[2]。

LDoS 是利用 TCP 拥塞控制机制或路由器主动队列管理机制的漏洞，通过估计合法 TCP 流的超时重传（retransmission time out，RTO）作为低速率攻击发包的周期 T，周期性地发送短脉冲，使得攻击流可以周期性地占用网络带宽，这样就会使合法的 TCP 流总是认为网络的负担很重，造成所有受其影响的 TCP 流进入超时重传状态，最终使得受害主机的吞吐量大幅度降低。这种攻击具有隐蔽性强、流量小等特点，很难被常规的针对传统拒绝服务攻击的检测机制检测到，可使受害机器长时间遭受攻击而不被发现，它所表现出的破坏性甚至比传统的 DoS 攻击更大，危害性更是不可估量[2, 7, 12]。如果该攻击技术被黑色产业链所掌握，那么后果将十分严重。因此，针对 LDoS 攻击的产生机理、检测算法和过滤方法的研究十分必要和紧迫，研究成果有助于阻断黑色产业链经营者利用 LDoS 攻击作为营利手段，避免攻击造成国家经济的巨大损失和社会形象的负面影响。

1.1.2　国内外研究概况

LDoS 从 2001 年被发现以来，引起了世界上很多研究者的关注。在国际上，Kuzmanovic 和 Knightly[3, 4]最早对 LDoS 的产生原理进行了比较详细的分析，并对 LDoS 的周期脉冲特性进行了深入研究，挖掘了 LDoS 攻击产生溢出的方法，提出了基于网络的防御思想；Cheng 等[13]首先提出了在频域（frequency domain）利用归一化累积功率谱密度（normalized cumulative power spectrum density，NCPSD）检测 LDoS 攻击的方法；Barford 等[14]提出了采用信号处理的方法检测网络中异常流量的方法；

Maciá-Fernández [15, 16]和 Chen[17]等比较完善地研究了在频域检测 LDoS 攻击的方法，并在嵌入式环境下进行了测试；Luo 和 Chang [18]对 LDoS 攻击的性能进行了仿真和试验，并采用小波（wavelet）检测技术在频域中检测 LDoS 攻击；Maciá-Fernández 等[19]研究了 LDoS 针对应用服务器的攻击模型。目前，国际上针对 LDoS 的研究大都集中在其检测和防御上[20]。

在国内，北京邮电大学信息安全中心的杨义先教授领导的研究团队研究了一种检测低速率拒绝服务攻击的方法及装置[21]；钮心忻教授领导的研究小组研究了低速率拒绝服务攻击的三级检测算法[22]；武汉大学计算机学院的何炎祥教授带领的研究小组开展了对 LDoS 攻击模型等的相关研究[23]，并提出一种基于小波特征提取的 LDoS 检测方法[24]；中国科学技术大学的研究小组研究了 LDoS 针对快速 TCP 攻击的性能[25]；国防科学技术大学计算机学院的张长旺等研究了基于拥塞参与度的 LDoS 攻击检测过滤方法[26]；浙江大学的魏蔚等研究了低速率 TCP 拒绝服务攻击的检测响应机制[27]和基于秩相关的检测分布式反射 DoS 攻击的方法[28]；上海交通大学研究了基于快速重传/恢复的低速率拒绝服务攻击机制[29]。

本书在分析 LDoS 攻击原理和产生机制的基础上，针对其攻击性能进行了研究，并采用信号处理技术，在基于功率谱密度（power spectral density，PSD）的检测和频域过滤 LDoS 攻击方面取得了一些进展[30-41]。

1.1.3　存在问题和发展趋势

DoS 攻击之所以相对容易形成，主要原因是 Internet 缺乏有效的认证机制，其开放的结构使得任意数据包都可以到达目的地。而且，现有很多 DoS 工具可以任意下载，并被加以利用，这为发起 DoS 攻击创造了便利。据报道，目前精心构造的攻击甚至能够达到 200Gbit/s 左右的攻击流量，足以充斥任何一个服务器的接入带宽[1]。因此，DoS 攻击的解决方案一直是网络安全研究领域的难点问题。

在合法 TCP 流和 LDoS 流发往同一目的地的情况下，LDoS 流表现出两个不同的重要行为[39]。

（1）LDoS 流的最高速率将保持不变，而 TCP 流呈线性增长。

（2）LDoS 流在相对固定的时间周期到达目的地，而 TCP 流是连续到达的。

1. *存在的问题*

采用现有的通信量分析方法，周期性脉冲很难在时间域被检测出来，这是因为平均共享的带宽并不是非常大。在分布式的情况下，成倍的傀儡机发起的攻击会进一步降低单个通信量的速率，因此检测更加困难。分布式攻击发起者可以通过降低最高速率或者延长攻击周期来降低平均通信量，所以用时间序列检测这类攻击是毫无效果的。现有的攻击检测手段基本是基于时间序列的，对 LDoS 攻击的检测是个盲点[39]。

目前 LDoS 攻击之所以没有在国内全面报道或者形成轰动效应的主要原因如下[39]。

（1）现有检测手段很难发现 LDoS 攻击。目前入侵检测手段采用时间统计的方法，即在设定的检测时间内对攻击包的个数进行统计，根据统计流量的大小来判定是否存在攻击。由于 LDoS 攻击脉冲的持续时间很短，远小于现有检测方法设定的平均检测时间，而且 LDoS 攻击的平均流量很小，只有正常流量的 10%～20%。因此，现有检测手段对于 LDoS 攻击的检测存在一定的缺陷。

（2）LDoS 攻击需要的专业知识较多。一般黑客即便掌握了 LDoS 攻击的产生技术，但由于攻击时间同步和流量汇聚等关键技术不能很好地解决，所以发起 LDoS 攻击的概率很小。

（3）当前大多数网络攻击是以金钱为利益驱使的。高技术、高危害度的攻击掌握在少数的黑客手中，在有利可图的情况下，出租攻击网络给出钱人，去破坏或者报复选定的目标。因此，黑客不轻易发起 LDoS 攻击。

2. *发展趋势*

在 DoS 攻击的处理上，目前国际上流行采用信号处理与网络流量数据处理技术相结合的方法，把经典的信号检测理论和滤波器理论应用到攻击流量的检测和过滤方法中[13, 14, 42]。例如，采用归一化累积功率谱密度作为检测 LDoS 攻击的判定依据[43, 44]，以及采用小波分析技术在频率分量中发现攻击分量等[24]。所以，本书研究的主要思路就是将 LDoS 攻击的流量当做小信号（small signal）处理，采用数字信号处理（digital signal processing，DSP）技术实现 LDoS 攻击的检测和过滤[31-33, 35, 36, 38-40]。

1.2 LDoS 攻击原理

LDoS 攻击可以分为两种形式[2, 12]：第一种是利用 TCP 拥塞控制机制[3, 4, 43, 44]；第二种是利用路由器主动队列管理机制[30, 45, 46]。这两种攻击形式没有本质的区别，都是利用系统自适应机制的漏洞，通过虚假的拥塞信号使端系统或链路处于不稳定的状态，这种不稳定状态最终导致系统服务质量（quality of service，QoS）大大降低[6, 7]。

LDoS 攻击的形式变化多样，但是基本特征始终不变。典型的 LDoS 攻击的数学模型如图 1-1 所示[3, 19]。

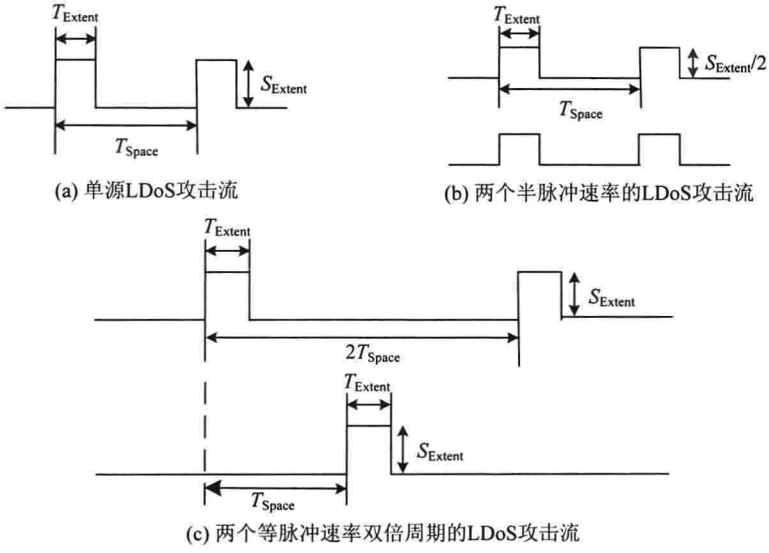
一个单源 LDoS 攻击脉冲序列可以用一个四元组表示为 $A(T_{\text{Extent}}, S_{\text{Extent}}, T_{\text{Space}}, N)$[2, 3, 12, 19]。其中，$T_{\text{Extent}}$ 是脉冲攻击长度，代表攻击者持续发包的时间段；S_{Extent} 是脉冲幅度，代表流量的最高速率；T_{Space} 表示两个脉冲之间的时间间隔；N 是一次攻击发出的脉冲总数，如图 1-1(a)所示。而多源 LDoS 攻击需要产生周期、幅度等特征一致的方波，这些方波到达受害者端恰好汇聚成一个足够大的脉冲，图 1-1(b)所示为两个半脉冲速率的 LDoS 攻击流；图 1-1(c)所示为两个等脉冲速率双倍周期的 LDoS 攻击流。

要想获得更佳的攻击效果，LDoS 攻击一般还需要具备以下必要条件[34, 47-50]。

（1）攻击的周期与 TCP 的 RTO 值相同。

（2）脉冲攻击幅度应足以造成包丢失。

（3）脉冲攻击长度应该比 TCP 流的往返时延大，从而引起拥塞。



(a) 单源LDoS攻击流　(b) 两个半脉冲速率的LDoS攻击流

(c) 两个等脉冲速率双倍周期的LDoS攻击流

图 1-1　LDoS 攻击模型

1.2.1　针对 TCP 拥塞控制机制的 LDoS 攻击

TCP 是目前互联网中使用最广泛的传输协议。根据美国世界通信公司（WorldCom）的统计，互联网上总字节数的 95%及总数据包数的 90%均使用 TCP 传输[51]。TCP 采用流量控制、拥塞控制和差错控制作为最基本的可靠性技术。其中，拥塞控制是为了避免由于网络拥塞而造成数据频繁重发继而带来更严重的网络拥塞。然而，TCP 的拥塞控制机制存在一定的安全漏洞，因此，攻击者可以利用 TCP 拥塞控制机制存在的漏洞发起 LDoS 攻击[8]。

TCP 拥塞控制机制，无论慢启动、超时重传还是和式增加、积式减小，其核心思想都是不断探测网络所能承受的最大传输上限。当发现网络数据包丢失时，认为达到网络传输上限，迅速减小拥塞窗口，避免给网络带来更严重的拥塞。LDoS 攻击正是利用这一机制，在大部分时间里保持沉默，而在特定时刻短时间内发送脉冲式攻击流，造成部分网络数据包丢失，使得 TCP 发送方误认为存在拥塞，开始重传并减小拥塞窗口。所以，LDoS 攻击可以致使一些反常现象出现，例如，正常 TCP 流吞吐量明显减小和间歇网络拥塞等[52, 53]。

1. TCP 拥塞控制

Internet 上的数据流无法在虚拟网络中进行资源预留，它总是在对网络资源状况一无所知的情况下开始发送数据。这种情况存在两个隐患：①如果一台非常快的工作站