网络拥塞控制及拒绝服务攻击防范

Network Congestion Control and Defense against DoS Attack

王秀利 著

北京邮电大学出版社
www.buptpress.com

北京市教育委员会共建项目专项资助

网络拥塞控制及拒绝服务攻击防范

王秀利　著

北京邮电大学出版社
·北京·

内 容 简 介

本书主要对网络拥塞控制和拒绝服务攻击防范进行了系统研究。首先，深入探讨了其原理，综述了其研究现状，详细分析了其存在的问题等；其次，将优化理论和控制理论中的许多方法和技术应用于网络拥塞控制和拒绝服务攻击防范中，提出了新的拥塞控制算法和攻击防范策略；最后，描述了网络模拟器 NS2 的模块组成、运行方式、脚本编写及代码结构等，详细说明了如何对 NS2 进行功能扩展以实现新的算法，并指出算法评价指标的获取方法。

本书细致而全面地展示了相关领域的研究进展和最新成果，既有较深的理论研究和全面的文献综述，又有网络模拟软件的使用及扩展等。本书具有完整性、新颖性和学术性，可供计算机网络、网络安全等相关领域的教学、科研和工程技术人员参考，也可作为相关专业研究生和高年级本科生的教学参考书。

图书在版编目(CIP)数据

网络拥塞控制及拒绝服务攻击防范/王秀利著. —北京：北京邮电大学出版社，2009

ISBN 978-7-5635-1967-5

Ⅰ. 网… Ⅱ. 王… Ⅲ. ①计算机网络—阻塞②计算机网络—安全技术 Ⅳ. TP393

中国版本图书馆 CIP 数据核字(2009)第 063240 号

书　　名：网络拥塞控制及拒绝服务攻击防范

作　　者：王秀利

责任编辑：崔　珞

出版发行：北京邮电大学出版社

社　　址：北京市海淀区西土城路 10 号(邮编：100876)

发 行 部：电话：010-62282185　传真：010-62283578

E-mail：publish@bupt.edu.cn

经　　销：各地新华书店

印　　刷：北京忠信诚胶印厂

开　　本：720 mm×1 000 mm　1/16

印　　张：9.25

字　　数：169 千字

印　　数：1—2 000 册

版　　次：2009 年 6 月第 1 版　2009 年 6 月第 1 次印刷

ISBN 978-7-5635-1967-5　　定　价：19.00 元

前　言

计算机网络发展至今，已成为一个庞大的非线性复杂巨系统，系统的规模和用户数量巨大且仍在不断增长，异质异构的网络不断融合发展，网络中有限的资源被越来越多的用户所共享使用，网络拥塞问题变得更加严重。另外，网络上还存在许多安全威胁，在各种攻击手段中，拒绝服务攻击是最常用的攻击手段。由于其容易实施、难于防范、难于追踪，从而成为较难解决的网络安全问题之一，并且它的攻击效果非常明显，严重危害信息的可用性，降低网络服务的质量，重要的网络服务时时有被攻破或崩溃的危险。这给各行各业带来了巨大的经济损失，导致重要的经济、政治和军事情报被窃取，甚至危及国家安全。如何透彻地认识和理解计算机网络这个人工非线性复杂巨系统，如何有效地管理和控制计算机网络，在理论上和技术上仍然面临许多困难和挑战。

网络拥塞控制属于计算机科学、优化理论和控制理论等学科的交叉领域。拥塞控制算法设计的关键问题是如何生成反馈信息以及如何对反馈信息进行响应。而拒绝服务攻击防范的重点则集中于两个方面：缓解攻击所造成的网络拥塞状况；防止被攻击主机资源耗尽。

作者根据多年的研究成果和经验，撰写了这本《网络拥塞控制及拒绝服务攻击防范》，希望能给广大读者提供借鉴和参考。作者关于此书内容的研究得到了中国科学院软件研究所王永吉研究员的大力帮助，在此表示诚挚的谢意。

本书的出版受到了北京市教育委员会共建项目专项资助，在此表示衷心感谢。还要特别感谢中央财经大学孙宝文教授和朱建明教授在本书出版过程中给予的大力支持和帮助。

在完成本书的过程中作者参阅了大量的文献，其中包括专业书

籍、学术论文、学位论文、白皮书、用户说明书等，书中有部分引用已经很难查证原始出处，作者注明的参考文献仅仅是作者获得相关资料的文献，没有一一列举出所有的参考文献，在此表示歉意和谢意。

再次向所有给予过作者任何形式帮助的各位同志表示感谢。

网络技术的发展非常快，新思想、新技术、新观点不断提出，加之作者水平所限，错误与疏漏之处在所难免，欢迎广大读者批评指正。

作　者

目　　录

第1章 绪 论

1.1 研究背景

随着互联网的飞速发展，互联网用户和应用都在快速地增长，人们对于网络的需求越来越大，对网络服务质量的要求也越来越高，拥塞已经成为一个十分重要的问题。在最初的 TCP 协议中只有流控制(Flow Control)，而没有拥塞控制(Congestion Control)，接收端利用 TCP 报头将接收能力通知发送端，这样的控制机制只考虑了接收端的接收能力，而没有考虑网络的传输能力，导致了网络拥塞崩溃(Congestion Collapse)的发生。1986 年 10 月，由于拥塞崩溃的发生，美国 LBL 到 UC Berkeley 的数据吞吐量从 32 kbit/s 跌落到 40 bit/s[1]。拥塞崩溃的发生严重降低网络的性能，从此之后，在拥塞控制领域开展了大量的研究工作。

网络拥塞现象的发生和网络的设计机制有着密切的联系。最初设计的网络是非面向连接的分组交换网络，所有的业务分组被不加区分地在网络中传输。网络中采用的服务模式为尽力服务模式(Best Effort)，网络能给出的唯一承诺就是尽自己最大的努力传输进入网络的每一个分组，但它无法给出一个定量的性能指标，如吞吐量、端到端时延和分组丢失率等。而无连接网络的节点之间在发送数据之前不需要建立连接。这使得在网络的中间节点上不需要保存和连接有关的状态信息。但是使用无连接模型难以引入“接纳控制”(Admission Control)算法，在用户需求大于网络资源时难以保证服务质量。因此网络的性能不仅仅是其本身可以确定的，还受用户施加负载的影响，很显然，这种网络体系结构缺乏一定的隔离和保护机制。网络中有限的资源是由多个用户共享使用的。由于没有“接纳控制”算法，网络无法根据资源的情况限制用户的数量。又由于缺乏中央控制，网络也无法控制用户使用资源的数量。由于网络用户和应用的数量都在迅速增长，当多个用户对网络的需求总量大于网络实际传输能力时，必然会导致网络拥塞的发生。

随着网络中有限的资源被越来越多的用户所共享使用，网络拥塞问题变得越来越严重。网络产生拥塞的根本原因在于用户（端系统）给网络提供的负载大于网络资源容量和处理能力，表现为数据包时延增加、丢弃数增大、上层应用系统性能下降等。网络研究人员一方面要研究如何利用和整合现有的网络资源，使网络达到最高效能；另一方面也要不断研究新的网络协议和算法，为网络发展做前瞻性的研究。因此，引进更多、更合理的拥塞控制机制对网络的稳定运行至关重要，网络拥塞控制研究也因此具有非常重要的理论意义和很高的应用价值。

然而，即使所有的链路和数据流都采用了拥塞控制机制，仍然可能会发生持续的拥塞。可能的原因之一是拒绝服务攻击（Denial of Service，DoS）。

从理论上讲，一旦主机连接到网络上，它就面临来自网络上的安全威胁，如拒绝服务攻击、后门攻击、特洛伊木马攻击等。常见的攻击种类及其所占比例如表 1.1 所示[2]。从表中可以看出，在各种攻击手段中，拒绝服务攻击是最常用的攻击手段。

表 1.1　常见的攻击种类及其所占比例

攻击种类	所占比例（%）
拒绝服务攻击	40
后门攻击	24
IP 欺骗	14
木马攻击	11
逻辑炸弹	10
其他	1

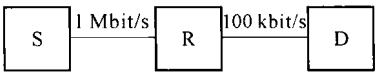
据计算机应急响应小组（Computer Emergence Response Team，CERT）统计，从 1989 年到 1995 年，DoS 类型的攻击以每年 50% 的速度递增。目前平均每周 DoS 类型的攻击超过 3 000 次，并且这种攻击的后果极具破坏力。首次分布式拒绝服务攻击（Distributed Denial of Service，DDoS）发生在 1999 年 8 月，黑客使用 Trinoo 攻击了美国明尼苏达大学，该工具集中了至少 227 台主机的控制权，攻击包从这些主机源源不断发往明尼苏达大学的服务器，造成其网络严重瘫痪。2000 年 2 月，雅虎由于受到 DDoS 攻击导致服务中断长达 3 小时，攻击来自互联网上多个网址。之后，美国 CNN、Amazon、eBay 等网站都遭到了类似攻击，致使这些网站被迫关闭，黑客们使用了同样简单的攻击手段，向网站发送大量的信息使网络阻塞从而导致系统瘫痪。在国内，新浪网遭到黑客长达 18 小时的攻击，致使电子邮箱系统完全瘫痪。

美国东部时间2002年10月21日下午5时左右，国际互联网系统的核心，位于美国、瑞典、英国、日本等国家和地区的13个DNS根域名解析服务器，遭受了有史以来规模最大、最复杂的一次分布式拒绝服务攻击，这次攻击持续1小时左右，导致7个服务器瘫痪。域名解析服务器是维系全球互联网正确通信的基础，如果攻击得逞，全世界范围的互联网用户将可能会觉察到连网速度减慢，或是根本无法连接，整个互联网将会崩溃。

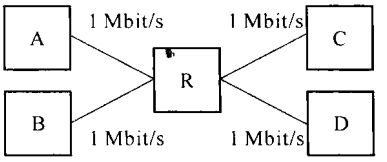
由于分布式拒绝服务攻击容易实施、难以防范、难以追踪，从而成为较难解决的网络安全问题之一。并且它的攻击效果非常明显，严重危害信息的可用性，降低网络服务的质量，致使重要的网络服务随时有被攻破或崩溃的危险。这给各行各业带来了巨大的经济损失，导致重要的经济、政治和军事情报被窃取，甚至危及国家安全。因此，研究分布式拒绝服务攻击防范策略同样具有重要的理论意义和很高的应用价值。

1.1.1 基本问题

拥塞总是发生在网络中资源“相对”短缺的位置。拥塞发生位置的不均衡反映了互联网的不均衡性[3]：首先是资源分布的不均衡，图1.1(a)中带宽的分布是不均衡的，当以1 Mbit/s的速率从S向D发送数据时，在R处会发生拥塞；其次是流量分布的不均衡，图1.1(b)中带宽的分布是均衡的，当A和B都以1 Mbit/s的速率向C发送数据时，在R处也会发生拥塞。互联网中资源和流量分布的不均衡都是广泛存在的。



(a) 带宽不均衡的情况



(b) 流量不均衡的情况

图1.1 网络资源不均衡的情况

网络拥塞产生的根本原因是网络资源需求超过了所能提供的极限，主要表现为瓶颈链路资源的缺乏[4]。

(1) 瓶颈链路缓存容量不足。分组交换网络是基于存储转发，数据进入交换设备，暂时存储于缓冲区，当速率超过网络的转发限度将引起滞留的分组超过缓存容量而丢弃。网络流量的突发性使得这一现象更加普遍。

(2) 瓶颈链路带宽容量不足。通信链路的容量是一定的，当数据流的传输速率超过网络的容量，将会导致拥塞发生。根据香农信息理论，任何信道带宽最大值即信道容量如式(1.1)所示

$$C = B\log_2(1+S/N) \tag{1.1}$$

其中，N 为信道白噪声的平均功率，S 为信源的平均功率，B 为信道带宽，S/N 即为信噪比。设计网络通信系统时，所有信源发送的速率 R 必须小于或等于信道容量 C，否则，传输速率超过信道传输极限值，则在理论上无差错传输是不可能的，所以在网络低速链路处就会形成带宽瓶颈，当其满足不了通过它的所有源端带宽要求时，网络就会发生拥塞。

(3) 处理器处理能力弱、速度慢也是引起拥塞的重要原因。路由器要根据要求完成数据包的转发，要实施队列管理、分组调度、路由表更新和路由选择等工作，现代因特网的吞吐量比较大，因此对路由器的 CPU 有较高的要求。如果路由器的处理速度跟不上高速链路，也会产生拥塞。

虽然拥塞源于资源短缺，但增加资源并不能避免拥塞的发生，有时甚至会加重拥塞程度[3]。例如，增加路由器缓存，表面上看可以防止或缓解由于拥塞引起的分组丢弃，但随着缓存的增加，端到端的时延也相应增大。因为分组的持续时间(Livetime)是有限的，超时的分组同样需要重传。因此，过大的缓存空间有可能使总延迟超过端系统重传时钟的值从而导致分组重传。这些分组白白浪费了网络的可用带宽，反而加重了拥塞。

随着互联网规模的增长，互联网上的用户和应用都在快速的增长，拥塞已经成为一个十分重要的问题。如果不在互联网中使用拥塞控制算法，拥塞崩溃的发生会严重降低网络的性能。因此，在互联网中使用拥塞控制算法对于互联网的稳定具有十分重要的意义。

围绕着 TCP 流量控制的拥塞控制一直是网络研究的一个热点。在互联网发展初期，拥塞控制主要是通过 TCP 协议中端到端基于滑动窗口的流量控制完成的[1]，TCP 的流量算法中也逐步增加了慢启动[1]、拥塞避免、快速重传[5]与快速恢复[6]等算法，以期对网络流量进行控制。目前，这方面的研究热点包括[7]：对“慢启动”过程的改进；基于速率的控制策略；ACK 过滤；减少不必要的“超时重传”和“快速重传”；显式拥塞通知(Explicit Congestion Notification，ECN)的使用；TCP-Friendly 的拥塞控制；在特殊网络环境(如无线链路、卫星链路和非对称链路等)中的拥塞控制。

随着应用需求的丰富和技术的发展，研究者开始认识到想完全依赖实现在终端系统上的策略与算法很难满足越来越多的复杂应用需求。于是，研究人员把注意力转向网络中的路由器等中间节点设备，期望通过增强它们的功能来实现端主机无法达到的目标[8]。就拥塞控制而言，网络中间节点有可能更及时，甚至提前准确了解网络的拥塞状态，并依此实施有效的资源管理策略，使网络能有效地避免拥

塞，或尽早从严重的拥塞状态中恢复过来。当然，对路由器功能的扩展要受继承性和延续性的限制，否则将影响技术的实用性。

早期路由器上的队列管理算法采用尾丢弃算法(Drop Tail)，即当路由器缓存仍有空间时，接收并缓存一切来不及处理的分组。当缓存空间耗尽时，丢弃所有新到来的分组。由于发送到路由器的分组呈序列状态，在该算法中这个序列末尾的分组被丢弃，所以被称为尾丢弃算法。目前因特网中广泛采用的传输控制协议仍是TCP协议，根据MCI的统计，总字节数的95%和总报文数的90%使用TCP传输[9]。在该协议下，当发送方检测到发送数据有所丢失时会降低并重新调整发送速率。当发送方的发送速率大于网络的处理能力时，路由器缓存会被不断消耗，直至耗尽。此时发送方新发的数据分组会被丢弃，当它检测到这一情况时，它会降低发送速率。因此，如果在路由器中增加智能预测环节，使得在路由器缓存被耗尽前就有计划的丢掉一部分分组，就可以提早通知发送方降低发送速率，避免可能出现的危险。这就是主动队列管理(Active Queue Management，AQM)的由来。AQM的主要优点是：减少网关的报文丢失；减少报文通过网关的延迟；避免死锁(Lock-out)行为的发生。

1998年，RFC2309[8]强烈建议在路由器队列管理算法中使用主动队列管理策略，并推荐随机早期探测(Random Early Detection，RED)[10]算法为候选算法。研究表明RED比Drop Tail具有更好的性能，但是RED的性能对算法的参数设置十分敏感[11]。近年来，非线性规划理论[12]和系统控制理论[13]被引入到拥塞控制的研究中，一些研究者尝试使用严格的数学模型来描述由端系统和网关共同组成的系统。相应地，出现了一些新的主动队列管理算法，如比例积分(Proportional Integral，PI)[13]、随机指数标记(Random Exponential Marking，REM)[11]、自适应虚队列(Adaptive Virtual Queue，AVQ)[14]等，但是这些算法仍存在反应速度慢、动态性能差等问题，需要进一步地研究。目前，主动队列管理算法已经成为拥塞控制研究中的技术热点之一。

拥塞控制算法的分布性、互联网的复杂性和对拥塞控制算法的性能要求使得拥塞控制算法的设计具有很高的难度。学术界在拥塞控制领域已经开展了大量的研究工作，研究人员一直在努力研究新的算法试图更好地解决网络拥塞问题。

另外，分布式拒绝服务攻击的危险性也已经超出人们的预想。分布式拒绝服务攻击主要针对互联网络和相关设备，它利用成百上千个被控制节点向受害节点发动大规模协同攻击。其主要应用了TCP/IP协议本身的漏洞和不足，通过大量消耗受攻击者的资源或网络带宽，导致网络或系统不胜负荷以致瘫痪而停止提供正常的网络服务，使合法用户不能访问或使用该资源，造成拒绝服务攻击。DDoS

攻击由于实现简单，难以防范和破坏性极大而被广泛应用。

以前，发动 DDoS 攻击的主要是专业人员，攻击程序特别是较大规模攻击程序的调试、配置和实现要花费一定的时间和精力，而现在，刚刚使用计算机的初学者也能通过 DDoS 攻击工具向顶级专业网站发动大规模的攻击，并且网上还隐藏着大量可能随时发动自动攻击的代码。

常见的分布式拒绝服务攻击工具有 Trinoo，Tribe Flood Network（TFN），Stacheldraht 和 TFN2K 等。

（1）Trinoo 允许同时攻击多个 IP 地址，攻击方式是 UDP Flood。

（2）TFN 的攻击方式呈现多样化，包括 ICMP Flood，SYN Flood，UDP Flood 和 Smurf 等，攻击时任选一种攻击方式。

（3）Stacheldraht 在欧洲和美国网络上出现，包含了 Trinoo 和 TFN 的特征，并引入了 IP 欺骗、指令消息的通信加密和后台程序的自动升级。

（4）TFN2K 是对 TFN 的改进，使 TFN 攻击更加难以识别和过滤。

分布式拒绝服务攻击可以分为两类。

（1）带宽耗尽型

带宽耗尽型主要是使目标网络拥塞，大量消耗网络带宽，导致网络不能提供正常服务。

（2）资源耗尽型

资源耗尽型是攻击者利用服务器处理缺陷，大量消耗目标服务器的关键资源，如 CPU、内存等，导致服务器无法提供正常服务。

由于 DDoS 攻击严重危害信息的可用性，降低网络服务的质量，因此需要对其进行防范。对于绝大部分 DDoS 攻击而言，防范重点集中于以下两个方面：缓解攻击所造成的网络拥塞状况；防止被攻击主机资源耗尽。

在 CERT 的报告中指出，到目前为止，还没有很好的办法解决分布式拒绝服务攻击问题。研究人员认为，除非修改 TCP/IP 的内核，否则，从理论上没有办法彻底解决分布式拒绝服务攻击，但通过一些技术手段，可以有效阻止一些 DDoS 攻击，降低其攻击的危害。

根据 DDoS 攻击的方法和特性，当前已经提出的防范 DDoS 攻击的主要方法有：修改配置和协议、反向查找攻击源头、攻击检测和过滤[15,16,17,18]

目前普遍认为，在独立站点上实现对 DDoS 攻击的有效防范是不可能的[19]。修改配置和协议可以防止 ICMP Flood 等利用协议、系统缺陷的少量攻击，但该攻击若转化为大流量的强行攻击则无法防范，同时它无法防范反射攻击。随着攻击

工具的自主性、隐蔽性、快速复制等特点的增强，反向查找攻击源头的方法已由非常困难成为几乎不可能，目前仍有研究人员利用数据挖掘等技术在进行研究。现有的攻击检测和过滤方法可以检测出常见的 DDoS 攻击，但此时已经对攻击带来的后果无能为力，整个受害子网出现拒绝服务现象。

文献[20]和[21]提出一种基于聚合拥塞控制(Aggregate-based Congestion Control，ACC)算法的回推(Pushback)，回推的思想是：当发生 DDoS 攻击时，被攻击网络的边界路由器会发生拥塞，从而产生丢包现象。从被丢弃的包中提取流量的特征，将符合此特征的网络包汇聚成一个或多个数据流，通过限制这些数据流的速率，从而达到阻止 DDoS 攻击的目的。为了减小 DDoS 对中间网络的影响，利用回推使位于 DDoS 攻击路径上的路由器之间相互合作，从而可以将防御的范围从被攻击网络向上延伸。回推被认为是目前比较有前景的 DDoS 攻击防范方法。

虽然基于 ACC 的回推能够较好地防范带宽耗尽型的 DDoS 攻击，但是防范资源耗尽型的 DDoS 攻击效果很差，因为资源耗尽型攻击占用的网络带宽很小，其主要目的是耗尽被攻击目标的关键资源。如 SYN Flood 攻击，每秒钟 500 个数据包足以对一个主机实施有效的拒绝服务攻击。一个数据包大小为 64 字节，速率为 256 kbit/s，对于大多数网络来说只是占用了较小一部分带宽。因此基于 ACC 的回推难以防范这类攻击。

另外，DDoS 攻击出现了一些新的趋势：

(1) DDoS 攻击将越来越多地采用 IP 欺骗技术；

(2) DDoS 攻击技术和工具将不断推陈出新；

(3) DDoS 攻击将会不断智能化，具有躲过入侵检测系统(Intrusion Detection System，IDS)检测跟踪和规避防火墙防御体系等特点；

(4) 针对路由器弱点的 DDoS 攻击将会增多；

(5) DDoS 攻击将更多地利用路由器的多点传送功能；

(6) DDoS 攻击将更多地针对 TCP/IP 协议先天缺陷进行攻击。

虽然 DDoS 攻击的原理比较简单，但 DDoS 攻击却屡屡得逞，DDoS 攻击依然是互联网面临的主要威胁。因此，研究人员一直在努力研究新的防范策略试图解决 DDoS 攻击问题或有效降低其危害。

解决 DDoS 的困难在于其分布式特性，以及攻击者采用伪造、随机变化报文源 IP 地址、随机变化攻击报文内容等方法，使得 DDoS 的攻击特征难以提取，攻击源的位置难以确定。

1.1.2 研究动机

网络拥塞控制本质上是一个如何共享资源的问题。在包交换网络中，所有的激活终端共享网络资源。这些资源包括节点处理能力、缓存空间和通信链路带宽。这三者中的任何一个都可能成为潜在的瓶颈，从而导致网络拥塞。从用户需求的角度来说，网络必须为所有用户的请求提供服务，然而用户的需求在传输起始时间、需求速率、持续时间上变化很大，在很多情况下还是突发的。从网络提供资源的角度来说，任何网络物理资源都有固定的上限能力。因此，用有限的资源去适应波动很大的用户需求，一定会出现网络资源不能满足用户需求的时候，此时就必须使用拥塞控制来管理用户流量对瓶颈资源的共享。

将网络拥塞或恰当的发送速率等信息通知给发送方的机制称为反馈。闭环流量控制和网络整体性能都依赖于反馈，如果没有反馈机制，源端就无从知晓如何调整发送速率，网络将变得不稳定，容易导致拥塞或空闲。拥塞控制算法设计的关键问题是如何生成反馈信息以及如何对反馈信息进行响应。

绝大多数 AQM 算法在很大程度上是依赖于直觉的、启发性的、针对局部个别问题的，没有全面、系统地运用理论工具加以分析研究，因此，借助适当的理论对保证算法的性能是非常必要的。

RED 算法的实质是采用比例控制器和低通滤波器。比例控制器的缺点是控制存在“稳态误差”(Steady-state Error)，稳态误差的大小依赖于网络的环境，这是平均队列长度随着网络流量增长的主要原因。有时可能出现误差超过缓冲的大小，从而引起振荡现象的发生。低通滤波器则降低了系统的反应速度。

PI 控制器通过增加积分环节来消除比例控制器中存在的稳态误差[22]。PI 主动队列管理算法的设计是在对 AQM 非线性模型进行局部线性化处理将其等效为二阶系统后，在忽略时滞的前提下，用经典的频域分析方法设计而成。在 AQM 算法中使用 PI 控制器虽然可以消除“稳态误差”，系统的稳定性和适应能力均有所增强。但同时也会减慢系统的反应速度，瞬态性能差。当网络中的流量发生很大变化时，使用 PI 控制器需要的收敛时间要远远长于使用比例控制器时的时间。从控制理论中得知，微分环节能反映系统偏差信号的变化率，具有预见性，能预见偏差变化的趋势，因此能产生超前的控制作用，可以改善系统的动态性能，在微分时间选择合适情况下，可以减小超调，减少调节时间[22]。在 PI 控制器中加入微分环节，就形成了比例-积分-微分(Proportional-Integral-Differential，PID)控制器。

AQM策略在高吞吐量和低时延之间做出合理平衡的关键在于始终将队列长度维持在一个较小的期望值，从控制系统的角度分析，这是典型的调节系统的技术目标。恰当地运用控制理论中的分析和设计方法对网络拥塞控制进行研究是值得进一步探索的方向。

本书的研究动机之一是把优化理论、反馈控制等用于网络拥塞控制，提出新的AQM算法以改善网络性能。

分布式拒绝服务攻击主要应用了TCP/IP协议本身的漏洞和不足，通过大量消耗受攻击者的资源或网络带宽，导致网络或系统不胜负荷以致瘫痪而停止提供正常的网络服务，造成拒绝服务攻击。

研究人员提出了许多检测DDoS攻击的方法，这些方法能够在一定程度上判断出DDoS攻击行为的发生，但很少详细描述如何对DDoS攻击进行反应，即如何有效地防范DDoS攻击。如文献[23]中提出了累积和改进门限算法来检测DDoS攻击，文献[24]中通过对网络流量的自相关性进行分析来检测DDoS攻击。另外，目前很多防范DoS/DDoS攻击的策略都只是针对特定攻击。如TCP SYN cookies可以有效防范TCP SYN攻击[25]，关闭ICMP响应可以有效防范ICMP洪水攻击等。

对于绝大部分DDoS攻击而言，防范重点集中于以下两个方面：缓解攻击所造成的网络拥塞状况；防止被攻击主机资源耗尽。根据DDoS攻击的方法和特性，当前已经提出的防范DDoS攻击的主要方法有：修改配置和协议、反向查找攻击源头、攻击检测和过滤[15,16,17,18]。

基于ACC的回推能够从被丢弃的包中提取流量的特征，将符合此特征的数据包汇聚成一个或多个数据流，通过限制这些数据流的速率，从而达到阻止DDoS攻击的目的。回推还使位于DDoS攻击路径上的路由器之间相互合作，从而可以将防御的范围从被攻击网络向上延伸。

虽然基于ACC的回推能够较好地防范带宽耗尽型的DDoS攻击，但是防范资源耗尽型的DDoS攻击效果很差，因为资源耗尽型攻击占用的网络带宽很小，其主要目的是耗尽被攻击目标的关键资源。因此ACC难以防范这类攻击。

Garg提出一种基于资源调节的DDoS攻击防范方法[26]，该方法基于被攻击目标端，它的思想不是标记攻击，而是标记被保护的资源。在资源调节器中维护服务器资源利用情况的状态，流向服务器的流量按照其资源消耗分类，基于包或流的资源使用情况，通过调节每一个流量分类的资源消耗，期望限制特定级别的攻击消耗，而其他的级别继续接受服务。