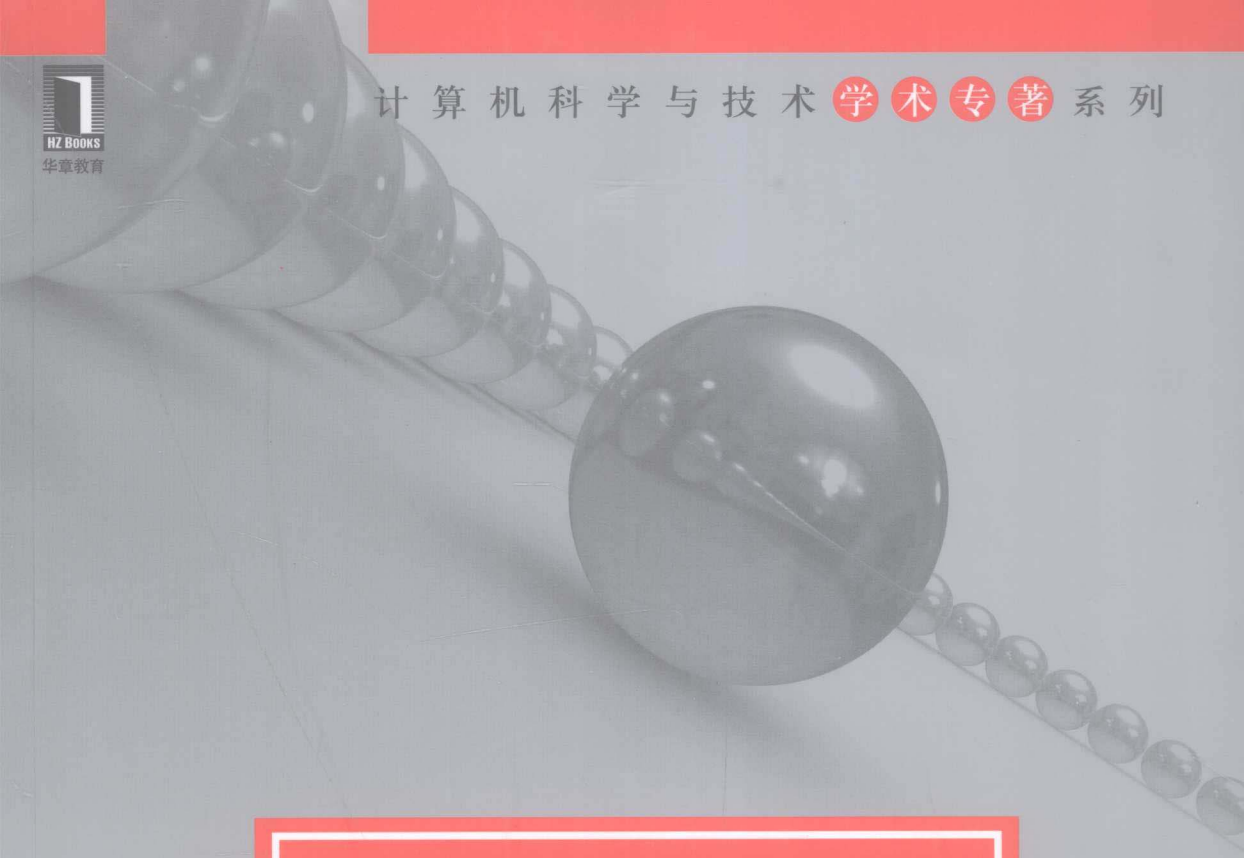
HZ BOOKS
华章教育

计算机科学与技术学术专著系列



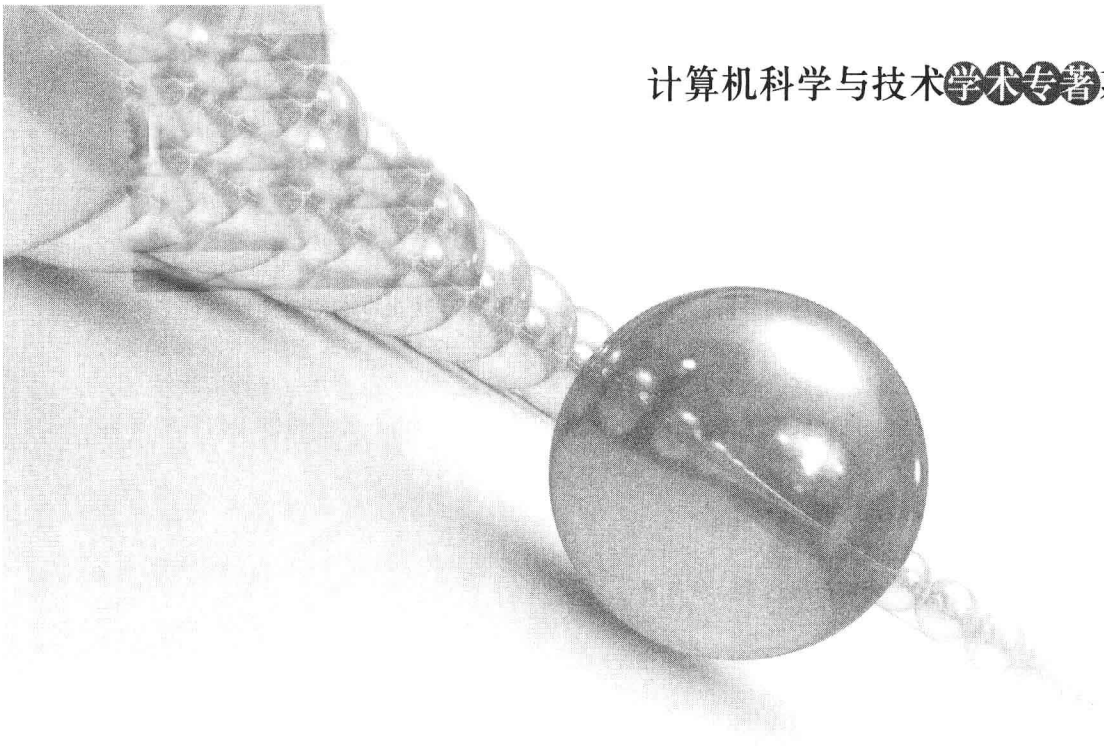
Reduction of Quality Attack and The Defense Methods

降质服务攻击及其防范方法

何炎祥 刘陶◎著

机械工业出版社
China Machine Press

计算机科学与技术学术专著系列



Reduction of Quality Attack and The Defense Methods

降质服务攻击及其防范方法

何炎祥 刘陶◎著

本书详细介绍了降质服务（RoQ）攻击的原理，对目前已提出的各种 RoQ 攻击方式进行了分类描述和建模；结合 RoQ 的攻击特征及规律，分别对 RoQ 攻击的单点检测、协同检测、主动防御方法进行了研究和探讨，介绍了一些新的检测和防范方法，并通过仿真实验对这些防范方法的有效性进行了验证和分析；对特定网络环境下 RoQ 攻击存在的可能性进行了研究和探讨；介绍了 RoQ 防范系统的原型设计与实现，并展望了该研究领域未来技术的发展趋势。

本书概念准确，层次清晰，叙述严谨，取材新颖，内容丰富，可供从事计算机软件、计算机网络、信息安全、网络安全等方面教学、科研、开发、管理等工作的科技工作者和高等院校的师生借鉴、学习和参考。

图书在版编目（CIP）数据

降质服务攻击及其防范方法/何炎祥，刘陶著. —北京：机械工业出版社，2011.6

ISBN 978-7-111-34570-1

Ⅰ. 降…　Ⅱ. ①何…　②刘…　Ⅲ. 计算机网络－安全技术　Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2011）第 084275 号

机械工业出版社（北京市西城区百万庄大街 22 号　邮政编码　100037）

责任编辑：王春华

北京京师印务有限公司印刷

2011 年 6 月第 1 版第 1 次印刷

170mm×242mm · 14.25 印张

标准书号：ISBN 978-7-111-34570-1

定价：55.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

客服热线：（010）88378991；88361066

购书热线：（010）68326294；88379649；68995259

投稿热线：（010）88379604

读者信箱：hzjsj@ hzbook.com

前 言 Preface

拒绝服务（Denial of Service，DoS）攻击一直是 Internet 面临的最为严峻的威胁之一。它主要通过连续向攻击目标发送超出其处理能力的过量数据，消耗其有限的网络链路或操作系统资源，使之无法为合法用户提供有效服务。在过去的几年中，DoS 攻击技术不断发展，造成的破坏性也越来越大。但近年来，出现了一类近似 DoS 攻击的新型攻击——降质服务（Reduction of Quality，RoQ）攻击。与传统 DoS 攻击相比，RoQ 攻击的攻击效率更高、隐蔽性更强、检测难度更大、更具有威胁性。

传统的 DoS 攻击尽管破坏性很大，但是其洪泛式、高频率、完全拒绝服务等特征致使其与正常网络流量相比具有一种异常统计特性，这样对其进行检测相对比较简单。RoQ 攻击与 DoS 攻击不同，其攻击目的不再是使目标系统完全丧失对正常请求的服务能力，而是降低目标系统对正常请求的服务质量。RoQ 攻击效果虽然不及 DoS 攻击明显，但隐蔽性更强，目标系统可能长时间地被 RoQ 攻击侵害而毫无察觉。而且，RoQ 攻击不再需要维持高速率攻击流来耗尽受害者端所有可用资源，而是利用网络或终端系统常见的自适应机制中存在的安全漏洞，通过间歇性地发送高强度攻击脉冲，降低受害者端的服务性能。RoQ 攻击可以看做是在 DoS 攻击基础上的改进形式，与 DoS 攻击相比，RoQ 攻击更加彻底地做到了有的放矢，因此攻击效率有了大幅度的提高，且更加有效地躲避了检测和防范。RoQ 攻击的提出给攻击防范问题的研究带来了新的挑战。

RoQ 攻击的威胁及应对技术研究将成为另一个重要研究课题与难点，及

时检测和防范降质服务攻击是保证网络计算环境安全的重要目标。目前国内对于降质服务攻击的研究刚刚起步。本书针对RoQ攻击，分别从攻击原理、攻击特征分析、攻击检测、攻击防御等方面，结合武汉大学网络安全团队的多年研究积累，进行了全面介绍。

本书共分9章，各章的主要内容组织如下：

第1章为绪论。该章介绍了本书的主要研究背景及研究意义；对当前相关研究现状进行了总结、归类与分析；给出了本书的研究目标和研究内容。

第2章详细介绍了RoQ攻击原理，对目前已提出的各种RoQ攻击方式进行了分类描述和建模。与传统DoS持续性攻击方式不同，RoQ攻击在短暂时间段内发送脉冲式攻击流，攻击脉冲必须与系统的恢复时间同步，以达到低强度、高效能的攻击目的。因此，精确选择攻击脉冲发送时间对攻击效果来说非常重要。该章主要对各种RoQ攻击的目标系统及攻击同步方法进行研究，并通过在NS2平台上进行的仿真实验对各种RoQ攻击的效果进行了分析。

第3章结合RoQ的攻击特征及规律，对Internet正常网络流与RoQ攻击流的差异进行了分析研究。首先介绍了一种基于小波特征提取的RoQ攻击单点检测方法，并详细讨论从整体框架到各部件的设计与实现。然后在NS2上进行仿真实验，评估系统的检测性能。

第4章结合RoQ的攻击特征及规律，对Internet正常网络流与RoQ攻击流的差异进行了分析研究，介绍了一种基于支持向量机的RoQ攻击单点检测方法。检测系统对攻击流量进行时频双域特征分析，使用CUSUM和离散傅里叶变换的方法对网络流量进行特征提取，将攻击的检测归结为一个多分类问题。引入支持向量机来解决这一分类问题，通过将获取到的实时网络流量归入不同的类，来判断该网络流量中是否含有攻击成分。由于综合考虑了时频两域中的多个特征，所以不仅能够对多种类型的攻击（DoS攻击、周期固定的RoQ攻击、周期变化的RoQ攻击）进行检测，而且保证了检测的准确率。NS2上模拟实验结果表明，该检测方法具有高检测率和低误警率，并且能检测出RoQ变种攻击，消耗计算资源少，具有良好的实用价值。

第5章对分布式RoQ攻击的检测方法进行研究。针对DRoQ攻击特点，

介绍了一种位于中间网络的分布式协同检测方法 DCRD（Distributed Collaborative RoQ Detection）。该章在单点小波流量特征提取的基础上，介绍了一种基于 D－S 证据理论的多点协同检测方法——通过各检测结点间的协同交互，组合各种特征证据对攻击进行综合判决。各检测结点之间采用分布式协同算法实现信息交互。仿真实验结果表明，DCRD 能够以较高精确度对分布式 RoQ 攻击进行检测，并于靠近攻击源处对其进行响应，有效减小了攻击及防范机制本身对合法流量的影响。

第 6 章以针对内容自适应机制的 RoQ 攻击为例，研究了针对终端系统的 RoQ 攻击免疫方法。本章介绍了一种改进的内容自适应机制，针对传统的内容自适应机制对于 RoQ 攻击防御能力差的缺陷，将 Q 学习机制引入到内容自适应决策流程中。通过对攻击态势的实时感知，Q 学习机制及时做出决策，对内容自适应机制的相应参数进行智能调整，实现了对 RoQ 攻击的免疫。本章最后通过实际网络实验对这一机制进行了验证。实验结果表明，所介绍的免疫机制能够有效地降低 RoQ 攻击对内容自适应机制决策的影响，从而保证其对外的服务质量。

第 7 章探索结构化 P2P 网络中 RoQ 攻击实现方式，通过周期性组织受控结点恶意退出，构造高搅动环境，大大地降低了系统的查询成功率，并增加了成功查询的时延。p2psim 上的仿真实验结果表明了对攻击影响理论估计的有效性。同时，也讨论了对这种攻击的检测和防范。

第 8 章对无线网络中的 RoQ 攻击进行详细分析，同时探讨相应的检测与防范方法。考虑到 Ad-hoc 网络是目前应用最为广泛的无线网络，我们以其为例分析无线网络环境下的 RoQ 攻击。

第 9 章对本书进行总结，对 RoQ 攻击相关研究中有待解决的问题进行了思考，并展望了后续工作。

本书所介绍的研究工作是经过武汉大学计算机学院众多科研人员多年学习、研究和工程实践沉淀的成果。参与本研究工作的人员包括：曹强、韩奕、钟海、陈伟、董伟、刘建博等；另外，钟海在本书的校正、协助编辑整理、修改书稿等方面做了大量工作，在此对他们表示衷心的感谢。

本书是国内第一部专门针对RoQ攻击的研究著作，对相关领域的研究人员具有一定的借鉴意义和参考价值。本书的出版得到国家自然科学基金“低速率的拒绝服务攻击模型和防范研究”（2007，项目编号：60642006）、国家自然科学基金“面向低速率拒绝服务攻击防范的安全适应性机制研究”（2008，项目编号：60773008）、国家自然科学基金可信软件重大研究计划项目“可信编译理论与实现方法研究”（2009，项目编号：90818018）和湖北省自然科学基金计划重点项目“可信计算的软件理论与关键技术研究”（2009，项目批准号：2008CDA007）等项目的资助，在此一并表示感谢。

降质服务攻击原理及其检测防范方法是当前处于科学前沿的论题，许多理论和思想还处于探索阶段，由于作者的水平和经验有限，错误和不妥之处在所难免，恳请读者给予批评指正，共同推进计算机网络安全研究的进步和发展。

作者

2011年4月于武汉

目　录
Contents

第1章 Chapter 1 绪 论

1.1 研究背景及意义

在信息化、数字化高度发达的今天，随着信息高速公路的建设和计算机网络特别是 Internet 的迅猛发展，信息的高速扩散性和不可控性使得不论是国家还是社会团体，乃至个人都面临着巨大的不可防范的安全性威胁[1]。我们一方面要保证正当的网络用户的通信安全，另一方面又要有效地阻止别有用心者利用网络进行犯罪活动。事实上，网络的开放性使得我们对网络信息的监测与管理更加困难，很难有效地避免利用网络的违法犯罪事件的发生，因此，有必要通过获取和分析网上传输的动态的、高速的信息，尽可能早地发现网上任何可疑的情况，进行及时有效的分析并恢复它的本来面貌，为国家的有关职能部门提供真实可靠的数据，将可能的危害抑制在萌芽状态；与此同时，为保证我们自己的通信安全、信息的真实性和完整性，必须有自己一套安全机制，以防止敌对势力的各种可能攻击。

拒绝服务（Denial of Service，DoS）攻击[2,3]是众多攻击中的一种，其目的是使计算机或网络无法正常提供服务。从网络攻击的各种方法和所产生的破坏情况来看，DoS 算是一种简单却很有效的进攻方式。DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务。最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。带宽攻击是指以极大的通信量冲击网络，使得所有可用网络资源都被消耗殆尽，最后导致合法的用户请求都无法通过。连通性攻击是指通过大量的攻击连接请求冲击计算机，使得所有可用的操作系统资源都被消耗殆尽，最终计算机无法再处理合法用户的连接请求。

目前网络中常见的 DoS 攻击大多采用分布式的形式实施。分布式拒绝服务（Distributed Denial of Service，DDoS）攻击是指借助于服务器/客户机技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动 DoS 攻击，从而成倍地提高拒绝服务攻击的威力[4]。DDoS 采用分布、协作的大规模攻击方式，主要瞄准比较大的站点，像商业公司、搜索引擎和政府部门的站点。DDoS 攻击是利用一批受控制的机器向一台机器发起攻击，这样来势迅猛的攻击令人难以防备，因此具有较大的破坏性。通常，攻击者使用一个偷窃账号将 DDoS 主控程序安装在一台计算机上，在一个设定的时间，主控程序将与大量代理程序（Agent）通信。Internet 上的许多计算机都已安装了这些代理程序，当它们收到指令时就会发动攻击。利用服务器/客户机技术，主控程序能在几秒钟内激活成百上千次代理程序的运行。自从 DDoS 引起学者的广泛重视后，针对 DDoS 攻击的防范方法研究已经有 5～6 年的时间，虽然还缺乏非常有效的方法，但其中出现了一些针对性比较强的防范方法，对某些特定类型的攻击有着较好的防范效果[5]。

近年来，拒绝服务攻击已逐渐成为 Internet 面临的最为严峻的威胁之一。DoS 攻击者只需简单地组织足够的傀儡机，向目标系统发送大量的攻击数据，使目标系统持续面临远远超出其服务能力的请求，即可使受害系统无法对合法的用户请求进行响应，限制网络资源对合法用户的可用性，严重降低网络服务性能。例如，2004 年 2 月发起的 MyDoom 病毒[6]，通过电子邮件和 P2P 网络的方式传送病毒程序，通过控制被感染机器向 SCO 和微软的官方网站发起 DDoS 攻击，SCO 主页彻底瘫痪，从此 MyDoom 病毒声名鹊起。2006 年 9 月，百度网站也遭受了有史以来最大规模的 DoS 攻击[7]，使其在全国的搜索服务瘫痪近 30 分钟。商业网络安全公司 Arbor Networks 2008 年 11 月发布的《全球网络基础设施安全报告》称，2008 年全球分布式拒绝服务攻击流量激增，突破 40Gb 大关，比 2007 年增长近 1 倍。各大 ISP 将绝大部分安全支出均用于防范 DDoS 攻击，承受能力已达上限。虽然对网络用户来说，（D）DoS 攻击可能仅仅只是有些讨人厌，损害性并不大，但是随着我们对网络越来越依赖，这些攻击一旦作用于敏感的资源和服务之上，将造成巨大的经济损失。就 2004 年的 MyDoom 攻击来说，其在全球所造成的直接经济损失已达 385 亿美元。

令人欣慰的是，要想完全淹没目标系统的服务能力，DoS 攻击首先需要获取并控制一群数量庞大的傀儡机[8]，例如 MyDoom 的成功实施就涉及 10～20 万台傀儡机。更加重要的是，就其本质来说，拒绝服务攻击非常容易被受害者端察

觉，有利于在攻击发生后立即启用防御机制对其进行阻止或者进一步对攻击者进行回溯追踪。这对于攻击者来说是非常具有震慑力的。但是，如果攻击者的目的不是使目标系统服务完全瘫痪，而仅仅只是造成目标系统所提供服务的质量或性能严重降级，比如资源利用率、系统稳定性或者服务质量等，那么成功实施攻击不再需要数量庞大的傀儡机，对于这样的攻击怎么办？如果受害者端无法较早地察觉攻击甚至无法感知攻击的存在怎么办？

最近几年，研究者们提出了一类近似 DoS 攻击的新型攻击——降质服务攻击（RoQ），与传统 DoS 攻击相比，RoQ 攻击[9—15]具有攻击效率更高、隐蔽性更强、检测难度更大等特点，比传统的 DoS 攻击更具有威胁性。

对于传统的 DoS 攻击，尽管其破坏性很大，但是其相同的攻击目的和原理使其存在两个共同的特点：

1）DoS 攻击的目的是使目标系统丧失对外提供服务的能力，因此其攻击所造成的影响非常明显。DoS 攻击一旦发生，受害者端会在短时间内发觉攻击的存在，这从某一方面来说也有利于管理员在较短时间内对其采取防范措施。

2）DoS 攻击的原理是通过被控制的主机系统（zombie 或 handler）向目标主机发送大量的数据包，形成超过目标主机能够承受的流量，造成目标主机的资源（带宽、内存和 CPU 等）耗尽。因此其需要攻击者采取一种压力（Sledge-hammer）方式向被攻击者发送大量攻击包，即要求攻击者维持一个高速率的攻击流。正是这种特征，使得各种传统 DoS 攻击与正常网络流量相比都具有一种异常统计特性，这样对其进行检测相对比较简单。因此，许多 DoS 检测方法都把这种异常统计特征作为识别 DoS 攻击的特征，一旦检测到攻击，就激活包过滤机制丢弃所有具有攻击特征的数据流传送的数据包或采用一定的速率限制技术来降低攻击影响。

降质服务攻击与拒绝服务攻击不同，其攻击目的不再是使目标系统完全丧失对正常请求的服务能力，而是降低目标系统对正常请求的服务质量，其攻击效果虽然不及 DoS 攻击明显，但隐蔽性更强，目标系统的性能可能长时间地被 RoQ 攻击侵害而管理员对此毫无察觉；且 RoQ 攻击不再需要维持高速率攻击流，耗尽受害者端所有可用资源，而是利用网络中常见的适应性控制机制（如 TCP 的拥塞控制机制、路由器主动队列管理机制）中所存在的安全漏洞[16]，通过周期性地在特定的短暂时间间隔内突发性地发送大量攻击数据包，从而降低受害者端的服务性能。由于 RoQ 攻击只是在短暂时间间隔内发送攻击数据包，相同周期其他时间段内不发送任何数据，这使得攻击流的平均速率比较低，与合法用户的数据流区别不大，不

再具有 DoS 攻击的异常统计特性，这样就很难用已有的方法对其进行防范。RoQ 攻击可以认为是 DoS 攻击的改进形式，与 DoS 攻击相比，RoQ 攻击更加彻底地做到了有的放矢，大幅度地提高了攻击效率，且更加有效地躲避了检测和防范。

如果将传统的拒绝服务攻击效果看做是洪水般的破坏，那么降质服务攻击则如同慢性毒药，使得计算机网络或终端系统性能逐渐下降，且相对 DoS 攻击，RoQ 攻击更难以检测。因此，RoQ 攻击的提出给网络攻击防范问题的研究带来了新的挑战。

RoQ 攻击的威胁及应对技术研究将成为网络安全领域另一个重要研究课题与难点。此类攻击虽还没有在现实的网络中大规模出现，但理论上已经证明这种攻击存在的可能性，并且在实验室特定的环境下进行了反复证实。近年来，在网络安全需求的强大推动下，网络安全领域的理论与技术的发展不断地跃上新台阶，然而相对于充满想象力与不可预测的网络发展来说，其发展却是滞后的。因此，虽然现在还没有在现实网络中大规模地出现 RoQ 攻击，但是如果我们能及早地研究此类攻击方法，就可以为研究防范此类攻击提供基础。掌握这种攻击的方法尚存在着一些技术难题，比如如何确定攻击的时间，如何同步攻击数据流，使其在特定的时间、特定的路由器上汇集，以形成脉冲攻击流。其次，由于 RoQ 和 DoS 的攻击原理不一样，不能完全套用传统的 DoS 检测和保护机制来检测与应对 RoQ，因此需要在了解 RoQ 攻击的基础上，使用针对性更强的方法解决 RoQ 的检测和防范问题。再者，同 DoS 攻击一样，RoQ 攻击也存在其分布式形式，即 DRoQ[17]。DRoQ 是一种协同攻击，需要汇集多个攻击源完成攻击目标，因此，最佳的防范方法应采用分布式的体系结构。然而不论是在传统的 DDoS 防范上，还是在 DRoQ 防范中，分布式的方法都存在着诸多困难，如在异构网络环境下消息的传递方式，知识的共享与理解，检测点的部署问题，防范系统本身的安全性和鲁棒性等，这些都是需要进行广泛研究的问题。最后，各种检测与防范机制都需要设置众多的参数，目前很多方法使用人工的方法进行设置，如何使用自适应的方法使参数达到最优化，也是一个值得研究的问题。总之网络安全威胁及应对技术研究将为整个网络计算环境的安全性与可靠性提供有力的支持。

及时检测和防范降质服务攻击是保证网络计算环境安全的重要前提，目前国内对于降质服务攻击的研究刚刚起步。本书将针对 RoQ 攻击，研究其攻击形成原理，归纳此类攻击的特征，并在此基础上研究检测和防范 RoQ 攻击的方法，为网络的可靠性和可信性提供安全保证机制。

1.2 RoQ攻击相关研究现状

1.2.1 攻击方法研究

对于降质服务攻击的研究尚处于开始阶段，近年来，这方面的相关研究工作出现在一流国际会议上，说明其受到了充分的重视。降质服务攻击的相关思想最早出现在2003年，在计算机网络方面的顶级会议SIGCOMM上Rice大学的Aleksandar Kuzmanovic首次提出了一种针对TCP协议的低速率拒绝服务攻击[9]。由于此种攻击隐蔽性非常强，所以Kuzmanovic形象地将其称为shrew（地鼠）攻击。

shrew攻击主要利用TCP数据流超时重传控制机制所存在的安全漏洞，通过周期性地发送低频率高强度脉冲攻击流，严重抑制正常TCP链接的流量。shrew攻击在大部分时间里是保持沉默的，但间歇性地在较短时间间隔内发送脉冲式的攻击流。由于TCP数据流的最小重传超时时间（RTO）是一致的，shrew攻击者可以根据此RTO精确计算发送攻击脉冲的间隔时间。当攻击目标链路上的正常TCP链接每次从超时等待中恢复过来时，shrew攻击者就发送攻击脉冲，使TCP链接的发送端误以为网络仍然存在拥塞，从而重新进入超时等待。这样正常TCP链接始终处于超时等待状态，传输流量趋近于零[18]。shrew攻击的效果可能不如传统DoS明显，但是它可以用有限的攻击代价（攻击数据流）获取更高的攻击效率。例如，在模拟实验中，SYN flooding攻击是一种常用的DDoS攻击，它对一个10M带宽的Web服务器发动攻击，1000包/秒攻击密度可以阻止约90%的合法用户访问Web页面，然而使用shrew攻击，平均使用110包/秒攻击密度就可以使网络性能下降60%左右。虽然shrew攻击的效果有所降低，但攻击效率却得到了提升。据统计，目前Internet上超过80%的流量均基于TCP传输协议，因此shrew攻击对于网络传输的潜在威胁非常大。最重要的是，shrew攻击具有很好的隐匿性，虽然其每次发送的攻击脉冲强度非常高，但是间歇式的攻击特性使其攻击流平均速率并不高，潜伏性非常强，可以在很长一段时间内作用于受害者而不被察觉[16]。以前大多数针对传统洪泛式DoS攻击所提出的防范方法对于shrew攻击来说不再有用[9,19]。

然而，shrew攻击还是存在缺陷的，因为shrew攻击是基于TCP超时重传这一具体的控制协议所存在的缺陷提出的，它只对TCP链接上传输的流量有影响，攻