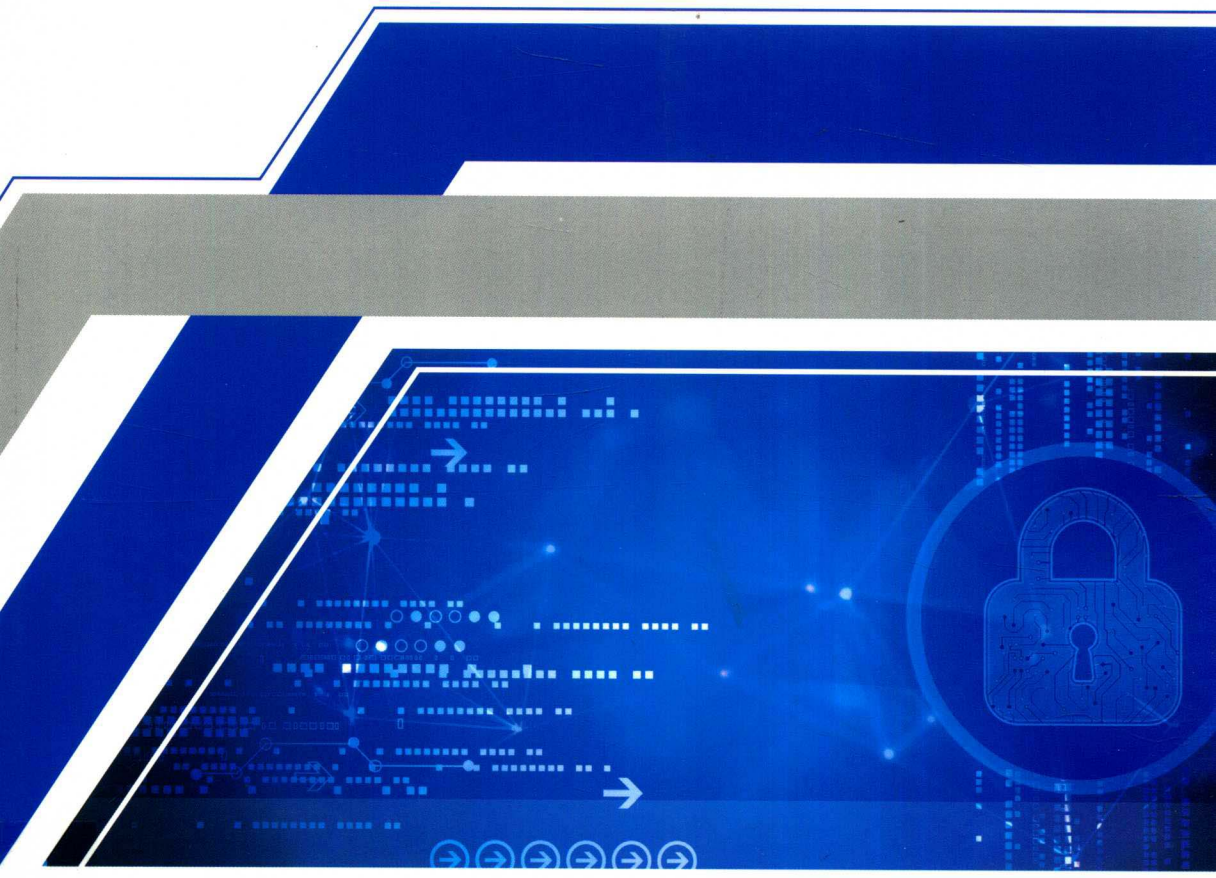
DDoS 的攻击源追踪与防御技术研究

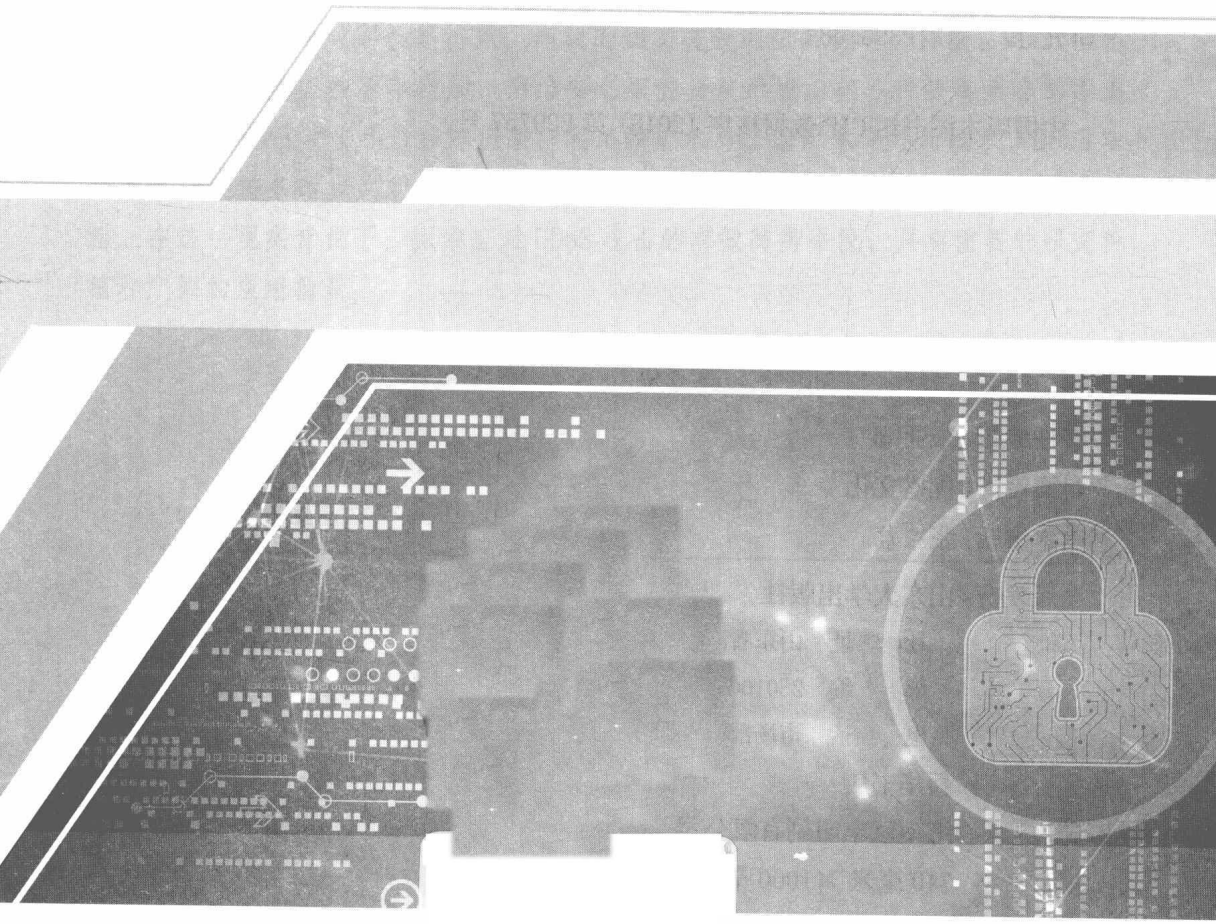
林玉香　著



山东大学出版社

DDoS的攻击源追踪与防御技术研究

林玉香 著



山东大学出版社

图书在版编目(CIP)数据

DDoS的攻击源追踪与防御技术研究 / 林玉香著. —
济南 : 山东大学出版社, 2018.9
ISBN 978-7-5607-6206-7

Ⅰ. ①D… Ⅱ. ①林… Ⅲ. ①计算机网络－安全技术
－研究 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2018)第229757号

责任编辑:宋亚卿
封面设计:优盛文化
美术编辑:张　荔

出版发行:山东大学出版社
社　　址　山东省济南市山大南路20号
邮　　编　250100
电　　话　市场部(0531)88363008
经　　销:新华书店
印　　刷:济南巨丰印刷有限公司
规　　格:710毫米×1000毫米　1/16
12.5印张　227千字
版　　次:2018年9月第1版
印　　次:2018年9月第1次印刷
定　　价:48.00元

内 容 提 要

分布式拒绝服务(Distributed Denial of Service, DDoS)攻击是Internet面临的严重安全威胁之一。与传统攻击手段相比，DDoS攻击具有隐蔽性强、强度大、攻击源分散、持续时间长等特点，尚缺乏切实有效的防御机制。目前，DDoS攻击的频繁程度与危害性逐年增加，网络安全形势日益严峻。在各种防御策略的围追堵截之下，DDoS攻击手法推陈出新，利用挖矿木马、僵尸木马等新技术，DDoS攻击黑色产业链条逐步实现了技术的自动化和操作的平台化，进一步降低了攻击门槛。在这一现实背景下，探索应对DDoS攻击的有效防御手段，具有重要的研究价值和广阔的应用前景。

目 录
CONTENT

绪 论

分布式拒绝服务（Distributed Denial of Service，DDoS）是指冒用连接在互联网上的第三方计算机，把过量的信息流发至根服务器，使其无法应付而瘫痪。发动 DDoS 攻击时，攻击者在客户端（Client）操纵攻击过程。每个控制傀儡主机（Handler）都是已被入侵并运行了特定程序的系统主机，且都能够控制多个攻击傀儡主机（Agent）。每个攻击傀儡主机也是一台已被入侵并运行特定攻击程序的系统主机。每个响应攻击命令的攻击傀儡主机都会向被攻击目标主机发送拒绝服务攻击分组。

0.1 研究背景和意义

互联网已经成为现代社会重要的信息基础设施，网络的迅速普及和广泛应用深刻改变了人类的生活方式。网络交友拉近了彼此的距离，电子商务改变了传统购物方式，网上办公加速了信息交互流程等，网络已经成为人们工作、生活中不可或缺的重要组成部分。网络带来巨大便利的同时，也潜藏着严重的安全隐患，一次短暂的网络服务中断可能危及人们的日常生活、金融秩序、经济稳定，甚至国家安全，带来无法估量的损失。因此，维护网络安全，保证网络与应用的可用性，对维持人们正常的生活秩序具有极其重要的意义。

众所周知，互联网是基于 TCP/IP 协议族的计算机网络。然而，TCP/IP 协议族在设计之初主要用于科学研究，是基于可信用户的，并没有考虑安全性问题。随着互联网的普及，可信用户这个假设不再成立，安全问题也随之而来。拒绝服务（Denial of Service，DoS）攻击就是利用协议漏洞形成的一种最常见的网络入侵形式。攻击者通过控制规模宏大的僵尸机，向目标主机发送源地址伪造的攻击包，致使它因资源不足而无法处理正常数据请求，甚至宕机。

进入 21 世纪以来，分布式拒绝服务对 Internet 呈现出越来越严重的危害性，

被公认为 Internet 最大的威胁之一，同时成为国内外网络安全领域研究的一个热点。2003 年 1 月，由于网络蠕虫的攻击，亚洲、美洲和大洋洲很多国家的 Internet 全部或部分瘫痪，攻击者对采用这样的方法获得傀儡主机产生了浓厚的兴趣。事实上，2003 年 8 月对全球网络造成巨大危害的“冲击波”以及后续的“震荡波”和“阻击波”正是以蠕虫形式迅速传播后，由所有被入侵主机同时发起了大规模 DDoS 攻击。

DDoS 攻击的出现极大地影响了互联网的应用前景，著名的案例有：1999 年发生了第一个记录在案的攻击事件，明尼森达大学的一台计算机被攻击后宕机两天；2000 年发生了第一个轰动全球的攻击事件，雅虎（Yahoo）、亚马逊（Amazon）以及易贝（eBay）等高盈利网站先后遭到袭击，损失高达 40 亿美元；2009 年，推特（Twitter）由于遭到大规模攻击导致 4 500 万用户数十个小时无法使用其服务；2010 年，由黑客自发构成的“匿名者”组织发起的“阿桑奇复仇行动”，先后攻击了贝宝、万事达、维萨和瑞士邮政银行等网站，致使这些网站瘫痪数个小时；2012 年，该组织又攻击了美国联邦调查局（Federal Bureau of Investigation，FBI）和司法部，并向亚拉巴马州州政府网站发起攻击。2012 年，Radware 公司在其所发布的《全球应用以及网络安全报告》中指出：2011 年，DDoS 攻击正式成为主流的安全威胁，特别是混合 DDoS 攻击的出现（在一次 DDoS 攻击中，同时使用多种 DDoS 攻击类型），使它的危害性到了无以复加的程度。2013 年 3 月，欧洲反垃圾邮件组织（Spamhaus）遭遇 300 Gbps 的攻击；2013 年 8 月，中国互联网络信息中心（China Internet Network Information Center，CNNIC）遭遇有史以来最大的 DDoS 攻击，部分“.cn”域名解析受到影响，导致访问缓慢或中断；2014 年 2 月，美国知名科技公司 Cloudflare 遭遇 400 Gbps 的 DDoS 攻击，大约 78.5 万网站受到影响，其中包括维基百科；2014 年 12 月，部署在阿里云上的一家知名游戏公司遭遇截至当年最大的 DDoS 攻击，攻击超过 14 小时，流量峰值达到 453.8 Gbps；2015 年 12 月，英国广播公司（BBC）遭遇几个小时的 DDoS 攻击，流量峰值达到 602 Gbps，在当年可以排进前 5 名；2016 年 10 月，美国最主要的 DNS 服务商 Dyn 遭遇大规模的 DDoS 攻击，此次攻击超过 1 000 万 IP 源，导致美国东海岸大面积断网。

目前，最大的 DDoS 攻击是美国知名安全研究人员布莱恩·克雷布斯（Brian Krebs）的安全博客遭遇的 DDoS 攻击，攻击流量峰值达到 665 Gbps。2018 年 3 月，某知名代码托管网站遭受了史上最严重的 Memcached DDoS 攻击，攻击流量峰值达到 1.35 Tbps；短短几天时间，美国一家服务提供商也受到了同样攻击，1.7 Tbps

的超高流量立刻刷新已有记录。不法黑客利用 Memcached DDoS 攻击反射放大的特点，凭借其超 5 万倍的反射放大倍数，一次次推高流量峰值，破坏程度升级，掀起了 DDoS 攻击风暴。

但是，今天的互联网仍然没有合适的应对策略来抵制攻击。如何缓解 DDoS 攻击，保护这些可能受威胁的公共网络及其附属设施，成为网络安全研究者们急需解决的问题。

0.2 国内外研究现状

Internet 的高速发展带动了信息产业的巨大进步，但网络上的恶意犯罪行为亦飞速增长。这其中包括恶意病毒、恶意木马、黑客入侵、垃圾软件、拒绝服务攻击等，而拒绝服务攻击又占据了恶意行为相当大的比例。据中国教育和科研计算机网（CERNERT）统计，近几年的攻击增长速率都是以两位数的比率突进，这大大影响了我们正常使用网络的需要。自 1998 年发生第一次大范围攻击以来，网络攻击的手段和数量就呈膨胀式发展，而中国 1999 年 9 月也遭遇了一次强大的攻击风波。

针对攻击的入侵，目前主要存在的手段是检测、防御与追踪。关于检测、防御体系的研究，各大安全设备和软件服务商提出了许多切实有效的防御手段。1999 年的攻击风波过后，北京神州绿盟信息安全科技股份有限公司率先进行了抗攻击产品的研究和开发，此后各大网络安全厂商和研究机构均把焦点放在了抗攻击方案和技术的研究上。2004 年，上海市科委将“大规模 DoS 攻击防御技术”作为年度重点研究的项目，北京大学计算机科学技术研究所将 DDoS 攻击防御产品作为重点研究的方案。与此同时，上海、北京、西安等地的高校也将目光转向了攻击防御体系的研究，并有人提出了攻击检测的形式化描述。

而对攻击追踪方案的研究，却没有跟上攻击的脚步。目前，网络追踪的方法主要有日志追踪、链路测试、ICMP（Internet 控制报文协议）追踪、包标记追踪、入口过滤等。在互联网服务提供商（ISP）、路由负载、带宽限制、实时性和存储能力等要求的限制中，以 ICMP 追踪、包标记追踪和日志方案最为人们所接受。这其中被学者和专家认定为最有可行性的方案是包标记追踪方案。包标记追踪方案的意思就是当网络或主机遭受攻击时，可以根据受害者收到的攻击路径上的包而重构攻击路径，而重构路径所需要的信息就是获取足够多的各个路由器的信息。

由于路由器的功能和作用，可以轻松地完成 IP 包的收集。最后，根据收到的包信息来重构攻击路径。

Savage 等（2001）对攻击追踪方案率先进行了研究，提出了概率包标记（PPM）方案。此后，Song 和 Perrig（2001）又在 PPM 的基础上进行了研究，提出了高级包标记和带认证的包标记追踪方案。Peng 等（2002）又在高级包标记方案的基础上提出了自适应概率包标记方案。

在国内，李德全（2004）就包标记方案提出了一些改进和分析；电子科技大学、北京邮电大学进行了一些可变概率包标记追踪方案的研究；江南大学对自适应概率包标记方案进行了深入的研究和改进。

DDoS 攻击的高强度特点和破坏性影响要求对攻击具有较强的预警能力，以尽早实施有效防御，遏制攻击效果的蔓延和恶化。同时，为配合采用法律手段对攻击行为进行审计追责，需要提供技术手段支持，实现对攻击源的准确定位，对恶意 DDoS 攻击进行有力的震慑。以上需求对 DDoS 攻击防护技术提出了严峻挑战。

首先，DDoS 攻击流量的隐蔽性导致攻击早期的行为检测困难。为了尽早检测出 DDoS 攻击，通常将攻击检测机制部署在靠近攻击源的位置。然而，距离攻击源越近，DDoS 攻击的流量越少，引起的网络流量异常也越不明显。异常检测的难度很大，现有的检测方法仍难以对攻击早期的流量进行准确的检测。

其次，DDoS 攻击者的隐蔽性导致攻击溯源困难。目前，DDoS 攻击主要结合僵尸网络实施，定位参与攻击的僵尸主机是攻击溯源的主要目标。由于采用源地址欺骗等技术，攻击流量自带的标识不能真实地反映僵尸主机的身份，因此需要攻击路径中的网络节点辅助完成定位。另外，发现 DDoS 攻击的实际操控者也是攻击溯源的重要目标。由于通过跳板技术控制攻击，操控者与攻击目标不直接交互，攻击操控者的溯源面临更大挑战。

最后，传统的关防式防御方法难以满足 DDoS 攻击预警的要求。关防式防御是当前应对 DDoS 攻击的主要方法，它通过在个别关键位置部署集中式防护机制，对目标系统进行保护。这种方法很难为攻击响应提供足够的预警时间，往往“发现攻击”即意味着“系统被攻破”，难以组织有效的响应。而且这种方法很可能形成新的性能瓶颈，成为 DDoS 攻击的间接目标。在 DDoS 攻击源分布性日益增强的条件下，通过网络中多个节点的高效协作，采用分布式防护方法是提高攻击检测预警能力的有效途径。

DDoS 攻击是当前 Internet 面临的最重要的安全威胁之一，频繁出现的 DDoS 攻击事件极其惊人的攻击强度和危害，使人们认识到这一网络安全问题的重要性。

面向 DDoS 攻击的防护技术成为网络安全领域的研究热点。针对上述技术挑战，研究人员和工业界为此进行了不懈的努力与尝试。目前，DDoS 已有的攻击防护方法主要包括攻击检测、攻击响应、攻击溯源和攻击预防。下面简要介绍上述四种防护方法。

0.2.1 攻击检测

攻击检测是防范 DDoS 攻击的第一道屏障，其主要任务是发现网络中的 DDoS 攻击，产生报警，从而触发攻击响应机制。DDoS 攻击检测方法包括误用检测和异常检测。误用检测通过特征匹配发现已知攻击类型，典型代表是 Snort 入侵检测系统。异常检测方法是当前的主流研究方向，根据攻击检测方法的目标，DDoS 攻击异常检测方法可分为存在性检测、受害者识别和攻击流量区分三个层次。从人们意识到 DDoS 攻击的巨大危害开始，研究人员对 DDoS 攻击的检测问题已经进行了十几年的深入研究，应对方法层出不穷，涉及小波分析、数据挖掘、信息论、统计分析等多个领域的知识。近年来，研究思路从集中式检测向分布式检测方向转变，后者更符合 DDoS 攻击的分布式特点，被评价为应对 DDoS 攻击的唯一有效方案。

0.2.2 攻击响应

攻击响应是尽快恢复攻击受害者的正常工作能力，保证服务可用性的必要手段。DDoS 攻击响应主要采用报文过滤和速率限制技术，消减攻击流量，缓解 DDoS 攻击的影响。在已知攻击报文特征的情况下，报文过滤机制能够有效地阻断 DDoS 攻击流量。然而，在大多数情况下，难以区分合法报文和攻击报文，有的 DDoS 攻击甚至使用合法报文发起攻击，因此报文过滤机制的适用范围有限。速率限制通过抑制聚合网络流量的发送速率，避免大量报文拥塞链路或淹没攻击受害者。典型的速率限制机制有 Pushback、PSP 等。按照部署位置的不同，攻击响应大致可分为受害者端、中间网络和攻击源端响应三类。比较来看，基于中间网络的分布式 DDoS 响应方法能取得更好的效果。

0.2.3 攻击溯源

攻击溯源的作用是追踪发起 DDoS 攻击的真正攻击者，如对于源地址欺骗的 DDoS 攻击，找到发出攻击报文的真实主机。攻击溯源能够为攻击响应机制提供真实的攻击源位置及攻击路径信息，更重要的是，能够为 DDoS 攻击的事后追责提供证据支持。对于 DDoS 攻击溯源问题，最新的研究热点集中在基于包标记（packet

marking）和日志记录（logging）的报文追踪方法，尤其是出现了很多结合上述两种方法的混合溯源机制（hybrid traceback），取得了较好的效果。现有的攻击溯源技术已经能够实现单个报文的追踪，一般需要转发路由器的支持，或标记报文头字段，或记录报文摘要。尽管现有研究在降低路由器的计算和存储开销方面下足了功夫，但攻击溯源机制与实际部署应用仍然有较大的距离。

0.2.4 攻击预防

攻击预防从破坏 DDoS 攻击形成的条件入手，研究如何防止 DDoS 攻击的发生。在当前的网络体系架构下，接收端被动接收报文，对发送端行为缺乏控制力。基于授权的攻击预防技术允许接收端控制发送端的发送速率，从源头遏制 DDoS 攻击流量的产生。发送端向接收端证明自身的计算能力或带宽资源，从而获得接收端允许发送的令牌。在部分研究中，接收端的授权令牌与报文转发路径相互关联，使中间网络路由器能够优先处理、转发携带令牌的网络流量。为了保护重要的服务资源免受 DDoS 攻击威胁，有人提出了基于目标隐藏的攻击预防方法，一般利用 Overlay 网络隔离服务器，使访问流量不能直接到达服务器。攻击检测、攻击响应和攻击溯源都是通过在现有的网络体系结构上“打补丁”的方式抵御 DDoS 攻击；攻击预防则需要改变现有的网络体系结构，或者通信双方的交互方式，这也是 DDoS 攻击预防技术始终处于模拟研究阶段的重要原因。

0.3 研究目的和研究内容

0.3.1 研究目的

任何网络都会受到拒绝服务攻击，这是由网络的特性决定的，但把攻击造成的损失降到最小的程度是能实现的。虽然攻击防御设备和软件已经取得了实质的进步，但对攻击源的查找和惩处始终处在一个原始的阶段，这在攻击防御上缺少了重要的一环。如果能提出一种高效实用的攻击追踪方案，那么无论是对现在网络攻击的受害者，还是对 ISP，都将会产生一定的实际价值。

简单而言，DDoS 攻击防御的安全目标非常简单，就是维护服务的可用性。如果从 DDoS 攻击的生命周期来分析，我们可以设置三条防线来实现这一安全目标。首先是做好 DDoS 攻击的预防工作，其次是在攻击发生时能够快速进行攻击检测

并实施过滤，最后是在攻击过程中或者攻击结束后进行攻击源追踪和标识。这三条防线必须协同工作方能取得最佳的防范效果。其中，追踪攻击作为重要的防线之一，可以通过攻击溯源，及时有效地发现攻击源头，一方面为缓解攻击提供了依据，另一方面为日后诉诸法律程序提供了取证依据。

追踪攻击是在攻击发生过程中，有效恢复攻击路径，准确追踪攻击发生的源头，有利于抑制攻击行为。在攻击结束后实施攻击追踪，一方面能够确认追踪的准确性，另一方面能够为攻击事后解决法律纠纷提供佐证材料。目前，提出的攻击源追踪算法大多需要 ISP 提供其路由拓扑信息，针对的攻击也仅限于直接类型的分布式拒绝服务，并且无法保障恢复出来的攻击路径的可靠性、准确性和时效性。

因此，更深入地研究 DDoS 攻击，有效地改善和弥补上面提到的 DDoS 防御技术的不足之处，进一步提高其性能，是我们研究这些防御技术要达到的目标。更为重要的是，在设计这些防御技术解决方案时合理地将它们之间的协同防御能力考虑在内，有助于设计出一种稳定、可靠、灵活和有效的 DDoS 综合防御体系。此外，为了使 DDoS 综合防御体系更好地融入信息安全综合保障体系，增进信息安全综合保障体系的整体防御能力，需要提出一种高效可行的联动解决方案。

如果能提出高性能的追踪方案，并且可以与网络防御、网络检测等软件设备共同工作，增加网络和系统的安全性，改变防火墙、入侵检测系统被动地防御入侵的局面，便可使计算机等网络设备更好地提供正常的网络服务。网络追踪可以得到攻击者，这样可以查到攻击的源泉，从源端屏蔽危害，有效地防止以后类似攻击行为的发生。进行 DDoS 攻击追踪研究，不但可以减少企业、单位和个人的经济损失，同时还可以肃清网络恶意流量，使网络工作处于一个更加有效的环境之下。不但如此，我们也可以改进方案的追踪效率，增强概率包标记的包在传输过程中的安全性，使追踪体系尽量在收到最少的包的状态下工作，使攻击者对标记包的破坏行为性降到最小。除此之外，我们还可以改进包淹没的概率，防止包在传输过程中被淹没和攻击。改进了的追踪方案可为以后类似的研究工作提供理论和技术支持，推动网络安全事业的发展和进步。

0.3.2 研究内容

本书拟从以下几个方面展开研究：

0.3.2.1 改进概率包标记追踪方案，提高攻击追踪的效率

提高标记的 IP 包在传输中的安全性，防止标记的包在传输的过程中受到劫持和攻击。原有的概率包标记方案在攻击中容易被攻击者修改地址和跳数。这样，

受害者想重构路径就不得不收集更加有效的包，而对收到的包进行判断。改进包在传输过程中被修改的概率，将大大改善重构路径的效率。

0.3.2.2 降低包标记路由器的标记负载

这可以使标记路由器在更轻松的环境下工作。基本包标记方案和高级包标记方案都存在着重复标记包的情况，这在一定程度上增加了路由器的负担。改进路由器标记包的重复工作，有利于提高路由器的工作效率。

0.3.2.3 降低受害者重构路径的困难度，提高可行性

受害者在重构路径时，需要收到足够多的包。但这不但加重了路由器的负载，同时加重了受害者重构攻击路径的负担。受害者处理标记包的时间过长和任务过重，某种形式上是对受害者遭受攻击的一种另类攻击。DDoS 攻击防御系统能减轻受害者重构路径的负担，改进追踪的效率。

0.3.2.4 提出一种基于路径的单包追踪溯源方法

在已提出的单包追踪溯源方法中，包记录是最常用的技术，但它会引起存储开销大和溯源精度低等问题。因此，本书提出一种基于路径的单包追踪溯源方法，借鉴网络的标签转发原理。该方法利用路由路径建立一条溯源路径，取代包记录。与已有方法相比，它拥有以下特点：路由器的存储开销只与经过它的路由路径有关，而与路径上转发包的数量无关；在路径回溯过程中查询路由器的数量只与路径长度相关，而与它的邻居数无关；溯源精度较高。

0.3.2.5 提出针对 DDoS 攻击初期隐蔽攻击流量的多阶段检测方法

在 DDoS 攻击发起初期，攻击流量的隐蔽性强，引发的异常不明显，这对 DDoS 攻击的早期检测提出了严峻挑战。同时，现有的基于流量属性的异常检测方法存在单一属性描述能力不足、多维属性可扩展性差等问题。针对上述问题，本书提出并研究了基于网络监控点视图和受害者视图的 DDoS 攻击模型，对攻击流量的隐蔽性进行深入的分析。分析表明：越靠近攻击源的位置，攻击流量的隐蔽性问题越突出；单属性的异常偏离程度难以提供足够的可检测性。以此为基础，本书提出一种包含网络流量状态预测、细粒度流量奇异点检测、可疑目的地址提取的多阶段 DDoS 攻击检测方法 MADOP。

0.3.2.6 提出一种基于包标记的 DDoS 攻击防御方案

现有的 DDoS 攻击检测方法主要利用控制平面传递局部检测的异常警报，全局检测设备往往根据异常警报内容给出最终决策，融合算法一般比较简单。当局部检测准确度不高时，整个系统的检测效率将非常低。针对上述问题，本书提出通过数据平面协同实现 DDoS 攻击早期检测与受害者识别的全新设计思想。定义

数据平面检测视图的概念，通过检测视图的精简和传递，使全局检测能够在全局异常流量的基础上进行，提高检测准确度。根据上述设计思想，本书提出一种基于包标记的 DDoS 攻击检测系统 Ddetector。

0.3.2.7 研究 DDoS 僵尸网络木马样本分析方法

在各种防御策略的围追堵截之下，DDoS 攻击的手法推陈出新，利用挖矿木马、僵尸木马等技术，DDoS 攻击的黑色产业链条逐步实现了技术的自动化和操作的平台化，进一步降低了攻击门槛。通过对 DDoS 僵尸网络木马样本的动态与静态进行综合分析，找到主机感染的挖矿木马病毒样本的特征，及时有效地总结出各类僵尸木马发作的特征、传播的手段，构建整套完整的针对个人和企业的解决方案。这样，可以提高主机的安全防护性能，及早发现潜在的威胁，处理已知的威胁，保障主机安全以及个人信息安全。

0.4 内容组织结构

本书共分为 9 部分：

绪论主要对本书的研究背景、主要内容、问题的提出以及本书的主要结构进行了介绍。

第 1 章主要介绍 DDoS 攻击的相关知识。首先，介绍目前常见的 DoS 攻击的基本特征；其次，对已提出的 DoS 攻击防御技术进行分类，指明反应式包过滤的适用场景和优势；再次，对反应式包过滤问题进行描述和定义，并给出相关的评价指标；最后，分析已提出的反应式包过滤技术存在的问题。

第 2 章提出了混合概率包标记方案以及基于可选项的概率标记方案。前者在攻击路径的重构上，大大减少了受害者重构路径所需要包的个数；后者在路由器处理时间上有明显的优势。

第 3 章提出了基于 AS 标记算法的路径重构方法，利用 C++ 封装路由节点类和处理数据流的方法来模拟发包的过程，把每个路由节点标记为 AS 边界路由或域内路由，针对不同的路由节点采用不同的方法处理数据流来模仿路由器标记方案。

第 4 章提出了一种基于路径的单包追踪溯源方法。首先，指出已有方法存在路由器存储开销大、溯源重构时间长、溯源精度低等问题；然后，为解决这些问题，阐述如何利用网络的标签转发原理建立溯源路径以及重构路径；最后，使用数学分析和实验仿真两种方法评价该方法的性能。

第 5 章针对 DDoS 攻击发起初期，攻击流量的隐蔽性强，引发的异常不明显的问题，提出一种包含网络流量状态预测、细粒度流量奇异点检测、可疑目的地址提取的多阶段 DDoS 攻击检测方法 MADOP。

第 6 章提出了一种基于包标记的 DDoS 攻击检测系统 Ddetector。主要针对现有的 DDoS 攻击检测方法主要利用控制平面传递局部检测的异常警报，全局检测设备往往根据异常警报内容给出最终决策，融合算法一般比较简单；当局部检测准确度不高时，整个系统的检测效率将非常低等问题。

针对 DDoS 攻击的手法推陈出新，利用挖矿木马、僵尸网络木马等技术，DDoS 攻击的黑色产业链条逐步实现了技术的自动化和操作的平台化，进一步降低了攻击门槛，第 7 章通过对 DDoS 僵尸网络木马样本的动态与静态进行综合分析，找到主机感染的挖矿木马病毒样本的特征，及时有效地总结出各类僵尸木马发作的特征、传播的手段，构建整套完整的针对个人和企业的解决方案。

第 8 章是对全书的总结和对未来的展望。