P2P网络安全及防御技术研究综述

刘 悦 李 强 李舟军
(北京航空航天大学计算机学院 北京 100191)

摘 要 基于P2P网络的各类应用逐渐占据了互联网应用中的重要地位,其采用的分布式结构在提供可扩展性和灵活性的同时,也面临着巨大的安全风险和挑战。首先概述了P2P网络的基本概念与特点,并说明了P2P系统与传统C/S结构系统的区别;随后详细介绍了目前对P2P网络威胁和影响最大的3种攻击方法:Sybil攻击、Eclipse攻击和DDoS攻击,指出了3种攻击方法的联系与区别;最后分别概述了针对这3种攻击方法相应的防御措施。

关键词 P2P网络,Sybil攻击,Eclipse攻击,DDoS攻击
中图法分类号 TP301 **文献标识码** A

Survey of P2P Network Security and Defense Mechanism

LIU Yue LI Qiang LI Zhou-jun
(School of Computer Science and Engineering, Beihang University, Beijing 100191, China)

Abstract The applications based on P2P networks have been playing an important role in the Internet. P2P networks with the distributed architecture are scalable and flexible while they are facing the enormous security challenges. This paper began with an overview of the concepts and features of the P2P network, and explained the difference between it and traditional C/S structure, then detailed the three popular methods of attack against the P2P networks: Sybil attack, Eclipse attacks and DDoS attack, and pointed out the relations and differences of the three kinds of attack, finally gave an overview of research on the defensive measures against the attacks.

Keywords P2P networks, Sybil attack, Eclipse attack, DDoS attack

1 引言

近年来,随着P2P[1,2](Peer-to-Peer)技术的日趋成熟,基于P2P网络的各种应用系统不断涌现和壮大。根据最新统计,目前同时在线用户数超过一百万的P2P文件共享网络有60余个,例如BitTorrent[3]、eMule[4]等;P2P流媒体服务是近几年成熟并迅速壮大的一项新技术,目前的大型网络如PPS[5]、PPLive[6]等的同时在线用户数也达到了数百万。另外,P2P技术在数据存储、数据库管理、Web搜索、网络缓存、网络电话等诸多领域都有重要应用。这些P2P网络系统在人们的网络体验中扮演了越来越重要的角色,甚至对人们的生活习惯乃至思维模式都具有不可忽视的作用。

P2P技术在自身发展与完善的同时,对全球的经济、政治、军事与文化都产生了重要影响,同时面临着来自多个方面的安全威胁。首先,P2P应用已经形成了一个完善的产业,许多IT服务公司利用P2P网络技术开发新产品,并实现了盈利;但是,P2P技术对传统版权管理机制的重大冲击使得传统经济实体的利益受损,而使其不断投入资金研发反P2P技术。其次,P2P应用对网络流量的大量占用,使其成为网络服务提供商(ISP,Internet Service Provider)的众矢之的,ISP也不断研发各种技术来过滤P2P流量。再次,由于P2P技术的无服务器特征,其共享信息可能涉及违法内容(如色情、暴力音像、军事、政治机密等),但却极易被无限制地传播,政府部门需要对其进行有效监管。另一方面,P2P技术的支持者一直在致力于研究各种有效手段,在保证其提供分布式服务的同时,提高其可靠性和安全性。

基于上述原因,近年来,P2P网络安全成为了一个新的研究热点。P2P技术存在的安全缺陷为网络攻击者提供了各种各样的机会。P2P网络面临的一些主要安全威胁有:由信息共享导致的知识产权纠纷、路由攻击、存取攻击、行为不一致攻击、目标节点过载攻击、穿越防火墙以及新型网络病毒的传播。研究者提出了若干的安全通信、信任管理等机制来防御上述攻击。但是由于P2P网络自身特性所限,P2P攻击和防御技术仍然是一个很有挑战的研究领域,同时也具有非常广泛的应用前景。充分研究P2P网络中各种可能的攻击和防御措施,对于实现有效的P2P网络监管尤为重要。

2 P2P网络概述

P2P网络是一种分布式网络,在这种网络中所有的节点

到稿日期:2012-09-22 返修日期:2012-11-07 本文受国家自然科学基金项目(90718017,60973105,61170189),教育部博士点基金(20111102130003)资助。

刘 悦(1988—),男,硕士生,主要研究方向为网络与信息安全,E-mail:lyue_061241@yahoo.cn;李 强(1982—),男,博士生,主要研究方向为网络与信息安全;李舟军(1963—),男,教授,博士生导师,主要研究方向为网络与信息安全、数据挖掘与文本挖掘。

是对等的，各节点具有相同的责任与能力以协同完成任务，每一个节点既能充当网络服务的请求者，又能对其他节点的请求做出响应。对等节点之间通过直接互联共享信息资源、处理器资源、存储资源甚至高速缓存资源等，无须依赖集中式服务器。

P2P 网络一般具有如下特点：

a)非中心化。网络中的资源和服务分散在所有节点上，信息的传输和服务的实现都直接在节点之间进行。

b)可扩展性。在 P2P 网络中，随着用户的加入，不仅服务的需求增加了，系统整体的资源和服务能力也在同步地扩展，理论上其扩展性几乎可以认为是无限的。

c)健壮性。由于服务是分散在各个节点之间进行的，部分节点在遭到破坏时对其它部分的影响很小。

d)隐私保护。在 P2P 网络中，由于信息的传输分散在各节点之间进行，而无需经过某个特定的中间环节，大大降低了用户的隐私信息被窃听和泄漏的可能性。

e)负载均衡。在 P2P 网络环境下，由于每个节点既是服务器又是客户机，减少了对传统 C/S 结构服务器计算能力、存储能力的要求，资源分布在多个节点，更好地实现了整个网络的负载均衡。

与传统 C/S 模式相比，P2P 网络弱化了服务器的功能，甚至取消了服务器。所有 P2P 节点在逻辑上是对等的，每个节点既充当服务器，为其他节点提供服务，也充当客户端，享用其他节点提供的服务。网络节点越多，P2P 网络的性能就越好、稳定性就越高。图 1 分别给出了 P2P 系统和 C/S 系统的结构示意图。

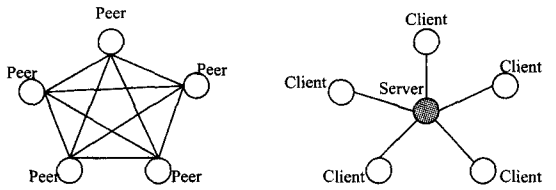

图 1　P2P 系统与 C/S 系统的结构示意图

3　P2P 网络攻击研究

P2P 网络是一种开放的、不受限制的网络，各 P2P 节点对整个网络的了解是十分有限的，每个 P2P 节点只需维护邻居节点的信息，并进行实时更新，就可以保证 P2P 网络的正常运行。所以，P2P 网络的安全问题也特别突出：恶意节点通过伪装自己，可自由加入或离开 P2P 网络，并可利用 P2P 节点的局限性来发动攻击或破坏网络的完整性。

目前，针对 P2P 网络的 Sybil 攻击[7-15]、Eclipse 攻击[16-22]、DDoS(Distributed Denial of Service，分布式拒绝服务)攻击[23-32]等的相关研究在国际国内获得了广泛关注。Sybil 攻击通过向 P2P 网络中引入多个恶意构造的节点来达到控制整个层叠网络的目的，它可以被用于监控发布和搜索流量、隔离特定共享内容等。Eclipse 攻击的目的是将若干个目标节点从 P2P 网络中隔离出去，劫持其通信信息，控制其网络行为。DDoS 攻击的目标是单个 P2P 网络节点，占用甚至耗尽其资源(如 CPU、带宽等)，使其不能正常提供服务。

3.1　基于 P2P 的 Sybil 攻击

Sybil 攻击最初是由 Douceur[7]在点对点网络环境中提出的，他指出这种攻击破坏了分布式存储系统中的冗余机制，并提出直接身份验证和间接身份验证两种验证方式。后来 Chris Karlof 等人[8]指出 Sybil 攻击对传感器网络中的路由机制同样存在着威胁。

Sybil 攻击，也称为女巫攻击，是指一个恶意结点非法地对外呈现出多个身份，通常把该结点的这些身份称为 Sybil 结点。Sybil 攻击方式主要有以下几种类型：直接通信、间接通信、伪造身份、盗用身份、同时攻击、非同时攻击。

在 P2P 网络中，用户创建新身份或者新节点是不需要代价的，攻击者可以利用这一漏洞发动 Sybil 攻击，伪造自己的身份加入 P2P 网络，在掌握了若干节点或节点身份之后，随意做出一些恶意的行为，例如误导正常节点的路由表，降低 P2P 网络节点的查找效率；或者在网络中传输非授权文件，破坏 P2P 网络中文件共享安全，消耗节点间的连接资源等，而且不用担心自己会受到影响。图 2 示出了在 P2P 网络中攻击者进行 Sybil 攻击的原理。

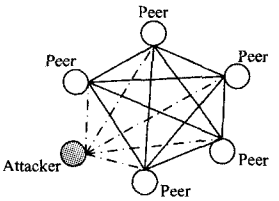

图 2　基于 P2P 网络的 Sybil 攻击原理

Sybil 攻击对 P2P 网络的攻击影响主要体现在以下几个方面：

a)虚假节点加入。在遵循 P2P 网络协议的基础上，任何网络节点都可以向 P2P 网络发送节点加入请求消息；收到请求消息的 P2P 节点会立即作出响应，回复其邻居节点信息。利用这个过程，Sybil 攻击者就可以获取大量的 P2P 网络节点信息来分析 P2P 网络拓扑，以便更高效地对 P2P 网络进行攻击或破坏。

b)误导 P2P 网络节点的路由选择。节点间路由信息的实时交互是保证 P2P 网络正常运行的关键因素之一。节点只需定时地向其邻居节点宣告自己的在线情况，就能保证自己被邻居节点加入到其路由表中。恶意的 Sybil 入侵者通过这个过程，可以入侵正常 P2P 节点的路由表，误导其路由选择，大大降低 P2P 节点的路由更新和节点查找效率，极端情况下，会导致 Eclipse 攻击。

c)虚假资源发布。Sybil 攻击者一旦入侵 P2P 网络节点的路由表，就可以随意发布自己的虚假资源。P2P 网络的目的是实现 P2P 用户间资源的分布式共享，如果 P2P 网络中充斥着大量的虚假资源，那么在 P2P 用户看来，这将是无法接受的。

3.2　基于 P2P 的 Eclipse 攻击

Moritz Steiner 等人[16]在 Kad 网络(最成功也是最流行的 P2P 应用之一)中提出了 Eclipse 攻击，并且给出了该攻击的原理。Eclipse 攻击是指攻击者通过侵占节点的路由表，将足够多的虚假节点添加到某些节点的邻居节点集合中，从而

将这些节点“隔离”于正常 P2P 网络之外。当节点受到 Eclipse 攻击时，节点的大部分对外联系都会被恶意节点所控制，由此恶意节点得以进一步实施路由欺骗、存储污染、拒绝服务以及 ID 劫持等攻击行为。因此，Eclipse 攻击对 P2P 网络的威胁非常严重。

P2P 网络的正常运行依赖于 P2P 节点间路由信息的共享。Eclipse 攻击者通过不断地向 P2P 节点发送路由表更新消息来影响 P2P 节点的路由表，试图使普通节点的路由表充满虚假节点。当 P2P 节点的路由表中虚假节点占据了较高的比例时，它对 P2P 网络的正常行为，包括路由查找或者资源搜索，都将被恶意节点所隔绝开，这也是这种攻击被称为月食攻击的原因。图 3 示出了在 P2P 网络中攻击者进行 Eclipse 攻击的原理。

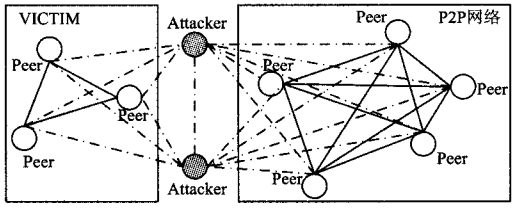

图 3　基于 P2P 网络的 Eclipse 攻击原理

Eclipse 攻击和 Sybil 攻击密切相关，它需要较多的 Sybil 攻击节点相配合。为了实现对特定 P2P 节点群的 Eclipse 攻击，攻击者必须首先设置足够多的 Sybil 攻击节点，并且向 P2P 网络宣称它们是“正常”的节点，然后使用这些 Sybil 节点与正常的 P2P 节点通信，入侵其路由表，最终把它们从 P2P 网络中隔离出去。

Eclipse 攻击对 P2P 网络的影响十分重大。对于 P2P 网络来说，Eclipse 攻击破坏了网络的拓扑结构，减少了节点数目，使得 P2P 网络资源共享的效率大大降低，在极端情况下，它能完全控制整个 P2P 网络，把它分隔成若干个 P2P 网络区域。对于受害的 P2P 节点来说，它们在未知的情况下脱离了 P2P 网络，所有 P2P 网络请求消息都会被攻击者劫持，所以它们得到的回复信息大部分都是虚假的，无法进行正常的 P2P 资源共享或下载。

3.3　基于 P2P 的 DDoS 攻击

DDoS 攻击是一种对 P2P 网络安全威胁最大的攻击技术之一，它指借助于 C/S 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攻击，从而成倍地提高拒绝服务攻击的威力。

传统的 DDoS 攻击分为两步：1）利用病毒、木马、缓冲区溢出等攻击手段入侵大量主机，形成僵尸网络；2）通过僵尸网络发起 DoS 攻击。常用的攻击工具包括：Trinoo、TFN、TFN2K、Stacheldraht 等。由于各种条件限制，攻击的第一步成为制约 DDoS 攻击规模和效果的关键。

近年来，研究人员通过潜心研发 P2P 技术和 DDoS 技术并将两者融合起来，成功研究出不需要建立僵尸网络即可发动大规模 DDoS 攻击的技术。该技术不仅成本低、威力巨大，而且还能确保攻击者的隐秘性。图 4 示出了在 P2P 网络中攻击者进行 DDoS 攻击的原理。

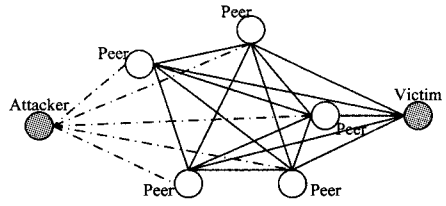

图 4　基于 P2P 网络的 DDoS 攻击原理

P2P 网络中具有数以百万计的同时在线用户数，这些节点提供了大量的可用资源，例如分布式存储和网络带宽。我们可以尝试利用这些资源作为一个发起大型 DDoS 攻击的放大平台。这种方式不必入侵 P2P 网络节点所运行的主机，只需要在层叠网络（应用层）中将其控制即可。理论上说，将 P2P 网络作为 DDoS 攻击引擎，如果该网络中有一百万个在线用户，则可以将攻击放大一百万倍甚至更多。

根据攻击方式的不同，基于 P2P 的 DDoS 攻击可分为主动攻击和被动攻击两种。基于 P2P 的主动 DDoS 攻击是通过主动地向网络节点发送大量的虚假信息，使得针对这些信息的后续访问都指向受害者来达到攻击效果的，具有可控性较强、放大倍数高等特点。这种攻击利用 P2P 协议中基于“推（push）”的机制，反射节点在短时间内会接收到大量的通知信息，不易于分析和记录，并且可以通过假冒源地址避过 IP 检查，使得追踪定位攻击源更加困难。此外，主动攻击在 P2P 网络中引入额外流量，会降低 P2P 网络的查找和路由性能；虚假的索引信息，会影响文件下载速度。

基于 P2P 的被动 DDoS 攻击通过修改 P2P 客户端或者服务器软件，被动地等待来自其它节点的查询请求，再通过返回虚假响应来达到攻击效果。通常情况下，会采取一些放大措施来增强攻击效果，如：部署多个攻击节点、在一个响应消息中多次包含目标主机、结合其它协议或者实现漏洞等。这种攻击利用了 P2P 协议中基于“取（pull）”的机制。被动攻击属于非侵扰式，对 P2P 网络流量影响不大，通常只能利用到局部的 P2P 节点。

3.4　小结

Sybil 攻击是 Eclipse 攻击成功实施的基础。Sybil 攻击的目标是单个物理节点在 P2P 网络上产生大量不同的身份，成功的 Sybil 攻击可以使发动 Eclipse 攻击变得更为容易。对单个节点进行 DDoS 攻击的前提是向 P2P 网络发布大量的虚假消息或被动地作出虚假响应，Eclipse 攻击可以帮助攻击者劫持网络节点间传递的信息，增大成功实施 DDoS 攻击的可能性。

Sybil 攻击只是冒充单个 P2P 网络节点，对 P2P 网络的影响是比较小的。Eclipse 攻击使得部分 P2P 节点脱离 P2P 网络，这对受攻击的节点来说是无法接受的。DDoS 攻击的目的是大量占用受害节点的资源，使其无法正常提供服务，因此 DDoS 攻击对 P2P 网络的影响是致命的。

4　P2P 网络安全防御研究

近年来，针对上述 P2P 网络的攻击方式，研究者提出了安全通信、信任管理等若干防御机制。

4.1　基于 P2P 的 Sybil 攻击防御研究

自从 Sybil 攻击出现以来，针对它的防御工作的研究一

直都没有中断过。对 Sybil 攻击的防御措施，大致可以归为以下几类：

a)信任认证。目前它被认为是防御 Sybil 攻击最通用的方法。通过一个授权中心，只有经过信任认证的节点才能加入 P2P 网络，共享和下载资源。Sepandar D. Kamvar 等人[9]最早提出了 EigenTrust 算法，其根据节点之间的信誉值，从网络中隔离信誉值较小的恶意节点，从而减小 Sybil 攻击的影响。Douceur[7]提出只有经过信任验证，才能完全消除 Sybil 攻击的影响，而且这是仅有的方法。Jean-Marc Seigneur 等人[10]根据信任度模型，提出了信任转移方法，即每个节点主动创建其邻居节点的信任度信息，节点在进行共享信息交换时，也交换节点的信任度信息，去除信任度低的节点。

b)资源测试。资源测试通过检测节点拥有资源(计算资源、存储资源、网络带宽等)的多少来验证节点的有效性，减弱 Sybil 攻击。George Danezis 等人[11]提出在使用 DHT 进行查询的过程中，尽量使用不同的节点集合，以确保至少有一部分查询结果是可用的，进而减缓 Sybil 攻击对网络性能的影响。Jochen Dinger 等人[12]基于稳定性和 ID 差异性等特点，对节点 ID 进行检测与分类，然后充分利用 P2P 网络的分布式特性，提出了一种名为 Self-Registation 的方法，以减缓 Sybil 攻击的可能性。

c)提高节点加入网络代价。通过限制节点的加入过程，例如只有具有一定计算能力的节点才能加入 P2P 网络，来减小 Sybil 攻击的可能性。王鹏等人[14]针对节点身份的认证方案，提出通过增加节点获取身份代价的方法，来尽可能地减少 Sybil 攻击。胡玲玲等人[15]基于小世界模型，提出了一种 Sybil 攻击防御机制，亦即将 Sybil 攻击团体的发现归结为最大流/最小割问题，引入虚拟节点并利用爬行器找到 Sybil 攻击团体，进而将其与 P2P 系统分开，从而减少 Sybil 攻击节点的数量，弱化 Sybil 攻击的影响。

4.2 基于 P2P 的 Eclipse 攻击防御研究

目前，大多数针对 Eclipse 攻击的防御措施主要体现在攻击检测、攻击容忍和攻击限制 3 种方法上。

a)恶意节点检测。Singh 等人[17]认为当拥有有限资源的恶意用户发动大范围的 Eclipse 攻击时，恶意节点的入度一般要高于网络中正常节点入度的平均值。基于这一事实，可以要求正常节点仅仅选择那些入度低于某一阈值的节点作为邻居节点，尽可能地限制恶意节点对正常节点的攻击。

b)攻击容忍，主要包括路由冗余与路由重置。Hildrum 和 Kubiatowicz[21]提出了一种通过在 Pastry 和 Tapestry 路由表中添加冗余表项的方法，来增加恶意节点占据路由表的难度，以减缓 Eclipse 攻击的危害。Castro 等人[20]提出了一种使用 2 个路由表进行路由的方法，一个路由表是优化路由表，另一个是验证路由表。通常情况下，节点优先使用路由效率相对较高的优化路由表进行路由，在路由检测失败的时候则依靠验证路由表通过安全冗余路由来重新进行路由。使用双路由表的方法由于优化路由表的毒化程度会不断加剧而具有一定的脆弱性，因此 Condie 等人[22]提出了一种通过诱发网络抖动来防御 Eclipse 攻击的方法，即周期性地将优化路由表重置为验证路由表，而在大部分情况下使用优化路由表进行路由更新。

c)攻击限制。Maccari 等人[18]提出一种通过外部验证服务来解决 Eclipse 攻击问题的方法，即通过使用验证服务来对节点 ID 进行签名，防止攻击者随意选择生成自己的节点 ID 并生成大量的节点，这样攻击者无法控制自己的节点在 ID 空间中的位置，亦无法侵占目标节点路由表的特定位置，也就无法成功实施 Eclipse 攻击。Awerbuch 和 Scheidelerd[19]提出不仅要对节点加入进行限制，还要对路由协议作出改进，要求网络中的所有消息都沿着特定的区域进行转发，以避免恶意节点产生的假消息在网络中传输。

4.3 基于 P2P 的 DDoS 攻击防御研究

基于 P2P 的 DDoS 攻击是一种应用层攻击，相对于网络层攻击而言，其更难于检测和防御。当前，针对基于 P2P 的 DDoS 攻击的防御技术主要包括基于验证的方法、基于成员管理的方法、基于信誉的方法和受害者端的方法。

a)基于验证的防御方法是指 P2P 节点收到任何消息后，首先通过一定措施验证消息中包含的地址是否有效，验证成功后再使用该信息。E. Athanasopoulos 等人[25]在直接验证的基础上，提出了安全列表机制，并通过 SEALING 算法计算安全列表。其核心是将直接验证失败的 IP 地址加入安全列表，之后针对该地址的访问都被忽略。X. Sun 等人[24]提出了直接验证和多点验证方法。直接验证是指节点获得节点 C 的信息后，直接发送消息到 C，以验证 C 的存在以及其是否能够对请求作出响应；多点验证中节点并不直接发送消息到 C，而是等到从其它 m 个节点中获得 C 的信息后再使用之。

b)基于成员管理的防御方法是指改进 P2P 系统的通信架构，改变成员间的合作关系，从而防御其被用来进行 DDoS 攻击。Yunhao Liu 等人[28]分析了无结构 P2P 网络内部的泛洪 DDoS 攻击，并提出针对“坏”节点的检测和防御机制 DD-POLICE，其基本思想是 P2P 网络的所有节点通过与其它 r 跳内邻居的协作来管理其直接邻居的查询行为，进而识别出可能的恶意节点。Daswani 等人[26]提出通过在极端节点层平衡查询流量来限制 Gnutella 的查询泛洪攻击。

c)基于信誉的防御方法是指在 P2P 节点之间建立信誉机制，根据交互历史和预期，确定节点消息的可信度。Jian Liang 等人[27]根据观察发现，攻击者会针对同一标题广播大量版本消息，并且每个攻击者容易使用相邻网段进行攻击，每个 P2P 节点自身维护本地信誉列表，忽略信誉值低的节点。另外，Yu Jie 等人[31]还提出可以将黑名单机制引入到信誉管理中。

d)受害者端的防御方法是指通过在受害者端采取和部署特定的防御措施，过滤攻击报文，来减轻其被攻击的影响。Jie Yu 等人[31]将应用层上的 DDoS 攻击进行抽象建模，并提出了在受害者端建立攻防结合的防御机制 DOW，其结合异常检测方法与代价方法，来降低攻击会话速率、攻击请求速率。Walfish 等人[35]提出了一种加速方法，该方法针对应用层 DDoS 攻击，以网络带宽作为代价，采用了以攻代守的策略，鼓励客户端发送更多请求。K. Cheung Sia 等人[29]认为网络管理员清楚下游主机具体提供了哪些服务，提出了在受害者端的上游路由器进行包过滤的方法。S. Ranjan 等人[30]提

出了由怀疑指派机制和 DDoS 弹回调度器组成的一种防御机制。

结束语 本文首先概述了 P2P 网络的基本概念与特点；然后重点介绍了目前对 P2P 网络安全威胁最大的 3 种攻击方法：Sybil 攻击、Eclipse 攻击和 DDoS 攻击；最后详细分析了针对这 3 种攻击的防御研究现状。

从上述分析来看，P2P 网络安全及其防御等各方面的技术尚未成熟，还存在许多问题亟待解决。同时，P2P 应用作为 Internet 上最流行和成功的网络应用之一，正处于不断的完善和发展之中，新的 P2P 网络安全及防御问题将无法避免。

参 考 文 献

[1] Maymounkov P, Mazières D. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric[C]// the First International Workshop on Peer-to-Peer Systems(IPTPS'02). 2002: 53-65

[2] Peer-to-Peer[OL]. http://en. wikipedia. org/wiki/Peer-to-Peer

[3] BitTorrent[OL]. http://www. bittorrent. org

[4] eMule[OL]. http://www. emule-project. net

[5] PPS[OL]. http://www. pps. tv

[6] PPLive[OL]. http://www. pplive. com

[7] Douceur J R. The Sybil attack[C]// Proceedings of IPTPS'02. 2002

[8] Chris, Wagner D. Secure routing in wireless senor networks: attacks and countermeasures[D]. Ad hoc Networks, 2003

[9] Kamvar S D, Schlosser M T, Garcia-Molina H. The EigenTrust Algorithm for Reputation Management in P2P Networks[J]. ACM 1-58113-680-6, 2003

[10] Seigneur J-M, Gray A, Jensen C D. Trust Transfer: Encouraging Self-Recommendations without Sybil Attack[C]// The Third International Conference on Trust Management iTrust. 2005

[11] Danezis G, Lesniewski-Lass C, Kaashoek M F, et al. Sybil-Resistant DHT Routing[C]// Computer Security - ESORICS. 2005

[12] Dinger J, Hartenstein H. Defending the Sybil Attack in P2P Networks: Taxonomy, Challenges, and a Proposal for Self-Registration[C]// ARES'06: Proceedings of the first International Conference on Availability, Reliability and Security, 2006

[13] Cornelli F, Damiani E, Samarati S. Implementing a reputation-aware gnutella servent[C]// Proc. Intl Wkshp on Peer-to-Peer Computing. 2002

[14] 王鹏，王琳，祝跃飞. 在 P2P 网络下 Sybil 攻击的研究与防御[J]. 微电子学与计算机，2006，23(4)：162-165

[15] 胡玲玲，杨寿保，王菁. P2P 网络中的 Sybil 攻击的防御机制[J]. 计算机工程，2009，35(15)：121-123

[16] Steiner M, En-Najjary T, Biersack E W. Exploiting KAD: Possible Uses and Misuses[J]. Computer Communication Review, 2007, 37(5)

[17] Singh, Ngan T, Druschel P, et al. Eclipse attacks on overlays: Threats and defenses[C]// Proceedings of INFOCOM'06. 2006

[18] Maccari L, Rosi M, Fantacci R, et al. Avoiding eclipse attacks on Kad/Kademlia: An identity based approach[C]// Proceedings of the IEEE International Conference on Communications. Piscataway, USA: IEEE Press, 2009

[19] Awerbuch B, Scheideler C. Towards a scalable and robust DHT [C]// Proceedings of the 18th Annual ACM Symposium on Parallelism in Algorithms and Architecture. New York, USA: Association for Computing Machinery, 2006

[20] Castro M, Druschel P, Ganesh A, et al. Secure routing for structured Peer-to-Peer overlay networks[C]// Proceeding of the 15th Symposium on Operating Systems Design and Implementation. New York, Association for Computing Machinery, 2002

[21] Hildrum K, Kubiatowicz J. Asymptotically efficient approaches to fault-tolerance in Peer-to-Peer networks[C]// Proceedings of the 17th International Symposium on Distributed Computing Lecture. Berlin, Germany: Springer-Verlag, 2003

[22] Condie T, kacholia V, Sankaraman S, et al. Induced churn as shelter from routing table poisoning[C]// Prodeedings of the 13th Annual Network and Distributed System Security Symposium. San Diego, USA: the Internet Society, 2006

[23] Mirkovic J, Dietrich S, Dittrich D, et al. Internet Denial of Service: Attack and Defense Mechanisms[R]. Prentice Hall PTR. 2004

[24] Sun X, Torres R, Rao S. DDoS Attacks by Subverting Membership Management in P2P Systems[C]// NPSec. 2007

[25] Athanasopoulos E, Anagnostakis K, Markatos E. Misusing Unstructured P2P systems to Perform DoS Attacks: The Network That Never Forgets[C]// Proc. ACNS. 2006

[26] Daswani N, Garcia-Molina H. Query-flood dos attacks in gnutella networks[C]// ACM Conference on Computer and Communications Security. 2002

[27] Liang Jian, Naoumov N, Ross K W. The Index Poisoning Attack in P2P File Sharing Systems[C]// IEEE Conference on Computer Communication. Barcelona, Spain, April 2006

[28] Liu Yun-hao, Liu Xiao-mei, Wang Chen, et al. Defending P2Ps from Overlay Flooding-based DDoS[C]// ICPP 2007. 2007

[29] Sia K C. DDoS Vulnerability Analysis of Bittorrent Protocol [R]. UCLA Tech. Report. Spring 2006

[30] Ranjan S, Swaminathanm R, Uysal M, et al. DDoS-Resilient Scheduling to Counter Application Layer Attacks under Imperfect Detection[C]// INFOCOM'06. 2006

[31] Yu Jie, Li Zhou-jun, Chen Huo-wang, et al. A detection and offense mechanism to defend against application layer DDoS attacks[C]// The Proceedings of the 3rd International Conference on Networking and Services. 2007

[32] Yu Jie, Fang Cheng-fang, Li Zhou-jun, et al. Mitigating Application Layer DDoS Attacks Via Leightweight and Effective Trust Management[J]. IET Communications, 2010, 4(16): 1952-1962

[33] Yu Jie, Fang Cheng-fang, Lu Li-ming, et al. A Lightweight Mechanism to Mitigate Application Layer DDoS Attacks[C]// The 4th International ICST Conference on Scalable Information Systems(INFOSCALE'09). Hong Kong, China, June 2009

[34] Yu Jie, Li Zhou-jun, Chen Xiao-ming. Misusing Kad protocol to perform DDoS attacks[C]// The 6th IEEE International Symposium on Parallel and Distributed Processing and Applications (ISPA'08). Sydney, Austrilia, December 2008

[35] Walfish M, Vutukuru M, Balakrishnan H, et al. DDoS defense by offsense[C]// The Proceedings of SIGCOMM'06. 2006