对等网络泛洪DDoS攻击的防御机制

耿 技，马新新

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】研究Gnutella协议的P2P网络中DDoS攻击，提出一种分布式的基于节点标识识别和节点流量实时检测过滤的自适应性DDoS攻击防御机制。通过在节点本地构建的信任和信誉机制对恶意节点主动阻断及对消息包的DDoS攻击特征的实时检测策略，实现对DDoS攻击的防范。仿真实验结果表明，该机制能有效地隔断网络中75%恶意消息数，节点能阻断80%的恶意消息数的转发，提高了网络抵御DDoS攻击的效能。

关 键 词 分布式拒绝服务攻击； 流量过滤； Gnutella协议； 负载均衡； 对等网； 信任和信誉

中图分类号 TP393.08 **文献标识码** A doi:10.3969/j.issn.1001-0548.2009.06.020

Mechanism of Defending P2P from Flooding-Based DDoS Attack

GENG Ji and MA Xin-xin

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract A distributed self-adaptive defense mechanism based on peer identification and real-time flow filtering is proposed in this paper under the research of DDos attacks in P2P network which is established on Gnutella protocol. In this mechanism, peers in such network can actively block the connection with malicious nodes by building local trust and reputation mechanism and keep away DDos attacks through real-time detection of the characteristic of DDos attack. Simulation result shows that our proposed distributed defense mechanism against DDos attacks can effectively improve the network resistance by obstructing 75% of the malicious messages and blocking 80% of the retransmission of them.

Key words DDoS; flow filtering; Gnutella; load balancing; P2P; trust and reputation

对等网技术(P2P)作为一种新型的基于应用层的通信和计算模型，是以现有Internet物理网络结构为基础构建的逻辑网络，具有可扩展性、鲁棒性、容错性和自组织性等特性[1]。网络中的每一个节点既可以向其他节点请求信息或服务，又可为其他节点提供信息或服务。充分利用网络边缘的用户资源，实现用户间的直接通信、信息对象的共享和互换，加快资源的搜索定位和下载，提供海量数据的存储，因而在协同计算、分布式存储和文件信息共享等领域得到极快的应用。

但P2P网络具有的如匿名性、动态性和开放性等为用户提供便捷的特性，却可能成为恶意用户入侵、破坏网络、发动攻击行为的安全隐患。如利用节点都具有路由转发的能力，恶意节点可随意更改路由转发信息、丢弃信息；将木马程序等恶意代码伪装成热点信息提供给网络中的其他节点下载；伪造大量不存在的节点标识和目的不可达信息，针对网络中某一节点甚至整个网络发动DDoS攻击。而产生上述安全隐患的主要原因是对等技术在最初设计时假定节点间是彼此信任的，以及节点间共享的资源是真实可靠的，将网络中的安全策略、方案由低层的网络层进行处理。但实际的P2P网络中，各节点基于同一兴趣自主的处理与其他节点的交互，节点间彼此是陌生的，可随意地加入或退出网络，节点的状态不确定，标识不唯一，对其个人行为后果没有任何责任可言。网络层的安全策略并不能应用于基于应用层的P2P网络，造成P2P网络易受DDoS攻击，并成为DDoS攻击其他系统的极好平台。

目前，根据对等网的路由搜索机制和网络逻辑拓扑结构特性可将P2P网络划分为集中式结构、非结构化分布式结构和结构化分布式结构3类[2]。在这3种结构中，以非结构化分布式结构的P2P网络如Gnutella的应用最为广泛，且该结构的P2P网络又最易受到DDoS攻击。因此，本文认为针对Gnutella的DDoS攻击防御机制的研究具有代表性，所取得的研究结果能很好地运用于其他结构的P2P网络中。

收稿日期：2008－08－29；修回日期：2009－05－04
基金项目：国家自然科学基金(60473090)
作者简介：耿 技(1963－)，男，教授，主要从事分布式处理、对等计算和网络与信息安全方面的研究.

1 Gnutell的P2P网络中的DDoS攻击

1.1 Gnutell的P2P网络中的DDoS攻击分析

Gnutell协议P2P网络中的DDoS攻击是一种基于应用层的DDoS攻击。与已有基于网络层的DDoS攻击相比，基于Gnutella的DDoS攻击无需事先控制一批傀儡主机，恶意节点只需向网络发送无用或恶意的消息包，利用其他节点的复制转发就能发起攻击。而造成攻击易发生的原因是由Gnutell协议的P2P网络的本身特性决定的。

(1) 恶意节点在基于Gnutella协议的P2P网络中发起DDoS攻击的操作简单，泛洪路由查询机制为DDoS攻击的扩散、传播提供了绝好的手段。(2) 恶意节点借助于泛洪机制进行DDoS攻击过程中，对查询消息包进行查询源地址的伪造或对转发的消息包进行重定的过程符合Gnutella协议的规约，无畸形的消息构造包、基于底层的TCP/IP协议也均是正常的消息传输，没有基于网络层的DDoS攻击过程所表现出来的具有一定特征的攻击模式，特征匹配检测对基于Gnutella的应用层DDoS攻击失效。(3) 基于Query/Query Hit消息机制进行共享资源查询，收到Query查询消息的任意节点“忠实”地在本地进行查询资源的查找，给出查询结果的回应或继续向网络中进行复制转发，对查询消息的真实性、查询消息来源节点的可信性不作判断。这种不加识别的接收来自恶意节点的无用查询消息，一方面消耗节点自身有限的资源，另一方面又将这些无用查询消息复制转发到其邻居节点，从而进一步消耗网络中其他节点的资源和计算处理能力，促使DDoS攻击的进一步扩散和传播。(4) 正常情况下只有当节点存储有匹配Query消息的资源时，节点才能够回复Query Hit消息。但恶意节点会对Query消息和回应的Query Hit消息包内容进行篡改，伪造大量不存在的节点标识和目的不可达信息，而Query/Query Hit消息交换由于没有采用消息完整性保护机制，缺乏对回应节点回传的Query Hit消息的进行验证的手段或策略，对回应节点也没有可信确认机制，从而无法保证Query Hit消息中的IP地址和端口号就是回复该Query Hit消息节点的IP地址和端口号。事实上，恶意节点可以对收到的每一个Query消息回复Query Hit消息，并且把它欲攻击的节点或虚构的IP地址和端口号填入QueryHit消息中。(5) P2P网络中各节点通信的匿名特性，使网络中无知的良性行为的节点在不知晓的情况下帮助恶意节点，对恶意消息进行转发，实现恶意信息的扩散，促使DDoS攻击发生。

1.2 DDoS攻击防范技术的分析

目前，针对DDoS攻击防范的研究主要有攻击阻断、流量识别与攻击源回溯、攻击类型检测和过滤[3]等3类。

DDoS攻击阻断的主要目的，就是针对DDoS攻击的发生需要事先入侵、控制大量傀儡机的特性，对可能受到攻击的系统进行漏洞补丁升级和病毒实时扫描，力图在DDoS攻击发生前就阻断DDoS攻击[4]。这种防范技术手段是基于对DDoS攻击的特性已掌握的前提，但基于Gnuella协议的P2P网络是节点基于共同兴趣构成的数目庞大的网络，很难保证网络中每一个节点都能抵御DDoS攻击，而且在P2P网络中小部分的恶意节点就能发起DDos攻击。

DDoS攻击类型的识别和回溯方法主要是针对DDoS攻击发生后所采取的策略和方法[5]。通常，回溯是基于IP地址的回溯，通过对消息包存储转发的路由器追踪和识别发起DDoS攻击的源地址，或通过发送特别的追踪回溯包获取攻击者的位置。但在基于Gnutella协议的P2P网络中，恶意节点发起DDoS攻击的查询消息包中没有发起节点的IP地址，而且节点间匿名通信的特性也使获取发起节点标识变得困难。

DDoS攻击类型的检测和过滤主要是针对可能发生的DDoS攻击事件进行实时检测，并对检测到的攻击进行响应[6]。常用的检测、过滤策略是针对受保护的系统，检测进出该系统的流量并进行有针对性的过滤以阻止假冒IP地址流量的数据包进出系统。但这种防范技术手段通常是在受防护的系统边界进行实时检测和过滤，而P2P网络是基于物理网络层上构建的逻辑网络，网络中各节点地位对等，每一个节点自主进行路由转发功能，没有明确的系统边界，因此，基于系统边界进行攻击的检测过滤无法应用于P2P网络。

上述对DDoS攻击防范技术的分析，得出的已有应对DDoS攻击的技术、防范手段都是基于网络层的DDoS攻击，无法适用于基于Gnutella应用层的DDoS攻击。因为基于Gnutella的DDoS攻击过程中，消息包的底层以正常的TCP连接和IP分组为前提，没有基于网络层DDoS攻击的标志特征(如TCP半开放连接或畸形IP数据报等)。攻击发生时，除了消息包的传输方向被重新定向外，所有的消息包都是合法的。因此能穿越所有基于IP层和TCP层的检测系统。由于已有防范方法无法识别基于Gnutella的泛洪的流量中是否隐藏有DDoS攻击流，且危害极大、隐藏性

极强，很难检测，需要设计一种针对基于Gnutell协议的P2P网络中DDoS攻击的防御机制，抵御基于应用层的DDoS攻击造成的危害。

针对Gnutella协议的P2P网络中的DDoS攻击，本文提出一种分布式的、基于节点标识识别和节点流量实时检测的过滤机制。通过在节点本地构建的信任和信誉机制，对恶意节点主动阻断与对消息包的DDoS攻击特征的实时检测过滤防御机制相结合，构建一种自适应性的抵御DDoS攻击的防范机制。

2　分布式防御机制

本文提出的分布式防御机制由两部分组成：(1) 基于节点信任和信誉机制；(2) 基于节点流量实时检测过滤策略。其中基于节点信任和信誉机制[7]是针对查询消息机制中DDoS攻击的发生是由于节点不可信、共享资源内容不可靠的分析结果，通过节点间的确定的信任关系，对邻居转发的查询消息的来源节点的可信度进行的判断，当消息是来自不可信的节点，节点直接阻断对该消息的转发，从而对恶意节点进行隔离，事先控制恶意行为的传播。

节点的信任和信誉机制采用本文提出的马尔科夫随机过程模型[8]对节点的行为进行计算。根据计算结果，节点得出与之进行过交互活动后的节点信任表和不信任表。当节点收到其邻居节点发来的消息包后，首先对消息包的来源节点标识的可信进行判定，比较不信任表中节点的标识信息。若节点被判定为不信任，则直接阻断与节点的链接，否则放行该消息包，进入下一步的流量实时检测。采用不信任节点的黑名单而非信任节点的白名单，是基于在P2P网络中恶意节点为隐藏自身恶意行为，有可能事先伪装成正常节点做可信的行为，但这种可信行为有可能转变为恶意行为。恶意行为肯定是恶意节点发起的行为，因此采用不信任节点的黑名单对来源节点的标识进行识别，作为对恶意行为节点的惩罚，从而对名单外的节点进行实时检测。

对节点收到的消息包进行实时检测过滤，是针对Gnutella协议的P2P网络中恶意节点利用泛洪查询机制发起的DDoS攻击是通过恶意节点向其邻居节点发送无用或恶意的消息，借助其邻居节点向网络中其他节点复制转发这些无用或恶意的消息的特性，在对节点可信判断完毕后，对消息包的DDoS攻击特征进行分析。由于Gnutella协议P2P网络的消量类型中绝大部分来自Query消息[9]，因此主要对该消息的来源进行检测过滤。

基于Gnutella协议的P2P网络中，Query泛洪的攻击包除了流量异常外，与正常消息包没有本质区别，可以对消息包的来源节点标识和TTL两个特征值的组合进行判断，在节点间建立一种分布式检测过滤策略。当节点接收到来自其邻居节点的查询消息时，不是对该消息进行复制转发，而是对该消息流量进行统计识别，当在一时间段内接收到某一邻居节点发送过来的消息量超过事先设定的阈值时，即判定消息包来自同一TTL半径，且是同一来源节点持续发送消息包数量达到事先设定的下限值K时，判定该节点的消息包是DDoS攻击特征包。该下限值的设定根据攻击包的数量和节点对服务效率的权衡得出，即在某一时间段收到来自同一节点的消息包数量达到K时，就判定该消息为攻击包。文献[10]通过实际的网络观察指出实际网络中任意节点平均每分钟发出的查询消息数不超过1条。而文献[3]通过实验结果得出网络中节点每分钟产生的查询消息数不超过40。本文提出在一段时间内同一节点连续的消息包达到服务效率的20%时，即K值为8时，判定该消息包为攻击包，对该节点的消息进行丢包策略。

丢包策略首先是对该节点的消息进行减半转发，这是对可能的DDoS攻击效能进行减缓；其次，继续对该节点的消息包进行检测，若下一个时间段内该节点的消息包仍是DDoS特征包，则在原有基础上持续对该节点的消息包进行减半转发，直至对该消息包的转发减至每次只转发一个包。若下一个时间段内该节点的消息包是DDoS特征包，且消息包的数量达到或超过服务效率的80%，即S值为32时，判定该节点为恶意节点，阻断对该节点的链接，并将该节点的标识存储于本地的信任和信誉的不信任节点黑名单。若下一个时间段内该节点的消息包数量不再是DDoS攻击包的特征，则说明DDoS攻击减缓或该节点的行为正常，则每次转发增加1个消息包。

通过在节点间建立分布式的DDoS攻击防御机制，以事先主动阻断和实时检测过滤相结合的技术手段，达到从恶意节点的最近处进行识别，隔止恶意消息的转发，防范DDoS攻击的目的。本文提出的分布式自适应DDoS防御机制流程如图1所示。对该机制流程的步骤描述如下：

步骤(1) 节点对消息包的来源节点标识与存储于本地信任和信誉列表的可信节点进行比较，若该来源节点标识判定为不可信，则转入步骤(5)；否则转入步骤(2)。

步骤(2) 对收到的消息包根据标识特征进行识

别，若不匹配DDoS攻击特征转入步骤(6)；否则转入步骤(3)。

步骤(3) 对DDoS攻击特征匹配的消息包进行丢包策略处理，转入步骤(4)。

步骤(4) 对与DDoS攻击特征匹配的消息进行丢包策略处理后的消息包进行判断，判断该消息包数量是否达到事先设定的上限，若未达到转入步骤(2)；否则转入步骤(5)。

步骤(5) 对进入的消息包对应的来源节点进行阻断链接处理，并将恶意节点的标识存入本地信任和信誉列表，转入步骤(6)。

步骤(6) 结束。

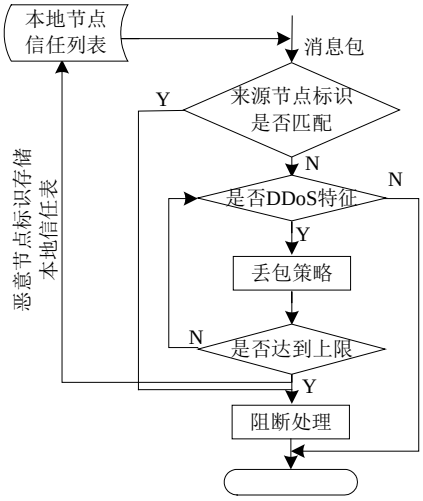

图1 分布式DDoS攻击防御机制流程图

本文提出的分布式DDoS攻击防御机制涉及的算法描述如下：

If(Pakcet(ID)==List(ID))

//消息包的来源节点标识可信判断

Dis(Paket(ID))

//调用阻断处理

end if

else

if(Packet(ID)是新来源节点的消息包)

if(Packet(ID,TTL)≧K)

//连续的包数量达到事先设定丢包策略的下限值K

$N_{\text{连续收到与DDoS攻击特征匹配的包}}=N_{\text{连续收到与DDoS攻击特征匹配的包}}/2$

Dr(Packet(ID,$N_{\text{连续收到与DDoS攻击特征匹配的包}}$))

//调用丢包策略

end if

end if

else

if ($t==\tau$)

//在设定时间到达时判断收到来自同一节点的消息包的数量

if($N_{\text{连续收到与DDoS攻击特征匹配的包}}<Q$)

//来自同一节点标识的消息数量降低至设定的下限Q则调整该节点的消息的转发数量，在丢包策略的基础上每次多转发新收到的1个消息包

$N_{\text{连续收到与DDoS攻击特征匹配的包}}=N_{\text{连续收到与DDoS攻击特征匹配的包}}+1$

if($Q<N_{\text{连续收到与DDoS攻击特征匹配的包}}<S$)

$N_{\text{连续收到与DDoS攻击特征匹配的包}}=N_{\text{连续收到与DDoS攻击特征匹配的包}}/2$

Dr(Packet(ID,$N_{\text{连续收到与DDoS攻击特征匹配的包}}$))

//调用丢包策略

end if

else

//若来自同一节点的消息包数量在丢包后持续上升达到丢包策略的上限值

Dis(Packet(ID))//调用阻断处理

end else

end if

end else

3 仿真实验及结果分析

仿真实验是在基于Peersim开放源代码的仿真平台实现Gnutella(ver0.4)协议的P2P网络，查询方式以泛洪方式进行，网络中各节点对位平等，网络拓朴结构随意，没有超级的节点结构。仿真实验各参数的设置如表1所示。

表1 仿真实验参数设定

参数名称	数 值
网络节点数	2 000
节点邻居数	3
消息的TTL	3
信息文件数	2 000

此外，针对Gnutell网络的查询消息在节点间进行转发时，转发节点将接收节点的标识存于本地，而将自身节点标识替代接收节点后进行转发，无法获取来源节点的标识。实验中对Query消息包进行扩展，Query消息包括头描述符、最低网速和搜索条件字段。其中，头描述符中指定消息的唯一标示、消息的类型描述符、消息的TTL和Hops、消息负载的长度。由于Query消息没有负载，所以负载长度字段为空。本文以负载长度字段作为分隔符来源节点标识字段，再以一空字段作为分隔其与最低网速和搜索条件字段，实现对Query消息的扩展。当某一节点发送查询消息时，其邻居节点首先会判断该字段是否为空，为空则将来源节点的标识字段添加，将自

身标识对来源节点标识进行替换后转发。Query消息包的重构结构如图2所示。

消息头描述符	来源节点ID		最低网速	搜索条件

图2　Query消息扩展结构图

实验中，当节点对查询消息复制转发时，首先将查询消息的来源字段标识缓存于本地缓存列表中，将自身标识替代来源标识，向其邻居节点进行复制传送，这说明节点收到的查询消息的标识都是来自邻居节点。基于此，实验中针对每个时间周期在节点进行复制转发处理前，针对每个邻居节点发送来的消息进行缓存，并对消息量进行统计，当来自某一邻居节点的查询消息量超过事先设定的阈值8时，该节点被确定为可疑节点，对确定为可疑邻居节点的消息转发量降低为50%，并优先将其他2个正常邻居节点的消息从各自的缓存区中取出放入转发消息队列中进行复制转发。同时，对判定为可疑节点的查询消息量进行统计检则，当下一个时间周期到来时，该可疑节点的查询消息量持续增长，则判定该节点为恶意节点，将其从本地邻居节点列表中删除，切断与该节点的链接。由于恶意节点发起DDoS攻击是借助与其直接相连的邻居节点将恶意消息发送到网络中，恶意节点尽其所有的计算资源和处理能力发送无用或恶意的消息，以尽可能快地达到DDoS攻击的效果，也为节点通过流量实时检测识别恶意节点提供了可靠依据。

本文分别针对无防御机制条件下恶意节点发起DDoS攻击和采用防御机制条件下恶意节点发起DDoS攻击2种不同的环境下进行仿真实验。实验结果如图3、图4所示。

图3中，由下向上的2条曲线分别表示采用防御机制的DDoS攻击和无防御机制的DDoS攻击。对比两种不同条件下DDoS攻击网络中的恶意消息总数，无防御机制条件下网络中恶意消息总数是采用防御机制网络中恶意消息总数的4倍，说明恶意节点利用Query泛洪查询机制发起DDoS攻击，引发网络中产生大量的无用消息。启动DDoS防御机制可以将攻击产生的无用消息量明显降低75%。此外，从图中可以看出两条曲线在第2个时间周期发生拐点，说明防御机制启动，对恶意消息进行丢弃，对恶意节点进行阻断。

图4中，曲线分布与图3一致，表示2种不同网络环境下，网络中节点收到恶意消息对比。比较曲线走势可以得知，采用防御机制后恶意节点发起DDoS攻击，节点在第3个时间周期启动防御机制将恶意消息数降低80%。通过对网络中恶意消息总数和节点收到恶意消息总数的实验结果分析，说明在节点间建立分布式的DDoS攻击防御机制能有效阻断恶意消息的扩散，阻止恶意节点利用Query泛洪查询消息机制进行DDoS攻击。

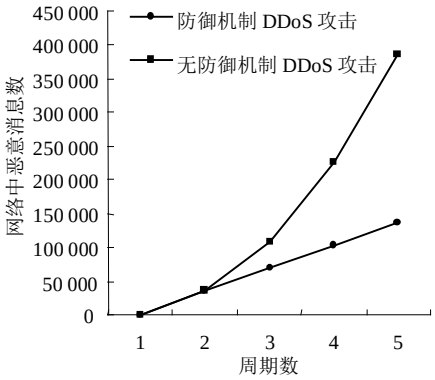

图3　防御机制防范DDoS攻击对比

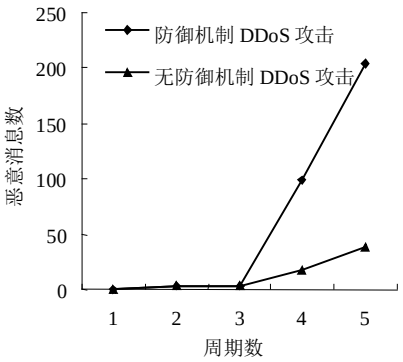

图4　防御机制节点收到恶意消息数对比

4　结 束 语

基于Gnutella协议的P2P网络中，Query/Query Hit消息的泛洪查询机制中没有对消息内容的确认机制，因而易被恶意节点利用发起基于应用层的DDoS攻击，使该体系结构极易受到DDoS的攻击并进一步成为危害Internet网络的攻击平台。已有的针对DDoS攻击的防范技术主要是网络层，不能应用于对基于应用层的DDoS攻击的防范，需要设计一种针对基于Gnutell协议的P2P网络中DDoS攻击的防防御机制，抵御基于应用层的DDoS攻击造成的危害。

本文针对Gnutella协议的P2P网络中DDoS攻击特性，提出一种分布式的基于节点标识识别和节点流量实时检测过滤的自适应性DDoS攻击防御机制。通过在节点本地构建的信任和信誉机制对恶意节点主动阻断及对消息包的DDoS攻击特征的实时检测策略，实现对DDoS攻击的防范。仿真实验结果表明，

本文提出的分布式DDoS攻击防御机制能有效地隔断网络中75%的恶意消息，节点能阻断80%的恶意消息的转发，提高网络抵御DDoS攻击的效能。

参 考 文 献

[1] SRIPANIDKULCHAI K. The popularity of gnutella queries and its implications on scalability[C]//Proceedings of International Conference on Peer-to-peer Computing. Linköpings universitet, Sweden: ACM Press, 2001.

[2] NAOUMOV N, ROSS K W. Exploiting P2P systems for DDoS attacks[C]//International Workshop on Peer-to-Peer Information Management. Hong Kong, China: IEEE Press, 2006.

[3] LIU Y H, WANG X M, LI X. Defending P2Ps from overlay flooding-based DDoS[C]//International Conference on Parallel Processing. Xian, China: IEEE Computer Society, 2007.

[4] CHANG R K C. Defending against flooding-based distributed denial-of-service attacks: a tutorial[J]. IEEE Communications Magazine, 2002, 51: 42-51.

[5] SAVAGE S, WETHERALL D, KARLIN A A. Practical network support for IP traceback[C]//Proceedings of ACM SIGCOMM. Stockholm, Sweden: Communications of the ACM, 2000.

[6] Request for Comments: 2827. Network ingress filtering: defeating denial of service attacks which employ ip source address spoofing[EB/OL]. [2008-06-25]. http://www.ietf.org/rfc/rfc2827.txt.

[7] 马新新，耿 技. 对等网络信任和信誉机制研究综述[J]. 计算机应用, 2007, 27(8): 1935-1941.
MA Xin-xin, Geng Ji. Survey of trust and reputa tion mechan ism on P2P network[J]. Computer Applications, 2007, 27(8): 1935-1941.

[8] MA Xin-xin, QIN Zhi-guang. The markov-based evaluation on trust and reputation in Peer-to-Peer[C]//International Conference on Communications, Circuits and Systems Proceedings. Guilin, China: IEEE Press, 2006.

[9] DASWANI N H. GARCIA-MOLINA. Query-flood Dos attacks in gnutella[J]. ACM Computer and Communications Security, 2002, 65: 181-192.

[10] JIANG H, JIN S. Exploiting dynamic querying like flooding techniques in unstructured peer-to-peer networks [C]//IEEE International Conference on Network Protocols. Boston, MA, USA: IEEE Computer Society, 2005.

编 辑 蒋 晓

(上接第974页)

[6] CRISTIANINI N, SHAWE-TAYLOR J. An introduction to support vector machines and other kernel-based learning mechods[M]. Beijing: Publishing House of Electronics Industry, 2000.

[7] 胡寿松. 自动控制原理[M]. 第3版. 北京: 国防工业出版社, 1994.
HU Shou-song. Principles of automatic controll[M]. 3rd ed. Beijing: National Defense Industry Press, 1994.

[8] LEE J Y, HUANG X, ROHRER R. A pole and zero sensitivity calculation in asymptotic waveform evaluation[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 1992, 11(5): 586-597.

[9] NIKOLOVA N K, BANDLER J W, BAKR M H. Adjoint techniques for sensitivity analysis in high-frequency structure CAD[J]. IEEE Transactions on Microwave Theory and Techniques, 2004, 52(1): 403-419.

[10] HSU C W, LIN C J. A comparison of methods for multiclass support vector machines[J]. IEEE Transactions on Neural Networks, 2002, 13(2): 415-425.

[11] HSU C W, CHANG C C, LIN C J. A practical guide to support vecor classification[EB/OL]. [2007-09-19]. http://www.csie.ntu.edu.tw/~cjlin/papers/guide/guide.pdf.

[12] KAMINSKA B, ARABI K, BELL I, et al. Analog and mixed-signal benchmark circuits-first release[C]// Proceedings of the 1997 IEEE International Test Conference. Washington D C, USA: 1997: 183-190.

[13] ALIPPI C, CATELANI M, FORT A, et al. Automated selection of test frequencies for fault diagnosis in analog electronic circuits[J]. IEEE Transactions on Instrumentation and Measurement, 2005, 54(3): 1033-1044.

编 辑 蒋 晓