伪装IP追踪技术综述

李毅超 王 钰 夏梦芹 曾家智
(电子科技大学计算机科学学院 成都610054)

A Survey on Marked IP Traceback

LI Yi-Chao WAMG Yu XIA Meng-Qin ZENG Jia-Zhi
(College of Computer Science, UESTC 610054)

Abstract More and more serious network attack makes it more impending to find out the source of attacker. In this paper, we analyze the status in development of methods such as ICMP traceback, marking packet, hop by hop, IPsec authentication and connection chain. We also put forward the tendency of marked IP traceback.

Keywords IP traceback, ICMP, IPsec authentication, Connection chain, Hop by hop

1 引言

网络协议和操作系统的缺陷导致了网络的安全问题。有关IP协议最重要的问题是IP地址的伪装。IP协议本身无法验证源地址段中的IP地址是发送者的IP地址。一台机器可以在一段时间内将自己伪装成另一台机器甚至路由器。对网络攻击各种各样的解决办法中IP追踪(traceback)是一种重在威慑的方法，一旦攻击者知道攻击能被追溯，进行攻击时会更慎重。在美国、日本等发达国家伪装IP追踪技术已成为学术界、企业界和政府部门普遍关心的重要问题之一。

2 主要技术路线及发展现状

对伪装IP追踪的研究主要集中在以下几个方向。

2.1 ICMP追踪技术(ICMP trace，简称iTrace)

这是一种利用ICMP消息进行追踪的技术。路由器产生一个包含被转发分组的部分信息的ICMP追踪消息，并将该消息发送到分组的目的地[3]，如图1[8]所示。通过寻找相应的ICMP追踪消息并检查它的源IP地址可以确定分组穿越的路由器。因为每个分组产生ICMP消息会增加网络通信量，所以每个路由器以1/20000的概率产生ICMP消息。在洪泛型攻击(flood-type attack)中，被攻击网络能收集到足够的ICMP追踪消息来构造攻击路径。

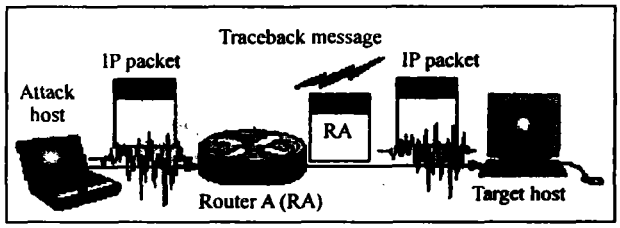

图1 ICMP traceback message

该技术的主要缺点是：路由器以1/20000的概率产生iTrace分组，故数量很小。对于分布式拒绝服务DDOS(Distributed denial of service)[1]情况，若每个从攻(slave)只产生小数量的攻击量，那么附近路由器选取恰当分组的概率就很小，也就是说，离受害者较近的路由器，因为接受的攻击量比较集中，发送能到达受害者的iTrace分组的概率就比较高，相反，离从攻较近的路由器发送能到达受害者的iTrace消息的概率却很低。因此，实际有用的ICMP分组数很小。故该ICMP追踪方法用于DDOS时效率很低。

文[6]等针对ICMP追踪存在的问题，提出了一种"意图驱动"的ICMP追踪("intension-driven"iTrace)的改进方法。这种方法可对付DDOS攻击。该方法采用了如图2所示的DDOS模型。

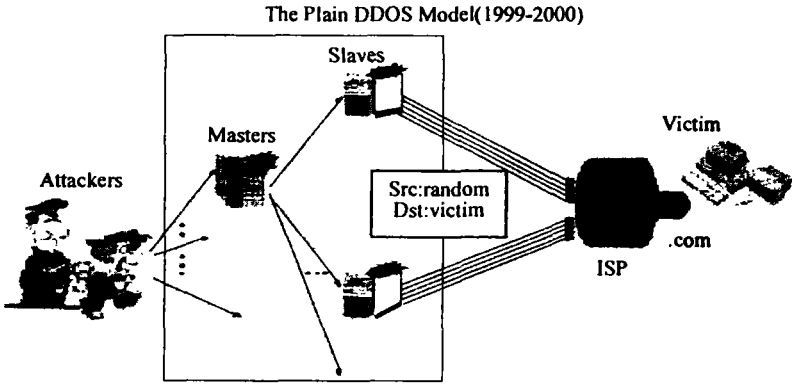

图2 DDOS模型

李毅超 硕士，讲师，研究方向：计算机网络、网络信息安全。王 钰 硕士，讲师。夏梦芹 硕士，博士研究生。曾家智 教授。

在该模型中，主攻(Master)从攻击者(attack)接受攻击命令，然后发送类似命令给一组从攻(Slave)，从攻收到来自主攻的攻击命令后，向受害者发起攻击。在利用了反射器(reflector)的分布式拒绝服务攻击中，它将向大量反射器(reflector)发送许多反射分组。从攻是被安装了 DDOS 从攻软件(slave software)的受侵主机。

"intension-driven"追踪法引入了一个关键概念"intension"。每一个目的结点都有一个"意图"(intension)值，如果该值为1，说明该结点希望接受 iTrace 分组，否则该值为零。如果包含在 iTrace 消息中的分组是一个攻击分组而且目标结点希望接受 iTrace 消息，那么该 iTrace 就是有用的。一个 iTrace 消息主要包含三块信息：产生消息的路由器标识，接受消息的目的地址，被路由器选中的分组。

"intention-Driven"将 iTrace 的功能分成两个不同的模块：决策(decision)模块和追踪产生(iTrace generation)模块。决策模块基于路由表(routing table)提供的信息决定：该路由器下一步该产生哪种 iTrace 消息，应向分组转发表(packet-forwarding table)中的哪一个入口发消息。分组转发表中新增加一追踪产生位(iTrace generation bit)。基于决策模块的决定，这一位置1，则使用这一入口的下一个数据包将被选中产生 iTrace。接着，追踪产生模块将处理选中的分组，发送一个新的 iTrace 消息。该过程如图3所示。

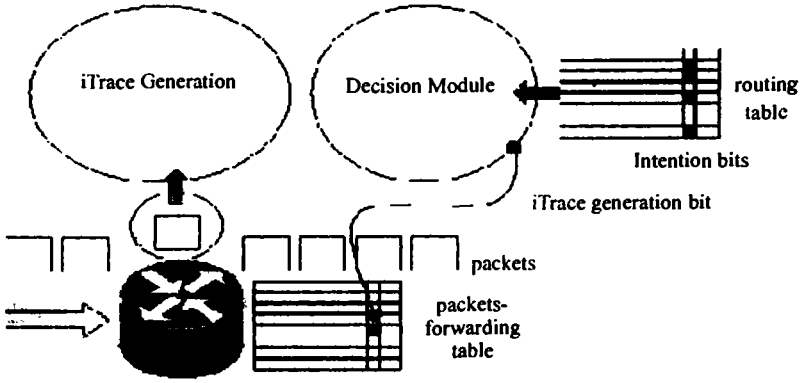

图3 "Intention-driven" method

2.2 包标记(Package marking)

包标记如图4所示[2]。当分组经过路由器时，路由器将自己的 IP 地址插入到分组中去。即分组中包含了路径信息。标记分组的接受者能利用其中的路由信息重构分组路径。

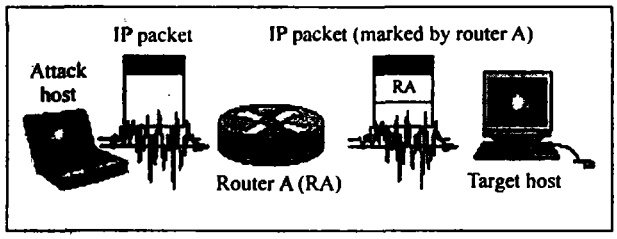

图4 包标记

路由器将自己的 IP 地址写入被转发的分组中，分组接受方能利用这些信息构造路径追溯到分组源地址。这就是所谓的确定性包标记(Deterministic packet marking，DPM)。由于该方法可能会显著地增加分组的长度，又出现了以一定概率标记分组 PPM(Probabilistic packet marking)方案。

所有的标记算法都有两个组件：由路由器运行的标记过程和由受害者运行的路径重构过程。算法的收敛时间由重构路径的分组数决定。

文[8]提出了一种改进的 PPM 模型：在标记过程中采用了分段标记方案(FMS，Fragment Marking Scheme)和边取样(edge sampling)算法。

在边取样算法中，路由器以一定的概率将部分路径信息写入到分组中。这个信息包括开始(start)、结束(end)两个 IP 地址的静态字段和距离(distance)字段。当路由器决定标记一个分组，它将自己的 IP 地址写入开始字段并置距离字段为0。如果距离字段为0，说明前一个路由器已经标记了这个分组，该路由器将自己的 IP 地址写入到结束字段。如果路由器不标记分组，它就增加距离字段。距离字段的值意味着分组从打标记路由器到受害者所经过的路由器的数目。

边取样算法需要将72比特的信息写入分组。而 IP 头的识别(identification)只有16位。FMS 采用了分段编码：将每个路由器的 IP 地址和冗余信息分成8段，概率地用其中一段来标记分组[8]。其标记过程如下：

```
Marking procedure at router R:
    let R' = BitInterleave (R, Hash(R))
    let k be the number of non-overlapping fragments in R'
    for each packet w
        let x be a random number from [0..1]
        if x < p then
            let o be a random integer from [0..k-1]
            let f be the fragment of R' at offset o
            write f into w. frag
            write 0 into w. distance
            write o into w. offset
        else
            if w. distance = 0 then
                let f be the fragment of R' an offset w. offset
                write f ⊕ w. frag into w. frag
            increment w. distance
```

图5 FMS 标记算法

该模型的缺点是受害者重构攻击路径时计算开销很大，当 DOS 由多重攻击者(multiple attacker)发起时，准确度很低。它对受侵路由器也很脆弱，如果一个路由器受侵，它会伪造标记，从而重构路径出错，因为受害者不能从所接收的分组信息中判断出一个路由器是否受侵。

文[7]提出了两种新的方案，先进标记方案(Advanced Marking Scheme)和鉴别标记方案(Authenticated Marking Scheme)，允许受害者能追踪伪装 IP 的大致范围。该技术具有网络和路由器开销小，支持增量配置(incremental deployment)，与以往的方法相比，该技术精确性高，重构大规模 DDOS 攻击路径所需计算开销小。鉴别标记方案支持有效的

路由器标记鉴别以防受攻击的路由器伪造标记。

先进标记方案采用新的编码方案，能有效准确地对付即使1000多个攻击者同时发起的 DDOS 攻击。如果受害者知道其上游路由器的构成图，不用知道全 IP 地址就能构造出攻击路径。将16位的标识(identification)字段分成5比特的距离(distance)字段和11比特的边(edge)字段。5比特能代表32个路由器，这对绝大多数的因特网路径是足够的。用两个独立的散列函数 h 和 h' 对路由器地址编码，输出11比特结果作为标记。路由器 R 以一定的概率标记分组 P 时，将 h[R]写入边字段，0写入距离字段。当 DDOS 的攻击者在60个左右时，该方案的准确度降低，因为11比特的散列结果不能避免冲突。为了对付更大规模的 DDOS 攻击，用两个相互独立的散列函数集代替两个散列函数。

鉴别标记方案：先进标记方案的根本缺点是没有鉴别包标记，结果是一个受侵的路由器能伪造上游路由器的标记。该方案对每个标记计算一个加密消息鉴别代码(MAC，Message Authentication Code)，利用该代码来鉴别路由器是否受侵。

2.3 逐跳追踪(Hop by hop traceback)

逐跳追踪就是一个路由器一个路由器地追踪，直到攻击源。文[2]认为 Hop by hop 追踪技术是比较可靠。因为大多数的追踪技术是针对洪泛型(flooding-style)拒绝服务攻击(DOS)，缺乏追踪单包(a single packet)攻击的能力。他们提出的方法中，路由器日志分组转发信息，然后利用这些日志信息逐跳地(hop by hop)从最后目的地到源地追踪每一个分组。用一种分布式的管理方法可使追踪通过各种配有不同接入政策(access policies)的网络。当分组被转发时，关于分组的信息保留在转发结点中用于追踪，甚至能用于单包攻击(single attack)。

该方法将要用到诸如 MAC 地址、ATM's 虚路径标识符/虚通道标识符(VPI/VCI)的链路层标识符来识别攻击路径中的结点。

网络中间转发结点改变分组的链路层标识符来匹配结点的接口标识符。尽管伪装分组的源 IP 地址比较容易，伪装中间转发结点的链路层标识符却很难。根据某个分组相对应的链路层标识符就能为每个转发结点标识出分组被转发到其相邻结点。

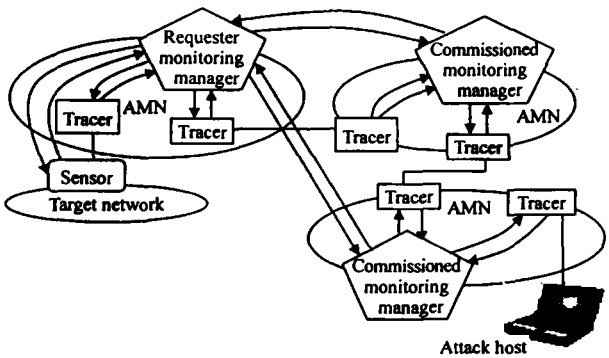

图6 逐跳追踪体系结构

转发路由器或追踪器保存有关到来分组及其链路层标识符的信息在缓冲中，通过搜索与攻击包相应的链路层标识符来确定转发该分组的相邻结点。如果通信量很高，旧数据很快会被新数据覆盖，使追踪不可能。为了节约存储空间，追踪器中存储一些 IP 头字段和一些 IP 数据。追踪开始于离目标最近的追踪器，由它标识转发分组的相邻结点，递归下去，直到攻击包的源地址。文[2]提出的追踪系统主要组件有三个：感应器(sensor)，追踪管理者(monitoring manager)和追踪者(tracer)。

感应器配置在目标地点，监测网络上的分组。当检测到一个攻击，它就向追踪管理者发出一个追踪请求。响应感应器的请求，追踪管理者控制追踪器并管理整个追踪过程。追踪器在转发结点中实现，维护被转发 IP 分组的日志信息。它通过比较日志信息与被追踪的分组信息来寻找追踪路径。

因特网的大小使得集中控制整个追踪过程和管理必要的追踪信息变得不可能。另外，配置了不同接入策略的网络去追踪来自其它网络的分组也是很困难的。采取了一种分布式的管理方法在特定的一组网络中来控制追踪过程和信息。该系统被称为自治管理网络(AMS，autonomous namagement network)。追踪管理者配置在每一个 AMN 中，在自己的 AMN 中执行追踪过程，管理追踪信息。如果追踪过程越出了 AMN 的边界，启动追踪的追踪管理者请求相邻 AMN 的追踪管理者追踪分组。

在逐跳追踪中，跳数(hops)越多，追踪的进程就越多。结果是追踪一个分组要花更长的时间，在追踪完成前，路由器中的追踪信息可能已经丢失。为了减少追踪的跳数，出现了从中心跳跃追踪(hop by hop from center)和通过覆盖网追踪(hop by hop tracing with an overlay network)两种方案[10]。

在从中心追踪的方案中，到受害者的通信量被重新路由到一个"中心"路由器("中心"是相对于总跳数直径)然后被丢弃。"中心"路由器成了受害者，追踪从它开始。这样最多需要 d/2+1跳(hop)，d 是骨干网最大跳数直径。

通过覆盖网络进行追踪首先得建立覆盖网，所谓覆盖网是将所有的边缘路由器和一个中央追踪路由器或一个由追踪路由器构成的简单网络连接起来。运用动态路由将向受害者去的通信量重新路由使其通过覆盖网。跳跃(hop by hop)追踪从离受害者最近的追踪路由器开始。这最多需 dt+1跳，dt 指覆盖网络的直径。

这种方法使特别的诊断特性只配置在边缘路由器和追踪路由器上，高负载高速率的传输路由器并不需要这些特性。追踪所需的跳数也只需2或3个。由于需创建一个覆盖网络，增加了网络的复杂性和额外的管理事务。所需的路由改变要求，若运行不当会对全球产生影响，导致操作上的危险。该方法与一般的逐跳追踪相比更适合 DDOS 攻击。当用于追踪 DDOS 攻击时，大量的边缘路由器要负担封装分组的额外开销，增加了间接损坏的可能性。

2.4 安全协议鉴别(IPsec authentication)

该方法是基于现存的 IP 安全协议。IPsec[11]的关键概念是两个网络实体间的安全关联(SA，security association)。安全关联的基本服务选项是鉴别和加密。网络管理者或设计者制定政策决定在哪建立一个特定的关联。SA 建立的位置决定了所需源识别信息量的多少，而该信息量通过检查攻击包的 IPsec 头得到。保证 IP 源地址可信的一个方法就是在任何两个可能通信的网络实体间建立 IPsec 安全关联。例如：一个分组的源 IP 地址是152.1.75.162，该分组通过 IPsec/AH 鉴别是来自152.1.75.162，那么可以认为源 IP 地址是真实的。如果这一分组被鉴别是来自152.1.75.129，那么则不能确定分组来自152.1.75.162。但这个分组是被152.1.75.129转发。如果是一个攻击包，则可以从152.1.75.129开始调查攻击。

这种方法花费太高而且是静态的。如果在所有的地方都

用 IPsec，即使没有攻击，也不得不维护 IPsec 开销。于是文[10]提出了采用动态安全关联(dynamic security association)技术、用于追踪基于网络(network-based)攻击的一种安全管理框架 DECIDUOUS。

它动态地决定何时何地建立 IPsec 关联。当检测到攻击，因特网密钥交换(IKE，Internet key exchange)协议在目标主机和管理域中的一些路由器之间建立 IPsec 安全关联(SAs)。路由器在 SA 末端加上 IPsec 头和一个隧道 IP 头，它包含转发分组的路由器的 IP 地址。如果攻击在进行中，一个 SAs 鉴别到一个攻击包，则这个攻击来自于相应路由器外的网络。接受者检查隧道 IP 头的源 IP 地址就能找到哪一个路由器转发了攻击分组。以更加灵活的方式建立关联。

由于这种技术利用了现存的 IPsec 和 IKE 协议，在管理域中没有必要实现一种新的协议来实现追踪。管理域外的追踪需要一种协助协议，IETF intrusion Detection working group(IDWG) 正在讨论这样的协议。

DECIDUOUS 需用和攻击检测系统(DIS)、攻击破坏控制系统(IDCS)一起工作。这种集成框架对于各种各样基于网络的攻击都很有效。

2.5 连接链(connection chain)

给定一系列主机 H1，H2，…，Hn(n>2)，当一个人(或一个程序)顺序地从 Hi 连接到 Hi+1(i=1，2，…，n−1)，则称连接序列(H1，H2，…，Hn)为一个连接链(connection chain)。攻击者通常通过这样的连接链向目标发起攻击。基于连接链的追踪是指，给定 Hn，识别出 Hn−1，…，H1。

这类方法主要有 DIDS[15]、CallerID 和 Thumbprinting 等。

文[5]提出的基于偏差(Deviation-based)的方法也属于这类。该方法在因特网上尽可能多的交通点(traffic point)上建立分组监视器(packet monitor)以在分组一级记录攻击者的活动。当一个主机受侵被作为中转点去入侵另一台机器时，通过比较主机上的分组日志和记录在因特网上的日志来找到最接近的匹配。引入了偏差的概念，即同一个分组流在两个连接上表现出的差异。实现一个系统来计算偏差，如果偏差足够小，两个连接一定在同一个连接链中。由此来找出一个攻击连接链。

文[14]等提出了另一种利用主动网络原理的入侵响应框架 SWT(Sleepy Watermark Tracing)。休眠的(sleepy)是指当没检测到攻击时，该方法不会引入开销。“主动”是指当检测到攻击，目标将注入一个水印(watermark)到逆向的攻击连接中，唤醒攻击路径上的中间路由器。

SWT 由两部分组成：SWT 被保卫主机(guarded host)和 SWT 保卫网关(guardian gateway)。后者支持 SWT。每个 SWT 被保卫主机有一个唯一的 SWT 保卫网关，它有一个指向保卫网关的指针。每个 SWT 保卫网关可能保卫着一个或多个 SWT 被保卫主机，它维护着一个被保卫主机表。

SWT 的核心由三个相互作用的部件组成：休眠攻击响应(SIR，Sleepy Intrusion Response)，水印相关(WMC，Watermark Correlation)和主动攻击(AT，Active Tracing)。SIR 接受来自 IDS 的追踪请求，调整主动追踪。水印相关使进入和出去连接通过水印相关联。主动追踪使网络中的不同组织相互协作共同追踪攻击源。

这三个部分通过 SWT 主机和 SWT 网关紧密地工作在一起。SIR 和 AT 构成 SWT 被保卫主机的 SWT 子系统。SIR 接到来自 IDS 的追踪请求后，协调 WMC 应用程序和 AT 模块发起从 SWT 主机到 SWT 网关的主动追踪。SWT 网关的 AT 模块收到追踪请求后，将水印提供给 WMC 模块。这个模块通过使进入和出去相关来提供关于下一跳 SWT 保卫网关的信息给 AT 模块。一旦 SWT 保卫网关发现关于连接链的下一跳信息，AT 将发送追踪信息到发起整个追踪的最初主机并通知下一跳的 SWT 保卫网关开始水标追踪。

3 存在的问题及发展趋势

伪装 IP 追踪有它的局限性。理想情况，IP 追踪应能找到发起攻击的那台主机。实际上使追踪通过防火墙进入企业内部网是很难的。最后追踪到的地址可能是防火墙地址，也是企业网的入口点。识别到组织，组织就能找出其内部发起攻击的用户。另外一个问题是追踪系统的配置。大多数的追踪技术要求改变网络，包括增加路由器功能和改变分组。为了提高追踪技术，应在实现时减少这些缺陷。

即使 IP 追踪找到了攻击源，这个源可能是攻击中的一个中转点(stepping-stone)。IP 追踪不能识别中转点后最终的源。利用中转点进行追踪正处于研究之中[17]。

在 IP 追踪技术被广泛配置前还有些操作上的问题需解决。通过不同的网络进行追踪，对追踪应该有一个共同的政策。为保护隐私还应有一些方针来指导处理追踪结果。未来，鉴别来自 IDSs(入侵检测系统)和 IP 追踪系统的结果将是焦点问题。

参 考 文 献

1 Denial of Service Attacks. CERT Coordination Center, Oct 1997. Available at : http://www. cert. org/tech_tips/ denial_of_service. html

2 Baba T, Matsuda S. Tracing Network Attacks to Their Sources. IEEE Internet Computing March. April 2002, 20～26

3 Belovin S, Leech M, Taylor T. ICMP Traceback Messages. Internet draft, work in progress, OCT, 2001. available online at http://www, ietf. org/internet-frafts/fraft-ietf-itrace-01. test

4 Ohta K, et al. Detection, Defense, and Tracking of Internet-Wide Illegal Access in a Distributed Manner. In: Proc. INET 2000, Internet Soc, Reston, Va. July 2000: available online at http://www. isoc. org/inet2000/cdproceedings/1f/1f-2. htm

5 Yoda K, et al. Finding a Connection Chain for Tracing Intruders: available online at http://www. laas. fr/～ esorics/notices/YE2000. html

6 Mankin A, et al. On Design and Evaluation of “Intention-Driven” ICMP Traceback”

7 Song D X, Perrig A. Advanced and Authenticated Marking Schemes for IP Traceback. IEEE INFOCOM 2001

8 Savage S, Wetherall D, Karlin A, Anderson T. Practical network support for ip traceback. In: Proc. of the 2000 ACM SIGCOMM Conf. Aug. 2000. available at: http://www. cs. washington. edu/homes/savage/traceback. . html

9 Adler M. Tradeoffs in Probabilistic Packet Marking for IP Traceback. Oct. 2001. available online: http://www. cs. umass. edu/～ micah/

10 Chang H Y, Chen P, Hayatnagarkar A, et al. Design and Implementation of A Real-Time Decentralized Source Identification System for Untrusted IP Packets: available at www. silicondefense. com/research/itrex/archive/tracing-papers/ chang00design_and_

implementation_of_realtime.pdf
11 Kent S, Atkinson R. Security Architecture for the Internet Protocol. Internet Draft, IETF, draft-ietf-ipsec-arch-sec-04.txt, March 1998. Network Working Group
12 Maughan D, Schertler M, Schneider M, Turner J. Internet Security Association and Key Management Protocol. Internet Draft, IETF, draft-ietf-ipsec-isakmp-09.txt, Network Working Group, 1998
13 Piper D. The Internet IP Security Domain of Interpretation for ISAKMP. Internet Draft, IETF, draft-ietf-ipsec-doi-08.txt, Network Working Group, 1998
14 Wang Xinyuan, et al. Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework
15 Snapp S, et al. DIDS (Distributed Intrusion Detection System)-Motivation, Architecture and Early Prototype. In: Proc. of 14th National Computer Security Conf. 1991
16 Stone R. CenterTrack: An IP Overlay Network for Tracking DoS Floods. Proc. 9th Usenix Security Symp., Usenix Assoc., Berkeley, Calif., Aug. 2000; available online at http://www.usenix.org/publications/library/proceedings/sec2000/stone.html.
17 Asaka M, et al. A Method of Tracing Intruders by Use of Mobile Agents. Proc. INET 99, Internet Soc., Reston, Va., June 1999. available online at http://www.isoc.org/inet99/4k/4k-2.htm.
18 Staniford-Chen S, Heherlein L T. Holding Intruders Accountable on the Internet. In: Proc. of IEEE Symposium on Sectrity and Privacy, 1995
19 Jung H, et al. Caller Identification System in the Internet Environment. In: Proc. of 4th USENIX Security Sympodium, 1993
20 Zhang Y, Paxson V. Detecting Stepping Stones. In: Proc. of 9th USENIX Security Symposium, 2000
21 Schnackenberg D. Dynamic. CooperatingBoundaryControllers. http://www.darpa.mil/ito/Summaries97/E2950.html, Boeing Defense and Space Group, March 1998

(上接第135页)

图1为24个用户情况下，分别用两种方法得到的结果，从图上可以看出二邻域的坐标下降法确实可以得到比半定规划方法更低的误码率。图2 为30个、40个用户的情况，其中在信噪比为13时，最上面的线表示40个用户用半定规划方法得到的结果，第二条为40个用户用二邻域的坐标下降法得到的结果，第三条表示30个用户用半定规划方法得到的结果，第四条为30个用户用二邻域的坐标下降法得到的结果，从图中可以看出对于30个用户、40个用户而言，也得到比半定规划方法更低的误码率。

图3是用户为24，第一个用户的信噪比为9(即 SNR(1)=9)，其它用户的信噪比变化时，第一个用户远近问题的仿真，从图中可以看出远近问题确实得到了有效控制。

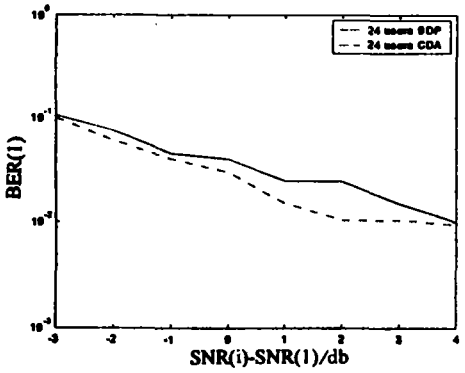

图3

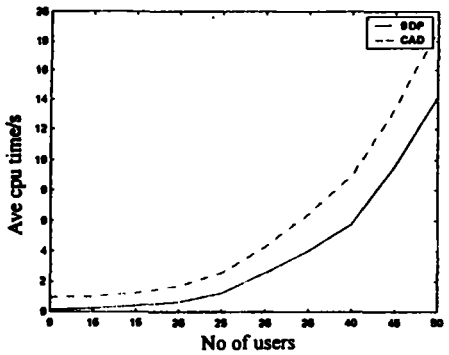

图4

图4为用户不同时，上面两种方法的时间比较，从图中可以看出虽然二邻域的坐标下降法用的时间比半定规划用的时间要长一点，但是误码率低，这说明基于半定规划的二邻域坐标下降法确实是解决多用户检测问题的一种有效途径。

注：本文所有仿真实验，是在 P Ⅱ 450，128M 内存的微机上用 Matlab5.3编程所得。

参 考 文 献

1 Verdu S. Multiuser Detection. Cambridge University press, 1998
2 Huitian P, Rasmussen L K. The application of semidefinite programming for detection in CDMA. IEEE. Selected in Communication, 2001, 19(8): 1442～1449
3 Moshavi S. Multiuser detection for DS-CDMA communications. IEEE Commun. Mag., 1996, 34: 132～136
4 Verdu S. Minimum probability of error for asynchronous Gaussian multiple-access channels. IEEE Trans. Inform. Theory 1986, 32: 85～96
5 Verdu S. Computation complexity of optimum multiuser detection, Algorithmica, 1989, 4: 303～312
6 Kailath T, Poor H V. Detection of stoch processes. IEEE trans. Inform. Theory, 1998, 44(6): 2230～2259
7 SANkaran C, Ephremiddes A. Solving a class of optimum multiuser detection problems with polynomial complexity, 1998, 44(5): 1958～1961
8 Varansi M K. Cyclic decision feedback multiuser sequence detection. Communication, control, and computing, 1994. 372～381
9 Wei L, Krasmussen L, Wyrwas R. Near optimum tree-search detection schemes for bit-synchronous multiuser CDMA system over Gaussian and two-path Rayleith-fading channels. IEEE trans Commun, 1991, 39: 725～736
10 nelson L B, Poor H V. Iterative multiuser receiver for CDMA channels: An EM-based approach. IEEE, trans, Commun, 1996 44(12): 1700～1710
11 nesterov Y E. Quality of semidefinite relaxation for nonconvex quadratic optimization CORE discussion paper #9719, Belgium, March 1997
12 Spoliak, Rendl F. Solving the Max-cut problem using eigenvalue. Discrete Appl, 1995, 62: 249～278
13 Nesterov Y, Nemirovsky A. Interior point methods in convex programming: theory and applications, SIAM. Philadelphia, PA, 1994