# [1]网络入侵追踪研究综述

张静 丁伟
（东南大学计算机系 江苏省计算机网络技术重点实验室，210096）

**【摘要】**入侵追踪系统是在网络上自动发现攻击者真实位置的系统，可以揭穿地址欺骗等攻击者常用的手段。入侵追踪系统可以分为两类：IP 报文追踪系统和面向连接的追踪系统。IP 报文追踪系统可以追溯到发送带有假冒源地址报文的攻击者真实位置，特点是需要利用路由器作为中间媒介。如果攻击者使用“跳板系统”作为攻击手段，那么面向连接的追踪系统可以追溯这类绕道而行的攻击者，发现隐藏在跳板系统后的真实攻击源。随着网络攻击事件的日益增多，开发面向当前网络环境，能够准确、实时追踪入侵者的系统是十分迫切的任务，有着广阔的应用前景。

**【关键词】**网络入侵检测；入侵追踪

## 1 引言

在制定目前 Internet 上使用的网络协议标准时，设计者们更多的是考虑到网络协议的可靠性和可扩展性，而不是它们所提供的安全服务和审计功能。因此，现有的网络模型是基于报文交换的一个比较简单的模型，建立在 TCP/IP 协议的基础上，与报文安全有关的服务，例如：可靠传输、集中控制和安全认证，都发生在进行传输的端实体上。网络报文的内容包括头部信息（报文和头部的长度、校验和、使用的协议类型和服务类型），报文的源地址和目标地址，以及负载数据。由此可以看到，源地址信息是由报文的发送者自行填入，这就产生了协议的漏洞：报文的发送方可以填入假的源地址信息，或者通过使用代理来改变源地址，从而隐藏自己的真实源地址，冒充其它终端进行通信[1]。而对于报文的接收方来说，如果没有采取一些有效的认证方法，也无法判定该报文是否确实来自于报文中的源地址。这种地址欺骗行为虽然可以通过使用 IPSEC 和一些认证技术来得到一定程度的避免，但由此会带来网络处理负担加重、密钥分配和管理，以及网络是否支持等问题，目前还不能广泛的应用。

入侵追踪的最终目标是能够定位攻击源的位置，推断出攻击报文在网络中的穿行路线，从而为入侵检测系统的事件处理、入侵响应决策提供有价值的信息，协助找到攻击者。同时也为网络安全管理员提供情报，指导他们关注入侵行为频繁发生的网段，采取必要的预防措施，以及及时发现成为入侵者“跳板”的主机或路由器。对于网络黑客而言，成熟有效的追踪技术对他们也有威慑作用，迫使他们为了防止被追踪到而减少甚至停止攻击行为。

追踪最直接的方式是寻找攻击源点的真实 IP 地址。但为了更好的隐蔽自己，一些网络攻击者通常并不直接从自己的系统向目标发动攻击，而是先攻破若干中间系统，让它们成为“跳板”，再通过这些“跳板系统”完成攻击行动。在这种情况下，IP 报文追踪系统只能追溯到直接发送攻击报文的“跳板系统”，而面向连接的追踪系统可以追溯这类绕道而行的攻击者，发现隐藏在跳板系统后的真实攻击源。

面向连接的追踪系统可以分为三类：基于主机的追踪系统，基于一般网络的追踪系统和基于主动网络的追踪系统。这些系统的共同特点是对网络传输情况由主动介入转为被动监听，避免了 IP 报文追踪系统使用的会造成网络额外负担的追踪方法，例如向网络主动发送

[1]受国家自然科学基金重点课题 90104031 资助。张静，硕士，主要研究方向为网络安全；丁伟，教授，主要研究方向为网络管理、网络安全、网络体系结构等。

测试报文或给报文做标记，而是采取旁路监听的方法，通过对监听得来的报文进行分析和记录，推算出攻击源的情况。

本文对目前具有一定代表性的网络入侵追踪技术分门别类地进行了较为详细的介绍和探讨，并指出了它们各自的利弊所在。

# 2 IP 报文入侵追踪技术

IP 报文追踪系统可以追溯到发送带有假冒源地址报文的攻击者真实位置，还可以发现在网络连接链中“前一跳”系统的信息，特点是需要利用路由器作为中间媒介。路由器是网络中进行报文转发的重要设备，因此如果在路由器中运行入侵追踪系统，就可以充分利用它“报文中转站”的特点，获得大量的信息。并且由于路由器分散在网络各处，使得入侵追踪系统的分布性取得实现基础。

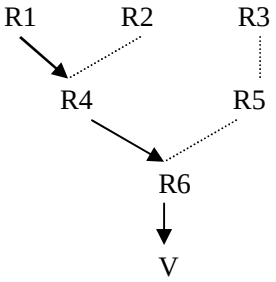
## 2.1 连接检测（Link Testing）

该方法只有在攻击进行的过程中有效，不适于事后才检测到的攻击。

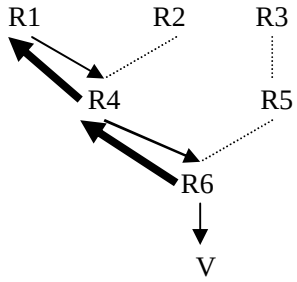
**入流量调试（Input Debugging）：**许多路由器允许使用入流量调试技术[2]，即管理员可以过滤出某些出口点的特定报文，并确定它们来自于哪个入口点。使用该技术进行入侵追踪，首先受害者必须确定它正在遭受攻击，并且描述出攻击报文的共同特征，然后通知网络管理员。管理员将在受害者的上行出口处进行入流量调试，发现攻击报文来自于哪个入口点，以及与该入口点相关的上行路由器，接着在上行路由器继续入流量调试过程。该过程将一直重复进行到发现攻击报文的源头或者追踪到了网络边界。

入流量调试技术的最大弱点是由此带来的管理负担比较重，它需要网管人员的积极配合和交流。如果没有合适的网管人员，或者网管人员缺乏技术支持，入流量调试将无法进行。

**洪水控制法（Controlled Flooding）[3]：**该方法采用向连接发送大量报文（即洪水）来观察对攻击报文传输产生的影响。受害者首先需要掌握网络的拓扑情况，强制处于上行路由的主机或者路由器向每一个连接分别发送“洪水”。由于路由器的缓冲区是共享的，因此来自于负载较重的连接上的报文，其被丢失的概率也相应较大。这样，通过向某个连接发送“洪水”后攻击报文的减少情况，就可以确定该连接是否传输了攻击报文。工作原理如下：




图一：攻击路线




图二：洪水控制法

在图一中，攻击报文从 R1 出发，经过 R4 和 R6，最终到达受害者 V。图二描述了受害者 V 强制 R6 向入连接 R4 和 R5 分别发送“洪水”，当 R6 向 R4 发送“洪水”时，检测到攻击报文的丢失率增大，因此判断攻击报文来自于 R4 的方向。接着 R4 重复以上过程，检测到向 R1 发送“洪水”时攻击报文丢失增加，最终追踪到攻击源来自 R1。

洪水控制法的缺陷在于该方法本身就是一种“服务失效”（denial of service）攻击，因此不能作为常规手段。而且使用该方法的机器要求能够维护网络的拓扑分布图，增加了管理

上的难度。该方法也不适于追踪分布式的网络攻击。

### 2.2 日志记录

在路由器中记录下与报文有关的日志[4]，然后再采用数据挖掘技术得到报文传输的路径。该方法的最大优势在于它能够在攻击结束后进行追踪，没有实时性的要求。但它对网络资源的需求也是巨大的，路由器必须有足够的处理能力和存储日志的空间。另外，数据库的完整性和安全性也是必须考虑的问题。

### 2.3 ICMP 追踪法

该方法的主导思想是路由器在转发报文的过程中，以很低的概率（例如 1/20000）随机地复制某个报文的内容，附加该报文下一跳的路由器信息后，将其封装在 ICMP 控制报文中发往该报文的目标地址[5]。受害机器负责收集这些特殊的 ICMP 报文，一旦收集到足够的信息即可重构报文的传输路径。由于路由器复制报文的概率很低，因此负载不会有较大的增加，该方法对网络资源的占用也很少。但是 ICMP 报文在某些网络中会被过滤掉，而且攻击报文掺杂在正常报文之中，被复制到的概率就更低，这就降低了信息的完整性。受害机器也需要花较长的时间来收集报文，对于不完整的信息无法准确地重构攻击报文的传输路径。

### 2.4 标记报文法（marking packets）

该方法的思想和 ICMP 追踪法有类似之处，它是路由器在转发报文的过程中，以一定的概率给报文做“标记”，标识负责转发它的路由器信息[4]。受害机器即可利用报文中的信息来重构它的传输路径。出于避免加重路由器处理负担的考虑，因此标记算法要求信息的压缩性很强，即用最少的数据来代表最多的信息。标记报文法的优缺点和 ICMP 追踪法相似。

**表 1　　IP 报文入侵追踪技术比较**

| | 管理负担 | 网络负担 | 路由器负载 | 分布式能力 | 事后追踪能力 | 预防性/反应性 |
|---|---|---|---|---|---|---|
| 连接检测 | | | | | | |
| 洪水控制法 | 低 | 高 | 低 | 差 | 无 | 反应性 |
| 日志记录 | 高 | 低 | 高 | 极好 | 极好 | 反应性 |
| 入流量调试 | 高 | 低 | 高 | 好 | 无 | 反应性 |
| ICMP 追踪法 | 低 | 低 | 低 | 好 | 极好 | 反应性 |
| 标记报文法 | 低 | 低 | 低 | 好 | 极好 | 反应性 |

由上表可以看出，ICMP 追踪法和标记报文法对网络负担，管理负担和路由器负载的影响最小，可以进行分布式追踪和攻击结束后追踪，从整体性能上来看要优于其它的追踪方法。

# 3 基于主机的追踪系统

顾名思义，基于主机的入侵追踪就是以被保护的主机为追踪基础，驻留在主机中，通过审计和监视经过主机的网络报文，以及与其它主机交互，来完成入侵追踪功能。

在通常的情况下，网络入侵者在到达到达最终的攻击目标前，会先登录若干“跳板”主机，取得对它们的控制并使之成为协助自己进行攻击活动的工具，从而方便进行远程控制和隐藏自己的真实位置，这就在攻击源和目标主机之间形成了一条“连接链”（connect chain）。当入侵者远程登录到一台主机，并通过该主机登录到另一台主机时，这种行为就称为“扩展连接”（extended connection）。

基于主机追踪技术的一个典型代表就是“身份识别系统”（Caller Identification System in the Internet Environment），缩写为 CISIE[6][7]。它工作在封闭的集中主机控制的网络环境中，由管理员进行统一控制和管理，所有的报文必须由管理员控制的机器产生。

## 3.1 CISIE 简介

CISIE 是为了在多台“跳板”主机追踪入侵者而设计，它的目标是向处于“扩展连接”的主机报警，提供前若干“跳”的连接信息。这样，被保护主机就可以据此来作出是否允许登录请求的决定。

CISIE 系统由两部分组成：身份识别服务器（CIS）和扩展的 TCP 封装（ETCPW）。CIS 负责跟踪每个远程登录到主机的用户；ETCPW 负责当有用户请求登录服务时，通知本地的 CIS 进行追踪。

CISIE 的工作原理：主机接收到有用户请求登录服务的信息时，ETCPW 指示本地的 CIS 形成对该登录进行追踪的请求，发送给前一跳主机的 CIS。该请求包括用来识别 TCP 连接的 TCP 端口号和主机地址。前一跳主机的 CIS 收到请求后，返回拥有该 TCP 连接的用户号，本地 CIS 存储该信息以备后用。第二步，从被保护主机的 CIS 开始，依次向它的前一跳主机的 CIS 核对用户身份的真实性，即本地存储的用户号信息和前一跳主机中的是否一致。如果均一致，则允许该用户登录；如果出现不一致的情况，则拒绝登录请求并报警，说明有假源地址欺骗的情况发生。

## 3.2 CISIE 系统的实现

在 CISIE 系统中，ETCPW 部分使用的是由 Wietse Venema 开发的著名的 TCP Wrapper[8] 的扩展，它对 TCP Wrapper 的功能做了一些修改，使之不仅能够向应用程序提供 TCP 连接两端的 IP 地址，还能提供端口号。当被保护主机接收到远程登录请求时，TCP Wrapper 就启动一个线程，把包含在登录请求中的 IP 地址和端口号传递给本地的 CIS，接着 CIS 据此来发送追踪请求。当追踪过程结束，CIS 将结果传递给 ETCPW，由 ETCPW 把结果标准化输出并调用脚本程序来允许或拒绝本次连接请求。

为了防止恶意的攻击者冒充前一跳的 CIS，或者请求 CIS 追踪合法的用户以达到扰乱系统工作的目的，CISIE 系统采用了一些安全措施来确保会话的安全。由于绝大多数的 CISIE 交互都是客户机请求和服务器的响应，因此可以使用服务器的公钥来加密客户机端的请求，并在请求信息中加入随机数。服务器可以在响应信息中返回这个随机数，并用客户机的公钥进行加密，使用自己的私钥对响应信息签名。这样可以避免大多数形式的“回放攻击”。

### 3.3 CISIE 系统的评价

CISIE 系统可以追踪到出现地址欺骗情况的主机，从而保护系统免受“可疑”用户登录造成的影响。但它也存在着缺陷：第一，CISIE 系统只能工作在封闭的集中主机控制的环境中，在开放的环境下不能有效的进行追踪；第二，CISIE 只能用于实时的追踪，即在攻击动作结束之前进行追踪，而一旦攻击停止，所有的连接信息都将消失，追踪就无法进行下去。

## 4 基于一般网络的追踪技术

该技术借鉴了基于主机的追踪技术的“连接链”概念，通过分析跳板主机之间 TCP 连接的属性和特征，采用信息摘录技术，把攻击报文流同其它报文流区别开来，从而发现攻击报文在网络中的穿行路线。采用这类技术的追踪系统必须安装在能够监听到所有网络报文的地点上。

该技术通常用于追踪采取远程登录办法（telnet，rlogin）进行攻击的黑客，在一连串连接链中，每条信道都负载着多个网络连接，而传送相同报文的连接特征必定是相同的，因此就可以找出某个攻击报文通过的信道路径。但是如果对连接中的所有信息都进行比对，则会浪费大量的存储空间，带来过多的处理负担，这就需要对连接内容进行摘录和归纳。这种信息的摘录被称为“指纹”（thumbprint），它是一小片摘录连接内容的数据，具有数据量少，内容敏感度强，鲁棒性，可追加性，易于计算，易于比较的特性。

**Thumbprint 技术[7]：**在该模型中，一些嗅包器被安排在网络的合适点上，每一个点都收集 TCP 流的信息。这些流按一定的时间间隔被分隔，通常是一分钟长度。用 128 个向量来指向 128 个 ASC 码在流中出现的次数，形成“指纹”。为了尽可能的收集连接信息，需要在网络中设置大量的代理（嗅包器）。当检测到有攻击发生时，就会通知所有的代理立即对监听的每个连接进行摘录比对，凡是符合攻击报文特征的连接即是攻击路径中的一段，如此可以一直追溯到攻击源或者系统覆盖的边缘。

该技术的优点十分明显：可以追踪分布式的网络攻击，系统负担小，由于是实时激发的，在没有攻击的情况下几乎不占用任何网络带宽和系统资源。但缺陷也是显而易见的，它只能追踪正在发生的网络攻击，一旦攻击行为结束，攻击报文在信道中销声匿迹，就无法进行信息摘录了，既没有任何事后追踪的能力。该技术也不能对加密的信息进行信息摘录，并且需要系统时间同步。

**Timing-based 算法[9]：**该算法依据网络流量的时间特征，而不是流量的数据内容，来产生信息摘录。由于用户在击键时有时间间隔，这些空白时间可以被检测到，因此可以作为连接的特征进行比对。该算法的优点是不需要系统时间同步，并且可以检测加密的流量。缺点是由于时间特征存在于整个流量之中，对每个连接必须从头到尾进行比对，造成算法的实时性比较差。

**Deviation-based 方法[10]：**该方法把两个 TCP 连接中报文流的差别定义为背离度，背离度不仅包括时间特征，也包括 TCP 的序列号。如果背离度很小，说明这两个 TCP 连接必定处于同一连接链中。该方法同样不需要系统时间同步，但实时性也不尽人意。

# 5 基于主动网络的入侵追踪技术

主动网络和一般网络的区别在于，它通过分布在网络各处、合适位置的代理，把网络连结成一个整体，不仅能够进行入侵检测和追踪，还可以加入响应功能，对入侵行为进行拦截和反击。这些代理互相之间通过协助和通信来完成追踪和响应动作。

## 5.1 DecIDUouS 系统

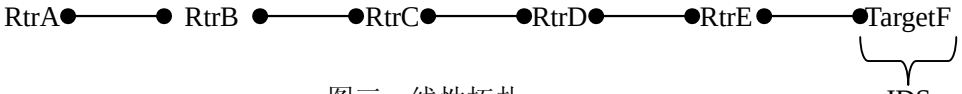
DecIDUouS 系统是 Decentralized Source Identification for Network－Based Intrusions 系统的缩写，它是用于识别网络入侵源点的安全管理框架[11][12]。在 DecIDUouS 中有两个核心概念，第一个是动态安全连接（dynamic security associations）的概念，它建立在 IETF 的 IPSEC/ISKMP 结构之上。IPSEC 的核心概念就是在两个网络实体之间的安全连接关系（SA），SA 的基本服务选项包括认证和加密，而 ISKMP 是为 SA 的建立、选项协商和拆链服务的。DecIDUouS 系统是通过攻击报文所经过安全连接的位置情况来推断出攻击源信息的。第二个核心概念是在不同协议层上的入侵检测系统和攻击源识别系统的管理信息集成，它预留了向低层协议的接口，使得无论是应用层还是网络层的入侵检测系统都能与之良好合作。

**DecIDUouS 系统的工作原理：**DecIDUouS 系统利用了 IPSEC 对报文来源的认证功能作为入侵追踪的基础，由于 IPSEC 报文头中的地址不可能假冒，因此 DecIDUouS 就可以根据这些真实的地址追溯到报文的源头，而不受假源地址的干扰。

一个很明显地用于确保 IP 地址可信的方法就是在任意两个需要通信的网络实体之间建立安全连接（SA），但这个代价过于昂贵和死板。这就导出了“动态安全连接”的概念：即动态地决定在何处、何时建立 SA，并撤销无用的 SA。

DecIDUouS 系统的运行还有一个假设，即所有的路由器都遵循“最短路径转发”原则，并丢弃那些不符合该原则转发来的报文。

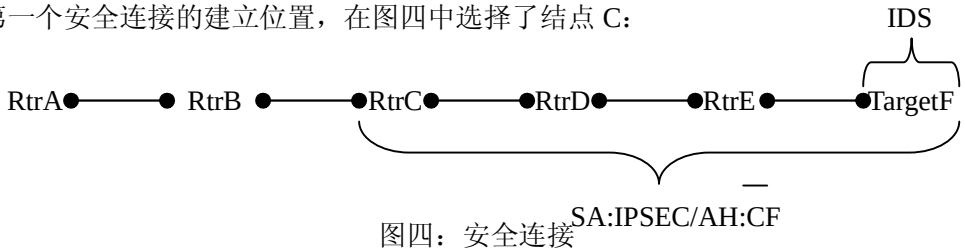
**线性网络拓扑下攻击源的识别原理：**




图三：线性拓扑

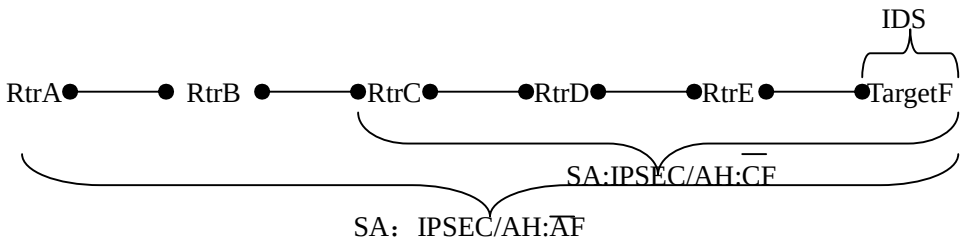
图三描述了一个有六个结点的线性网络拓扑情况，假设这六个结点在同一个管理域内，可以任意建立安全连接。其中结点 F 为攻击目标。

当结点 F 遭受不明来源的攻击时，运行在 F 上的 IDS 系统将检测到有攻击发生，并将情况报送 DecIDUouS 系统。接着 DecIDUouS 系统按照某种算法（通常是选择中间点）来确定第一个安全连接的建立位置，在图四中选择了结点 C：




图四：安全连接

这就意味着结点 C 将负责转发和认证所有目标为结点 F 的报文。如果在 IDS 继续检测到的攻击报文中，有的报文经过结点 C 的认证，而另一些没有，就可以判定至少有一个攻击源在结点 A 到 C 之间，其它的攻击源在 C 到 F 之间。这样以结点 C 为分界，将线性拓扑分为两个攻击带（attack zone）。接下来在这两个攻击带之中分别建立安全连接，逐步缩小范围。例如在结点 A 建立安全连接，如图五所示：




图五：安全连接

如果在后续收到的攻击报文中没有经过结点 A 认证的，则可推断攻击源来自结点 B、C 或者它们中间的连接。

**一般网络拓扑情况下攻击源的识别：**

对于一般的网络拓扑情况，DecIDUouS 系统将把它映射为线性拓扑，然后分别按照以上两种情况处理。在这里引入了最短路径的概念：所谓结点 Vx 和 Vy 之间的最短路径 SD（Vx，Vy），就是在 Vx 和 Vy 之间最少的跳数。映射算法从攻击目标出发，将网络中的结点按照与攻击目标最短路径递增的顺序排列，从而把一般的拓扑转换为线性的排列。

DecIDUouS 系统在接收 IDS 报送的报文信息同时，它会判断对攻击的检测是否已经包括在已经建立的 attack zone 中。如不是，就可能需要建立一个新的 attack zone 来追踪攻击。另外，DecIDUouS 还需要判断一个新的 SA 是否需要建立、老的 SA 是否需要拆除，并负责更新本地的安全政策库。

DecIDUouS 系统的局限性在于它只能追踪正在发生的攻击，它需要在攻击的进行过程中，通过不断建立安全连接来确定攻击源的位置。一旦攻击结束，无法搜集更多的信息，DecIDUouS 系统就失效了。

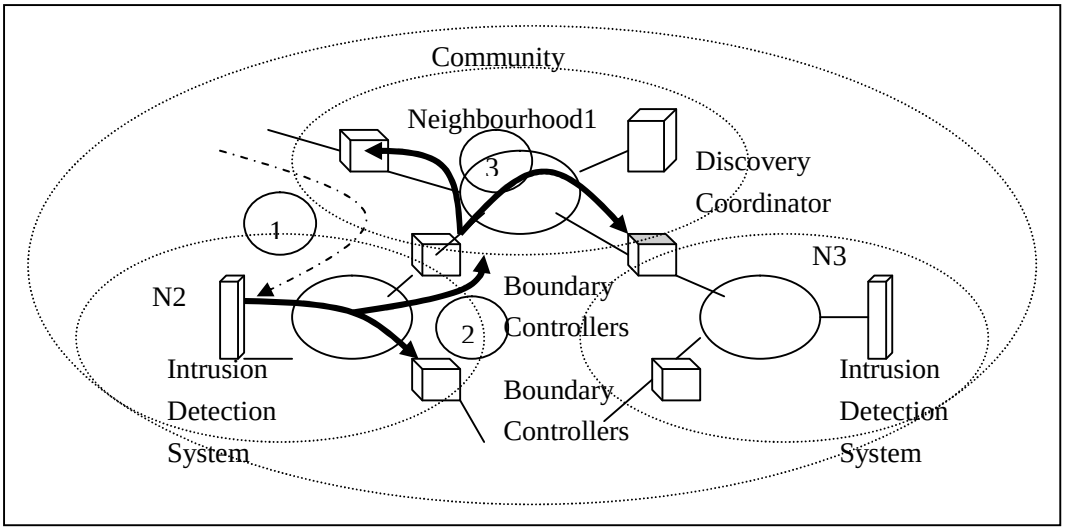
## 5.2 协同的入侵追踪和响应框架（CITRA）

CITRA 是 Cooperative Intrusion Traceback and Response Architecture 的缩写[13][14]，它是一个协同的入侵追踪和响应框架。CITRA 使得入侵检测系统、路由器、防火墙、安全管理系统和其它的系统能够相互协同起来，实现以下四个目标：（1）在网络边界内追踪入侵者；（2） 阻止或者减少入侵造成的后续破坏；（3） 汇报入侵活动情况；（4）在网络范围内进行协同的入侵响应。换言之，CITRA 是一个集中式的体系结构，它把独立开发的组件进行低成本的集成，并使得对其中的任何组件可以进行灵活修改。

CITRA 能够同时完成入侵追踪和响应这两大功能，它的核心部分引入了一个新的协议，称为入侵检测和隔离协议，即 IDIP（Intruder Detection and Isolation Protocol），这是一个应用层的协议，用来协调入侵追踪和隔离。使用 IDIP 协议的系统被组织为若干 IDIP 社区，以此为进行追踪和协同的基本单位。每个 IDIP 社区就是一个管理域，其中负责入侵检测和响应功能的系统被称为 Discovery Coordinator(简称 DC)，它是 IDIP 社区的核心。一个 IDIP 社区内可分为若干邻居域，邻居域是使用 CITRA 体系的系统集合。邻居之间通过边界控制器（Boundary Controller）互相连接起来。

IDIP 的设计目标是实现各系统之间的信息共享，以达到进行协同追踪和响应的层次。IDIP 社区中的每个系统都必须负责存储报文信息或者网络连接情况，一旦有攻击发生，即可相互进行信息交换和查询。系统之间的相互协作主要是通过互发消息（message）来完成。

IDIP 协议是一个双层的结构，分为应用层和消息层。应用层完成入侵追踪和隔离，使用三种消息类型：追踪消息、汇报消息和 DC 指令。消息层的功能是为应用层通信提供安全保障，对消息进行加密、认证，起着安全传输平台的作用。




图七：IDIP 社区

图七描述了一个 CITRA 社区，由三个邻居域组成，DC 在第一个邻居域中，邻居域之间用边界控制器相连。

图中的黑线描述了当有攻击发生时，CITRA 社区是如何进行追踪的：第一步：入侵检测系统检测到有攻击发生。第二步：入侵检测系统随即向它的每一个邻居结点发送追踪消息。该消息包括了对攻击事件的描述和/或对入侵连接的描述。这样其它的 IDIP 结点就可以根据这样的信息来判断自己是否处于攻击路径上。第三步：当邻居结点收到追踪消息后，将追踪消息里的信息和本地存储的信息进行比较，判断攻击报文是否经过自己或由自己转发过。如果是的话，该结点就继续将追踪消息发送给它的所有邻居结点，并向 DC 发送汇报消息；如果自己不在攻击路径上，仅仅向 DC 发送汇报消息，对追踪消息不进行转发。该过程一直进行到追踪至攻击源或者 CITRA 网络的边界。

在 CITRA 网络中，DC 是管理中心，它负责接收所有结点发送的汇报消息，从而获得整体的入侵情况，重构出攻击路径，并且反馈响应指示给各个结点，令其终止不合适的响应动作或加载新的响应措施。

CITRA 的优势在于它是一种分布式的入侵追踪技术，并且它的追踪不受时间限制，即使在攻击结束后的一段时间也可以进行，增强了它的适应性和灵活性。由于它的大部分动作都是自动进行，因此不会给管理员带来过多的负担。但是它也存在缺陷，即在 CITRA 管理域内所有的系统都必须按照 CITRA 框架设计和运行，以确保消息的相互流通和信息共享，一旦处于攻击路径上的某个系统不兼容，追踪就无法进行。

## 5.3 Sleepy Watermark Tracing (SWT)

SWT[15]是一种基于主动网络的入侵检测框架，在没有检测到攻击的情况下，SWT 不会给网络造成任何负担，处于“休眠”状态。在有攻击被检测到的时候，系统被激活，攻击目标会向网络连接注入水印（watermark），并唤醒攻击路径上的中继路由器。

**SWT 的基本概念：**为了有效地追踪，必须通过观察离主机最近的路由器或网关来监控主机，这类网关称为“守护网关”。离主机最近的，负责转发入流量的守护网关称为“Incoming 守护网关”，负责转发出流量的称为“Outgoing 守护网关”。一个主机可以有不止一个的 Incoming 或 Outgoing 网关。“守护网关集合”为一台主机的入和出守护网关总和，对任意守护网关集合 G，把凡是守护网关为 G 的子集的那些主机定义为 G 的“被保护主机”。定义连接链中主机之间的连接为“leap”，用<>表示。一个 leap 可以包括多跳，或物理网络中的多

个连接，由以下 5 个元素描述：<协议号，源地址，源端口号，目标地址，目标端口号>。这样追踪问题就被定义为发现并排序在入侵路径上的主机的守护网关，或者（同等地）发现入侵路线上地 leaps。

**SWT 的框架：**SWT 框架包括两个部分：SWT 被保护主机和 SWT 守护网关。在信任模型中，SWT 被保护主机只有一个守护网关，并且它维护一个指向其网关的指针。每一个 SWT 守护网关保护一个或多个主机并维护一张保护主机的列表。在一台 SWT 被保护主机上的 IDS 和 SWT 应用程序也是 SWT 支持的组件，IDS 是 SWT 追踪的最初发起者。

SWT 的核心包括三个交互的部分：睡眠入侵响应（SIR），水印综合（WMC）和实时追踪（AT）。SIR 负责接收来自 IDS 的追踪请求，协调事实追踪和跟踪追踪信息，WMC 综合出和入的 watermark 连接，AT 负责协调网络的不同部分来协同追踪入侵源。

通常 SIR 和 AT 驻留在被保护主机上，当 IDS 发出追踪请求时，SIR 就调动 WM 应用程序和 AT 模块来初始化从本机到守护网关的实时追踪。在 SWT 守护网关上，AT 模块负责接收追踪请求并向 WMC 提供 watermark。WMC 综合出连接和入连接的情况，反过来也向 AT 模块提供下一个 leap 的 SWT 网关信息。一旦 SWT 守护网关发现下一个 leap 的信息，AT 将向初始的主机发送这部分的追踪信息并通知下一个 leap 的 SWT 守护网关开始 watermark 追踪。

**Watermark：**watermark 是一小块信息，可以用于唯一地标识一个连接。Watermark 应该可以易于嵌入并检索，对网络的一般用户不可见。Watermark 还必须能够综合多个连接并保持不变，watermark 属于应用层。为了证明连接的相关性，必须对出流量和入流量进行相关性分析，把 watermark 做为相关性分析的基础。于是相关性分析就简化为扫描那些具有相同 WM 的出、入流量。当一个 SWT 守护网关扫描入流量时，它就把流量 WM 登记起来，当它扫描出流量时，它就把具有相同 WM 的流量匹配起来。

**SWT 的评价：**SWT 的优点在于它不会给网络造成额外负担，没有误报率，漏报率很低，以及它具有实时追踪的特性。但是 SWT 只能工作在主动网络中，不适合目前绝大多数的网络情况，并且对于报文 watermark 的研究到目前为止还十分缺乏。

# 6 结论

随着近年来网络黑客活动的不断增长，网络安全技术越来越显示出其重要性。各种入侵检测系统、防火墙、安全管理系统为网络的安全提供了一定的保障，但是它们只能被动地检测攻击的发生，向管理员提出警示，但无法从根本上解决网络的安全问题。而入侵追踪系统则可在一定程度和范围内追溯到攻击的源头，为入侵响应和堵截提供明确的方向和信息，对入侵者产生威慑作用，降低入侵行为的危害程度，是网络安全技术中一个重要的发展方向。

IP 报文追踪技术实施起来比较简单，但它会给网络造成额外负担，而且由于需要路由器的支持，牵涉到各生产厂家之间的统一和协作，不可避免地会给路由器带来管理和处理能力上的负担，因此这类技术的发展空间有限。在面向连接的追踪技术中，基于主机的追踪技术对网络环境要求严格，适用性和普遍性比较差。因此今后更为重要的发展方向是分布式的，采用代理技术，能够将各种网络设备充分利用和集成起来的框架技术或者体系结构。

# 参考文献


【1】 L. T. Heberlein and M. Bishop，“Attack class: Address spoofing”，Natl. Information Systems Security Conf., Oct 1996, pp.371-378

【2】 F. Ferguson and D. Senie，“Network ingress filtering: Defeating denial-of-service attacks which employ IP source address spoofing”. RFC 2827,2000.

【3】 R. Stone，“CenterTrack: An IP overlay network for tracing DoS floods” ，In Proc.2000 USENIX Security Symp，July 2000, pp.199-212

【4】 Stefan Savage, David Wetherall, Member IEEE, Anna Karlin, and Tom Anderson “Network Support for IP Traceback”.IEEE/ACM TRANSACTIONS ON NETWORKING VOL.9, NO.3, JUNE 2001

【5】 Steven. M. Bellovin, “ICMP Traceback Messages”， Internet Draft: Draft-bellovin-itrace-00.txt，2000

【6】 JUNG, H.T., KIM, H. L., SEO, Y. M., CHOE, G., MIN, S. L., KIM, C. S., AND KOH, K. “Caller id system in the internet environment”. In UNIX Security Symposium IV Proceedings(1993), pp. 69-78.

【7】 Florian Buchholz, Thomas E. Daniels, Benjamin Kuperman, Clay Shields，CERIAS，Purdue University，“Packet Tracker Final Report”.

【8】 VENEMA, W. TCP wrappers .

【9】 Y. Zhang and V. Paxson. Detecting Stepping Stones. In Proceedings of 9th USENIX Security Symposium, 2000

【10】 Kunikazu Yoda，Hiroaki Etoh， “Finding a Connection Chain for Tracing Intruders”，IBM Tokyo Research Laboratory

【11】 Y. Chang，P. Chen，A. Hayatnagarkar，R. Narayan，P. Sheth,，N. Vo，C. L. Wu，S. F. Wu，L. Zhang, X. Zhang，Computer Science Department North Carolina State University F. Gong， F. Jou，C. Sargor，X. Wu，Advanced Networking Research MCNC，“Design and Implementation of A Real-Time Decentralized Source Identification System for Untrusted IP Packets”，1999 IEEE

【12】 H. Y. Chang，R. Naragan，S. F. Wu，B .M. Vetter，X. Wang，M. Brown， J. J. Yuill，Computer Science Department North Carolina State University，C. Sargor,，F. Jou，F. Gong，Advanced Networking Research MCNC，“DecIDUouS: Decentralized Source Identification for Network-Based Intrusions”.

【13】 Dan Schnackenberg，Harley Holliday，Randall Smith， The Boeing Company, Phantom Works，Kelly Djahandari，Dan Sterne，NAI Labs, Network Associates，“Cooperative Intrusion Traceback and Response Architecture(CITRA)”.

【14】Dan Schnackenberg Boeing Phantom Works，Kelly Djahandari, Dan Sterne NAI Labs, Network Associates， “Infrastructure for Intrusion Detection and Response” ， Proceedings of the DARPA Information Survivability Conference and Exposition (DISEX)

【15】 Xinyuan Wang, Jim Yuill, Department of Computer Science of North Carolina State University. Douglas S.Reeves，Department of Electrical and Computer Engineering of North Carolina State University. S. Felix Wu, Department of Computer Science of University of California at Davis. “ Sleepy Watermark Tracing: An Active Network-Based Intrusion Response Framework”.

# Summarize of Network Intrusion Traceback

Zhang Jing　　Gong Jian
(Computer Department of Southeast University, Network Technology Key Lab, 210096)

Traceback system is a system for finding the hacker's real location on the network autonomously。It can be divided into two kinds: IP Packet Traceback system, and Connection Traceback system. The goal of IP Packet Traceback system is to traceback the Real Source that send the IP Address Spoofed packet，focused in the method that uses the intermediate routers。The Connection Traceback system traceback the Real Source of Detoured Intrusion，the detoured attack is an attack that is done via several systems。Because of more and more attackers emerging in recent years, the model that can apply to the current Internet should be developed，and Real-time traceback system is needed to actively defense the hacking。

**[key words]** Network Intrusion Detection; Intrusion Traceback