基于硬件分区和IP报文还原的网络隔离与信息交换*)

田新广[1,2] 邱志明[1] 孙春来[2] 李文法[2,3] 段洣毅[2,3]
(海军装备研究院博士后工作站 北京 100073)[1] (北京交通大学计算技术研究所 北京 100029)[2]
(中国科学院计算技术研究所 北京 100080)[3]

摘 要 网络隔离技术是目前网络安全领域研究的热点内容。针对多网接入应用环境下的安全隔离需求,本文设计了一种网络安全隔离与信息交换系统,采用基于硬件分区的网络隔离技术和基于IP报文还原的内容深度处理技术,实现了多个外部网络接入一个内部网络时外网间的安全隔离和内外网间的安全通信。本文设计的系统已应用于实际网络环境,表现出良好的安全性能。

关键词 网络隔离,硬件分区,报文还原,信息交换

Network Isolation and Switching Based on Hardware Region Division and IP Packet Reintegration

TIAN Xin-Guang[1,2] QIU Zhi-Ming[1] SUN Chun-Lai[2] LI Wen-Fa[2,3] DUAN Mi-Yi[2,3]
(Postdoctoral Working Station of Navy Equipment Academe, Beijing 100073)[1]
(Institute of Computing Technology, Beijing Jiaotong University, Beijing 100029)[2]
(Institute of Computing Technology, The Chinese Academy of Sciences, Beijing 100080)[3]

Abstract Network isolation has been an active research topic in the field of network security for many years. The design scheme of a network isolation and switching system is presented in this paper, which is applicable to the safety connection of one internal network with multiple external networks. The system employs hardware region division technique to realize the isolation of multiple external networks, and adopts IP packet reintegration technique to perform the safe packet switching between internal and external networks. The application of the system in practical network connections shows that it can achieve high security performance.

Keywords Network isolation, Hardware region division, Packet reintegration, Switching

随着互联网上黑客病毒泛滥、计算机犯罪等威胁日益严重,防火墙的攻破率不断上升,因此迫切需要比传统防护手段更为可靠的安全措施。网络隔离(Network Isolation)是近年来发展起来的一种高强度的网络安全技术,主要用于机密网络的防护和信息交换,是在保证信息可实时交换的前提下防护等级最高的安全措施。目前,网络隔离技术还不够成熟,业内缺乏标准和规范,这使得研制出来的隔离系统在功能和性能上差别很大。现有的网络隔离技术主要有硬件卡隔离、数据转播隔离、空气开关隔离、通道隔离等,其中通道隔离技术通过专用通信硬件和专有安全协议,并利用加密验证机制及应用层数据提取和鉴别认证技术,进行不同安全级别网络之间的数据交换,不仅能够有效地把内外部网络隔离开来,而且可高效地实现内外网数据的安全交换,透明支持多种网络应用,成为当前网络隔离技术的发展方向。

在网络隔离系统的应用中,通常会遇到多个外部专网同时接入到一个内部局域网的情况,这时不仅要保证外网与内网之间数据交换的安全性,而且需保障不同外网间的相互隔离。针对这种应用需求,我们设计并研制了一种网络安全隔离与信息交换系统,该系统采用了基于硬件分区的安全隔离技术和基于IP报文还原的内容深度处理技术,能够实现多个外部网络接入一个内部网络时外网间的安全隔离和内外网间的安全通信。该系统的设计思想和关键技术对其它网络安全隔离系统的开发和应用也具有重要的参考价值。目前,该系统已应用于实际的网络环境,并表现出良好的安全性能。

1 总体设计方案

基于硬件分区和IP报文还原的网络安全隔离与信息交换系统主要由硬件预处理与隔离交换、内网内容深度处理、外网内容深度处理和管理控制等功能单元组成。硬件预处理与隔离交换的主要硬件逻辑包括报文安全过滤处理和硬件隔离分区交换;内网内容深度处理和外网内容深度处理单元完成对网络业务数据的内容还原、多层次协议解析和相应的安全检查及审计日志记录,并将审计信息发送给管理控制单元,其中内网内容深度处理单元负责内部发起连接请求的以太网数据处理,外网内容深度处理单元统一负责外部发起连接请求的以太网数据处理;管理控制单元主要完成对系统各组成部分(包括硬件预处理与隔离交换、内网和外网内容深度处理单元等)的管理和审计命令配置、管理审计服务以及重定向高层协议处理等功能,其中对硬件预处理与隔离交换单元的命令配置和重定向高层协议处理是通过管理控制接口进行,内部

*)国家"九七三"重点基础研究发展规划项目(2004CB318109);国家"八六三"高技术研究发展计划项目(863-307-7-5);国家242信息安全计划项目(2005C39)。**田新广** 博士后,主要研究方向:网络安全、信号与信息处理;**邱志明** 研究员,博士生导师,主要研究方向:最优化设计;**孙春来** 高级工程师,主要研究方向:通信网络;**李文法** 博士,讲师,主要研究方向:网络安全、入侵检测;**段洣毅** 研究员,博士生导师,主要研究方向:网络安全、计算机应用。

的管理审计信息则通过内部管理审计网络接口进行交换，管理控制单元还提供一个外部管理审计网络接口，外部的台式微机可通过此接口登录到系统，以实现对系统的配置与管理控制。硬件预处理与隔离交换单元通过硬件功能处理卡实现，其控制逻辑使用 FPGA 芯片。内网内容深度处理单元、外网内容深度处理单元和管理控制单元均通过集成 CPCI 通用高性能处理控制卡实现。该系统的总体设计如图 1 所示。

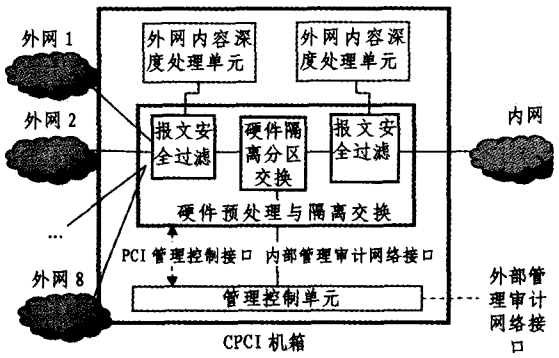

图 1　系统总体结构图

该系统在设计上的主要特点在于：(1)可从硬件上保障多个外网的相互隔离，硬件预处理与隔离交换单元一方面可以进行分区配置，不允许跨区交换；另一方面可以记录某报文的来源，如果由于有意或无意地进行了有关过滤配置，导致跨区交换，硬件将拒绝转发操作。(2)可从硬件和软件两个方面保证内网和外网之间数据交换的安全性，软硬件单元间的数据通信都采用专有协议封装，减小了被破解和欺骗的可能性。而且，内容深度处理软件避开协议栈路径，走自主抓包和自主发送的数据路径，可减小受黑客和木马程序控制的可能性。(3)支持多个外部网络同时接入，保证多网接入的灵活性和高效性。

2　硬件预处理与隔离交换

硬件预处理与隔离交换的具体逻辑包括报文安全过滤处理、分区隔离交换网络、访问控制与格式转换，其逻辑如图 2 所示。

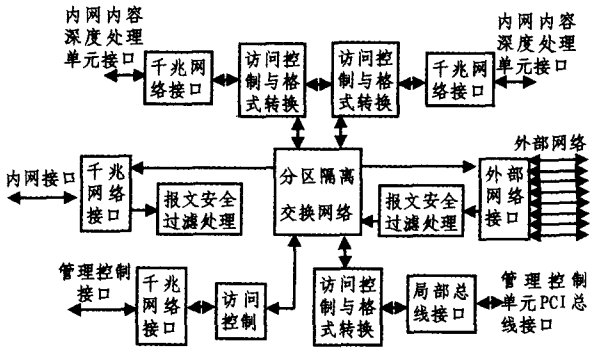

图 2　硬件预处理与隔离交换的逻辑图

分区隔离交换网络是实现硬件分区交换的核心逻辑，它由多个端口(内网、外网、内网内容深度处理单元、外网内容深度处理单元及管理控制单元端口)的数据缓存和交换网络组成。数据缓存用于输出端口阻塞时的数据存储，平滑链路流量；多个外网链路对应一个交换端口，由内部格式封装时指示子端口；内部千兆网络对应一个交换端口；端口间是否能够进行报文交换是按照其所在的转发区域进行控制的，只有在同一交换区内的端口才能进行数据交换，其分区控制通过各网络接口所属的访问控制模块及报文安全过滤模块一起完成，各端口具体划分如下：(1)内部网络端口与多个外部网络端口间可互相交换数据，由安全过滤处理模块控制，只有通过过滤检查的报文才能进行交换；(2)多个外部网络端口在交换网络上视为一个端口，它们之间不能进行交换；(3)管理控制单元可与内网内容深度处理单元和外网内容深度处理单元进行数据交换；管理控制单元可接收两个报文安全过滤处理逻辑产生的日志报文，但不能与外部网络进行数据交换。分区隔离交换网络的交换分区可由管理控制单元根据需要灵活进行配置，一旦配置完成，所有交换都由硬件完成；分区隔离交换网络支持优先级控制，优先级可配。

报文安全过滤处理是对于内、外部网络接口来的报文，根据接口进行来源区分，进行预处理，包括根据安全策略的访问控制、一定程度的内容检查(如关键字检查)以及硬件防火墙功能的检查(包括地址转换、状态检测等)，并决定下一步的处理目标。报文安全过滤处理逻辑具体包括：(1)地址转换(NAT)逻辑：根据配置的规则产生地址转换表，进行相关的地址和端口转换。(2)状态检测：对连接状态表进行匹配搜索，判断是否是正常协议状态；通过状态检测的报文可直接进入包过滤与转发决策逻辑，否则进行规则处理，创建信息的状态表项。(3)规则处理：提取 IP 报文的五元组信息，与过滤规则进行匹配，获取匹配信息决定是否要动态更新状态检测表或者 NAT 表。(4)包过滤与转发决策：根据前面逻辑处理结果对报文进行相应处理；如果是非法报文直接丢弃，如果是要进行分区交换的报文，根据流量统计信息，判断其是否查过预定流量，如未超出，则确定其转发目的地，进行内部格式封装后送分区交换模块，否则丢弃该报文；如果与分区隔离配置冲突，隔离接口间有互通信息企图，则丢弃报文，形成控制报警信息重定向给管理控制单元。访问控制与格式转换对送给交换网络的报文进行源目的端口检查，禁止不同分区的报文进行交换，并实现对专有协议格式的封装与解封装。

3　基于 IP 报文还原的内容深度处理

内网和外网内容深度处理均采用了基于 IP 报文还原和专用协议封装的安全处理机制，两个内容深度处理单元的功能均通过内容深度处理软件实现，该软件由管理控制服务端、安全策略管理、基于 IP 报文还原的访问控制与内容处理、硬件预处理与隔离交换单元接口以及协议栈与网络驱动等模块组成，具体组成模块如图 3 所示。

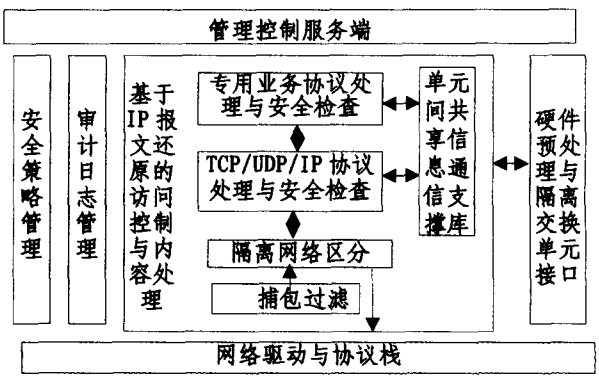

图 3　内容深度处理软件的组成模块示意图

管理控制服务端负责对各功能模块进行配置，支持本地和远程的管理配置界面，其配置通过安全策略管理模块写入相关的安全策略库中；管理控制信息包括软件初始化配置信息、安全策略配置信息、面向管理审计服务的安全审计配置策略信息。安全策略管理模块：接收管理控制服务端模块发送的安全策略配置命令，进行安全策略操作维护（包括插入、删除、修改和查询等）；其操作都通过安全策略库管理来实现，安全策略库是在内存区中维护的安全策略结构数组，安全策略为数据路径上各层次协议处理模块进行查找。审计日志管理模块接收管理控制服务端模块发送的安全审计配置命令，进行日志配置，并接收数据处理路径上的日志操作调用，实现插入、删除日志的动作。

基于 IP 报文还原的访问控制与内容处理模块（包括捕包过滤、隔离网络区分、TCP/UDP/IP 协议处理与安全检查、专用业务协议处理与安全检查、单元间共享信息通信支撑库等子模块）、硬件预处理与隔离交换单元接口以及协议栈与网络驱动等模块完成数据处理路径上的重要功能。其中，单元间共享信息通信支撑库支持两个内容深度处理单元间控制信息的通信，满足对共享信息专有协议封装/解封装和通信状态维护的需要。TCP/UDP/IP 协议处理与安全检查子模块接收网络中的数据报文，通过 IP 协议、TCP/UDP 协议还原，从中剥离出应用层信息，然后交给专用业务协议处理与安全检查模块；该模块通过网络协议栈捕包，逐层进行 IP 协议还原和 TCP/UDP 协议还原，得到应用层数据，根据配置的安全策略进行访问控制和安全内容检查，并形成审计日志；该模块维护各协议层对应的数据报文缓冲。专用业务协议处理与安全检查子模块处于 TCP/UDP/IP 协议处理与安全检查模块之上，对专用业务协议进行判别，根据配置的安全策略进行访问控制、安全内容检查和审计记录，对需要进行安全检查的数据进行处理，然后交给专用业务数据数据安全检查模块去处理；其中，不同的专用业务协议具有不同的协议状态机进行维护，该状态机由 IP 报文触发，并根据 TCP/IP 协议还原模块提供的传输层数据进行应用数据的还原，并维护一个业务数据缓冲；对于分片的数据报文，该模块可判断对应的 IP 报文序列是否最后一个报文，对于非结尾报文，则进行数据隔离交换，否则只有通过了安全检查的报文才进行隔离交换。

4 管理控制

管理控制通过控制软件和审计软件实现，其中控制软件实现对系统各组成部分的管理和控制，并建立与数据转发路径交互通路，接收硬件预处理与隔离交换单元的重定向数据，进行相应的复杂协议处理后，动态维护硬件预处理与隔离交换单元的各种表项。控制软件基于 Linux 操作系统，其组成模块如图 4 所示。

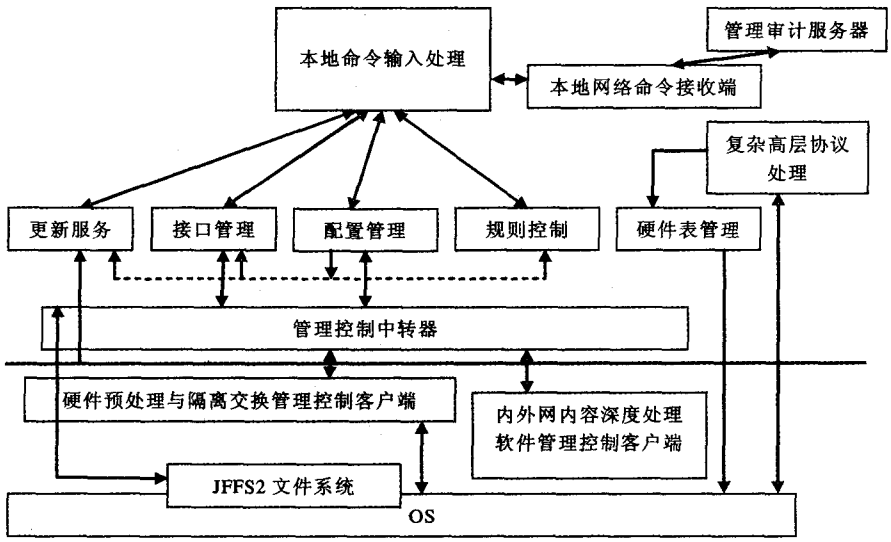

图 4　控制软件的组成模块示意图

控制软件的主要功能模块包括：(1)本地命令输入处理模块：进行命令定义、命令解析、控制台服务器和 Telnet 服务器；(2)接口管理模块：控制各以太网接口的工作方式；(3)配置管理模块：对用户键入的正确命令进行记录，用于后续查询和初始执行；(4)规则控制模块：对网络流量的安全过滤处理过程进行安全策略配置和管理；(5)管理控制中转器模块：将接收的管理配置命令进行解码，根据不同的执行目标发送给不同对象；给本地硬件预处理与隔离交换单元的管理配置信息发送给本地管理控制客户端处理，给远程内容深度处理软件的配置信息则发送内容深度处理软件管理控制客户端，各客户端将执行结果集中返回给管理配置用户；(6)复杂高层协议处理模块：支持特殊协议的 NAT 处理，其中与硬件隔离交换单元间的网络数据交换避开网络协议栈，并进行专有协议封装和解封装；(7)硬件表管理模块：对硬件隔离交换单元中各表项进行动态维护，给出相关表维护管理的 API，以支持复杂高层协议处理。

审计软件以管理审计 Web 服务方式接收管理员命令，实现对系统的远程监控、配置管理、审计数据维护和操作；该软件由浏览器端、服务器端及管理接口三部分组成；其中浏览器端提供给用户的浏览器 Web 界面，远程对设备实现配置、管理和审计；服务器端运行在 J2EE 容器和 Web 容器中，接收用户从浏览器端发来的各项配置、管理和审计命令，通过相应的管理业务逻辑和数据库操作，实现其各项功能；管理接口：通过网络通信，实现对设备的各种实际管理接口，包括远程配置接口、日志接口和状态信息接口等；安全管理接口则实现与安全综合管理工作站的信息交换。

结束语　本文设计了一种用于多网接入的安全隔离与信

（下转第 95 页）

同时，该算法是健壮的，能够应付 push 和 pop 循环中出现的栈失衡的情况。即在单个循环中 push 或者 pop 只发生一个，或者 push 和 pop 不平衡(push 指令比 pop 指令多，或者 pop 指令比 push 指令多)，这种算法仍能产生正确的地址栈图且包含所有程序点的地址栈。

5 隐式系统调用的检测

同段中的 call 调用是近过程调用。它将执行如下操作，如图 4 中正常 call 调用所示：将栈指针(esp)减去两个字节并将指令指针(eip)压入栈(eip，它包含了紧跟着 call 指令后的指令地址)，然后将要调用过程的地址插入到 eip 中。最后，一条 ret 指令从近过程调用中回退。

图 4 中，列出了三种隐式 call 指令调用技术。E，L0，L1 等存在于指令左边，它们代表指令的地址，而箭头"→"右边的数字代表控制流。在图 4 的中间列中，使用了 push/jmp 组合指令模拟 call 指令。指令 1 将入口点代码压栈，指令 2 将 call 指令后的指令地址压栈，即返回地址压栈，指令 3 装载函数 fun 的有效地址到寄存器 eax，指令 4 跳转到 fun 函数相应的地址。当 fun 函数返回时，控制权返回到指令 2 压入栈的返回地址处。因此，没有显示地使用 call 指令，但是达到了正常 call 指令调用的目的。通过该代码的地址栈得到的地址栈图可以检测这种隐式调用的迷惑手段。在地址栈图中，指令 6 回溯到指令 2 中最初压入栈的返回地址。通过对指令语义的观察，检测出 call 指令的调用。

在图 4 的右边列中，结合 push/ret 或 push/pop 指令隐式地模拟 call 指令。前四条指令和上例中语义一样。在指令 5 执行完 ret 或 pop eip 后，便将指令 4 中压入栈的地址便弹入到 eip 中，控制权便转移到 fun 函数中，实现了隐式 call 指令调用。如图所示的地址栈形成的地址栈图可用来检测这种隐式调用的迷惑手段。在地址栈图中，指令 5 中回溯到在指令 2 中压入的返回地址，通过观察 eax 得出结论：函数 fun 被调用。

6 实验

在 Windows 平台下，用 IDAPro 反汇编工具对两种恶意代码样本进行反汇编，然后使用地址栈图的相关方法对其进行检测，得出以下结论：

在 Win32. Evol 病毒中，使用了 push/pop 组合指令隐式执行 call 指令以到达系统调用的目的(以 LoadLibraryA 为例)。首先它将函数名字装载进一个寄存器中，然后把它压栈，最后弹出栈将控制权转移。以下为 Win32. Evol 示例代码：

```
lea eax, [ebp+var_14]
mov dword ptr [eax], 'daoL'
mov dword ptr [eax+4], 'rbiL'
mov dword ptr [eax+8], 'Ayra'
mov byte ptr [eax+0ch], 0
push eax
…
pop
```

该病毒使用的 push/pop 组合指令和图 4 右边列中一样以相同的方式隐式地模拟 call 指令。

而在 Win32. Giri 病毒中，却使用了图 4 中间列中的 push/jmp 组合指令来隐式执行系统调用。以下为 Win32. Giri 中隐式调用 GetTickCount 的示例代码：

```
mov dword ptr [eax], 'TteG'
mov dword ptr [eax+4], 'Ckci'
mov dword ptr [eax+8], 'tnuo'
mov dword ptr [eax+0ch], 0
push eax
lea ebx, var-func
jmp ebx
…
ret
```

因此，通过图 4 右边列和中间列的地址栈图便能检测出这类病毒的隐式的系统调用。

所以，地址栈图相关的检测方法可以有效地检测出恶意代码中使用组合指令执行的隐式系统调用。

结论 本文提出了一种检测具有迷惑技术的隐式系统调用的方法。该方法使用操作栈空间相关指令的地址，生成一种能够表示所有程序点处栈变化的地址栈图，图中的每一条路径都表示一个地址栈。检测结果表明，使用地址栈图能有效地检测恶意程序中具有迷惑技术的隐式系统调用。但是迷惑技术并不只局限于 call 指令，而且还包括参数比较的迷惑技术，返回指令的迷惑技术等，在下一步的工作中，将对此做进一步的研究。

参 考 文 献

1 Jordon M. Dealing with Metamorphism [EB/OL]. In: Virus Bulletin, 2002. 4～6
2 Lakhotia A, Singh P K. Challenges in Getting Formal with Viruses [EB/OL]. In: VirusBulletin, 2003. 14～18
3 Linn C, Debray S. Obfuscation of Executable Code to Improve Resistance to Static Disassemby [C]. In: The 10th ACM Conference on Computer and Communication Security 2003, Washington D. C, 2003
4 Collberg C, Thomborson C, Low D. A Taxonomy of Obfuscating Transformations l [R]: [Department of Computer Science, University of Aukland Technical Report 148]. July 1997
5 Barak B, Goldreich O, et al. On the (Im)possibility of Obfuscating Programs [C]. In: Advances in Cryptology (CRYPTO'01), 2001
6 Christodrescu M, Jha S. Static Analysis of Executables to Detect Malicious Patterns [C]. In: The 12th USENIX Security Symposium (Security '03), Washington D. C, 2003
7 Mohammed M. Zeroing in on Metamorphic Viruses [C]. In: The Center for Advanced Computer Studies. Lafayette, LA: University of Louisiana at Lafayette, 2003
8 Christodrescu M, Jha S, et al. Semantics Aware Malware Detection [C]. In: IEEE Symp. Security and Privacy, 2005
9 Lakhotia A, Karim M E, et al. Phylogeny Using Maximal pi-Patterns [C]. In: The 14th EICAR Conf, 2005

(上接第 83 页)

息交换系统，采用基于硬件分区的安全隔离技术和基于 IP 报文还原的内容深度处理技术，实现了多个外部网络接入一个内部网络时外网间的安全隔离和内外网间的安全通信。系统的设计方案和关键技术对其它网络安全隔离系统的开发和应用也具有重要的参考价值。

参 考 文 献

1 Bajcsy R, Kesidis G, Levitt K. Cyber defense technology networking and evaluation [J]. Communications of the ACM, 2004, 47 (3): 58～61
2 Algirdas A, Jean-Claude L, Brian R, et al. Basic Concepts and Taxonomy of Dependable and Secure Computing [J]. IEEE Transactions on Dependable and Secure Computing, 2004, 1(1): 11～33
3 Matthew V, Philip K C. Learning nonstationary models of normal network traffic for detecting novel attacks [A]. Proceedings of KDD'02 [C], Edmonton, Alberta, Canada, 2002. 376～385
4 李贵山，戚德虎. PCI 局部总线开发指南[M]. 西安：西安电子科技大学出版社，2001
5 陈颖. 基于包过滤的个人防火墙的研究与实现[D]. 西安：西安交通大学研究生院，2002
6 田新广. 基于主机的入侵检测方法研究[D]. 长沙：国防科技大学研究生院，2005
7 孙宏伟，田新广，张尔扬. 一种改进的 IDS 异常检测模型[J]. 计算机学报，2003，26(11)：1450～1455
8 田新广，高立志，张尔扬. 新的基于机器学习的入侵检测方法[J]. 通信学报，2006，27(6)：108～114