# IPSec实现保密数据传输的技术研究

王心灵,朱学永,郑 美
(解放军电子工程学院 网络信息管理中心,安徽 合肥 230037)

**摘 要**:文中在对IPSec协议体系和Linux下TCP/IP协议栈深入分析的基础上,利用IPSec协议,构造了一个试验性的VPN模型,在Linux平台下实现了保密数据传输。并对所实现的IPSec模块和传输系统进行了测试、分析和应用研究,证明本系统模型是可行的和可靠的。

**关键词**:网络安全;保密数据传输;IPSec;ESP;AH;VPN
**中图分类号**:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2006)08-0235-04

# Research on Applied IPSec Technology to Implement Secret Information Transportation

WANG Xin-ling, ZHU Xue-yong, ZHENG Mei
(Network Information Administrative Center, PLA Electronic Engineering Institute, Hefei 230037, China)

**Abstract**: Based on deep analysis of IPSec and Linux TCP/IP protocol stack, designed a tentative VPN model of applying IPSec, and implemented transportation of confidential data on Linux platform. It is demonstrated that the model is reliable and feasible by the test and analysis of the system.

**Key words**: network security; secret information transportation; IPSec; ESP; AH; VPN

## 0 引 言

随着网络技术的高速发展,网络已经普及到社会的各个方面,但是它在提供开放和共享资源的同时,也不可避免地存在着安全隐患。如何保障机密信息在网络中安全传输,成为人们日益关注的焦点。IPSec的提出正是为了有效地解决网络安全问题。IPSec为IP及上层协议提供了完整性、数据源身份认证、抗重播攻击、数据内容的机密性和有限通信流量机密性等安全服务。由于IPSec的强大功能和诸多优势,使得IPSec具有广泛的应用前景,而只有开发出自己的IPSec产品,才能真正保护网络安全,所以对IPSec的研究和实现具有重要的意义。

## 1 IPSec协议概述

### 1.1 IPSec协议简介

IPSec是IETF(因特网工程任务组)于1998年11月公布的IP安全标准[1],是在IP层为IP业务提供保护的安全协议标准,目标就是把安全集成到IP层。其基本目的就是把密码学的安全机制引入IP协议,通过使用现代密码学方法支持保密和认证服务。IPSec协议主要提供两种网络安全机制:

(1)通过认证头(AH, authentication header)提供了数据完整性和身份认证;

(2)通过加密头(ESP, encapsulation security payload)提供了IP报文的数据加密。

IPSec组件包括安全协议认证头(AH)和封装安全载荷(ESP)、安全联盟(SA)、密钥交换(IKE)及加密和验证算法等。通过IP安全协议和密钥管理协议构建的IP层安全体系结构的框架,能保护所有基于IP的服务或应用。并且当这些安全机制正确实现时,它不对用户、主机和其它未采用这些安全机制的Internet部件有负面影响。由于这些安全机制是不依赖于具体的密码算法独立,所以在选择和改变算法时不会影响其它部分的实现,对用户和上层应用程序是透明的。

目前IETF正在制定新版本的IPSec协议草案,正在讨论的版本是草案第6版[2]。新版本的基本概念没有多大变化,但在如下几方面作了扩展:修改了处理模型以适应新的应用场合、改善了性能和简化了实现方法,其中包括将转发与SPD分离,SPD缓冲的处理,增加了对等端授权数据库(PAD),将SA与IKE和SPD连接。对SPD的实体进行重新定义以提供更多的灵活性。对老版本保留的SPI进行了定义。对隧道模式的SA,SG,在应用IPSec前,允许对数据包进行分片。修改了PMTU的处理等等。预计新标准将在2006年初定稿。

收稿日期:2005-11-14
作者简介:王心灵(1975-),女,安徽阜阳人,硕士研究生,研究方向为计算机网络安全;朱学永,教授,硕士研究生导师,研究方向为网络安全技术。

### 1.2 IPSec 协议工作机制

IPSec 在两种模式下工作:传输模式和隧道模式[3]。

1)在传输模式下,安全协议头(AH/ESP)紧跟在 IP 头及其选项之后,并位于其它上层协议头之前(如 TCP/UDP)。加密或认证传输层及其上层数据。

2)在隧道模式下,安全联盟等同于用安全联盟保护一条 IPIP 隧道。在隧道模式下的 IP 报文有一个外层 IP 头,它定义了 IPSec 协议处理的终点,同时还有一个内层 IP 头,它定义了这个 IP 报文的最终信宿的地址。安全协议头界于外层 IP 头与内层 IP 头之间。如果采用的是 AH 协议,那么能认证外层 IP 头的部分信息和所有内层运载的数据;如果是 ESP 协议,那么可以加密保护内层 IP 包运载的数据,而不保护外层 IP 头信息。图 1 为使用不同模式下的 IP 数据包。

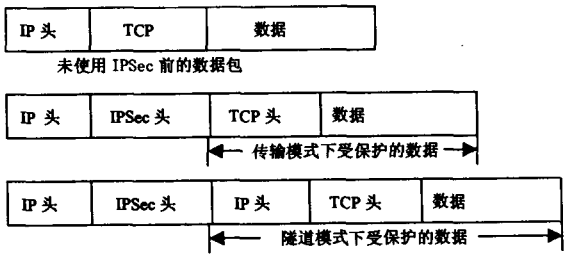


图 1 使用不同模式的 IP 数据包

## 2 应用 IPSec 协议实现保密数据传输的方法

为了在军网上实现保密数据传输,对 IPSec 协议体系和 Linux 下的 TCP/IP 协议栈进行深入分析,重点研究了在 Linux 平台下嵌入 IPSec 以实现数据传输的技术。设计了一种在 Linux 网络协议栈 IP 层中加入 IPSec 处理模块的方式,实现了 IPSec 协议的基本模块,完成对 IP 数据包进行加密和认证的功能;并构建了安全策略数据库和安全联盟数据库;最后对其查询性能进行分析。本实现可以应用于主机上,也可以用在安全网关中。

### 2.1 在 IP 层上实现 IPSec 功能的总体框架

在具体实现时,分别在 IP 包所流经的三条路线上加入 IPSec 处理模块:在本地接受数据包的路线上加入 IPSec 接受模块;在本地包发送的路线上加入 IPSec 发送模块;在转发包的路线上加入 IPSec 的转发模块。图 2 是加入 IPSec 处理模块后的 IP 包流程图[4]。

### 2.2 IPSec 接受模块

IPSec 接收模块主要实现了对 IP 包的解密和认证等功能。该模块主要通过调用两个函数来实现:ah_input() 主要实现对接受 IP 包的认证功能;esp_input() 主要实现对接受 IP 包的解密和认证功能。同时 IPSec 接收模块还调用了安全联盟库和安全策略库查询函数。该模块尽量避免 IP 层分段重组这些功能,充分利用 IP 层本身的功

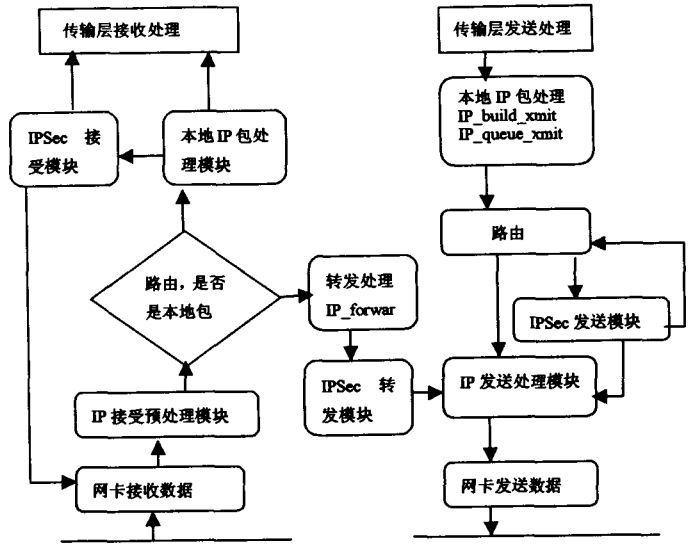


图 2 在 IP 层实现 IPSec 处理模块框架图

能。IP 数据包路由后进入本地 IP 数据包处理和分片重组,在交与上层处理之际才调用了该模块。这样设计可以实现 IPSec 接收模块和 IP 层无缝隙的整合,使接受模块只单一负责解密和认证的功能,从而简化了处理流程。

### 2.3 IPSec 发送模块

IPSec 发送模块主要实现对 IP 发送包的封装、加密和认证的功能。在此模块中主要调用了 ah_output() 和 esp_output() 两个函数:ah_output() 实现对发送包认证的功能;esp_output() 实现对发送 IP 包的加密和认证功能。IPSec 发送模块不仅提供了加密和认证的功能,而且还实现数据包外出时查询安全联盟库和安全策略库等功能。

为了实现和 IP 层更好的整合,修改“目的缓存”数据结构为“可堆叠的目的缓存”[5]。图 3 为“可堆叠的目的缓存”结构示意图[5]。

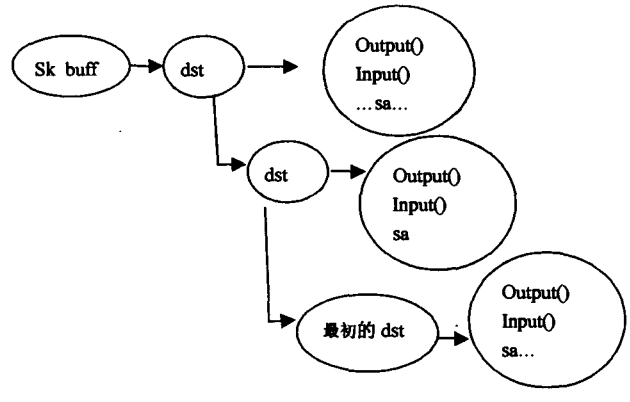


图 3 “可堆叠的目的缓存”结构示意图

“可堆叠的目的缓存”是一个 dst{|的堆栈,dst{|结构定义了一个指向安全联盟的指针,并定义 IP 数据包的输入函数和输出函数的指针:一个指向输入函数 input(),另一个指向输出函数 output(),从而对 IP 层数据进行加工处理。其中“可堆叠的目的缓存”dst{|栈最初的输出函数 dst->output() 赋值为 ip_output()。随后插入的 dst{|,它的输出函数的赋值由路由查询结果和 IPSec 策略表查

询结果来决定。最后所有的 dst{}组成一个堆栈,由 sk_buff->dst 所指向。该信息包在 IP 层的流程也就由可堆叠的 dst{}栈中的 dst->output()函数所控制了。dst{}在生成的过程中,它的外出处理函数可以被赋值为 ah_output()或 esp_output(),这样就可以对外出数据包进行加密或认证,实现 IPSec 外出模块和 IP 层无缝的整合。

### 2.4 IPSec 转发模块

IPSec 转发模块包括两部分:

(1)对接受包的策略检查。在网关上实现 IPSec,主要是隧道模式。IPSec 转发包首先进入 IPSec 的接受模块,经过解密或认证的处理后,去掉外部头,又重新发送到 IP 的接受队列,进入 IP 层[5]。这时该 IP 包所在的 sk_buff 中的 sec_path 结构记录了 IP 包所进行的一系列的 IPSec 处理及其所使用的安全联盟。在此调用策略检查函数,判断是否正确应用了策略。

(2)完成转发包的加密、认证的功能。其具体的流程和外出包的加密、认证相似。

总之,IPSec 转发模块是利用 IPSec 接受模块和发送模块的功能,既对转发包进行策略校验,又对转发包进行加密和认证,为构建 VPN 提供了广阔的舞台。

### 2.5 SPD 和 SADB 的设计及其性能分析

#### 2.5.1 安全策略库和安全联盟库的功能

IPSec 处理 IP 数据包的细节取决于 IPSec 协议的具体实现,IPSec 协议没有对此做出规定。但为满足互操作性,且有最基本的管理能力,协议处理的外在特性必须有统一要求。因此,IPSec 协议规范给出了一个外在特性的模板,该模板包含两个数据库[1]:安全策略数据库(Security Policy Database,SPD)和安全联盟数据库(Security Association Database,SADB)。前者存放了对于出入一个主机或安全网关的 IP 数据包所应采取的安全策略。后者存放了系统所有的安全联盟和它们所使用的参数。安全策略是网络安全系统的重要组成部分和灵魂。安全联盟是它的最终体现和执行形式。二者有机结合,缺一不可。

#### 2.5.2 结构设计及其性能分析

根据 IP 包在网络层的流经路线,安全策略库(SPD)设计为三个表:进入策略表、外出策略表和转发策略表,以供当地接受包、当地外出包和转发包查找策略,进行加密和认证的处理。根据使用安全策略和安全联盟的路线,安全联盟数据库(SADB)分为两个表:一个是外出安全联盟表,一个是进入安全联盟表。以转发数据包为例,来说明 IP 包是如何使用安全策略表和安全联盟表。数据包转发一般发生在网关(或路由器)上,IP 数据包采用隧道模式,外部头目地地址是该网关的地址。数据包在进入 IP 层时,经过路由判断后,首先转入当地处理,查找"进入安全联盟表",进行 IPSec 处理。在送入上层协议之际,根据"进入策略表"进行策略检查。如果是隧道模式,重新排队进入 IP 层。这次 IP 包在路由转发后进入 ip_forward(),在此查找"转发策略表",检查该 IP 包是否按照转发策略进行了 IPSec 的接受处理。然后查找"外出策略表",根据外出策略,查找"外出安全联盟表" 找到外出安全联盟(束),进行外出的 IPSec 处理,然后发送出去。

安全策略数据库(SPD)是一个数组 + 单链表结构。数组的元素是策略表。每个策略表是以单链表形式组织的。这种设计的特点是便于查找、插入和删除。可以根据 IP 包方向直接定位到某个单链表。查找操作的对象主要是单链表,单链表是一种动态结构,整个可用存储空间可为多个链表共同享用,每个链表占用的空间不需预先分配划定,可以由系统响应需求即时生成。因此,建立线性表的链式存储结构的过程就是一个动态生成链表的过程。如果单链表长度为 $n$,其查找、插入时间复杂度为 $O(n)$,空间复杂度为 $O(n)$。

安全联盟库(SADB)的设计如下:哈希表 + 双向循环链表,哈希表的每个元素是双向循环链表。哈希表是进行快速查找的一种有效的组织方式。根据给定的关键字代入哈希函数进行计算,根据哈希值得到记录的位置。哈希表的主要作用是根据关键字可以快速地找到某个 sa 所在的双向循环链表。然后再对双向循环链表进行查找。哈希函数主要是进行位计算,时间复杂度为常数量级 $O(1)$。所以查找的主要对象是双向链表。最坏情况下,双向链表的查找时间复杂度为 $O(n)$。因此,哈希表的最坏时间复杂性为 $O(n)$。哈希表的空间复杂性 $O(D+n)$,其中 $D$ 为哈希表长度,$n$ 为记录元素个数。

以上设计,可以提高安全联盟库和安全策略库的运行效率,降低资源消耗量。

## 3 传输系统的测试和分析

军事训练信息网是专用网,为"秘密级"网络,对网络的安全性、稳定性和高效性等都有很高的要求。如何把需要保护的数据隐蔽地、完整地传送到正确的目的地址,是当前备受关注的问题之一。本课题也就是在这种情况下产生的。基于上面的设计,在军事训练网上构造了一个试验性的 VPN 模型,对所实现的 IPSec 及传输技术进行了测试和试用。测试分为功能测试和性能测试两部分,图 4 为试验环境,内部网 A 和内部网 B 之间通过公用网搭建一个虚拟专用网。

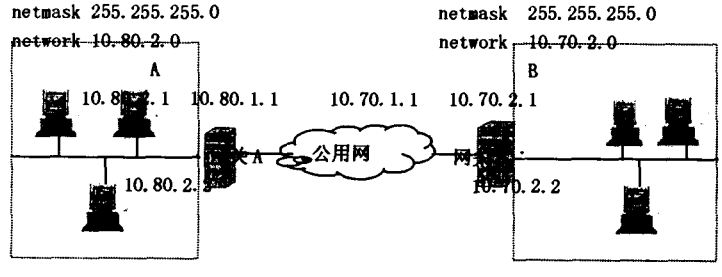


图 4　试验环境

### 3.1 功能测试

功能测试一:在网关 A 和网关 B 上配置 IPSec,保护

两个网之间的通信安全。这样在网 A 任意一台主机和网 B 内的任意一台主机之间的通信(10.80.1.1 - 10.70.1.1)在公网上传输时都可以得到保护。如图 5 所示。

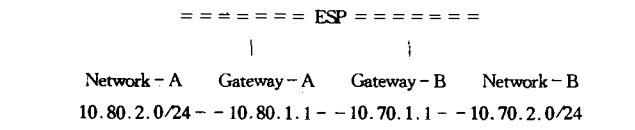


图 5 网关上安全联盟和安全策略的配置

在网关 A 和网关 B 配置 ESP 之后,先用网络 A 内的一台主机(如 10.80.2.2)带填充字符 ping 网络 B 内的一台主机(如 10.70.2.2),其命令如下:

ping -p feedfacedeaddeed 10.70.2.2

这时在网关 A 或网关 B 上运行窃听程序 tcpdump,运行命令如下:

tcpdump -X -s 0 -i eth0

tcpdump -X -s 0 -i eth1

其中 eth0 是网关 A(或 B)上与公用网相连的网卡,eth1 是网关 A(或 B)上与内部网相连的网卡。该命令可以捕获 eth0 或 eth1 上流经的完整数据包。

在 eth1 上捕获结果如下:

```
20:29:31.776703 10.70.2.2 > 10.80.2.2: icmp: echo request (DF)
0x0000 4500 0054 0051 4000 3c01 25bf 0a46 0202  E..T.Q@.<.%..F..
0x0010 0a50 0202 0800 cafa 4e03 5200 3ee9 3d40  .P......N.R.>.=@
0x0020 b8c3 0c00 face feed dead deed face feed  ................
0x0030 dead deed face feed dead deed face feed  ................
0x0040 dead deed face feed dead deed face feed  ................
0x0050 dead deed                                ....
```

在 eth0(与公用网上相连的网卡)捕获的结果如下:

```
20:39:27.387434 10.70.1.1 > 10.80.1.1: ESP(spi=0x00010004,seq=
0x12c) (DF)
0x0000 4500 007c 3c34 4000 3c32 eb84 0a46 0101  E..|<4@.<2...F..
0x0010 0a50 0101 0001 0004 0000 012c 7842 aa13  .P.........,xB..
0x0020 d5fc dd42 b402 4c7c cf89 595b 7ee8 3f62  ...B..L|..Y[.?b
0x0030 6de5 14f3 f149 3d66 df03 5790 49e4 19f9  m....I=f..W.I...
0x0040 d47f 9fca f247 62d2 4b87 e8fe b963 7792  .....Gb.K....cw.
0x0050 faab f728 7585 40e8 1f9c b9f4 0f80 0fe2  ...(u.@.........
0x0060 30ca 397f 155f 0542 f258 a5ab 7c13 42e8  0.9..._.B.X..|.B.
0x0070 eee6 d6fc c7e2 1be0 edff 8677
```

在网关 B 上捕获的数据和网关 A 上相同。从以上捕获结果可以看出,在网关上使用了隧道模式的 esp 后,从和公用网相连的网卡到另一个和公用网相连的网卡之间,传输的是 10.80.1.1 和 10.70.1.1 的 IP 地址,并且数据包得到了加密。如果在公用网上进行监听的话,监听者在不知道密钥的情况下是无法知道数据包的头部和载荷信息的。从而起到了机密性的安全保护。同时也可以看出,在网关上也完成了隧道两端的封装和解封装功能,在和局域网相连的网卡上截获的数据包是明文形式,一是为封装前的数据包,二是经过 IPSec 转发模块解封装后的数据包。从而验证了隧道模式的封装和解封装的保护功能。

功能测试二:在网关进行配置只能保护进行通信时两个网络之间传输数据的安全,而无法保证在局域网内不被窃听。为了防止在局域网内被人窃听和修改,在安全性要求很高的情况下,有必要实施端到端的加密保护。如图 6 所示。

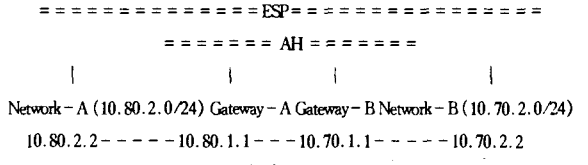


图 6 嵌套使用的配置

在主机上一般实施传输模式的 ESP 和 AH 保护。经过在网关的两个网卡上进行监听,可以观察到 10.70.2.2 和 10.80.2.2 之间传输的数据已被加密。IPSec 可以嵌套使用。

从第一例测试结果来看,通过 VPN 网关,确实建立了一条通过公网的安全通道,所有的数据包都得到了加密保护,监听者无法进行通信分析,获得数据真正的源和目的地址,更无法获得数据的真实内容。第二例的测试针对局域网内的窃听和篡改事件,可以实施端到端的加密和认证,来提高信息保密的安全度。

### 3.2 性能测试

在性能测试中,主要测试加入 IPSec 处理模块对系统性能的影响。性能测试表明,IPSec 模块的加入对系统性能有一定的影响,随着传输数据量的增加,造成的时延随之增大,但这种影响可以容忍,且略优于其他 IPSec 系统。从图 7 也可以看出,如果把 IPSec 处理模块用于安全网关,很多数据需要处理时,可能会累积时延,对用户要求的服务质量产生一定的影响。

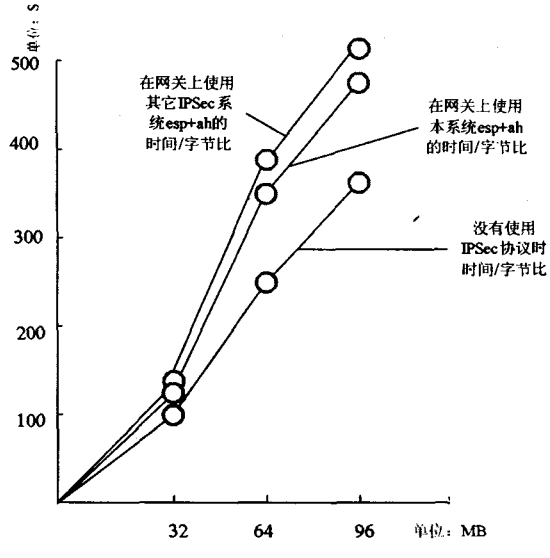


图 7 实施 IPSec 后对系统性能影响

## 4 结束语

本系统是在深入分析 IPSec 协议草案 6 的基础上,进行设计和实现的。测试结果表明,该系统可以实现保密数据安全传输的功能。但 IPSec 模块的加入增加了 IP 包在 IP 层的处理时间,造成了系统性能的下降。因此,在下一

(下转第 242 页)

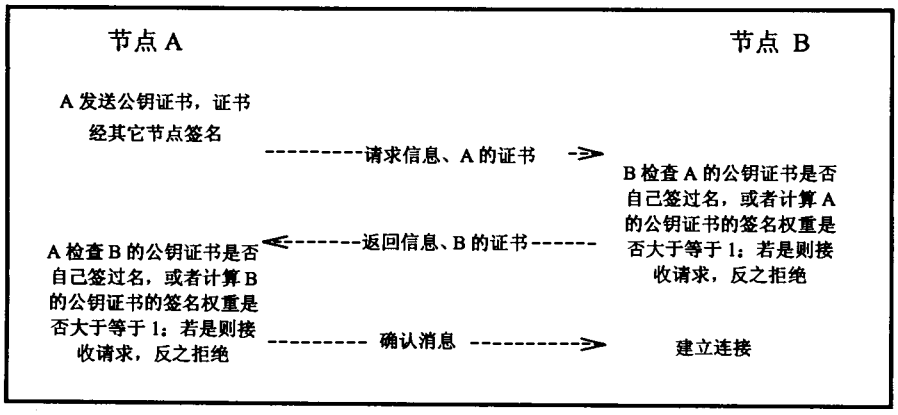


图 3 新的连接过程

认的成熟算法(如 RSA 算法等),其安全性能达到广泛的认同。

(2) 如果某节点的私钥丢失或被窃,并不会影响到整个网络的安全运行,只要及时公布、传递公钥证书撤销信息,就可以使其影响限制在很小范围内,同时新的信任模型可以有效防止内部节点的欺骗。

(3) 具有很好的可扩展性,将来也完全可以利用来解决各 SS 节点对 BS 节点的认证授权,这样既解决了原标准里的单向认证问题,也丰富完善了标准中的认证机制。

(4) 整个连接过程的认证过程不需要 BS 的支持与干预,没有中心支撑节点,避免了单点失效,增加系统稳定性。网状信任模型很像人类社会自然的信任关系,更加可靠、更加稳定。

新的方式具有突出的优越性,然而仍存在一些需进一步改进的地方:

①节点如何方便快捷地查询到其它节点的公钥证书。PGP 建议用户把自己的经过其它不同用户签名的公钥收集在一起,发送到一个公共场合,以方便用户查询、认证。

②公钥证书的注销问题。这是 PGP 系统及利用网状信任模型的系统中普遍存在的一个严重问题,即用户如何及时了解到某一个公钥证书已经失效,避免被欺骗。庆幸的是 BS 的存在可以较好地解决这些问题,也即,虽然 BS 对于 SS 之间通信不是必需的,但 BS 完全可以用来作为集中公布节点公钥证书和在线查询证书注销列表的地方,而且 BS 可以很方便地把证书注销信息及时通知到每个用户。

## 4 总 结

IEEE 802.16 是一种富有发展前景的新技术,将会是未来最重要的宽带无线接入技术之一。然而,其安全性能一直不能让用户完全放心,从而限制了其进一步的推广与发展。文中首先分析讨论了 IEEE 802.16 安全机制和 Mesh 模式中节点间信任模型及连接过程中存在的安全问题。然后借鉴 PGP 系统中信任模型的原理提出了新的信任模型与连接方式,较好地解决了这一问题。分析表明新方法要比原来的方法更为安全。下一步的工作将是,利用实验的或模拟的方式验证此方法的有效性;扩展 IEEE 802.16 的认证机制。

**参考文献:**

[1] IEEE. IEEE 802.16 - 2004. IEEE Standard for Local and Metropolitan Area Networks Part16: Air Interface for Fixed Broadband Wireless Access System[S]. 2004.

[2] Eklund C, Marks R B, Stanwood K L, et al. IEEE Standard 802.16: A Technical Overview of the Wireless MAN Air Interface for Broadband Wireless Access[J]. IEEE Communications Magazine, 2002,40(6):98 - 107.

[3] Johnston D, Walker J. Overview of IEEE 802.16 Security [J]. IEEE Security and Privacy,2004,2(3):40 - 48.

[4] Arbaugh W A. Wired on Wireless[J]. IEEE Security and Privacy,2004,4(1):26 - 27.

[5] Marks R B. Advances in Wireless Networking Standards[J]. Pacific Telecommunication Review,2002,4(2):30 - 37.

[6] 傅 坚.无线宽带固定接入系统的安全性分析[J].计算机工程, 2004,30(6):14 - 15.

[7] 刘海龙,张其善. PGP 中的信任问题及解决办法[J].北京航空航天大学学报,2003,29(3):278 - 282.

[8] Garfinkel S. PGP: Pretty Good Privacy[M]. [s.l.]: O'Reilly & Associates, Inc.,1996.

(上接第 238 页)

步的研究中,继续跟踪学习 IPSec 协议新标准,优化系统模块结构,寻求高速加密、认证算法,以提高系统的性能。

**参考文献:**

[1] Kent S, Atkinson R. Security Architecture for the Internet Protocol(RFC 2401)[EB/OL]. http://www.ietf.org/rfc/rfc2401.txt.,1998 - 12.

[2] Kent S,Seo K. Security Architecture for the Internet Protocol [EB/OL]. http://ftp.cc.ntut.edu.tw/ftp/Documents/Internet - Drafts/draft - ietf - ipsec - rfc2401bis - 06.txt., 2005 - 03.

[3] Doraswamy N, Hartins D. IPSec, 新一代因特网安全标准[M]. 京京工作室,等译.北京:机械工业出版社,2000.

[4] 汤 隽,李 超.基于 Linux 和 IPSec 的 VPN 网关[EB/OL]. http://linuxipsecvpn.cosoft.org.cn,2001 - 12 - 13.

[5] Yoshifuji H, Miyazawa K, Sekiya Y. Linux Ipv6 Networking past, present and future[A]. Proceedings of the Linux Symposium[C]. Ottawa, Ontario, Canada: [s.n.], 2003. 507 - 516.