MPLS VPN安全方案设计及仿真

赵巧霞[1]，　孟相如[1]，　张　发[2]

(1. 空军工程大学电讯工程学院，陕西西安 710077；2. 空军工程大学工程学院，陕西西安 710038)

摘　要：针对MPLS VPN系统存在的安全隐患，综合IPSec和MPLS的技术特点，提出了一种适合MPLS VPN的安全解决方案。并采用离散事件系统建模原理，建立了一个MPLS VPN仿真系统，对方案进行了验证，仿真结果表明该方案是可行的。

关键词：MPLS VPN；安全性；IPSec；离散事件系统；仿真

中图分类号：TP393.09　　文献标识码：A　　文章编号：1009-3516(2005)04-0063-04

随着Internet的蓬勃发展，通过IP实现虚拟专用网(VPN：Virtual Private Network)已成为业界主流[1]。但由于IP网络固有的特性，基于IP的VPN安全性存有不足；同时由于采用无连接的数据传输方式，服务质量(QoS)无法保证，服务等级(CoS)无法实现[2]。近年来提出的采用多协议标记交换(MPLS：Multi Protocol Label Switching)技术实现VPN的思路，可以提供服务质量保证和服务等级技术，但在安全方面还有不足之处。MPLS VPN主要安全问题是当数据从客户路由器发送到供应商边缘路由器时，数据包其实是未经过任何安全处理的，任何感兴趣的人都可以将其截获用于各种合法或非法的目的。本文综合IPSec和MPLS的技术特点，提出了一种适合MPLS VPN的安全解决方案。该方案解决了VPN采用MPLS在公用骨干网进行第二层传输存在的信息不能自动加密，容易因误发或连接中断造成信息泄露等问题。为验证本文提出的安全方案，对实际的MPLS VPN进行简化、抽象，将其抽象为一个多级排队系统，采用离散事件系统建模原理，建立了一个MPLS VPN仿真系统。在Windows 2000/XP环境下，用C++语言实现了该仿真平台。

1　MPLS VPN网络结构

MPLS虚拟专用网是目前MPLS技术在业务提供商(ISP)网络中很流行的一种应用，其特点是允许网络发展可伸缩的IPv4第三层的VPN骨干业务。与IP VPN相比，MPLS VPN可用于发展和管理增值业务(其中包括商用数据网络)，并能给商业用户提供电话业务。

MPLS VPN网络结构如图1所示，整个网络包括三种设备：用户边缘(CE：Customer Edge)路由器、提供商边缘(PE：Provider Edge)路由器和提供商(P：Provider)路由器[3]。这种网络结构的思想是：主要的功能由PE路由器实现，对P路由器的要求仅仅是支持MPLS包的转发，而对CE路由器则没有任何附加要求。

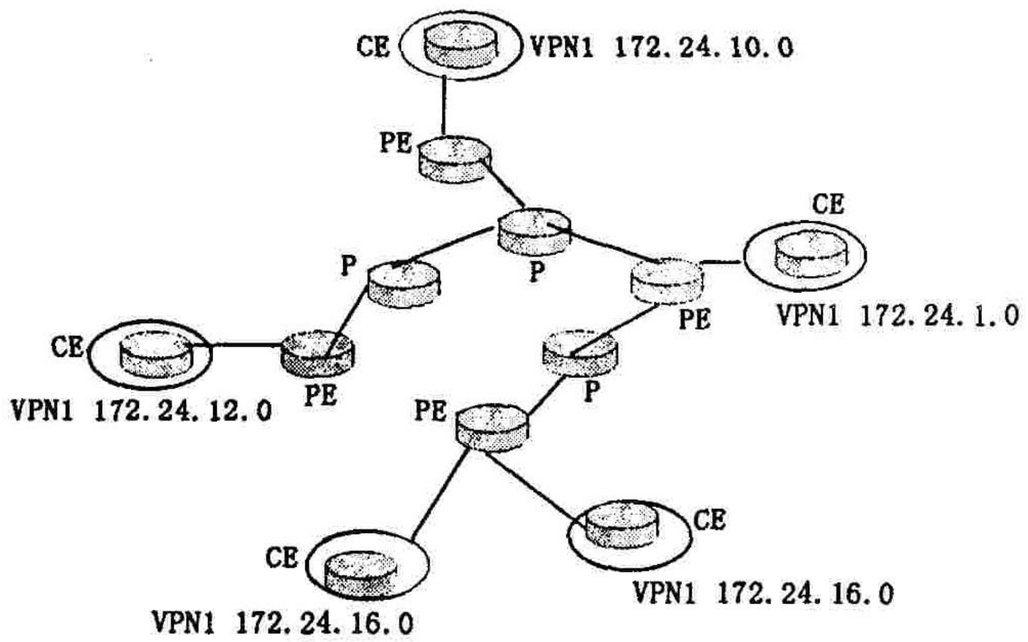

图1　MPLS VPN网络结构图

收稿日期：2005-03-11
作者简介：赵巧霞(1971-)，女，山西芮城人，讲师，硕士生，主要从事VPN网络安全技术研究；
孟相如(1963-)，男，陕西西安人，教授，博士生导师，主要从事宽带通信网络与视频技术研究.

2 MPLS VPN 安全方案设计

本文综合 IPSec 和 MPLS 的技术特点,提出了一种适合 MPLS VPN 的安全解决方案。实现方法为:利用 IPSec 协议在客户路由器端对 IP 数据包进行加密,在 MPLS 边缘路由器端对数据进行封装。具体过程如下:

1)数据包由工作主机发送到同一局域网内的客户路由器 CE;

2)CE 根据数据包的源和目的地址判断其是否需要加密;

3)如判断结果是需要加密,则调用 SPD 和 SADB 采用相应的策略进行加密;

4)加上 ESP 头的数据包由 CE 传送到服务提供商边缘路由器 PE;

5)PE 根据数据包逻辑端口来确定其 VPN ID,并加上 VPN 封装头;

6)PE 根据 VPN ID 查找转发表确定转发等价类 FEC;

7)PE 通过标签映射将一个标签指派给 FEC;

8)PE 由标签生成 MPLS 头,对已加密的数据包进行封装;

9)PE 将已封装好的数据发送至 MPLS 骨干网中。

为提高数据处理效率,本文使用 IPSec 的加密功能,并将加密处理工作分散到各客户路由器,以减轻服务提供商边缘路由器的数据处理工作量,以消除瓶颈问题。

2.1 封装安全载荷 ESP 对 IP 数据包的加密

封装安全载荷 ESP 是 IPSec 的一种协议,对 ESP 包的标识则是通过 IP 头的协议字段来进行的。一个受 ESP 保护的 IP 包的结构如图 2 所示。ESP 头包括 SPI 和序列号,ESP 尾包括填充项、填充项长、下一个头和验证数据(可选)[2]。其中,SPI 值和 IP 头之前的目标地址以及协议结合在一起,用来标识用于处理数据包的特定的那个安全联盟。序列号是一个独一无二的、单向递增的、并由发送端插在 ESP 头的一个号码。通过序列号,ESP 具有了抵抗重播攻击的能力。SPI 和序列号均经过了验证,但却都没有加密。ESP 保护的实际数据包含在载荷数据字段中。填充项用于在 ESP 中保证边界的正确,也可用来隐藏载荷数据的真正长度。填充长度字段定义添加多少填充,用来恢复载荷数据的真实长度,下一个头字段表明数据类型。

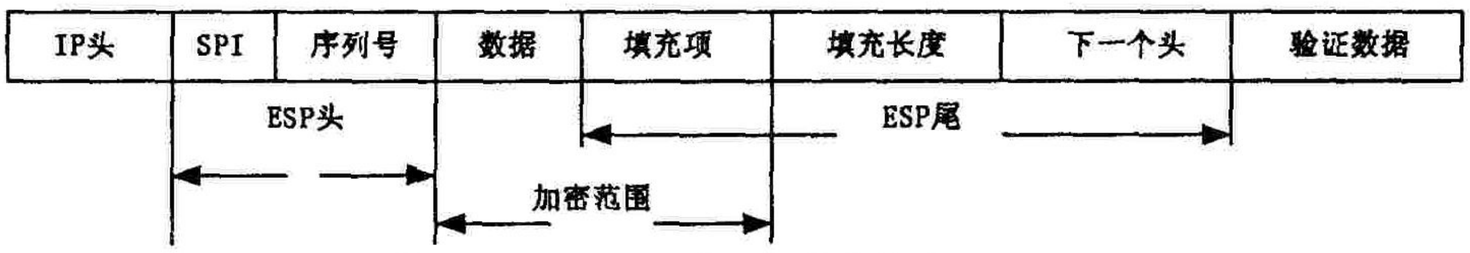

图 2 传送模式下受 ESP 保护的 IP 包

2.2 加密处理主流程

加密处理程序完成该方案的主要功能,该程序在客户边缘路由器上运行。一旦接收到客户端发送过来的 IP 数据包,即对其目标地址进行判断,以确定是否加密及安全策略,进行适当的处理后通过特定的逻辑端口发送至服务商边缘路由器上。加密处理程序如图 3 所示。

首先程序被 IP 数据发送时间激活,并从 IP 数据包中取得其源和目的地址 saddr 和 daddr。根据该地址在 SPD 中查找是否对其使用安全策略。如果找不到则不进行处理,将此 IP 数据包直接送出;否则根据相应 SPD 记录条目中的策略号 spd_policy,在策略数据库 policy 中查找相应的 IPSec 协议和使用的加密算法。同样地,根据其源和目的地址 saddr 和 daddr,在 SADB 数据库中查找相应的安全联盟 SA,如果找不到或者生存期已满(如果是硬生存期已满则删除此 SA),则调用 IKE 函数进行 SA 协商,将协商结果存入

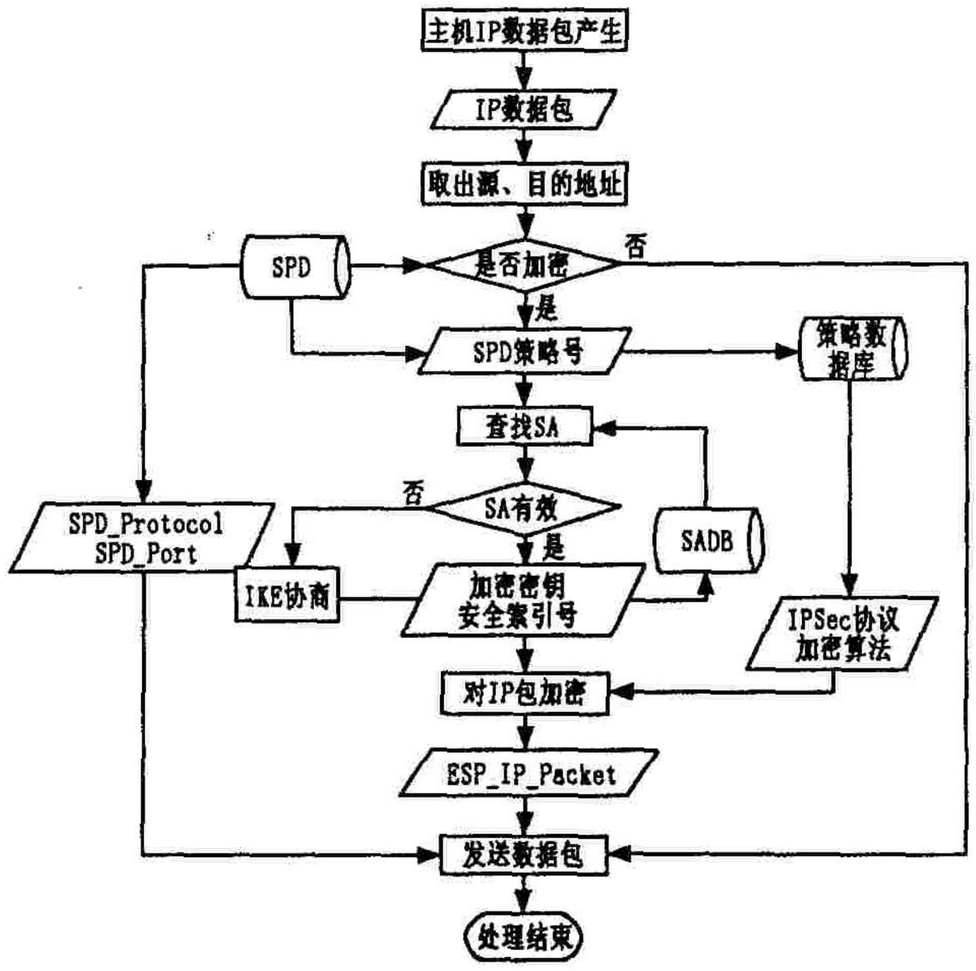

图 3 CE 对数据包的加密处理算法流程

SADB 数据库中。然后与找到 SA 的 IP 数据包一样，增加其序列号字段，取出其加密的密钥 sa - key 和安全索引号 sa_spi 再结合先前取出的 IPSec 协议和使用的加密算法，就可以调用 IP 数据包处理函数 ip_crypt，对原有的 IP 数据包进行加密处理。处理完毕后，根据从 SPD 中取得的中间协议 spd_prtc 和端口号 spd_port 将已经 IPSec 处理的数据包 esp_ip_packet 进行再一次打包。如此处理的目的是保证该数据包能够从指定的逻辑端口进入路由器中，以使路由器能根据特定的逻辑端口号确定其 VPN ID，以保证数据包在服务商核心网中能够正确并安全传输。此处，VPN ID 对于客户端的用户完全保密，其对应的逻辑端口号由服务商负责分配和发送。数据的接收可以看作是发送的逆过程。

3　MPLS VPN 离散事件系统仿真

不管是从其地域特性，还是从其所涉及到的设备来看 MPLS 网实际上是一个比较庞大的系统，采用离散事件系统仿真原理可以将图 1 所示的 MPLS VPN 结构图抽象为一个较简单的系统如图 4 所示，我们仅讨论其中的几个细节：IP 数据包的产生与发送，IP 数据包的加密。

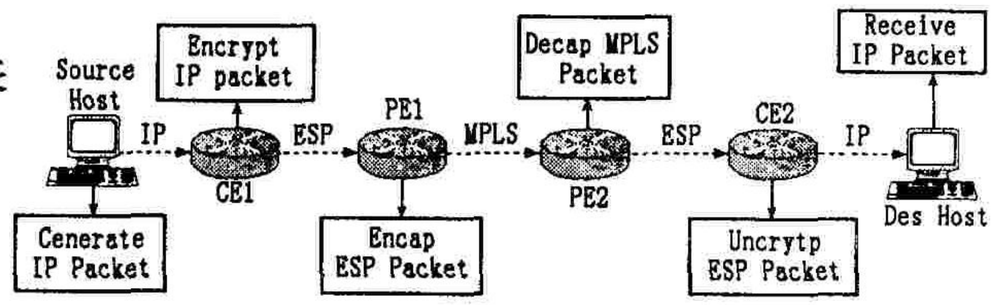

图 4　抽象后 MPLS VPN 结构图

在该图中每个设备的功能为：主机：产生和发送 IP 数据包；CE1：对 IP 数据包进行加密；PE1：对加密后的数据包进行封装后传给 MPLS 网络；PE2：对封装的 MPLS 数据包进行解包；CE2：对数据包进行解密。本文在 WINDOWS 2000/XP 平台上，采用离散事件系统仿真的方法，用 C + + 实现了 IP 数据包的模拟产生、发送、加密等过程。这里主要介绍仿真过程的主要算法及流程图。

3.1　MPLS VPN 的主仿真程序

按离散事件系统仿真原理设计仿真程序，采用事件调度法推进仿真钟。仿真框图如图 5 所示。其中最重要的是时间控制子程序与事件处理子程序。在每次仿真程序执行时，首先要由初始化子程序使系统处于一个设定的初始状态。时间控制子程序读取事件表，推进仿真时钟到下一事件发生时刻，事件处理子程序根据事件类型调用相应处理模块处理该时刻发生的事件，如在某特定时刻有 n 个原发事件，则要循环 n 次，而原发事件如带有后续事件，则需要调用它的后续事件子程序。

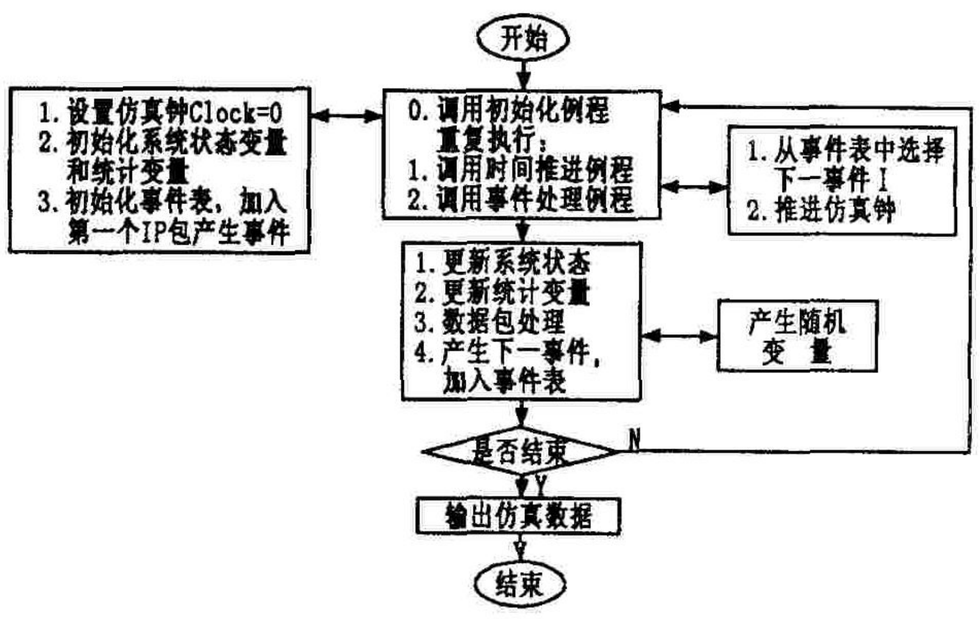

图 5　MPLS VPN 仿真框图

3.2　MPLS VPN 系统事件关系

本文所仿真的系统被看作一个多级排队系统，PE 和 CE 作为服务台各有两个队列，一个是数据包到来队列，一个是数据包发送队列。系统主要有以下几类事件：IP 包产生事件，IP 包到达事件，IP 包加密事件，加密后的 ESP 包发送事件，ESP 包封装事件及 ESP 解包事件和 ESP 包解密事件等。该系统的事件关系如图 6 所示。

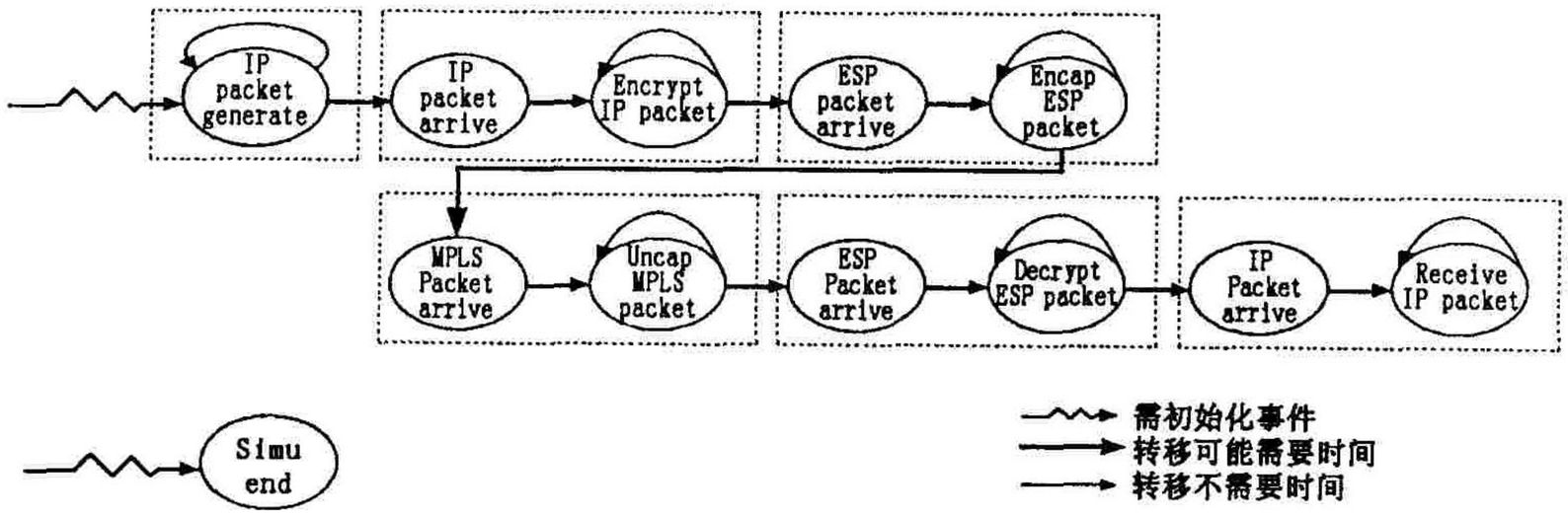

图 6　MPLS VPN 仿真事件关系图

本文采用事件调度法来推进仿真时钟。当事件发生时,需根据事件类型调用相应的事件处理例程(由于在接收端的事件处理和发送端类似,故不再说明)。

1)发送 IP 数据包事件

在该系统中源主机的功能是按事先给定的规律不断的产生 IP 数据包。在发送事件中,首先根据待发送的数据构造 IP 数据包,然后送入发送队列,产生下一发送事件,加入事件表中。

2)IP 数据包到达 CE 事件

CE 的接收缓冲器用队列表示,当源主机发出的 IP 数据包经过线路传输到达 CE 时,首先需要判断 CE 处理器是否空闲,若空闲则立即按 IPSec 处理逻辑进行处理,调度处理结束事件;否则加入缓冲队列等待。

3)CE 加密 IP 数据包事件

当 CE 处理器空闲,且等待队列非空时,取出队首 IP 包进行加密处理,调度下一处理事件。

4 结论

近年来 MPLS VPN 无论在理论研究还是在实际应用上均取得了很大进展,但是 MPLS VPN 的安全性问题尚未得到解决。本文针对 MPLS VPN 的安全问题,把 MPLS 和 IPSec 结合使用建立 VPN,即在客户路由器(CE)端用 IPSec 对 IP 数据包进行加密,在网络边缘路由器(PE)端采用 MPLS 技术进行封装。并采用离散事件系统仿真的方法,用 C + +语言实现了该方案的仿真。仿真结果表明 MPLS VPN 采用本文所设计的方案,具有更高的安全性能。

参考文献:

[1] 虞红芳,呼 钢,李乐民. 在传统 ATM 交换机上实现 MPLS 及其关键技术[J]. 电子科技大学学报,2000,29(4):434 - 439.

[2] 汪海航,潭成翔,师成江. 基于 IPSec 的 VPN 安全模型研究[J]. 计算机应用研究,2001,(6):56 - 60.

[3] 秦雅娟,林 生. 多协议标记交换技术及其性能[J]. 西安电子科技大学学报,1999,26(4):78 - 85.

[4] 吴 江,赵慧玲. 对多协议标记交换技术的体系结构及其应用的研究[J]. 中国通信,1994,(4):45 - 50.

[5] Casey Wilson,PeterDoak. 虚拟专用网的创建与实现[M]. 钟 鸣,魏允韬. 北京:机械工业出版社,2000.

(编辑:门向生)

Design and Simulation of Security Solution for MPLS VPN

ZHAO Qiao- xia1, MENG Xiang- ru1, ZHANG Fa2

(1. The Telecommunication Engineering Institute, Air Force Engineering University, Xi' an, Shaanxi 710077, China; 2. The Engineering Institute, Air Force Engineering University, Xi'an, Shaanxi 710038, China)

Abstract: MPLS VPN is an important technique for the implement of VPN, which is capable of overcoming some vital shortcomings of IP network and attracts wide attention. Combining the advantages of IPSec with those of MPLS, a security solution is put forward. MPLS VPN is modeled as a discrete event system. Then a simulation platform of MPLS VPN is built with C + + The security solution is verified and the result shows that it is feasible.

Key words : MPLS VPN; security ; IPSec ; discrete event system; simulation