基于高速边缘路由器的IPSec处理部件的研究*)

荣 霓 龚正虎 苏金树
(国防科技大学计算机学院 湖南长沙410073)

Study on the Technologies of IPSec Security Processing Unit in High Speed Boundary Routers

RONG Ni GONG Zheng-Hu SU Jin-Shu
(School of Computers, National University of Defence Technology, Changsha 410073)

Abstract High Speed Boundary Routers (HSBRs) are emerging due to improvement of network technologies. The peculiarity of HSBR requires high efficient security packets processing unit. This paper analyzes the characters of HSBR and introduces a IPSec security engine model based on the distributed paralleled HSBR prototype. Future develop of HSBR is given as well.

Keywords High Speed Boundary Router (HSBR), IPSec Engine

1 引言

随着网络技术的发展特别是网络安全技术的发展，路由器作为网络传输过程中的重要设备，对报文安全、正确和快速的转发起着越来越关键的作用，随着Internet和Intranet的连接速度越来越高，安全风险越来越大，高速边缘路由器应运而生。

定义1 高速边缘路由器(HSBR)是指位于Intranet和Internet之间，担负路由和安全防护的高速路由器。其线速一般要达到G比特级，总体速度达到数十G甚至T比特级，加密报文占报文总量的60%甚至更多，安全连接达到几万个以上。

HSBR所处位置的特殊性，决定了它比一般的路由器应该具有更强大的功能：一方面，网络速度的不断提升直接要求位于网络边缘的路由器具有更高的处理速度；另一方面，安全问题的日趋严重也对边缘路由器的安全性支持提出了更高要求。相对于核心路由器等骨干网路由交换设备，HSBR的安全指标更高，需要对它的安全管理体系进行合理的设计。

作为网络安全重要研究领域的IPSec[1]协议技术正被越来越广泛地应用于各种网络设备中，对于地处内、外网络安全的HSBR来说，实现IPSec具有重要的意义：IPSec是IETF提出的协议级安全框架，为网络安全问题的底层解决提供了一个通用的技术；协议族中的AH[2]和ESP[3]协议是IPv6中安全相关的组成部分，在HSBR上实现IPSec可以在技术发展上保证与下一代网络标准兼容；随着IPSec协议的不断完善发展以及IPv6的广泛使用，在边缘路由器上不提供对IPSec的支持将是不可想像的。目前，除了各个权威组织对协议标准本身的制定和不断完善外，大量的国外厂商也投入到以IPSec协议为安全引擎的网络设备研制中，在这种情况下，研制拥有自主产权的基于IPSec的HSBR对我国计算机安全技术的发展和应用具有重要意义。

但是，在HSBR上实现IPSec协议是比较困难的：由于HSBR所处的位置，决定了基于HSBR的IPSec实现比一般的主机实现或小规模路由器实现的安全连接(SA)数更多、传输速度更快，因此将要求HSBR中的IKE[4]实现能够进行更快速的处理，更少地占用系统资源，采取更灵活的激活和管理模式，以及提供更方便的配置和更强的人机交互能力，而IPSec协议本身的数据库管理和查询也需要得到改进和加强。在这种情况下，有必要研究适用于HSBR的高效IPSec引擎模型和实现策略。

2 IPSec安全引擎模型

2.1 HSBR各功能平面与IPSec的相关性分析

文[5]给出了基于安全平面划分的路由器平面划分策略，据此，可以得到HSBR中各平面中与IPSec相关的功能如下：

数据路径功能 主要包括：(1)转发决定生成：根据分组的目的地址查找路由表，确定每一分组的输出端口和下一跳地址。由于使用了IPSec，分组需要通过IPSec的安全审查，以区分是否IPSec报文。如果是，则必须转交IPSec安全引擎进行相应的处理以还原报文。(2)背板转发：由于IPSec的引入，还必须在转发前完成相关操作，即对于IPSec分组，安全引擎必须对它进行IPSec封装，同时按照新的报头地址决定输出端口。分组一旦完成转发决定，通过背板传送至输出端口，若不能立即传送，则进行排队，如果队列没有足够的空间，分组将被丢弃。(3)输出链路调度：分组到达输出端口后，在发送之前再进行排队。对于IPSec报文，可以通过仔细调度每一分组的离开时间来满足不同的延迟和吞吐率要求。

控制功能 主要包括系统配置、管理和路由表信息的更新等。

安全功能 是HSBR的重要功能，除了通用路由器的安全功能外，还包括与IPSec协议相关的功能，即：(1)IPSec安全引擎的设置，包括使用的加密算法、公共密钥生存周期等。(2)安全策略和安全连接的管理。(3)与其他协议的互操作性处理，如NAT等。

2.2 HSBR的IPSec报文出、入站策略分析

当报文从输入端口进入HSBR后，传统报文转发策略的

*)基金项目：国家自然科学基金项目(90104001)。荣 霓 博士研究生，研究方向：网络安全，新一代高速路由器体系结构等。龚正虎 博士生导师，研究领域：网络安全，协议工程，高速路由器体系结构。苏金树 博士生导师，研究领域：新一代高速路由器体系结构，网络安全。

由输入进程进行预处理——放入相应的输入队列中——多条输入队列的报文通过转发网络送入相应的输出队列——经过输出进程的统一处理交给输出端口的路径将随着 IPSec 的引入而发生变化。文[1]中给出了指导性的出站、入站报文处理流程，如果运用于具体的 HSBR 实施，以下的一些处理步骤将是实现的难点：

出站 IP 报文处理中 SA/SA 束选择部分：由于每个出站报文都要与 SPD 相比较以决定如何处理该报文，因此该操作是一个速度敏感的过程，特别是当 SPD 很大的时候。目前，基于网络安全策略的配置方式和效率的限制，该部分的实现主要集中于软件，主要采用顺序/双向链表访问策略，少数公司采用了 HASH 算法和2叉树搜索来进行优化。

出站 IP 报文处理中数据包的选择域符与 SA 束的选择域符匹配部分：该过程需要涉及 SAD 数据库的快速查找。目前大部分实现的 IPSec 应用规模都较小，使用优化技术的产品不多。但是，由于我们的研究是针对 HSBR 的应用，SA 的数量将是十分巨大的。当 HSBR 速度达到 T 级的时候，即使保守的估计，SA 的数量也将高达数兆，这时如果不采用查找优化技术来加速查找的话，将使得上述的处理阶段成为整个实现的瓶颈。

入站 IP 报文处理中在 SPD 中进行报文入站策略匹配部分：这里也存在一个查表优化问题。通过在 SAD 中保留指向 SPD 相关表项的回调指针，可以使用回调指针来完成该查询匹配。

2.3 基于分布并行 HSBR 模型的 IPSec 安全引擎结构

使用 NP 和 ASIC 是目前路由器硬件设计中应用日趋广泛的技术。考虑到 HSBR 的性能指标和功能特点，我们认为，HSBR 应该采用基于 NP 和专用 ASIC IPSec 处理引擎的分布并行实现技术，并提出以下的实现模型(见图1)。

其中，NP 为网络处理器，IPSecE 为 IPSec 安全引擎，包含 IPSec 报文的硬件快速处理通路和 SA 从控制器。

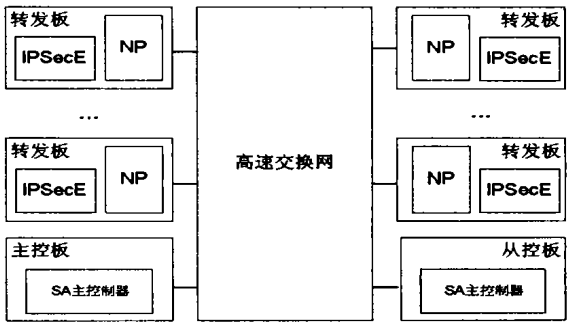

图1 并行分布式 HSBR 模型

该模型采用了分布方式实现数据通路的功能。这种方式使得主控 CPU 只负责控制通路处理，而将中低端路由器中用 CPU 实现的数据通路功能转移到各线卡上。这种方式是网络处理器与接口一对一地集成，其代表产品如银河玉衡9108核心路由器，特点是转发性能随接口数量自动增加。而另一种基于网络处理器与接口分离的方式，虽然转发性能可以根据需要配置，但是不利于规模的扩展。

本系统中，线速转发报文是通过网络处理器(NP)来实现的。NP 被置于线卡的快速通路上，通过基于硬件的 IPSec 报文分类，NP 将充分发挥对普通 IP 报文或者经 IPSecE 处理还原的 IP 报文的处理速度优势。目前，网络处理器能够处理多种接口速率，而且可以保持线速转发。文[6]给出了目前较流行的网络处理器，大部分都可以在 HSBR 中进行使用。

图2给出了基于该分布并行结构的 IPSec 安全引擎组成模块。

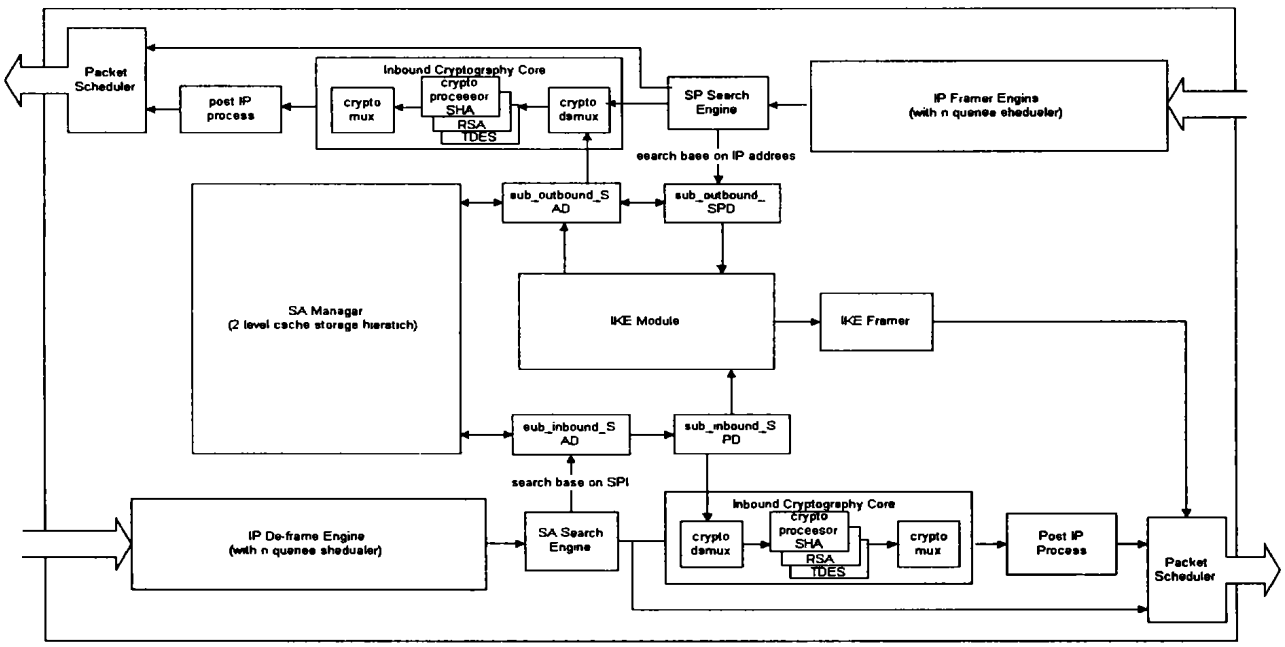

图2 IPSec 安全引擎组成模块示意图

该实现在 FlowThrough[7]技术的基础上，引入两级存储体系来进行 SAD 的存储和管理。通过将存储层次机制引入到 SAD 的管理中，可以保证出、入站报文查表过程的快速实时。在该存储体系中，主控加入了全局 SA 主控制器，在各线卡上使用 SA 从控制器。从控被置于 IPSecE 中，包含大容量的 cache 以便进行 SA 的分布存储。文[8]中分析了基于 M * N 的 MESH 网结构的快速路由器 cache 结构，得出的结论是数据块主处理器只需 M 比特，而转层节点只需 N 比特来记录共享情况。因此，该 SA 分布控制机制实现的代价是较低的。另外，系统还对 IKE 的处理和相关数据的存储进行了优化，

使用了基于 HASH 表存储的保护套件封装机制[9]。该机制可以解决目前多数系统中存在的以下问题：(1)由于两阶段协商涉及较多的状态，SV 和 SAM 处于分离的状态，SV 的变化不能直接作用到 SAM 上。(2)当待协商的 SA 数量较大时，基于线性链表的 SAM 保存和查找将消耗大量的时间(平均查询时间为 O(n))。该方式 IKE 实现的最大好处是使得 IKE 中 SA(包括 SA 素材)的管理得到保护套件的统一维护；同时，通过 HASH 表的组织，提供了快速查询的基础。该实现结构简单，易于硬件实现。一旦散列摘要部分的哈希计算采用硬件来实现，将显著缩短第三条消息的时间间隔，从而进一步提高 IKE 系统的整体性能。该存储机制的一个示意图如图3所示。

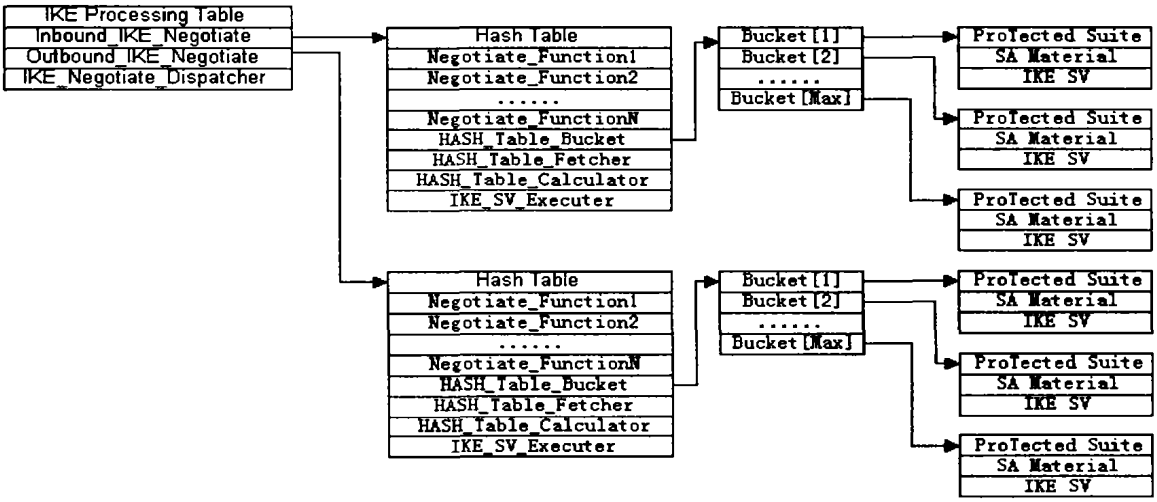

图3 基于 HASH 表存储的保护套件封装机制

从以上分析可以看出，整个 IPSec 安全引擎模型结构灵活，扩展能力强，是一个适于工程实现的高效 HSBR 模型。

总结和展望 HSBR 实现是一个在理论和工程上都有较大意义的课题。随着网络技术的进一步发展，大量原属于 MPP 的技术正在向以分布 NP 为主体的路由器平台迁移。本文分析了 HSBR 的功能和在 HSBR 上实现 IPSec 协议的特点，提出的基于分布并行结构的 HSBR 模型结构灵活、处理快速。可以预期，随着新一代网络处理器和现有微处理器之间的不断融合，以及大量专用芯片的出现，HSBR 将向更高速、更大规模的方向发展，可以提供更快的报文处理速度和更丰富的功能。

参 考 文 献

1 Kent S, Atkinson R. Security Architecture for the Internet Protocol. RFC2401. 1998. 11

2 Kent S, Atkinson R. IP Authentication Header. RFC2402. 1998: 15

3 Kent S, Atkinson R. IP Encapsulating Security Payload (ESP). RFC2406. 1998. 27

4 Harkins D, Carrel D. The Internet Key Exchange (IKE). RFC2409. 1998. 8～12

5 荣霓，龚正虎. 高速边缘路由器中 IPSec 安全引擎实现技术. 计算机工程与科学，2002

6 苏金树. 超高性能路由器. 中兴通讯技术，2001，8：34

7 NetOctave 公司. About the NetOctave FlowThrough Security Architecture. NetOctave NSP4200 Security Processor. 2002

8 汪波. 多处理器系统中高效 Cache 协议的实现方案与模拟：[博士论文]. 2001. 22～27

9 荣霓，龚正虎. 基于强安全通信策略 HLA 改进模型的研究与实现. 计算机研究与发展，2002

(上接第119页)

换。与采用单进程转换模型相比，有以下益处：1)进程 C_P 与 C_Q 可以单独执行，直至需要同步操作时，所以转换器可以并行运行，提高转换效率；2)转换器由两个进程 C_P 与 C_Q 构成，它的状态及转移被分成两部分，所以在调试时，比对单个转换器更容易调试；3)构造的转换器由两个转换进程组成，此方法不仅适合单网关结构，也适合半网关结构。

参 考 文 献

1 Saleh K, Jaragh M. Synthesis of protocol converters: annotated bibliography. Computer Standards &Interface, 1998, 19: 105～117

2 Lam S S. Protocol conversion. IEEE Transactions on Software Engineering, 1988, 14(3): 353～362

3 Takei K, Okumura K, Araki K. Design of gateway system between different signaling protocols of the multimedia session on the Internet. In: The 15th Intl. Conf. on Information Networking, 2001. 297～302

4 Shu J C, Liu M T. A synchronization model for protocol conversion. The 8th Annual Joint Conference of the IEEE Computer and Communications Societies, 1989, 1: 276～284

5 Shu J C, Liu M T. Protocol conversion between complex protocols. In: The 9th Annual Intl. Phoenix Conf. on Computers and Communications, 1990. 584～590

6 Shu J C, Liu M T. An approach to indirect protocol conversion. Computer Networks and ISDN Systems, 1995, 21(2): 93～108

7 Saha D. Verifying the progress properties of a heterogeneous protocol system in an internetworking environment. Computer Communications, 1995, 18(5): 384

8 Dutta S K, Saha D, Das P K. Design of a parallel protocol verification system. The IEEE Region 10 Annual Conference on Speech and Image Technologies for Computing and Telecommunications, 1997, 2: 425～428

9 Hallal H, Negulescu R, Petrenko A. Design of divergence-free protocol converters using supervisory control techniques. The 7th IEEE International Conference on Electronics, Circuits and Systems, 2000, 2(1): 705～708