第34卷 第19期 计 算 机 工 程 2008年10月
Vol.34 No.19 Computer Engineering October 2008
·安全技术· 文章编号：1000—3428(2008)19—0147—04 文献标识码：A 中图分类号：TP309

VPN安全网关IKEv2-EAP/SIM扩展研究与设计

胡 平[1]，唐佳佳[1,2]，陆建德[1]
(1. 苏州大学计算机科学与技术学院，苏州 215006；2. 苏州科技学院计算中心，苏州 215009)

摘 要：以往安全网关的实现偏重于单一功能，且认证方式不够灵活。该文对最新IKEv2动态密钥协商机制进行研究和分析，结合EAP可扩展认证机制的优点，提出将EAP/SIM认证框架引入IKE认证体系的思路，给出实现方案，设计了基于EAP/SIM的增强型可扩展IKEv2系统。IKEv2-EAP系统以RADIUS为认证服务器实现AAA功能，使用新的IKEv2-EAP/SIM交互建立了安全的IPSec隧道，使VPN网关功能更趋灵活、强大及多样化。

关键词：EAP协议；SIM认证；IKEv2系统；RADIUS服务器；VPN网关

Research and Design of IKEv2-EAP/SIM Extension in VPN Security Gateway

HU Ping[1], TANG Jia-jia[1,2], LU Jian-de[1]
(1. School of Computer Science and Technology, Soochow University, Suzhou 215006;
2. Computing Center, Suzhou University of Science and Technology, Suzhou 215009)

【Abstract】Anciently, the implementation of security gateway only emphasizes on one side function and the authentication way is not flexible. This paper researches and analyzes deeply on latest IKEv2 protocol of dynamic key negotiation mechanism and combines the advantages of EAP, then gives a solution that introduces the EAP/SIM authentication framework into IKE authentication system and designs an enhanced extensible IKEv2 system based on EAP/SIM. IKEv2-EAP system takes RADIUS as the authentication server implementing AAA functions and employs up-to-date IKEv2-EAP/SIM interaction setting up the secure IPSec channels. This makes the function of VPN gateway more flexible, stronger and diversity.

【Key words】EAP protocol; SIM authentication; IKEv2 system; RADIUS server; VPN gateway

1 概述

早期的IKEv1建立SA需要进行多轮协商，消息往返次数太多，其复杂性带来一些安全及性能上的缺陷，在实际应用中极大地影响系统的效率和性能。新发布的IKEv2较IKEv1做出了许多重大改进。文献[1]指出IKEv2保留了IKEv1的基本功能，同时兼顾了高效性、安全性、健壮性和复杂性的要求，以IKEv2取代IKEv1作为新一代的密钥交换协议标准已逐渐成为业内人士的共识。EAP是一个通用的身份认证协议，它与RADIUS服务器结合支持多种认证方法。文献[2]指出IKEv2除支持预共享密钥和数字签名2种认证方法外，同时引入对EAP协议的支持，增加认证方式的灵活性，使响应方更易从EAP认证服务器中分离出来。文献[3]指出EAP-SIM认证方法基于SIM卡中的数据和算法，通过使用多重认证三元组(RAND, SRES, Kc)来创建认证应答和更安全的会话密钥，并采用A3/A8加密算法保证安全性。

2 IKEv2动态密钥交换与EAP扩展认证过程

2.1 IKEv2动态密钥交换过程的分析

IKE动态密钥交换协议为VPN IPSec双方提供用于生成加密密钥和认证密钥的密钥信息，对IPSec实体进行认证并在实体间建立IPSec安全关联SA。IKEv2交互过程分为2个阶段：(1)初始交互：建立IKE_SA(IKE_SA_INIT交互)和第1个CHILD_SA(即IPSec SA)。(2)在第1阶段建立的安全关联(IKE_SA)的保护下创建一个或多个CHILD_SA或进行消息交互。在初始交互过程中需要先对双方实体进行身份认证，确定IKE_SA_INIT交互建立的IKE_SA是可信以及安全的，才能建立相应的CHILD_SA。动态密钥交换过程如图1所示。

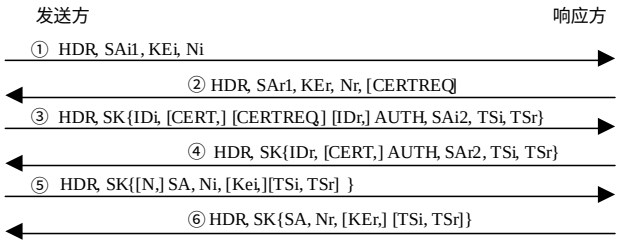

图1 IKEv2动态密钥交换过程

消息①~消息④为初始交互过程。其中，消息①、消息②为IKE_SA_INIT交互，主要用于协商加密算法、交换nonce值并完成D-H密钥交换，计算生成用于加密和完整性验证的后续交互密钥材料；消息③、消息④为IKE_AUTH交互，用于验证前2条消息、交换身份信息和证书，同时采用预共享密钥或数字签名方式进行身份认证，建立IKE_SA和第1个CHILD_SA。除IKEv2消息头外，IKE_AUTH交互中的消息都使用IKE_SA_INIT交互时生成的密钥材料进行加密和完

基金项目：江苏省自然科学基金资助项目(BK2004039)
作者简介：胡 平(1983－)，女，硕士研究生，主研方向：计算机网络与网络安全，网络协议分析与设计；唐佳佳，硕士研究生；陆建德，教授
收稿日期：2007-11-18 **E-mail：**ping_hp0901@163.com

整性保护，保证身份信息不被恶意第三方获取。

消息⑤、消息⑥为交互的第 2 阶段创建 CHILD_SA，可由通信的任一方在初始交换结束后发起，以生成额外的 CHILD_SA 或进行重新密钥协商(rekeying)。消息⑤发送 SA 提案，交换 nonce 和流量选择符 TSi, TSr；消息⑥对 SA 提案和流量选择符进行响应，交换 nonce。消息可选择的进行 DH 值的交换以实现完美向前保密(PFS)。

IKEv2 定义了消息交互来实现在密钥协商期间通信一方告知对方发生的错误或通知某些事件。消息交互必须在初始交互后，在协商完成的 IKE_SA 保护下进行。交互中的消息包含零个或多个通知载荷 N、删除载荷 D 或配置载荷 CP 等。

2.2 IKEv2 中的 EAP 扩展认证过程分析

EAP认证机制无须在链路控制阶段预协商过程中指定，只需先行说明使用EAP认证，采用的具体认证方法将推迟到认证阶段再指定。这就允许认证方在决定采用何种认证机制前得到更多的信息，还允许将认证方从认证服务器分离出来，认证方无须清楚每一种认证方法，只是作为认证服务器的代理转发数据包，而由认证服务器来真正实施各种认证方法。IKEv1 仅仅支持数字签名和预共享密钥 2 种方式。前者需要进行PKI的部署，实施和管理都比较复杂；后者安全强度比较低。IKEv2 继承原有的认证方式，并将EAP认证思想引入 IKE交互的认证过程， 提高了认证方式的灵活性和可扩展性。IKEv2/EAP认证的初始交互过程分析如图 2 所示[2, 4]。

图 2　带 EAP 的 IKEv2 初始交互过程

消息③不发送 AUTH 载荷，表明使用 EAP 认证。接收方的 IDr 在消息④发出，此消息里的 AUTH 载荷由接收方的私钥签发，进行第 1 次对接收方的认证，并把 SAr2 的响应推迟到 EAP 交互以后发送。消息⑤、消息⑥执行 EAP 交互，对 IPSec 双方实体进行身份认证，衍生主会话密钥 MSK。消息⑦、消息⑧创建第 1 个 CHILD_SA，响应消息③中的 SAr2, TSi, TSr，AUTH 载荷由衍生的 MSK 产生。

另一方面，根据RFC3579[5]，在RADIUS协议中也引入了对EAP的支持，在原协议的基础上增加了 2 个新属性：EAP- Message和Message-Authenticator，利用EAP的特性支持多种认证协议。且在NAS作为RADIUS的客户端时，并不需要处理EAP数据包，仅仅作为透明传输代理，对用户传来的EAP数据包重新封装成RADIUS数据包发送给服务器，对服务器过来的数据包解析出EAP消息再发送给用户。

3　基于 IKEv2-EAP/SIM 系统扩展设计

以往对 VPN 安全网关的研究大致分为 2 个方向：(1)集中完成 IPSec 功能，为远程用户与网关间或网关与网关间建立安全隧道，对远程用户的认证方式仅局限于数字证书和预共享密钥 2 种。但前者需部署 PKI，后者安全强度较低并且不够灵活、不易管理。(2)集中于将 RADIUS 客户端功能嵌入 VPN 网关以实现对内部网络用户的认证、计费、授权，远程用户与网关之间仅仅采用明文传输或安全性不高的 CHAP 协议，导致用户信息容易泄露。本文根据两者的优点与不足，在安全网关中同时实现 IPSec 及 RADIUS 客户端功能，并采用最新的 IKEv2 协议，引入 EAP/SIM 认证，既保证了远程用户与安全网关间数据传输的安全性，又实现了对远程用户的 AAA 功能，能实现双向认证和动态密钥分发，提高了认证方式的灵活性。

3.1　EAP 认证方法的选取

常用的 EAP 认证方法有 EAP-MD5, LEAP, EAP-TLS, EAP-TTLS, EAP-SIM 和 EAP-AKA 等。EAP-MD5 方法简单，但安全性不高并且是单向认证不能产生主密钥；EAP-TLS 安全性高且是双向认证可以产生主密钥，但双方均需数字证书；EAP-TTLS 能够提供双向认证和动态密钥分发，但认证服务器需要提供数字证书；EAP-SIM 基于移动用户的身份识别模块，可以产生主密钥；EAP-AKA 是 3GPP 研究的一项 3G 和 WLAN 融合的双向认证方案，基于对称密钥认证，主要在通用移动通信系统(UMTS)中运行，向下兼容 GSM 认证。在 EAP 方法的选取上，一方面由于 EAP-MD5 方法简单不能产生 MSK 不便采用，另一方面非常流行的 EAP-TLS/EAP-TTLS 是基于证书的双向认证，与 IKE 中引入 EAP 方式认证的初衷相违背。EAP-AKA 实现相对复杂，所以本文采用 EAP-SIM 方法作为具体的 EAP 认证方法来设计实现。

在基于 SIM 卡的双向认证机制中，首先由客户对认证中心认证，客户端将由 Challenge 报文带来的服务器端的 MAC 与本地通过同样的数据和算法得到的 MAC 进行比较。若不一致，则认为认证中心非法，中止本次认证；若一致，则客户端将本地生成的另一鉴别码 MACSRES 通过回复报文返回认证中心，认证中心将收到的 MACSRES 与本地的鉴别码 MACSRES 进行比较，若一致，则认证通过，发送认证成功报文；反之，发送认证失败报文。

利用文本文件来模拟 SIM 卡相关信息，用 3 组 RAND 计算得到 3 组 SRES 和 Kc，并把 SRES 和 Kc 作为产生鉴别码的种子，进行计算产生最终的鉴别码 MAC 和 MACSRES，并将值放入 EAP-SIM 报文的 AT_MAC 属性值中进行传递。

3.2　基于 IKEv2-EAP/SIM 系统接口设计

在本设计中(如图 3 所示)，响应方在查询发起方第 3 条消息是否含有 AUTH 载荷来确定发起方是否使用 EAP 方法。若采用 EAP，则进入 EAP 身份认证过程。

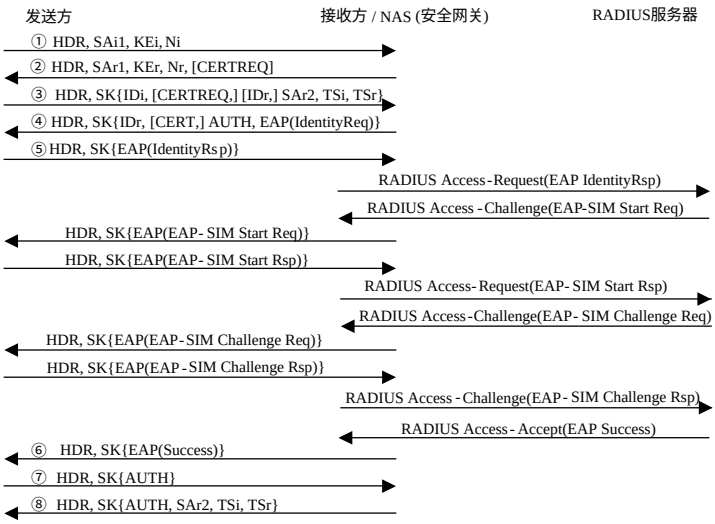

图 3　IKEv2 的 EAP/SIM 认证交互设计

图 3 中部列出了 EAP/SIM 具体的交互过程。在 EAP 交互结束后，确定了发起方的身份，同时生成了主会话密钥 MSK，才能继续进行 IKE 交互，继续 IKE_SA 的建立。而为了确保 EAP 交互的安全性，避免中间人攻击，将 EAP 交互过程嵌入在 IKE 交互过程中，并用 IKE_INIT 阶段协商的密钥实施加密和完整性保护。

4 基于 IKEv2-EAP/SIM 的系统实现

4.1 EAP/SIM 认证方法客户端实现

IKE 交互中的发起方在 EAP 交互中充当客户端的身份，响应方充当服务器身份。发起方只能从响应方收到 IKE 消息，从消息相关字段中获取 EAP 载荷，从中解析出相应的 EAP 消息内容。通过对 EAP 消息内容的解析和应答，实现 EAP 交互，完成 EAP 认证。EAP 载荷中的 EAP 消息由 5 个字段组成：code, identifier, length, type 和数据。

当发起方收到 EAP 载荷时，取出其中的 EAP 消息，判断 code 字段的值，若为 EAP_SUCCESS，则计算 auth_data 填充 AUTH 载荷；若为 EAP_FAILURE，则 EAP 认证失败，中止此次 IKE 交互；若为 EAP_REQUEST，则判断 type 字段的值：若是 EAP_ IDENTITY，则说明需要发起方表明其身份，发起方生成带有本方 ID 的 EAP 响应消息；若 type 字段的值为 EAP_SIM(18)，则对 EAP-SIM 的子属性进行判断，根据不同的阶段(SIM-START 或 SIM-CHALLENGE)构造不同的 EAP 响应消息，具体如图 4。

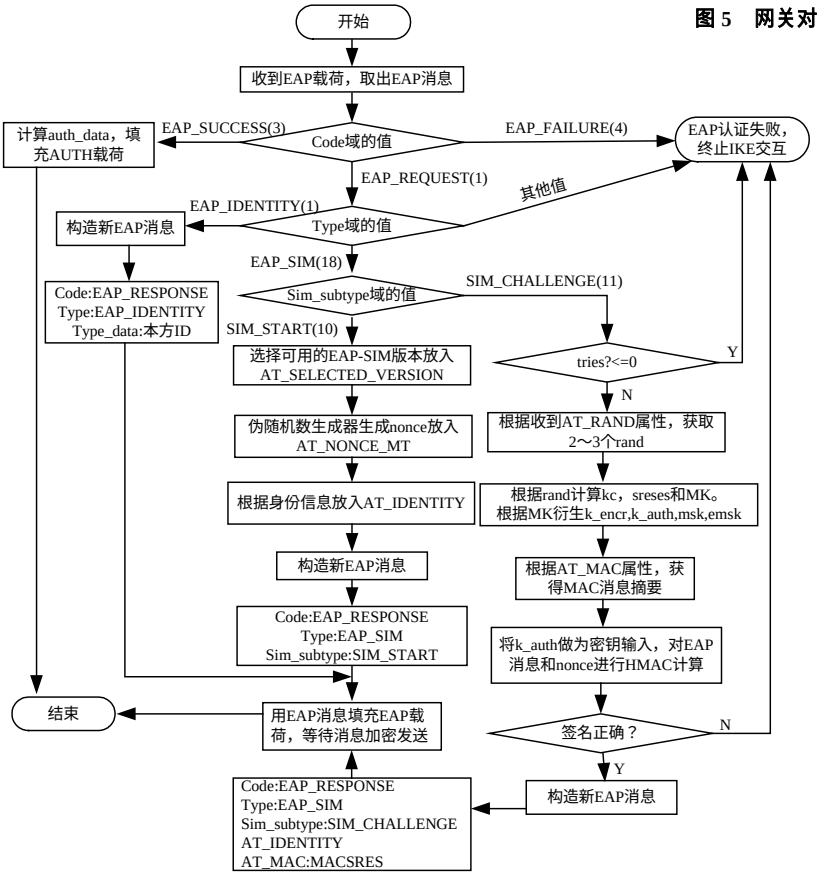

图 4　EAP/SIM 认证方法客户端实现

将构造好的 EAP 消息封装在 EAP 载荷中，在 IKE_INIT 阶段协商好的密钥 SK_ei 保护下发送到响应方。其中：AT_MAC=HMAC-SHA1-128(K_aut,EAP packet| 3*SRES)；MK = SHA1(Identity|3*Kc| NONCE_MT| Version List| Selected Version)。

4.2 网关对 IKEv2-EAP 响应的具体处理过程

网关对 IKEv2-EAP 响应的具体处理过程如图 5 所示。

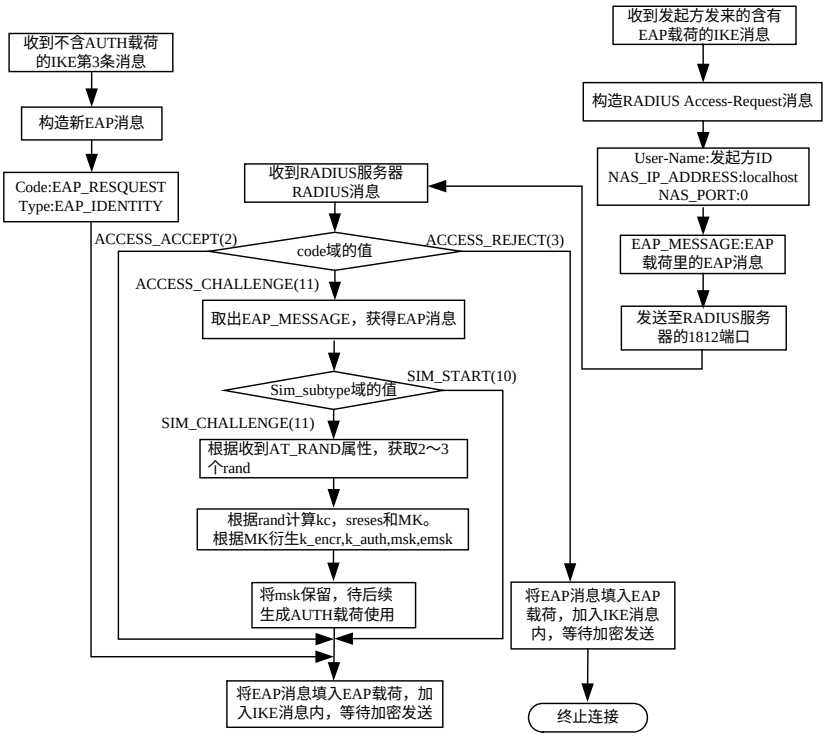

图 5　网关对 IKEv2-EAP 响应处理过程

响应方即网关作为 EAP 交互中的服务器，需要将客户端的 EAP 响应信息传递到 RADIUS 服务器进行认证，同时将 RADIUS 服务器的请求信息返回给发送方。

当响应方从 IKEv2 消息中获取 EAP 载荷，并取出其中数据部分得到 EAP 消息时，其直接将 EAP 消息封装成 RADIUS 消息报文发送到 RADIUS 服务器 1812 端口。当从 RADIUS 服务器获得 RADIUS 消息报文时，需要先将 RADIUS 报文解析，取出 code 字段值进行判断，若为 ACCESS_ACCEPT，则取出消息中的 32 位的 MS-MPPE-Recv- Key 属性值与 32 位的 MS-MPPE-Send-Key 属性值，合并后构成 MSK 保留待后续生成 AUTH 载荷，然后取出 RADIUS 消息中 EAP_MESSAGE，封装到 IKE 消息的 EAP 载荷中继续 IKE 交互。主要设计的 API 函数有

(1)收取从 RADIUS 服务器发来的包：

RADIUS_PACKET *rad_recv(int fd);

(2)发送数据到 RADIUS 服务器，等待响应：

int rad_send(RADIUS_PACKET *packet, const RADIUS_PACKET *original, const char *secret)

(3)检查 RADIUS 包，计算摘要，解析属性：

int rad_decode(RADIUS_PACKET *packet, RADIUS_ PACKET *original, const char *secret);

(4)对从发送方收到的 EAP 消息，进行封装发送：

static int sendrecv_eap(private_eap_authenticator_t *this, RADIUS_ PACKET *rep)

4.3 AAA 认证服务器端处理

本系统使用的 AAA 认证服务器是使用 FreeRADIUS 搭建的，后台使用 MySQL 来存放用户信息。具体的 EAP/SIM 认证由 RADIUS 服务器完成。具体处理流程如图 6 所示。

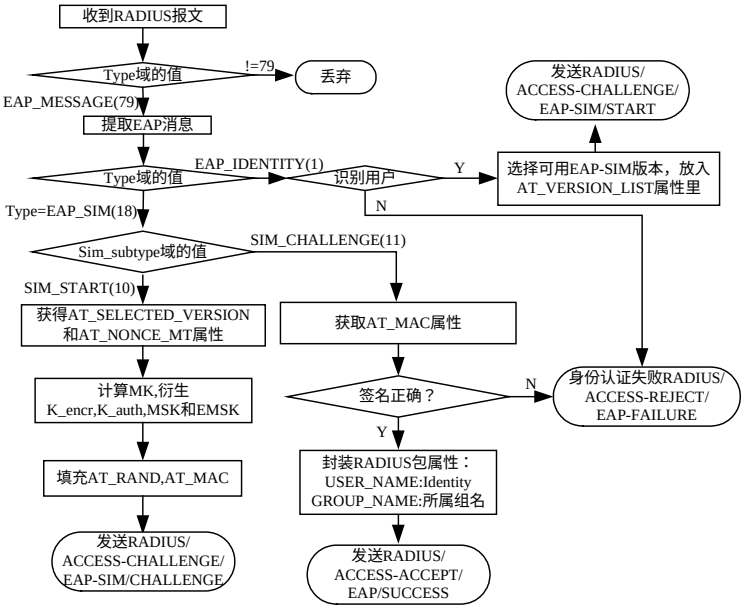

图 6　AAA 认证服务器端处理流程

当 RADIUS 服务器收到网关发来的含有 EAP 身份响应消息，加入 EAP SIM_START 请求消息，并加入 AT_VERSION_LIST 属性列举本 AAA 系统所支持的 EAP/SIM 版本，封装成 RADIUS ACCESS_CHALLENGE 消息发往网关；当 RADIUS 服务器收到 EAP SIM_START 响应消息时，根据 EAP 客户端的身份 Identity、选取的版本号 AT_SELECTED_VERSION 属性和 AT_NONCE_MT 属性计算主密钥 MK，并从 MK 中导出加密密钥 K_encr(用于保护 AT_ENCR_DATA)、认证密钥 K_auth(用于计算 AT_MAC), MSK 和 EMSK。构造 EAP 消息，填入 AT_RAND 和 AT_MAC 属性，封装成 RADIUS ACCESS_CHALLENGE 消息发送给网关。当 RADIUS 服务器收到网关 EAP SIM_ CHALLENGE 响应消息后，用 MAC 算法对数据进行散列，与收到的 AT_MAC 比较，若相同则认证通过，发送 RADIUS ACCESS-ACCEPT(EAP(SUCCESS)) 消息，否则 RADIUS ACCESS-REJECT(EAP(FAILURE))。其中，MK = SHA1(Identity|n*Kc|NONCE_MT|VersionList|SelectedVersion)。

5 结束语

本文将 EAP/SIM 认证方法引入 IKEv2，实现双向认证和动态密钥分发，加入了 AAA 服务器接口设计，增加了对各种 EAP 认证方法的支持，所设计的系统既继承了原有认证体系；也增强了 IKEv2 的扩展性，在 VPN 机制中结合了 AAA 功能，使远程接入用户认证更加安全。

参考文献

[1] 高　翔, 李亚敏, 郭玉东, 等. IKEv2 协议安全性分析与改进[M]. 计算机应用, 2005, 25(3): 75-76, 84.

[2] Kaufman C. Internet Key Exchange (IKEv2) Protocol [EB/OL]. (2005-12-17). http://www.ietf.org/rfc/rfc4306.txt.

[3] Haverinen H, Salowey J. Extensible Authentication Protocol Method for Global System for Mobile Communications(GSM) Subscriber Identity Modules(EAP-SIM)[S]. RFC 4186, 2006-01.

[4] IETF. Internet Draft: Extension for EAP Authentication in IKEv2 [EB/OL]. (2006-06-26). http://tools.ietf.org/html/draft- eronen-ipsec-ikev2-eap-auth-05.

[5] Aboba B, Calhoun P. RADIUS(Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol(EAP) [EB/OL]. (2003-09-24). http://www.ietf.org/rfc /rfc3579.txt.

（上接第 117 页）

由图 4 可知，采用本 QoS 框架的网络，在网络负载趋于饱和的情况下，通过降低低优先级业务(优先级 4 和优先级 5)的带宽占用量(分别降低 100 Kb/s)，高优先级(优先级 7)的新申请接入流在申请时间(250 s)后不久能够接入网络，并获得了其请求的带宽(200 Kb/s)。由图 5 可知，随着网络规模的加大，本 QoS 框架相对于 SWAN 模型其业务的端到端时延维持在较低水平。综合来看，本文提出的 QoS 框架能够达到预期的效果，既能够保证高优先级的业务优先使用网络资源，又能够满足不同类型的业务流的端到端时延要求。

4 结束语

本文提出的 QoS 框架，能够区分不同优先级的业务和不同 QoS 要求的业务，保证高优先级的业务对网络资源的优先使用权。本 QoS 框架具有很好的自适应性以及可扩展性，适合新时期的 Ad Hoc 网络要求。

参考文献

[1] Zhou Bosheng, Marshall A, Lee T H. A Cross-layer Architecture for DiffServ in Mobile Ad-hoc Networks[C]//Proc. of 2005 International Conference on Communications and Mobile Computing. [S. 1.]: IEEE Press, 2005: 833-838.

[2] Ramani R, Karandikar A. Explicit Congestion Notification in TCP over Wireless Network Personal Wireless Communications[C]// Proc. of 2000 IEEE International Conference on Digital Object Identifier. [S. 1.]: IEEE Press, 2000: 495-499.

[3] Bennet J C R, Zhang H. WF2Q: Worst-cast Fair Weighted Fair Queuing[C]//Proceedings of IEEE INFOCOM'96. Palo Alto, CA, USA: [s. n.], 1996: 143-156.

[4] Zhu Kai, Viniot Y. Achieving End to End Delay Bounds by EDF Scheduling Without Traffic Shaping[C]//Proceedings of IEEE INFOCOM'01. Alaska, USA: [s. n.], 2001.