研究报告

EAP－FAST 在公共无线局域网安全接入控制中的研究及实现

曹　萍，裴文江
（东南大学无线电工程系，南京　210096）

[摘要]　Cisco 公司于 2004 年提出基于隧道的灵活认证协议（EAP－FAST）以替代存在安全漏洞的 LEAP 认证协议，该协议具有安全性和易部署性的特点。文章论述了基于 802.1x 协议的 EAP－FAST 认证协议及其实现技术，并在公共无线局域网（PWLAN）综合实验平台上实现了 EAP－FAST 认证的客户端、认证者、认证服务器端功能。

[关键词]　公共无线局域网；端口访问控制协议（802.1x）；基于隧道的灵活认证协议（EAP－FAST）
[中图分类号]　TP393.17　　[文献标识码]　A　　[文章编号]　1009－1742（2005）12－0078－05

1　前言

无线局域网（WLAN）以其方便、快捷、廉价等诸多优势，在企事业内部和公共热点地区等领域的应用中很快取得了长足发展和巨大成功。按照其应用场合和规模，可将 WLAN 的模型分为：针对企业用户或特殊用途的小型单独 WLAN 网络；针对广域的面向公众的新型 WLAN 接入网。后者作为一种新的公共宽带移动数据接入业务，具有广泛的应用前景，且对用户数据接入和传递的安全性有很高的要求。

由于无线局域网信号传输开放性，有线网络容易实现的接入认证是 PWLAN 安全性的瓶颈。为了提高无线网络的安全性，在 IEEE802.11b 协议中包含了一些基本的安全措施，包括无线网络设备的服务区域认证 ID（ESSID），MAC 地址访问控制以及 WEP 加密等技术。可是上述认证方式安全性较弱，促使 IEEE802.11 工作组制定了 802.1x[1] 安全认证协议来解决无线局域网用户的身份接入认证问题。按鉴权凭证不同可分为两类：强口令认证及公钥证书身份认证。强口令认证中的身份凭证即为用户名和密码，数据交互没有加密保护，安全性弱，优点是易于部署；公钥证书身份认证中用户和服务器利用公钥证书作为凭证，安全性高，但缺点在于供应商需要 PKI 设施管理证书，难于部署。目前通常采用的认证协议类型包括 EAP－MD5，EAP－TLS，LEAP，EAP－PEAP，EAP－TTLS。由于 LEAP 认证协议在字典攻击下是不安全的，因此 Cisco 公司于 2004 年提出 EAP－FAST 认证协议，具有安全性高和易部署性的特点。

笔者介绍公共无线局域网的安全体系结构，研究基于 802.1x 端口访问控制的 EAP－FAST 安全认证协议内容和特点，在 PLWAN 接入控制部分实现了 EAP－FAST 进行用户接入身份认证。

2　公共无线局域网安全体系结构

PWLAN 作为广域的面向公众的新型 WLAN 高速互连接入网，由于涉及到网络的拓扑结构、移动、漫游、认证、授权、加密、计费等多方面的问题，安全特性要求严格且复杂。PWLAN 安全体系包括网络接入控制和蜂窝网两部分，它们之间通过 IP 骨干网相互通信，如图 1 所示。

PWLAN 接入部分包括：移动终端（MT），无

[收稿日期]　2004－09－29；修回日期　2004－11－13
[基金项目]　“八六三”国家高技术研究发展计划资助项目（2002AA143040）
[作者简介]　曹　萍（1980－），女，江苏丹阳市人，东南大学无线电工程系硕士生，主要研究方向：信息安全

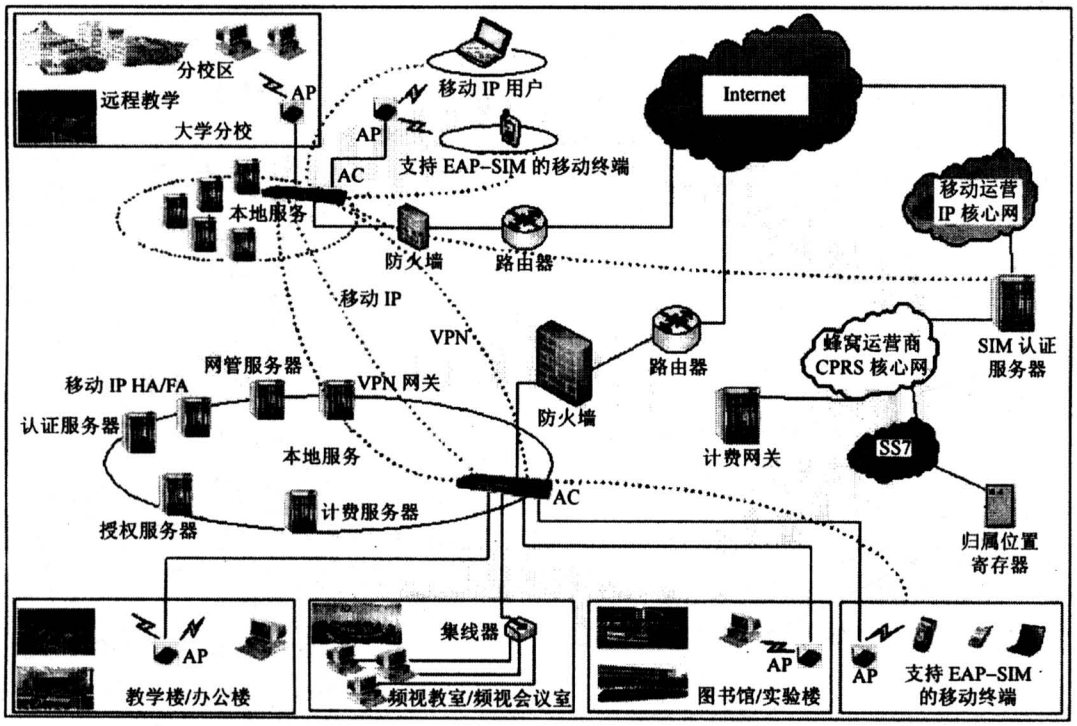

图 1　公共无线局域网安全体系结构（校园网型）

Fig.1　In fracture of secure system in public wireless local area network (campus-wide model)

线接入点（AP），接入控制器（AC），认证服务器（AS）等部分。移动终端为无线网卡以不同接口接入计算机终端，同时通过标准的 802.11x 空中接口接入无线接入点。无线接入点是 WLAN 的小型无线基站设备，完成 802.11x 标准的无线接入功能。它是一种网络桥接器，是连接有线网络与无线局域网的桥梁。接入控制器对来自不同接入点的数据进行汇聚，提供包括用户安全控制、认证控制、计费信息采集、网络安全管理等的用户控制管理功能。同时 AC 通过与 AAA 服务器交互为 PWLAN 提供有关用户的 AAA 信息，AC 可以直接和 AAA 服务器相连，也可以通过 IP 骨干网相连。AAA 服务器的认证中心主要设备是 RADIUS 服务器，用以存储用户的身份信息，并完成用户的认证功能；而计费中心则完成用户的计费功能。

3　端口访问控制协议的体系结构

802.1x 协议为基于端口的访问控制协议，它的体系结构包括 3 个重要部分：客户端、认证者、认证服务器。客户端（申请者）一般为一个用户终端，该终端通常需要安装客户端软件，当用户有上网需求时，通过启动这个客户端软件发起 802.1x 协议的认证过程。为了支持基于端口的接入控制，客户端需支持 EAPOL 协议。认证者在认证过程中起到传送认证信息的功能，所有的认证工作在申请者和认证服务器上完成。认证服务器，通常采用 RADIUS 服务器，该服务器可以存储有关用户的信息，通过检验客户端发送的信息来判别用户是否有权使用网络系统提供的网络服务。802.1x 标准采用现有的认证协议——EAP 认证协议[2]，EAP 帧包含在 802.1x 帧中，被称为 EAPOL，在申请者和认证者之间传输；认证者与认证服务器间同样运行 EAP 协议，EAP 帧中封装了认证数据，将该协议承载在其他高层次协议中，如 RADIUS，以便穿越复杂的网络到达认证服务器，称为 EAP over RADIUS。作为端口控制协议，802.1x 协议结构中的认证者对应于不同用户有两个逻辑端口：控制端口和非控制端口。非控制端口始终处于双向连通的状态，不管是否处于授权状态都允许申请者和局域网中的其他机器进行数据交换，主要用来传递 EAPOL 协议帧进行认证数据协商；控制端口只有在认证通过的状态下才打开，允许客户进行网络资源的访问等操作。

4　EAP－FAST 协议[3]研究

EAP－FAST 是基于 802.1x 认证协议，采用

TLS[4]加密隧道的安全认证技术。它针对强口令认证和公钥证书认证方式的优缺点，引入了受保护的访问密钥代替公钥证书，以求建立一条基于 TLS 的加密隧道，从而在加密隧道的保护下进行用户身份数据的传输，保证了用户数据不被攻击者获得。同时，利用强口令认证作为隧道内部认证方式，进行双方身份的认证，降低了部署难度。

4.1 基于 TLS 的加密隧道构建

EAP－FAST 使用了一种受保护的访问凭证（PAC）来生成加密隧道。该密钥由 TLS 可选密文套件中的加密算法保护，由客户端或者服务器产生。以 TLS－RSA－WITH－RC4－128－SHA 加密套件为例，在此加密套件下，PAC 密钥经 RSA 不对称加密之后传输。根据非对称加密算法特性，此时只有拥有 RSA 私钥的一端才能正确解开此报文，保证除了服务器和客户端之外的第三方无法获得 PAC。认证双方都获得 PAC 之后，将 PAC 作为密钥发生种子，派生出隧道加密套件所需的全部密钥。图 2 为隧道建立所需密钥的分层结构。

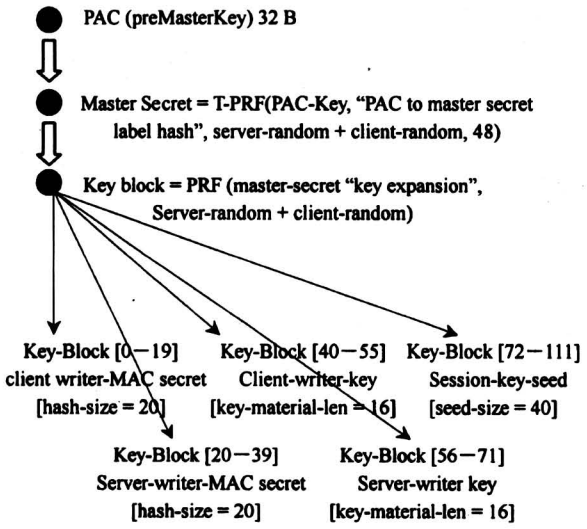

图 2 密钥生成材料的密钥分层结构图

Fig.2 The hierarchy of key material

Master Secret 是整个 FAST 认证的主会话密钥，可以根据 FAST 协议中给出的 T－PRF 公式由 PAC 计算得出。随后利用 PRF 公式由 Master Secret 派生得到密钥生成材料（Key-Block），如图 3 所示，得出双方建立隧道所需的密钥：writer－MAC－secret 密钥长度为 20 b，作为计算明文摘要的 SHA1 算法的密钥；writer－key 密钥长度为 16 b，作为对明文进行 RC4 流加密的密钥。

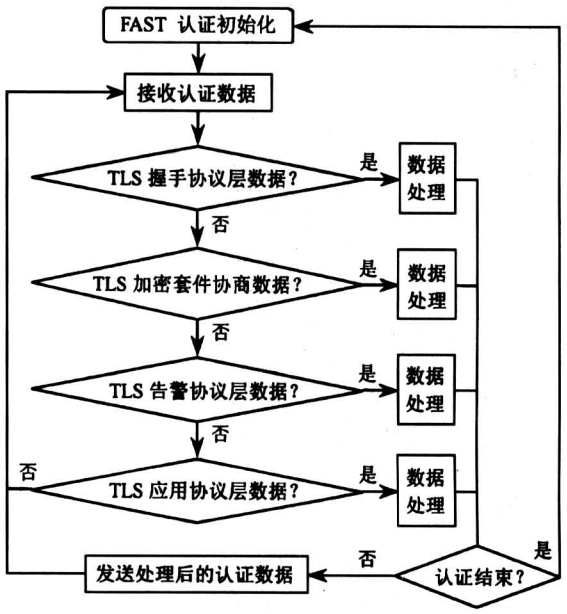

图 3 FAST 认证数据处理流程图

Fig.3 Authentication data processing flow chart of FAST

4.2 受加密隧道保护的内部认证

在成功建立加密隧道的基础上，方可进行 FAST 认证第二阶段。加密隧道中，通常采用强口令认证方式（＜username，password＞作为凭证）进行隧道内认证。加密隧道会对内部认证的明文数据用 writer－MAC－secret 计算摘要，并经过 writer－key 的 RC4 加密之后传输。受隧道保护的相互认证包括受 TLS 加密隧道保护的完整 EAP 会话，以及使用 Result-TLV 和 Crypto-Binding TLV 的受保护终端结尾。所有的 EAP 报文都需要封装在 EAP Message TLV 中。

4.3 认证流程

FAST 协议的认证阶段可以根据 TLS 隧道建立的先后分成两部分：双方协商 PAC，建立加密隧道；在加密隧道中进行内部认证。具体说明如下（以客户端产生 PAC 为例）：**a**. 服务器端向客户端请求发送身份，客户端同意后，双方开始 FAST 认证。**b**. 客户端和服务器端交换 client hello 信息，协商好加密算法列表。客户端随后接收服务器发送的 rsa 公钥，将 PAC 加密后发送给服务器端，服务器端利用 RSA 私钥解密，得到 PAC。**c**. 进行加密套件修改协商，成功则 FAST 认证第一部分完成，双方根据 PAC 生成加密隧道所需密钥。**d**. 加密隧道中，服务器和客户端协商内部认证方法，并交换认

证数据。随后客户端和服务器互相发送 Crypto－Binding TLV 包，若双方的 Crypto－Binding TLV 包都合法，发送成功状态的 Result TLV，反之发送失败的 Result TLV。此时认证结束，服务器端根据认证结果发送成功或失败包给客户端。

5　EAP－FAST 认证协议在 PWLAN 综合实验平台中的实现

EAP－FAST 的网络实体可以分为 FAST 客户端、认证者、FAST 服务器和内部认证服务器 4 部分。下面就分别按其在 PWLAN 接入控制部分中模块化实现的关键技术进行论述。

5.1　FAST 客户端——客户端内嵌模块

作为 PWLAN supplicant 的内嵌 FAST 认证模块，设计重点在于对客户端认证数据流的处理，对所有认证方式而言，其认证状态决定了数据处理如何跳转，将 FAST 认证状态分为 5 种：认证初始化（fastInit），握手数据交互阶段（inHandshake），密文规约修改阶段（inCipherChange），应用层数据交互阶段（inApplication）以及认证中出现错误时的告警协议数据交互阶段（inAlert）。FAST 认证初始化之后，数据处理核心根据上述 FAST 认证的 5 种状态进行处理。上述状态是不能提前跳转的，即收到相应阶段数据包的同时，根据认证的当前状态才能决定是否应该进行数据处理，如果数据不按流程到达，处理平面发出告警并开始等待下一次认证数据的接收。数据处理流程见图 3。

5.2　认证者——接入控制器内嵌模块

认证者是作为接入控制器 AC 中的子模块来设计。接收到的 EAPOL 包经过 AC 的认证者模块处理后把 EAP 包发送给认证服务器，得到认证结果后并调用接入控制引擎中的相应接口来设置用户状态。认证者包含 3 个主要功能模块及认证者状态机。**a**. 802.1x 管理信息库接口，负责向 MIB 库中读写 802.1xMIB 量，为 802.1x 平台访问 MIB 库提供一个统一的接口。**b**. 802.1x 本地处理：接收来自接入控制引擎传递的 EAP 数据包，并放入用户状态数据区中；向用户发送和接收 EAP 包或 EAPOL 包的同时设置在用户状态数据区中的 802.1x 状态机信号量，发送 EAP 包时需要将 EAP 包封装成 EAPOL 包再发送；认证成功或失败需要调用接入控制引擎中的相应的接口改变用户状态。**c**. 802.1x 远程处理：接收来自访问控制引擎传递的 EAP 数据包，并放入用户状态数据区中；向 AS 发送和接收 EAP 包的同时设置在用户状态数据区中的 802.1x 状态机信号量。**d**. 7 个认证者状态机：Authenticator Key Transmit，Authenticator PAE，Authenticator Timer，Backend Authentication，Controlled Directions，Key Receive，Reauthentication Timer 等分别完成了 802.1x Specification 中定义的各个相应的状态机功能（见 802.1x specification[1]）。

5.3　FAST 服务器与内部认证方法服务器——认证服务器内嵌模块

将 FAST 服务器和内部认证方法服务器融合为一个实体，作为 PWLAN AAA 认证服务器的 FAST 认证处理子模块，其认证处理流程和客户端类似。主要区别为在该模块中实现了一种内部认证方法 MD5[5] 作为 FAST 隧道建立后的强口令认证方式。

5.4　EAP－FAST 认证协议在 PWLAN 综合实验平台中的实现

PWLAN 综合实验平台包括基于 MPC860 自主开发的无线接入点，主要功能为：支持二层隔离，IAPP 协议，基于用户数量和流量的负载均衡方式，MAC 过滤，基于 Telnet，Console 和 SNMP 的网管功能，支持用户的漫游切换，802.1x 认证机制，64/128 位 WEP，TKIP 及 AES 加密，ESSID 及 MAC 地址访问控制等，并已开始批量生产。自主开发无线接入控制器主要功能为：支持 Web 认证、802.1x 认证，虚拟 SIM 认证、绑定认证及快速认证等认证功能；提供访问控制、带宽控制、移动 IP，AnyIP，VPN 等功能、计费采集和安全传输，全面体现 IP 网络的安全性与可管理特性；本地业务包括本地认证、计费、虚拟 SIM 开户、用户管理、计费规则管理、日志管理、用户挂历系统、内置 DHCP 服务器、内置 Portal 服务器，可节约组网成本并提高组网灵活性；自主开发网络管理系统包括对接入控制设备、接入点设备、主机实时拓扑结构管理、性能管理、配置管理、故障管理、日志管理、网络运行监控、用户管理等功能。在实现过程中 EAP－FAST 模块充分考虑了系统的整体结构，目前已在 PWLAN 综合实验平台上调试并运行成功。

6　结语

虽然 PWLAN 为移动用户提供了一种高速移

动数据接入手段，但是作为一种新的公共宽带移动数据接入业务，它的广泛应用还面临着巨大的挑战，同时也为 PWLAN 技术和业务的发展提出了要求，带来了机遇。EAP－FAST 作为 PWLAN 接入认证中采取的一种身份认证协议，是一个可扩展的构架，它允许使用预先公布的密钥来建立一个受保护的隧道，以用于相互间的认证。在研究 FAST 认证协议的特点与实现技术基础上，已在 PWLAN 综合实验平台上调试并运行成功，为下一步面向校园的安全无线网络试点的开设提供了一种关键身份认证技术。

参考文献

[1] IEEE Standard 802.1x－2001 Standard for Port based Network Access Control [S]. http: //standards. ieee. org/getieee802/download/802. 1X－2001. pdf, 2001

[2] Blunk L. PPP Extensible Authentication Protocol (EAP), RFC2284 [S]. http: //www. ietf. org/rfc/rfc2284. txt? number＝2284, 1998

[3] Cam-Winget N, McGrew D, Salowey J, Zhou H. EAP Flexible Authentication via Secure Tunneling (EAP－FAST), Internet Draft [S]. http: //www. ietf. org/internet-drafts/draft-cam-winget-eap-fast-01. txt, 2004－02－09

[4] Dierks T, Allen C. The TLS ProtocolRFC2246 [S]. http: //www. ietf. org/rfc/rfc2246. txt, 1999

[5] Rivest R. The MD5 Message-Digest Algorithm, RFC1321 [S]. http: //www. ietf. org/rfc/rfc1321. txt, 1992

The Research and Implementation of EAP－FAST Protocol in Public Wireless Local Area Network

Cao Ping, Pei Wenjiang

(*Department of Radio Engineeing, Southeast University, Nanjing* 210096, *China*)

[**Abstract**] Since the LEAP wireless authentication protocol is vulnerable to dictionary attacks, the flexible authentication via secure tunneling (EAP－FAST) was introduced by Cisco Corporation in 2004, which establishes a mutually authenticated protected tunnel to protect the authentication data. This friendly and easily deployable network access solution will be widely used in WLAN. The authors research and design this protocol in public wireless local area network, and implement the function of EAP－FAST peer, authenticator and FAST server in PWLAN integrate experimentation flat.

[**Key words**] public wireless local area network; port based network access control (802.1x); flexible authentication via secure tunneling (EAP－FAST)

(cont. from p.77)

[**Abstract**] Based on the characteristic of malleable iron, the technology of multistage heat treatment for malleable iron was investigated successfully. Compared with the present technology, the time of graphitizing annealing using new process was saved about 50%. The microstructure, with uniform distribution of fine polycrystal of graphite nuclei and full elimination of carbide, was obtained. Comprehensive mechanics performance of product exceeded that of present international standard . Two brands of KTH400－12 and KTZ750－02 can be added on the base of present international and "malleable iron" standards . Those products, such as line tool, pipe fitting for railway, engine piston of car etc, with better performances and credible qualities treated by the technology, were welcomed by users.

[**Key words**] malleable iron; cementite; multistage heat treatment; graphitizing annealing