DOI:10.7544/issn1000-1239.2015.20131376
52(3):671-680,2015

无线网络中身份认证协议选择方法

赵 婧 李 鑫 邓凌娟 李兴华 马建峰
(西安电子科技大学计算机学院 西安 710071)
(zhaojing201534@gmail.com)

A Selection Method for User Authentication Protocols in Wireless Networks

Zhao Jing, Li Xin, Deng Lingjuan, Li Xinghua, and Ma Jianfeng
(*School of Computer Science and Technology, Xidian University, Xi'an* 710071)

Abstract Generally, in wireless networks there are a certain number of candidate user authentication protocols which can be selected from, and how to select one that can fulfill the user's personalized requirements is an unsolved problem. There already are some studies on the authentication protocols, but most of them are from the protocol designers' perspective. To the best of our knowledge, this paper is the first to study how to select authentication protocols with considering the user's personalized requirements in wireless networks. From the perspective of users, we propose a solution that guides users to select from different authentication protocols according to their personalized requirements, taking into users' most concerning factors, e.g., security, energy consumption, authentication delay and their preference. The energy consumption is defined as the sum of the energy consumption of user transmitting, receiving messages and cryptographic operations involved in the process of interaction. The cryptographic operations include Hash algorithm, RSA key exchange, digital signature, symmetric encryption and decryption algorithm. Adopting our solution to the EAP protocols in WLAN, we evaluate the security and performance of the EAP-PEAP, EAP-TLS, EAP-TTLS/MD5 and EAP-TTLS/MSCHAPV2. The results show that, regardless of how users set the weight, EAP-TTLS/MSCHAPV2 and EAP-TTLS/MD5 are always better than EAP-PEAP and EAP-TLS.

Key words user authentication protocol; wireless network; security; performance; energy consumption

摘 要 无线网络中通常存在多种身份认证协议可供选择,如何选择一个能够满足用户个性化需求的协议是个尚未解决的问题.从用户的角度出发,针对无线网络的特点,在综合考虑了用户最为关心的几个要素,如协议的安全性、能量消耗、认证时间以及用户偏好的基础上,提出了解决方案.将能量消耗定义为用户发送、接收消息能量消耗以及交互过程中密码操作所涉及的能量消耗之和.其中,密码操作包括Hash算法、RSA密钥交换、数字签名以及对称加解密算法.实验部分对EAP-PEAP,EAP-TLS,EAP-TTLS-MD5和EAP-TTLS-MSCHAPV2这4种最为常用的协议进行比较,结果表明不管用户如何设置权值,EAP-TTLS/MSCHAPV2和EAP-TTLS/MD5总是优于EAP-PEAP,EAP-TLS.该方案通过考虑用户对身份认证协议的安全性以及性能方面的要求,按照用户的个性化需求进行了协议方案的选择.

收稿日期:2013-10-23;**修回日期**:2014-04-29
基金项目:国家自然科学基金项目(U1135002,61372075,61202389,61372075,61303221);中央高校基本科研业务费专项资金项目(K5051303004);国家密码发展基金项目(MMJJ201201004);地理信息国家重点实验室开放课题(SKLGIE2013-M-4-1)

关键词 身份认证协议;无线网络;安全性;性能;能量消耗

中图法分类号 TP393

随着无线通信技术的发展,无线网络在人们的生活中扮演着越来越重要的角色,但其开放性又要求其具有更加强健的安全保护机制.身份认证是保证无线网络安全至关重要的一个技术手段.研究人员已经在该方向上做了大量的工作:据维基百科介绍,目前在 WLAN 中存在 40 多种 EAP 认证方法[1-3];研究人员也针对 RFID 提出了众多的认证方法[4-7];在无线传感器网络也存在大量的认证协议[8-11].但这些工作主要是从设计者的角度出发,针对某一个具体认证协议开展研究,对其安全性和性能进行分析评估.但从用户角度来说,他们对认证协议的需求是多样的,不同的用户对认证协议有不同的要求:某些用户可能对协议的安全性非常重视,对协议的性能不太关注,而有的用户可能对认证协议的能耗非常在意,但对安全性要求不高.另外,即使同一个用户,他在对认证协议的需求也是动态变化的,如果用户在接入网络后想要进行的操作仅仅是访问网页、浏览新闻,那么他对安全性要求可能就不高,而对认证协议的性能比较关心;但如果他想要进行的操作是访问网上银行进行在线支付,那么他对认证协议的安全性要求就比较高,而对协议的性能就不太关注.因此面对众多的认证协议,如何选择一个满足用户个性化需要的协议,是一个非常有意义的问题.而越来越多的无线网络能够同时支持多种认证协议,如 Wi-Fi 和移动通信[12]等,这为用户认证协议个性化的选择提供了可能.目前已有的工作如文献[13-14]也涉及到了协议选择的问题,但他们主要是针对一般的安全协议而非认证协议来设计的,认证性只是作为其中影响协议选择的一个要素来考虑.而认证协议选择则是将认证协议本身作为研究对象,将影响认证协议的诸多因素考虑进来,特别是认证时延和身份保护等,这些因素在一般的认证协议选择中并未进行考虑,因此这些方案不完全适合无线网络认证协议的选择.

我们从用户的角度出发,针对无线网络的特点,综合考虑用户最为关心的 3 个因素:认证协议安全性、性能(认证能耗、认证时间)以及用户偏好,提出一种指导用户选择无线认证协议的方法.另外,我们将所提的方案用于 4 种 EAP 认证方法,发现 EAP-TTLS/MSCHAPV2 和 EAP-TTLS/MD5 总是优于 EAP-PEAP 和 EAP-TLS.据我们所知,我们是第一个针对无线网络认证协议选择开展研究的.

1 相关工作

ITU-T X.805[15]定义了安全性的 8 个安全维度:接入控制、认证、不可否认性、数据保密性、通信安全、数据完整性、可用性和隐私.但这些安全维度之间存在冗余,而且也并不完全适合无线网络中认证协议的选择.因此我们结合无线网络认证协议的特点,将其安全性简化为 4 个维度:密钥交换性、数据完整性、数据保密性和用户身份保护性.

在传统的 OSI 模型中,不同层需要不同的安全协议为其提供安全保护,例如:TLS 工作在传输层;IPSec 工作在网络层;而对于数据链路层,则通过 WEP/WPA/WPA2 对 Wi-Fi 提供安全保护.文献[16]中作者提出利用安全策略 P 来描述安全性,这里的安全策略集成了不同层的安全协议,而每个安全协议提供某些安全特征,例如:认证性、完整性等.如:P\{802.1x-EAP-TLS-WEP-128-IPsec-3DES-MD5\},这里 P 由 2 个不同层的安全协议组成:通过数据链路层上的 802.1x-EAP-TLS-WEP-128,以及网络层上的 IPsec-3DES-MD5 提供 5 个安全特性:消息认证、双向认证、不可否认性、保密性以及数据完整性.继而作者给出了相对安全指标的定义,为每个安全特征关联相关权值来表示一个安全策略的安全强度.该方法还研究了安全性对系统性能的影响,但在系统性能方面并没有考虑能量消耗.而现实情况下,无线网络中终端的电量或计算能力有限,用户会比较在意协议的能量消耗.

在进行安全协议选择时,仅考虑安全性有时候并不能够满足不同用户的需求,性能也是影响协议选择的一个重要因素.文献[13-14]提出了综合考虑安全性和性能的协议选择方案.文献[13]针对如何在传输过程中提供合适的用户数据保护的问题,提出了一种自动选择协议的方案.它从安全性、服务质量和能量消耗 3 个方面进行安全协议的选择.为了在给定情况下选择出最好的协议,首先根据选定的 3 个标准(安全性、服务质量和能量消耗)设置需求来淘汰不适合的协议;继而分别对每个标准进行参数化,通过加权求和来获得对协议的总体评价.针对安全性,用户可根据自身需求定义安全特征.注意到

无线媒体的状态是随时间动态变化的,进而对应用程序的性能和 QoS 都会带来影响. 文献[14]提出了一种移动计算环境下设备动态选择安全协议的方案:根据无线媒体参数、系统资源使用、设备硬件资源、应用定义的 QoS 标准以及期望数据的安全级别,通信双方动态选择安全协议. 但它主要是针对一般的安全协议,而不是认证协议本身来设计的,而无线网络认证协议有自己的特殊性,如安全性方面需要考虑诸如身份保护等特性,性能方面需要考虑认证时间等,且他们仅考虑了用户对安全性中某一方面(如不可否认性)的偏好,并没考虑用户对能量消耗和认证时间的偏好,而在现实中,有的用户对安全性要求高,而有的用户对能量消耗和认证时间更偏重,因此该方案不能满足用户个性化的需求.

综上所述,上述研究主要是针对一般的安全协议来设计的,认证性是他们考虑的一个方面,但他们均不是将认证协议本身作为研究对象,没有将影响认证协议选择的诸多因素(如身份保护、认证时间)等考虑进来. 因此这些方案不完全适合无线网络认证协议的选择.

2　身份认证协议选择方案

针对目前研究所存在的问题,在对认证协议分析的基础上,根据无线网络的特点,我们综合考虑了协议的安全性、性能以及用户偏好,提出了针对无线网络的身份认证协议选择方案,从备选的若干标准化协议中选出一个满足用户个性化需求的协议. 我们假定这些标准化的备选认证协议都是安全的.

在安全性方面,身份认证协议的安全性是通过使用密码套件(如加解密算法、Hash 及消息认证码算法等)来得以保证,因此,我们通过研究密码套件分析其安全强度. 性能方面,影响协议性能的因素主要有 2 个方面,即能量消耗和认证时间. 其中能量消耗由 3 部分组成:发送时的能量消耗、接收时的能量消耗以及使用加解密算法过程中的能量消耗,认证时间可以通过实验测量获取. 同时,由于以上因素对不同的用户来说,其重要性也可能不同,有些用户希望能量消耗小一些,而有些用户则希望认证时间短一些,所以为了能够选择出最适合用户需求的认证协议,用户可以通过设置相关权值 W 来分别对安全性、能量消耗和认证时间的重要性进行度量,相关权值 W 越大,其重要性对于该用户来说也就越高.

具体方案如下:

$$U=\underbrace{W_{\text{sec}}V_{\text{sec\_1}}}_{\text{安全}}+\underbrace{W_{\text{e\_con}}V_{\text{e\_con\_1}}+W_{\text{au\_time}}V_{\text{au\_time\_1}}}_{\text{性能}},\tag{1}$$

其中,W_{sec},$W_{\text{e\_con}}$,$W_{\text{au\_time}}$ 分别是用户对安全性、能量消耗以及认证时间设置的权值,该权值满足 $W_{\text{sec}}+W_{\text{e\_con}}+W_{\text{au\_time}}=100\%$;而 $V_{\text{sec\_1}}$,$V_{\text{e\_con\_1}}$,$V_{\text{au\_time\_1}}$ 则是通过对安全性 V_{sec}、能量消耗 $V_{\text{e\_con}}$ 和认证时间 $V_{\text{au\_time}}$ 归一化得到. 对用户来说,协议 U 值越大,其适用性越好.

2.1　安全模块分析

认证协议是以密码学为基础的消息交换协议,其目的是为开放网络环境中的通信主体提供身份认证功能. 身份认证是网络安全研究的主要目标之一,认证协议本身的安全性对通信安全至关重要. 认证协议实现的安全机制包括:

1) 数据传输的机密性. 利用加密算法对协议传输的数据进行加密.

2) 身份验证机制. 基于证书利用数字签名方法或共享密钥实现服务器和客户端之间的身份验证.

3) 消息完整性验证. 消息传输过程中使用消息认证码算法来检验消息的完整性.

对于认证协议来说,其安全强度主要取决于所采用的密码算法. 因此,认证协议的安全强度可由加密套件进行描述,密码套件确定了认证过程中使用的密钥交换算法(如 Diffie-Hellman)、加解密算法(如 3DES)和消息摘要算法(如 SHA). 另外,用户身份保护是无线网络身份认证协议的一个重要特性. 因此,结合认证协议的特性,我们给出衡量其安全强度的方法:

$$V_{\text{sec}}=\omega_K I_K+\omega_C I_C+\omega_I I_I+\omega_U I_U,\tag{2}$$

其中,ω_K 为提供密钥交换特性的权值;ω_C 为提供认证消息机密性的权值;ω_I 为提供认证消息完整性的权值;ω_U 为提供用户身份保护特性的权值.

式(2)中,若某项特性存在则相应的 $I_{(\cdot)}$ 值为 1,不存在则为 0. 权值是根据加密算法、密钥长度、加密模式等影响因素来给定的. 为了方便计算,由式(3)对 V_{sec} 进行归一化处理得到 $V_{\text{sec\_1}}$(假设 $V_{\text{sec\_max}}$ 为所有被选协议中 V_{sec} 的最大值,$V_{\text{sec\_min}}$ 为最小值),即:

$$V_{\text{sec\_1}}=\frac{V_{\text{sec}}-V_{\text{sec\_min}}}{V_{\text{sec\_max}}-V_{\text{sec\_min}}}.\tag{3}$$

2.2　性能模块分析

无线网络中,在进行身份认证协议选择的时候,各认证协议的性能也是至关重要的. 对性能进行分

析时,从用户的角度出发,针对无线网络的特点,综合考虑用户最为关心的 2 个因素,即能量消耗和认证时间.

1) 能量消耗

能量消耗由 3 个部分组成:用户发送消息能量消耗、用户接收消息能量消耗和交互过程中数据加解密等的能量消耗.具体公式如下:

$$V_{e\_con} = E_R + E_D + E_T, \tag{4}$$

其中,E_R 为接收消息的能量消耗,E_D 为数据加解密的能量消耗,E_T 为发送消息的能量消耗.

在文献[17]中,实验使用设备型号为 Compaq iPAQ H3670,该设备的网卡型号为 Cisco Aironet 350 Wireless LAN Mini PCI Card Client Adapter AIR-MPI 350.该网卡遵守 IEEE 802.11b 标准,带宽为 11 Mbps.该网卡发送消息的能量消耗功率 P_T 和接收消息能量消耗功率 P_R 分别为 1881 mW 和 1089 mW[18].

根据式(5)可计算得到发送消息的能量消耗 E_T 以及接收消息的能量消耗 E_R.其中 t 为消息的发送、接收时间,即:

$$E = P \times t. \tag{5}$$

数据加解密的能量消耗 E_D,该值主要参考文献[10, 17]的能量计算方法,并结合实验来得到.

能量消耗 V_{e_con} 通过式(6)进行归一化得 $V_{e\_con\_1}$,其中所有被选协议中 V_{e_con} 的最大值为 $V_{e\_con\_max}$,最小值为 $V_{e\_con\_min}$,即:

$$V_{e\_con\_1} = \frac{V_{e\_con\_max} - V_{e\_con}}{V_{e\_con\_max} - V_{e\_con\_min}}. \tag{6}$$

2) 认证时间

认证时间 V_{au_time} 通过实验获取,同理,进行归一化处理:

$$V_{au\_time\_1} = \frac{V_{au\_time\_max} - V_{au\_time}}{V_{au\_time\_max} - V_{au\_time\_min}}. \tag{7}$$

3 方案应用于 EAP 认证协议

由于 EAP 方法在无线网络中使用最为广泛,且已经标准化,所以我们以 EAP 协议为例,利用所提的认证协议选择方法找出最符合用户需求的认证协议.

下面以 EAP-TLS 和 EAP-PEAP 为例,对其主要交互过程进行简要描述.

EAP-TLS 认证交互过程如图 1,其认证机制基于 PKI 公钥机制,通过认证中心签发的证书对双方身份进行认证,并在身份认证的同时确定会话密钥以用于后续的通信信息加密.

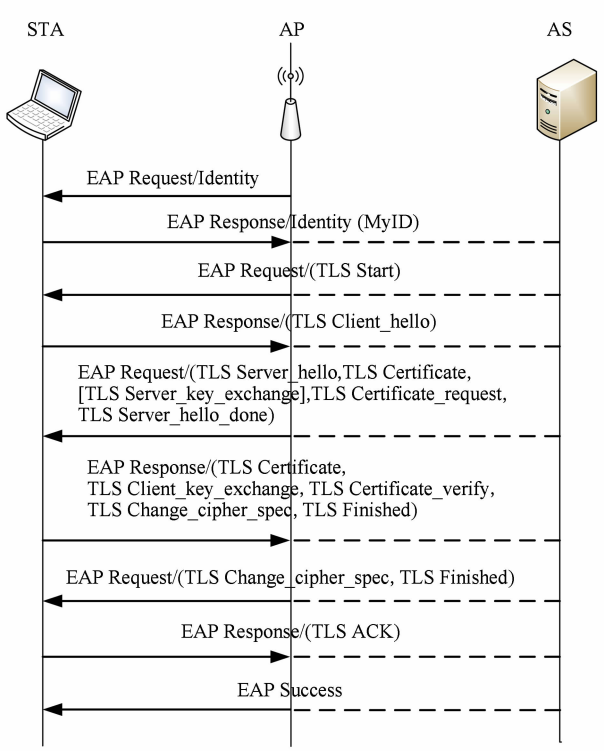


Fig. 1 EAP-TLS authentication process.

图 1 EAP-TLS 认证过程

EAP-PEAP 认证交互过程如图 2 所示:

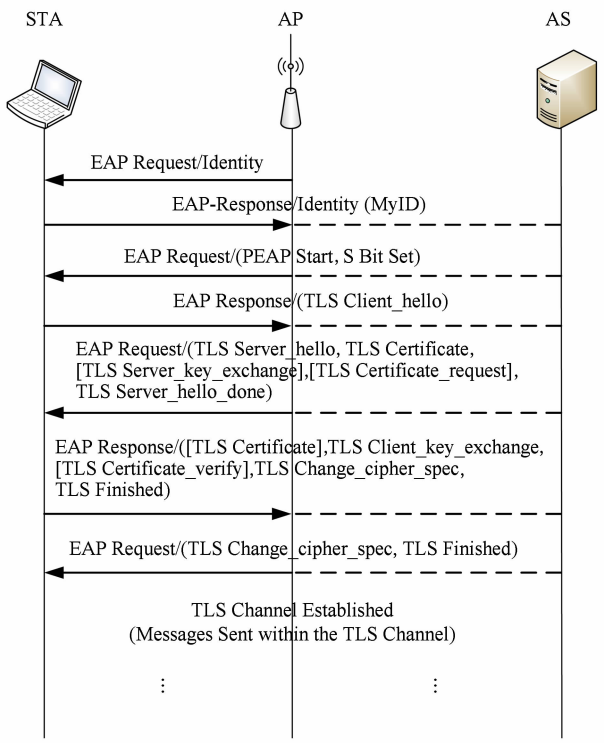


Fig. 2 EAP-PEAP authentication process.

图 2 EAP-PEAP 认证过程

首先,协议会使用类似于 EAP-TLS 的方式建立一个 TLS 隧道来实现外层身份验证,即 STA 利用 AS 的公钥证书实现对 AS 的身份认证;之后,内层身份验证在 TLS 隧道内进行第 2 次 EAP 交换,AS 通过公钥证书或共享密钥实现对 STA 的身份认证.

而 EAP-TTLS 与 EAP-PEAP 之间些微的差异在于内层身份验证的处理. EAP-TTLS 使用加密信道来实现相互认证,EAP-PEAP 则是在加密信道内进行第 2 次 EAP 交换.

3.1　EAP 各认证协议的安全性分析

由于 EAP 各认证协议在认证过程中,是通过协商的密码套件来保证认证过程的安全性. 密码套件的选择有多种组合,我们根据 EAP 方法相对应的 RFC [1-3],选择出 EAP 各方法中最常用的密码套件,并给出了密码套件中每个安全特征关联的相关权值,如表 1 所示:

Table 1　The Weights of Security Suite

表 1　安全套件相关权值

Security Feature	Security Mechanism	Weight
Key Exchange	RSA/DSS	1
Confidentiality	RC4	1
	3DES	2
	AES	3
Data Integrity	MD5	1
	SHA	2
	SHA256	3
User Identity Protection	TLS Tunnel	1

常用的密码套件,有以下 4 种。

1) EAP-PEAP:

TLS_RSA_WITH_RC4_128_MD5;

2) EAP-TLS:

TLS_RSA_WITH_3DES_EDE_CBC_SHA;

3) EAP-TTLS/MD5:

TLS_RSA_WITH_AES_128_CBC_SHA;

Table 2　The Security Strength of EAP Authentication Protocols

表 2　EAP 各认证协议安全强度

EAP Authentication Protocol	V_{sec}
EAP-PEAP	4
EAP-TLS	5
EAP-TTLS/MD5	7
EAP-TTLS/MSCHAPV2	7

4) EAP-TTLS/MSCHAPV2:

TLS_RSA_WITH_AES_128_CBC_SHA.

由表 1 和式(3),通过计算得到 EAP 各认证协议的安全强度 V_{sec} 如表 2 所示.

3.2　EAP 各个认证协议的性能分析

为了获取 EAP 各个认证协议的数据包大小和认证时间,我们搭建了测试床,其拓扑结构如图 3 所示:

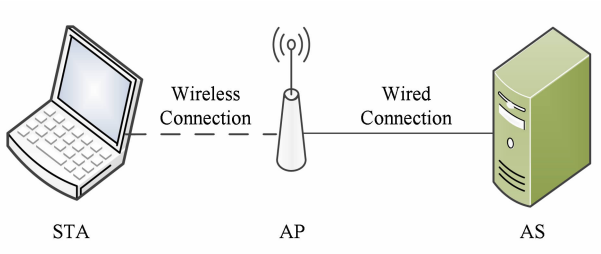


Fig. 3　Test network topology.

图 3　实验测试网络拓扑

实验使用的硬软件资源如下:

1) STA 端

惠普台式机 1 台,其 CPU 为 2.26 GHz Core2 Duo,内存为 2 GB,操作系统为 Linux Fedora 14,内核版本为 2.6.35.6-45.其无线网卡为 PCI TP-LINK TL_WN550G 54 Mbps. 我们用 OpenSSL 程序来提供加解密等操作,其版本为 openssl-1.0.0d. 安装了 wpa_supplicant 客户端模拟程序,其版本为 wpa_supplicant-0.7.3.

2) AP 端

惠普台式机 1 台,其 CPU 为 2.26 GHz Core2 Duo,内存为 2 GB,操作系统为 Linux Fedora 14,内核版本为 2.6.35.6-45.其无线网卡为 PCI TP-LINK TL_WN550G 54 Mbps. 安装了相同的 OpenSSL. 我们采用 hostapd 作为 AP 端程序,版本为 hostapd-0.7.3.

3) AS 端

惠普台式机 1 台,其 CPU 为 3.0 GHz Core2 Duo,内存为 2 GB,操作系统为 Ubuntu 10.10. 我们采用 freeradius 作为认证服务器软件,版本为 freeradius-server-2.1.10.

EAP 各认证协议中客户端数据包收发情况如表 3 所示.

3.2.1　能量消耗计算

本文从 3 个方面对 EAP 各个认证协议的能量消耗进行了计算:客户端发送消息能量消耗 E_T、客户端接收消息能量消耗 E_R 及密码操作所涉及的能量消耗 E_D(Hash 算法、RSA 密钥交换、数字签名、对称加解密算法).

Table 3 The Data Packet Size of Client in EAP Authentication Protocol

表 3 EAP 认证协议中客户端收发数据包大小 B

EAP Authentication Protocol	Send	Receive
EAP-PEAP	765	3 122
EAP-TLS	2 790	3 056
EAP-TTLS/MD5	579	2 965
EAP-TTLS/MSCHAPV2	553	2 981

1) 客户端发送消息能量消耗 E_T

通过利用式(5)和表 3 我们计算得到,客户端发送消息消耗的能量,如表 4 所示:

Table 4 The Energy Consumption of Client Transmitting Messages

表 4 客户端发送消息能量消耗 E_T μJ

EAP Authentication Protocol	E_T
EAP-PEAP	1 045.84
EAP-TLS	3 816.55
EAP-TTLS/MD5	791.90
EAP-TTLS/MSCHAPV2	756.16

2) 客户端接收消息能量 E_R

通过式(5)和表 3 可得到 EAP 认证协议客户端接收消息的能量消耗,如表 5 所示:

Table 5 The Energy Consumption of Client Receiving Messages

表 5 客户端接收消息能量消耗 E_R μJ

EAP Authentication Protocol	E_R
EAP-PEAP	2473.12
EAP-TLS	2420.85
EAP-TTLS/MD5	2347.88
EAP-TTLS/MSCHAPV2	2360.95

3) 密码操作所涉及的能 E_D

该部分能量消耗包括 4 个方面:Hash 算法能量消耗、RSA 密钥交换能量消耗、数字签名能量消耗和对称加解密能量消耗.

① Hash 算法能量消耗

客户端计算已交互的握手消息(除 change_cipher_spec 消息外所有已交互的消息)的 Hash 值,利用协商好的密钥和密码套件处理 Hash 值,并通过 Finished 消息发送给服务器,且客户端需验证服务器发送的 Finished 消息. 而对于 EAP-PEAP 及 EAP-TTLS,TLS 通道建立成功后的认证过程将借助 HMAC 的密钥,对要在 TLS 通道内进行认证的消息做安全的摘要处理. 因此,参考文献[17]的 Hash 算法能量消耗值,表 6 中得到 EAP 中各认证协议 Hash 能量消耗.

Table 6 The Energy Consumption of Hash Algorithm

表 6 Hash 算法能量消耗 μJ

EAP Authentication Protocol	Energy Consumption
EAP-PEAP(MD5)	4 536.37
EAP-TLS(SHA)	8 673.75
EAP-TTLS/MD5(SHA)	5 143.37
EAP-TTLS/MSCHAPV2(SHA)	5 131.77

② RSA 密钥交换能量消耗

在 EAP 认证过程中,客户端验证服务器的证书合法后,利用证书中的公钥加密客户端随机生成的 premaster secret,并通过 Client_key_exchange 消息发送给服务器. 文献[17]给出了非对称加密算法能量消耗结果,表 7 中计算得到 EAP 各认证协议加密 premaster key(48B)的能量消耗.

Table 7 The Energy Consumption of RSA Key Exchange

表 7 RSA 密钥交换能量消耗 μJ

EAP Authentication Protocol	Energy Consumption
EAP-PEAP(RSA)	15 970.00
EAP-TLS(RSA)	15 970.00
EAP-TTLS/MD5(RSA)	15 970.00
EAP-TTLS/MSCHAPV2(RSA)	15 970.00

③ 数字签名能量消耗

由于 EAP 各认证方法中仅有 EAP-TLS 是基于证书利用数字签名方法实现服务器对客户端的身份验证,即客户端需计算已交互的握手消息、主密钥的 Hash 值,利用自己的私钥对其进行加密,通过 certificate verify 消息发送给服务器. 由文献[17]数字签名能量消耗值,得到 EAP 中各认证协议数字签名能量消耗,如表 8 所示:

Table 8 The Energy Consumption of Digital Signature

表 8 数字签名能量消耗 μJ

EAP Authentication Protocol	Energy Consumption
EAP-PEAP(RSA)	0
EAP-TLS(RSA)	546 500.00
EAP-TTLS/MD5(RSA)	0
EAP-TTLS/MSCHAPV2(RSA)	0

④ 对称加解密能量消耗

在 EAP-TLS 的最后阶段,客户端利用协商好的密钥和密码套件处理已交互消息的 Hash 值,并

通过 Finished 消息发送给服务器. EAP-PEAP,EAP-TTLS 在建立 TLS 隧道后,内层身份验证是使用 TLS 加密信道,来实现相互认证. 待加解密的数据包大小由实验测得,加解密算法的能量消耗参考文献[17],得到密码套件的加解密数据信息如表 9 所示:

Table 9　The Information of Cipher Suite Encryption

表 9　密码套件加解密数据信息

EAP Authentication Protocol	Cipher Suite	Energy Consumption /(μJ·B^{-1})	Size of Packets /B
EAP-PEAP	RC4	3.93	629
EAP-TLS	3DES	6.04	40
EAP-TTLS/MD5	AES	1.62	347
EAP-TTLS/MSCHAPVZ	AES	1.62	33

由表 9 计算可得 EAP 中各认证协议中客户端对称加解密的能量消耗,如表 10 所示:

Table 10　The Energy Consumption of Encryption on Client

表 10　客户端加解密的能量消耗　μJ

EAP Authentication Protocol	Energy Consumption
EAP-PEAP	2 471.97
EAP-TLS	241.60
EAP-TTLS/MD5	562.14
EAP-TTLS/MSCHAPV2	545.94

从表 9 中可以看出,加解密 1 B 的数据时,RC4 算法的能量消耗为 AES 算法能量消耗的 2.4 倍. 此外,由于加密套件不同,EAP-PEAP 待加密的数据包大小为 EAP-TTLS/MD5 待加密数据包大小的 1.8 倍. 综合以上 2 个原因,EAP-PEAP 加解密总能量消耗为 EAP-TTLS/MD5 加解密总能量消耗的 4.4 倍.

⑤ 密码操作所涉及的能量消耗 E_D

通过表 6～9 得到密码操作所涉及的能量消耗 E_D,其值如表 11 所示:

Table 11　The Energy Consumption of Cryptographic Operations E_D

表 11　密码操作所涉及的能量消耗 E_D　μJ

EAP Authentication Protocol	Hash Algorithm	Key Exchange	Digital Signature	Symmetric Encryption	E_D
EAP-PEAP	4 536.37	15 970.00	0	2 471.97	22 978.34
EAP-TLS	8 673.75	15 970.00	546 500	241.60	571 385.4
EAP-TTLS/MD5	5 143.37	15 970.00	0	562.14	21 675.51
EAP-TTLS/MSCHAPV2	5 131.77	15 970.00	0	545.94	21 647.71

4) 总能量消耗计算

再根据式(4)、式(5)和表 4、表 5、表 10,得到 EAP 各协议的能量消耗,如表 12 所示:

Table 12　The Total Energy Consumption of EAP Authentication Protocols

表 12　EAP 各认证协议总能量消耗　μJ

EAP Authentication Protocol	E_T	E_R	E_D	V_{e_con}
EAP-PEAP	1 045.84	2 473.12	22 978.34	26 497.30
EAP-TLS	3 816.55	2 420.85	571 385.40	577 622.80
EAP-TTLS/MD5	791.90	2 347.88	21 675.51	24 815.29
EAP-TTLS/MSCHAPV2	756.16	2 360.95	21 647.71	24 764.82

3.2.2　认证时间

在无线网络中,认证时间也决定了用户最终的选择. 我们进行 50 次测试,获得 EAP 各认证协议的认证时间,如图 4 所示.

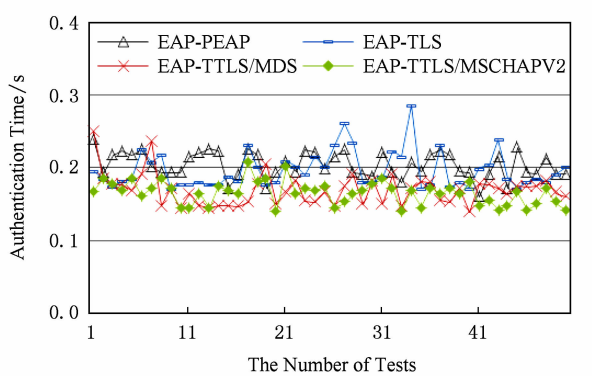


Fig. 4　The authentication time of EAP authentication protocols.

图 4　EAP 各认证协议认证时间

最终的认证时间 V_{au_time} 为实验结果的平均值,如表 13 所示:

Table 13 The Authentication Time of EAP Authentication Protocols

表 13 EAP 各认证协议认证时间 s

EAP Authentication Protocol	Authentication Time
EAP-PEAP	0.204 165
EAP-TLS	0.197 078
EAP-TTLS/MD5	0.169 300
EAP-TTLS/MSCHAPV2	0.165 168

3.3 实验结果

通过式(3)、式(7)、式(8),对 EAP 各认证协议安全性、能量消耗和认证时间进行归一化处理得到 V_{sec_1}, $V_{e\_con\_1}$ 和 $V_{au\_time\_1}$,如表 14 所示:

Table 14 The Normalized Value of EAP Authentication Protocols' Security and Performance

表 14 EAP 各认证协议安全性和性能归一化值

EAP Authentication Protocol	Security	Performance	
	V_{sec_1}	$V_{e\_con\_1}$	$V_{au\_time\_1}$
EAP-PEAP	0	0.997	0
EAP-TLS	0.333	0	0.182
EAP-TTLS/MD5	1	0.999	0.894
EAP-TTLS/MSCHAPV2	1	1	1

用户对协议进行选择时,需根据用户的特定需求,设置相应的权值 W_{sec}, W_{e_con}, W_{au_time},且满足 $W_{sec}+W_{e\_con}+W_{au\_time}=100\%$;我们根据式(1)和权值间的约束关系,分别将 W_{sec}, W_{e_con} 和 W_{sec}, W_{au_time} 以及 W_{e_con}, W_{au_time} 作为自变量,通过 MATLAB 编程得到图 5~7,从不同侧面对 EAP 各认证协议 U 值进行对比.

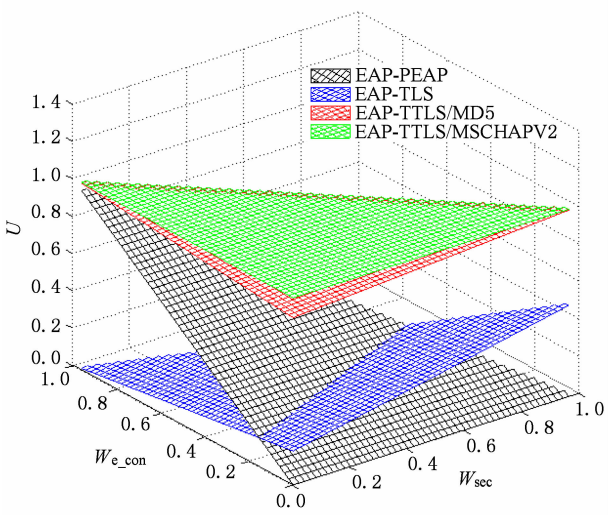


Fig. 5 The variation of U with W_{sec} and W_{e_con}.

图 5 U 值随 W_{sec} 和 W_{e_con} 的变化图

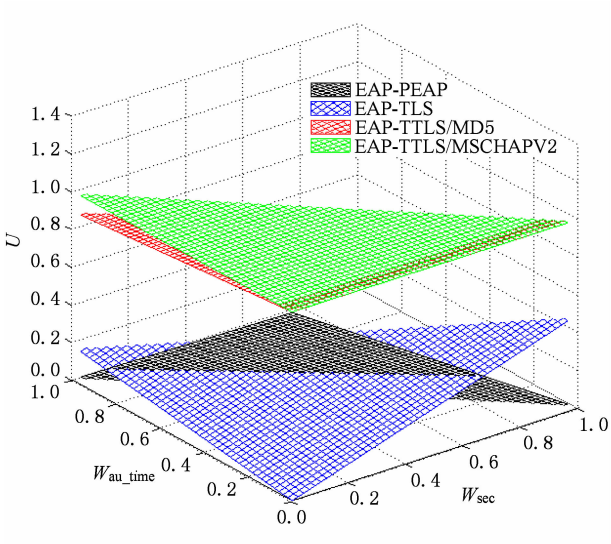


Fig. 6 The variation of U with W_{sec} and W_{au_time}.

图 6 U 值随 W_{sec} 和 W_{au_time} 的变化图

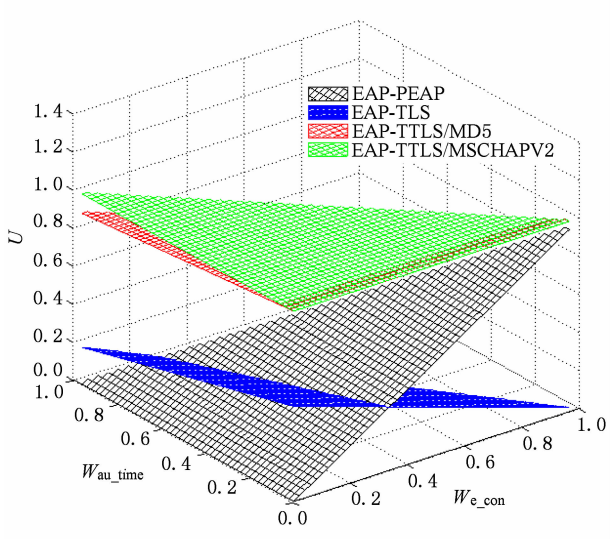


Fig. 7 The variation of U with W_{e_con} and W_{au_time}.

图 7 U 值随 W_{e_con} 和 W_{au_time} 的变化图

通过表 14 和图 5~7,我们可以清晰地发现,在 EAP 各认证协议中不管用户如何设置权值 W_{sec}, W_{e_con} 和 W_{au_time}, EAP-TTLS/MSCHAPV2 和 EAP-TTLS/MD5 总是优于 EAP-PEAP, EAP-TLS.

实验结果分析:1)安全性. 与 EAP-TLS 不同, EAP-TTLS 能够提供用户身份保护特性; EAP-TTLS 采用的 Hash 算法是 SHA,优于 EAP-PEAP 采用的 MD5;且 EAP-TTLS 使用 AES 加密算法,而 AES 算法的安全性高于 EAP-TLS 和 EAP-PEAP 所使用的 3DES 和 RC4. 2)性能. EAP-TTLS 是基于共享密钥而不是证书实现服务器对客户端的身份验证,且其传输的数据经过了压缩,从而减小了发送时的能耗,并缩短了认证时延. 基于上述分析, EAP-TTLS/MSCHAPV2 和 EAP-TTLS/MD5 在

安全性和性能 2 方面均优于 EAP-PEAP 和 EAP-TLS,与实验结果相符.

当用户设置的安全性、能量消耗和认证时间相关权值满足不同条件时,将得到 EAP 各认证协议 U 值的不同排序:

1) 当 $W_{sec}<997/333\ W_{e\_con}-182/333\ W_{au\_time}$ 时,$U_{EAP\text{-}TTLS/MSCHAPV2}>U_{EAP\text{-}TTLS/MD5}>U_{EAP\text{-}PEAP}>U_{EAP\text{-}TLS}$;

2) 当 $W_{sec}=997/333\ W_{e\_con}-182/333\ W_{au\_time}$ 时,$U_{EAP\text{-}TTLS/MSCHAPV2}>U_{EAP\text{-}TTLS/MD5}>U_{EAP\text{-}PEAP}=U_{EAP\text{-}TLS}$;

3) 当 $W_{sec}>997/333\ W_{e\_con}-182/333\ W_{au\_time}$ 时,$U_{EAP\text{-}TTLS/MSCHAPV2}>U_{EAP\text{-}TTLS/MD5}>U_{EAP\text{-}TLS}>U_{EAP\text{-}PEAP}$;

4) 若用户仅看重安全性,则可设置 $W_{sec}=1$,$U_{EAP\text{-}TTLS/MSCHAPV2}=U_{EAP\text{-}TTLS/MD5}>U_{EAP\text{-}TLS}>U_{EAP\text{-}PEAP}$.

4 结　论

本文提出一种指导用户选择无线网络身份认证协议的方法.相对于以往的安全协议选择方案,本方案具有如下特点:1)考虑到无线网络身份认证协议自身的特性,如认证时延、身份保护等,设计出针对性更强的认证协议选择方法.2)从用户的角度出发,综合考虑用户最为关心的几个要素(如:协议的安全性、能量消耗、认证时间)以及用户偏好,提出满足用户个性化需求的解决方案.最后,将设计的认证协议选择方案应用于 4 种 EAP 认证方法的比较,在 Linux 平台下进行实验,理论分析和仿真结果表明 EAP-TTLS/MSCHAPV2 和 EAP-TTLS/MD5 总是优于 EAP-PEAP,EAP-TLS.

参　考　文　献

[1] Simon D, Aboba B, Hurst R, et al. The EAP-TLS Authentication Protocol [S]. Fremont, CA: The Internet Engineering Task Force (IETF), 2008

[2] Funk P, Wilson S. Extensible Authentication Protocol Tunneled Transport Layer Security Authenticated Protocol, Version 0 [S]. Fremont, CA: The Internet Engineering Task Force (IETF), 2008

[3] Palekar A, Simon D, Salowey J, et al. Protected Extensible Authentication Protocol (PEAP), Version 2. 0 [S]. Fremont, CA: The Internet Engineering Task Force (IETF), 2002

[4] Lee Yongki, Batina L, Singelee D, et al. Low-cost untraceable authentication protocols for RFID [C] //Proc of the 3rd ACM Conf on Wireless Network Security. New York: ACM, 2010: 55-64

[5] D'Arco P, Santis A. On ultralightweight RFID authentication protocols [J]. Dependable and Secure Computing, 2011, 8(4): 548-563

[6] Wei Hui, Hwang Shiang, Chin Yehhao. A mutual authentication protocol for FRID [J]. IT Professional, 2011, 13(2): 20-24

[7] Piramuthu S. RFID mutual authentication protocols [J]. Decision Support Systems, 2010, 50(2): 387-393

[8] Kumar P, Choudhury A, Sain M, et al. RUSAN: A robust user authentication framework for wireless sensor networks [J]. Sensors, 2011, 11(5): 5020-5046

[9] Rautray R, Sarangi R. A survey on authentication protocols for wireless sensor networks [J]. International Journal of Engineering Science and Technology, 2011, 3(5): 4253-4256

[10] Chen Tienho, Shih Weikuan. A robust mutual authentication protocol for wireless sensor networks [J]. Electronics and Telecommunications Research Institute Journal, 2010, 32(5): 704-712

[11] Yeh Lien, Chen Tienho, Liu Pinchuan, et al. A secured authentication protocol for wireless sensor networks using elliptic curves cryptography [J]. Sensors, 2011, 11(5): 4767-4779

[12] Li Xinghua, Ma Jianfeng, Park Y, et al. A USIM-Based uniform access authentication framework in mobile communication [J]. EURASIP Journal on Wireless Communications and Networking, 2011, 2011(15): 1-12

[13] Volker L, Werle C, Zitterbart M. Decision process for automated selection of security protocols [C] //Proc of the 33rd IEEE Conf on Local Computer Networks. Piscataway, NJ: IEEE, 2008: 223-229

[14] Rocha B, Costa D, Moreira R, et al. Adaptive security protocol selection for mobile computing [J]. Journal of Network and Computer Applications, 2010, 33(5): 569-587

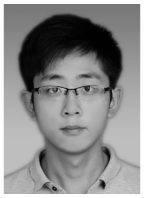
[15] ITU. Security Architecture for Systems Providing End-to-end Communications [S]. Geneva: International Telecommunication Union-Telecommunication Sector (ITU-T), 2003

[16] Agarwal A, Wang Wenye, McNair J Y. An experimental study of cross-layer security protocols in public access wireless networks [C] //Global Telecommunications Conf (GLOBECOM'05). Piscataway, NJ: IEEE, 2005: 1747-1751

[17] Potlapally N, Ravi S, Raghunathan A, et al. Analyzing the energy consumption of security protocols [C] //Proc of the 2003 Int Symp on Low Power Electronics and Design. New York: ACM, 2003: 30-35

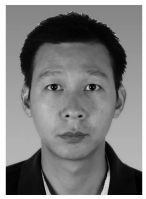
[18] Chiaravalloti S, Idzikowski F, Budzisz L. Power consumption of WLAN network elements, TKN-11-002 [R]. Berlin: Telecommunication Networks Group, 2011

Zhao Jing, born in 1989. Master. Her main research interests include network security, game theory and location privacy protection.



Li Xin, born in 1989. Master candidate at Xidian University. His main research interests include network security, android security and 5G security (xdulixin@163.com).

Deng Lingjuan, born in 1988. Received her MEn degree in computer system structure from Xidian University. Her main research interests include computer networks and information security(dlingjn@gmail.com).



Li Xinghua, born in 1978. Received his MEn and PhD degrees in computer science from Xidian University, in 2004 and 2007, respectively. Member of China Computer Federation. His main research interests include wireless networks security, privacy protection, cloud computing, and security protocol formal methodology(xhli1@mail.xidian.edu.cn).

Ma Jianfeng, born in 1963. Received his MEn and PhD degrees in computer software and communications engineering from Xidian University, Xi'an, China, in 1988 and 1995, respectively. Member of China Computer Federation. His research interests include information security, coding theory, and cryptography(jfma@mail.xidian.edu.cn).