无线网络安全技术及 AES 在 WEP 中的应用

伍珏彤　刘冬九
（中南财经政法大学信息学院　武汉 430074）

摘　要　随着无线网络的普及，其安全问题越发引人注目。本文首先对无线局域网进行了概述，然后介绍了目前无线局域网中几种主要的安全技术，最后重点针对 WEP（有线对等保密）技术中采用的 RC4 算法存在的问题，提出了用 AES（高级加密标准）替代 RC4 算法的解决方案。

关键词　无线局域网，WEP，RC4，AES

Safety Techniques of Wireless Networks and Applications of AES in WEP

WU Jue-Tong　LIU Dong-Jiu
(School of Information, Zhongnan University of Econmics and Law, Wuhan 430074)

Abstract　Currently, with the popularity of wireless networks, security problems become more and more important. In this paper, the author supplies an overview of wireless network protocols, and then, introduces several main wireless safety techniques, for the weakness of RC4 algorithm, advances a better solution-using the latest AES algorithm to replace RC4.

Keywords　WLAN, WEP, RC4, AES

1　无线局域网概述

无线局域网是指以无线电波、激光、红外线等无线媒介来代替有线局域网中的部分或全部传输媒介而构成的网络。它不仅可以作为有线数据通信的补充和延伸，而且还可以与有线网络环境互为备份。

IEEE802.11 是 IEEE 在 1997 年提出的第一个无线局域网标准，主要用于解决办公室局域网和校园网中，用户与用户终端的无线接入，业务主要限于数据存取，速率最高只能达到 2Mbps。

802.11 定义了两种类型的设备，一种是无线站，通常是通过一台 PC 机和一块无线网络接口卡构成，另一个称为无线接入点（Access Point，AP），它的作用是提供无线和有线网络之间的桥接。一个无线接入点通常由一个无线输出口和一个有线的网络接口（802.3 接口）构成，桥接软件符合 802.1d 桥接协议。接入点就像是无线网络的一个无线基站，将多个无线接入站聚合到有线网络上。无线终端可以是 802.11PCMCIA 卡、PCI 接口、ISA 接口，或者是在非计算机终端上的嵌入式设备（例如 802.11 手机）。

IEEE802.11 标准的核心是基本服务群（BBS, Basic Service Set），如图 1 所示，模型由一个或多个无线设备所组成，它们同一个唯一的基站联系。如果没有回连到一个有线网络，这称为独立型基本服务群。

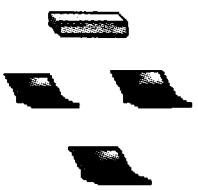

图 1　基本服务群

如果在无线网络中没有基站，该网络则被称为自组网（adhoc network）。这意味着网络内部所有的无线通信均由自组网成员直接完成。图 2 描述了基本的自组网。

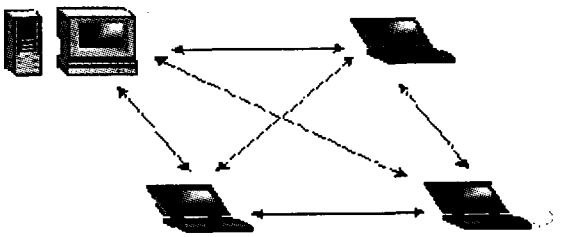

图 2　点对点模式

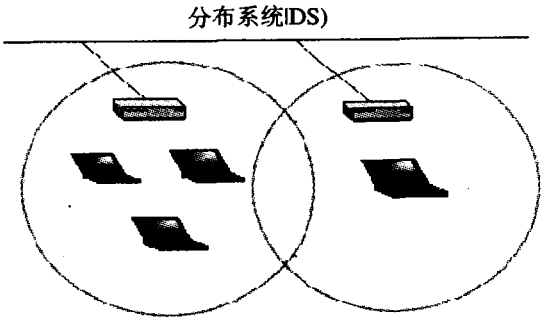

图 3　扩展服务群

当基本服务群经由基站与有线网络相连接时，它被称为基本构架型基本服务群，基站成为无限设备和有线网络联系的纽带。如果移动设备处于独立的基本构架型基本服务群中，那么移动的范围将限制在以基站为中心的一个有限区域。然而在扩展服务群（ESS, Extended Service Set）中，IEEE802.11 体系允许用户在多个基群之间移动。在一个扩

展服务群中，多个基站可以相互交换信息，并可将漫游设备从一个基群转移到另一个基群，扩展服务群采用分布式系统中间件，分布式系统成为无线局域网的核心。图3是一个扩展服务群的模型。

由于802.11在速率和传输距离上都不能满足人们的需要，因此，IEEE小组又相继推出了IEEE802.11b、IEEE802.11a和IEEE802.11g三个新标准。三者之间技术上的主要差别在于MAC子层和物理层。

另外，蓝牙标准、HomeRF工业标准是无线局域网所有标准中与802.11协议最主要的竞争对手。它们各有优劣，各有自己擅长的应用领域，有的适合于办公环境，有的适合于个人应用，有的则一直被家庭用户所推崇。

2 无线网络所采用的安全机制

由上可见，无线网络是通过无线电波传输数据，我们通常用一种非常灵敏的天线来接收这些数据。但问题在于它的数据传播是开放的，换句话说就是其他用户甚至那些怀有恶意的黑客通过某些特殊手段也能够接收到这些信号，因此其安全性十分脆弱。目前无线网络的主要风险体现在服务盗用、数据盗取，数据破坏、干扰正常服务几个方面，这些风险在XP无线网络中同样存在，它们成为制约无线技术更进一步发展的瓶颈，因此，各国专家学者对这些问题进行了研究，提出了很多的解决方案。

2.1 WEP协议加密

WEP是一种基于RC-4算法的40bit或128bit加密技术。它使用RC4对称流加密算法产生一个伪随机数序列，移动终端和AP可以配置4组WEP密钥，加密传输数据时可以轮流使用，允许加密密钥动态改变。密钥流和被传输的数据通过一个简单的异或运算产生密文。通过使用WEP技术，可以避免数据在无线链路上传输时被泄漏。WEP加密技术工作于无线网络的运输层。可以对TCP、IP、IPX和HTTP各种协议数据单元进行加密。

2.2 端口访问控制技术(802.1x)

该技术也是用于无线局域网的一种增强性网络安全解决方案。当无线工作站与AP关联后，是否可以使用AP的服务要取决于802.1x的认证结果。如果认证通过，则AP为用户打开这个逻辑端口，否则用户不能接入网络。

后来又出现了802.1x的扩展认证机制，包括可扩展身份验证协议-传输层安全(EAP-TLS)，可扩展身份验证协议-信息摘要算法(EAP-MD5)。该功能通过远程访问拨入用户服务(RADIUS)，服务器提供简单的集中用户认证。在这种方式下，RADIUS服务器不需要证书或者安装在无线工作站中的其他安全信息。用户注册时，RADIUS服务器只是检查用户名和口令，如果匹配，就通知无线访问点允许该客户端访问网络服务。

2.3 动态安全链路(DSL)技术

动态安全链路技术采用128位密匙，但与WEP2截然不同的是，动态安全链路技术采用的钥匙是动态分配的，而WEP2采用的钥匙是手工输入和维护的。动态安全链路技术针对每一个会话(session)都自动生成一把钥匙，并且即使在同一个会话期间，对于每256个数据包，钥匙将自动改变一次。采用动态安全链路技术时，要求无线访问点AP中维护一个用户访问列表，而在用户端请求访问网络时进行用户名口令的认证，只有认证通过之后才能连通。

2.4 虚拟专用网(VPN)技术

VPN是目前市场上最安全的解决方案，能够阻止无线黑客入侵公司局域网或从汽车、建筑物内，甚至建筑物附近截取机密信息。企业可以部署VPN来支持鉴权和加密要求。通常的做法是将WLAN设置成单独的局域网部分，并通过VPN网关将该部分连接到企业局域网上。利用VPN，所有无线用户在得到许可访问企业局域网之前首先由VPN网关进行鉴权。VPN网关只向拥有机器中所具有的有效软件证书或令牌的用户授权。客户机到VPN服务器的数据包使用IP安全协议IPSec(IP Security)加密。因此黑客将无法破解这些数据包的内容。

2.5 采用无线局域网鉴别和保密基础结构WAPI

2003年5月我国颁布了我国境内惟一合法的无线网络技术标准WAPI，国外的无线产品只有符合这一标准才准许进入我国市场。WAPI采用国家密码管理委员会办公室批准的公开密钥体制的椭圆曲线密码算法和秘密密钥体制的分组密码算法，分别用于WLAN设备的数字证书、密钥协商和传输数据的加解密，从而实现设备的身份鉴别、链路验证、访问控制和用户信息在无线传输状态下的加密保护。

3 WEP技术中RC4算法存在的问题

3.1 RC4算法构造

RC4算法是RSA安全公司的Ron Rivest与1987年提出的可变密钥长度的序列密码。RC4采用OFB模式，密钥流与明文独立分开。密钥以字节为单位，共有r个字节(且r可变)，$1\leqslant r\leqslant 256$。它是一种基于表置乱原理的序列密码体制。以一个较大的表为基础，即利用8×8的s盒：$S_0, S_1, \cdots, S_{255}$，在变长密钥控制下对0,1,…,255的数进行置换，目的是产生乱数序列。

RC4算法构造：一个2^r个r比特构成的S表(定义$0\sim 2^r-1$的一个排列)，两个r比特计数器(初植为0)。一般地，r比特为一个字，RC4内存量仅为2^r+2个字，即$r(2^r+2)$比特。$r=8$时，满足256B。通常称(2^r+2)个字为内部状态，算法启动后，在两个计数器的相互作用下，每一时刻都输出一个字的乱数。

RC4算法所产生随机字节简要描述：

$i=(i+1)\bmod 256$；$i_t=i_{t-1}+1$

$j=(j+S_i)\bmod 256$；$j_t=j_{t-1}+S_{t-1}(i_t)$

interchange S_i 和 S_j；$S_t(i_t)=S_{t-1}(j_t)<-->S_t(j_t)=S_{t-1}(i_t)$(交换)

$t=(S_i+S_j)\bmod 256$；$z_t=S_t(S_t(i_t)+S_t(j_t))$

$k=S_t$

其中，字节k与明文异或得到密文，或与密问异或得到明文，加密速度相当DES的10倍。符号“+”为模2^n算术运算。

RC4的变化空间约为$256!\times 256^2\approx 2^{1700}$种可能状态组合。所以RSA没有短循环，具有高度非线性，能抵御差分攻击和线性分析。

3.2 RC4算法应用于WEP中存在的问题

(1)RC4是一种常用于SSL连接的数据流加密算法，广泛应用于计算机加密通信领域。但是它的密钥生成算法(Key Scheduling Algorithm)存在漏洞，利用此漏洞，攻击者能逆转RC4算法的加密过程，从而获取密钥将已加密的信息解密。实现这一过程并不复杂，只需要使用一台个人电脑对

(下转第244页)

了具体、有效的途径。

但是在 PSP 的测量中未引入软件测量刻度，因此无法对测量的意义本身进行评价[6]。通过 PSP 的实践表明 PSP 使个体工程师的关键性能得到了提高包括工程师的估算和计划能力，其开发的软件的质量，工作过程的质量，但是到目前为止没有足够的数据能够说明个体的生产率得到了提高。

参 考 文 献

1 Humphrey W S. A Discipline for Software Engineering. Reading, Ma.: Addision-Wesley, 1995

2 Fenton N E. Software Metrics: A Rigorous & Practical Approach. 清华大学出版社, 2003. 97～98

3 paulk M C. Applying SPC to the Personal Software Process, www. sei. cmu. edu, 2003

4 Hayes W, Over J W. The Personal Software Process: An Empirical Study of the Impact of PSP on Individual Engineers: [Technical Report CMU/SEI-97-TR-001]

5 郑丽娟，王保义，宋雨．影响 PSP 的关键因素分析．华北电力大学学报，2003, 30(1)

6 侯红，郝克刚，郭小群．软件测量刻度及选择方法．计算机科学，2005, 32(5)

7 www. iturls. com

(上接第 88 页)

加密的数据包进行分析，经过几个小时的时间就可以破译出信息的全部内容。

(2)WEP 在链路层采用 RC4 加密技术来防止非授权用户的监听以及非法用户的访问。可是，静态 WEP 密钥对于 WLAN 上的所有用户都是通用的。这意味着如果某个无线设备丢失或者被盗，所有其他设备上的静态 WEP 密钥都必须进行修改，以保持相同等级的安全性。这将给企业网络带来费时费力的、不切实际的管理任务。

(3)在 RC4 中，存在弱密钥。所谓弱密钥，就是密钥与输出之间存在超出一个好密码所应具有的相关性。在 24 位的 IV 值中，有 9000 多个弱密钥。攻击者收集到足够的使用弱密钥的包后，就可以对它们进行分析，只须尝试很少的密钥就可以接入到网络中。

4 AES 代替 RC4 的解决方案

4.1 AES 设计原理

AES 为分组密码体制，分组长为 128 比特，密钥长可以为 128、192 和 256 比特三种。AES 加密算法的数据处理单元是字节，128 比特的分组信息被分成 16 个字节。AES 算法中引入矩阵的概念，分组的 16 个字节按顺序被复制到一个 4 * 4 的矩阵中，称为 state(状态)，AES 的所有变换都是基于状态的变换。AES 变换是由轮函数通过多轮迭代实现的，根据密钥长度的不同，轮函数的迭代次数也不一样，对应上面的三种密钥长度，迭代次数分别为 10、12、14 轮。轮函数的构成包括非线性，扩散和密钥调度几种元素。非线性变换的目标就是通过较小较简单的非线性元素得到大的复杂化的非线性构件。在轮函数的每一轮迭代中，包括四步变换，分别是字节代换运算(ByteSub())、行变换(ShiftRows())、列混合(MixColumns())以及轮密钥的添加变换(AddRoundKey())，其作用就是通过重复简单的非线性变换、混合函数变换，将字节代换运算产生的非线性扩散，达到充分的混合，使加密后的分组信息统计特性分布更均匀，在每轮迭代中引入不同的密钥，这样便以最简单的运算代价得到最好的加密效果，实现加密的有效性。

4.2 AES 加密算法性能分析

(1) AES 有较长的密钥，密钥长度可为 128bits、192bits 和 256bits 三种情况，明显提高了加密的安全性，同时，对不同机密级别的信息，可采用不同长度的密钥，执行灵活性较高。

(2) 在 AES 中，由于密钥扩展函数的特点，所产生的轮密钥随机性很强，对初始密钥的选取也没有特别的限制，可抗击穷举密钥的攻击。

(3) AES 的均衡对称结构既可以提高执行的灵活度，又可防止差分分析方法的攻击。

(4)AES 算法的实现更简单、有很强的扩散性能，能把非线性部件产生的非线性很快地扩散开，形成的密码有很高的随机性。可有效地防止差分分析和线性分析的攻击。

(5) 因为一个一般的积分均衡子集经过一轮迭代后，就可以使加密结果面目全非，实际上 Rijndeal 经 4 轮迭代后，便可抗击积分密码分析了。

最后，AES 算法在所有的平台上都表现良好，其操作比较容易抵御对物理层实现的某些攻击，能很好地适应无线网络的发展。因此，无论是从安全还是实现的难易度上考虑，采用 AES 替代 RC4 算法是一种最明智的选择。

结束语 任何事物都有一个出现、繁荣和灭亡的过程。AES 代替 RC4 的解决方案，从以上的分析中来看，它显示出其无可比拟的优越性，但随着科学技术的发展，任何一项技术都有被淘汰的可能，因此，我们只有不断地跟踪和研究最新技术，不断发现和解决无线网络所存在的问题，才能使我国信息安全技术迈上一个新的台阶，使无线网络更快地得到普及和发展！

参 考 文 献

1 Daemen J, Rijmen V. AES Proposal: Rijndael. AES Algorithm Submission. Sept. 1999

2 Gladman B. A Specification for Rijndael, the AES Algorithm, Oct. 2000. Available at: http://fp. gladman. plus. com/cryptography_technology/

3 吴世忠，祝世雄，等. 应用密码学. 机械工业出版社，2000

4 卢开澄. 计算机密码学. 清华大学出版社，1998

5 Nechvatal J, et al. Report on the Development of theAdvanced Encryption Standard (AES). National Institute of Standards and Technology, Oct. 2000

6 林柏钢. 网络与信息安全教程. 机械工业出版社，2004