2004 年 10 月
第 6 卷第 10 期

中国工程科学
Engineering Science

Oct. 2004
Vol.6 No.10

学术论文

WLAN 802.11/11b 数据加密机制的安全分析

宋宇波，胡爱群，蔡天佑
（东南大学信息安全研究中心，南京 210096）

[摘要] 在 802.11 标准中的加密采用 WEP 协议，用于提供链路层数据传输的安全保护。目前，在原有 WEP 的基础上提出了一些改进方案，能提高 WEP 的安全性能，但理论上缺少严密的安全分析。笔者通过数学模型对这些解决方案以及原有 WEP 协议进行量化分析，推导出机制内各模块与整个安全机制间安全性能的对应函数关系，并比较了这些方案间安全性能的差异，证明这些安全机制可以提高原有 WEP 的安全性能，在理论上为用户提供如何构造满足所需安全性能的 WLAN 数据加密增强机制。

[关键词] WLAN；安全分析；WEP；密钥更新
[中图分类号] TP393.17 [文献标识码] A [文章编号] 1009－1742（2004）10－0032－07

1 前言

一直以来，人们希望能够得到高效率、高质量、低商业成本的服务，无线网络的产生和不断发展均基于这种需求。无线局域网（WLAN，wireless local area network）作为有线局域网的延伸，能方便地以无线方式将计算机联网，满足人们对移动办公日益增长的需求，因而在近几年取得了长足的发展。特别是随着以 IEEE802.11 为代表的网络标准的成熟，用户可以享受从 1 Mb/s 到 11 Mb/s 甚至 54 Mb/s 的高带宽无线通信。但无线网络给人们带来便利的同时也带来了新的问题，特别是安全问题。由于数据的传输是通过无线电波在空中传播进行的，这使得的数据的窃听和伪造变得非常容易，因此需要采用针对无线传输的安全机制来保护通信。

无线局域网通信的 802.11 标准[1]引入 WEP（Wired Equivalent Privacy）协议来解决无线环境下的安全问题并相信 WEP 可以提供与有线传输数据加密相同的安全性能。WEP 协议主要提供数据传输的机密性保护，该协议作为 802.11 标准的一部分，被广泛的使用，尽管该协议采用了安全性能良好的 RC4 加密算法[2]，但是 WEP 根本无法实现设计者的最初目标，协议中存在的一些重大缺陷使得无线传输的数据可以轻而易举地被窃听和篡改。许多方案在原有 WEP 的基础上提出了改进和安全增强机制，这些解决方案为了保证与原有 WEP 协议兼容，主要通过快速更换加密密钥来弥补原有 WEP 的缺陷，其思路是合理的，但缺乏理论上的依据和令人信服的安全分析。笔者通过数学模型对这些机制做出量化的安全分析，从而推导出机制内各模块原有的安全强度与整个安全机制间安全强度的对应关系，并比较了这些方案间安全性能差异，从而在理论上指导用户如何构造满足所需安全性能的 WLAN 数据加密增强机制，证明了这些安全机制可以在一定程度上提高原有 WEP 的安全性能。

2 现有的研究

WEP 协议为 802.11 无线网络提供链路层数据通信的安全保护[1]，其设计目的是提供 3 方面的安

[收稿日期] 2003－11－07；修回日期 2004－02－08
[基金项目] “八六三”高技术计划资助项目（2002AA143010）
[作者简介] 宋宇波（1977－），男，江苏无锡市人，东南大学博士研究生

全保护：数据机密性、访问控制和数据完整性。WEP 的核心是 RC4 序列密码算法，其基本原理是用密钥作为种子通过伪随机数产生器（PRNG）产生伪随机密钥序列（PRKS），加密端用该序列和明文相异或后得到密文序列，解密端用该序列和密文相异或后恢复出明文。

协议的制定者认为该协议的安全性依赖于针对密钥进行强力破解的难度，128 b 版本的 WEP 协议可以抗拒目前利用最高性能计算机进行的强力破解。但文献[3, 4]指出，根本不需要强力破解就可以攻击该协议，而且 WEP 密钥长度的多少与某些攻击方式的难度没有多少关系。WEP 使用的 iv 空间过小，且使用流加密算法 RC4 进行加密，流加密算法的一个重要缺陷是如果使用相同的 iv ‖ SK 加密 2 个消息时，攻击者可以获得：

$$C2 \oplus C1 = \{P1 \oplus \mathrm{RC4}(\mathrm{iv} \| \mathrm{SK})\} \oplus \{P2 \oplus \mathrm{RC4}(\mathrm{iv} \| \mathrm{SK})\} = P1 \oplus P2 \quad (1)$$

如果其中的一个消息明文已知，另一个消息的明文立即就可以获得。在现实世界中，由于明文有足够的信息量使得可以直接从 $P1 \oplus P2$ 中得到 $P1$ 和 $P2$[5]。为了防止这种攻击，WEP 采用 iv ‖ SK 作为密钥，其中 SK 不变，iv 每传输一次就变换来获得不同的密钥流，iv 以明文的方式传送。WEP 协议中的 iv 空间只有 24 b，假设一个繁忙的 AP 在一个平均带宽为 5 Mb/s 的信道传输长度为 1500 B 的数据帧，iv 的空间将在半天内耗尽。

iv 在 WEP 协议中主要提供 2 个功能，一是用来生成加密密钥，一是作为状态计数器进行传输以保证加解密双方的状态保持同步。从文献[3, 4]指出的缺陷来看，如果简单地增加 iv 的空间（例如 iv 扩展为 128 b，考虑到这样会导致整个密钥过长，也可以取 $K_i = \mathrm{Sk} \oplus \mathrm{iv}$，iv 取 128 b），似乎可以解决上述的问题。但 WEP 协议还存在另一个重大缺陷，当 iv 满足形式（$A+3$，$N-1$，x）时，可以利用 iv Weakness[6, 7]攻击方法进行攻击。当密钥为 128 b 时，攻击的时间复杂度仅为 $O(2^{32})$，文献[8]给出了一个改进攻击方式，其攻击的时间复杂度可以缩小为 $O(2^{31})$。

分析可知 iv Weakness 攻击方法针对的主要不是 RC4 本身，而是 WEP 对 RC4 的不当使用。WEP 设计者简单地将 iv 和密钥相接作为 RC4 的密钥，而没有考虑这样做的合理性。同样，即使取 $K_i = \mathrm{Sk} \oplus \mathrm{iv}$，$K_i$ 和 iv 之间也不过是简单的线性关系，也就是说，iv 若满足形式（$A+3$，$N-1$，x），则 K_i 同样满足形式（$A+3$，$N-1$，x），仍可以利用 iv Weakness 进行攻击。因此，K_i 和 iv 之间的关系至少要求是非线性的，密钥初始化算法的安全性对于整个加密机制是非常关键的。在同样使用 RC4 算法的 SSL 中，由于在输入到 RC4 前使用了 MD5 函数，使前后的 RC4 密钥不是简单线性关系，从而保证了 SSL 的安全。可见，WLAN 中的安全漏洞很大程度上在于 WEP 对 RC4 的误用。

为了解决链路层数据加密的安全隐患，文献[4]指出了主要的解决思路：一是完全抛弃现有的 WEP 协议，使用新的安全协议，如文献[9]提出的使用 AES 算法替代 WEP。这种思路虽然可以提高 WLAN 的安全性，但对于现有已售出的支持 802.11 系列的无线网卡来说将无法得到升级。这种思路可以作为长期的解决方案，但不适合现有无线网络的升级，其升级成本太大。其次由以上分析可以看出，WEP 的主要漏洞在 iv 和密钥之间的关系，如果在原有 WEP 的模块上改进密钥的生成机制，就可以提高其安全性能。这方面的方案有 Nextcomm 公司的 Key-hopping 技术[10]，以及 IEEE 的 TKIP 协议[9, 11, 12]。

由于一个加密协议的安全性能与该协议使用的加密算法以及协议本身有很大关联，进行横向比较，困难较大。一些文献对协议安全性能的理论分析进行了探讨，并提出了一些理论，比较成功并得到广泛应用的有文献[13]提出的定量分析安全性能的概念和方法，它通过定义安全性能优势函数来定量比较加密机制。在此基础上，文献[14]讨论了定量分析伪随机数生成器的安全性能；文献[15]讨论了定量分析对称块加密机制的安全性能；文献[16]证明了通过添加密钥更新机制可以提高对称块加密机制的安全性能。这种量化的分析安全性能得到了广泛的应用，很多块加密算法都是利用该方法提供安全性能上的证明。如 RFC2104 的 HMAC 算法[17]以及 AESOCB 模式[18]。目前，主要的块加密机制都被证明是合理安全的，但缺乏对流加密机制的安全分析。而在无线环境下，由于传统的块加密机制数据处理速度无法适应高速率的无线传输，WEP 协议使用了流加密算法 RC4，上述文献的相关结论无法直接引入来证明新的解决方案（如 Key-hopping，TKIP 协议）是安全有效的。

3 相关数学模型的建立和描述

WEP将RC4的输入密钥分为2部分：24 b的初始向量iv和40 b的密钥SK。每加密一次iv需改变一次，iv以明文的形式随着密文数据帧C发往接收方。SK为BSS中各STA所共享的秘密信息，通常由管理员手工配置和分发。一共可以有4个SK，通信时选择其中1个使用。由于担心密钥空间太小导致安全性下降，一些设备制造商也使用128 b密钥（SK长度为104 b）WEP2协议。当接收方无法正确解密收到的数据包，它将丢弃所有收到的帧，802.11以这样的方式提供访问控制。为了保证数据的完整性，WEP中采用CRC32算法作为消息认证算法，并将数据的消息认证码ICV′作为明文的一部分一同加密。接受端在解密密文后，重新计算消息认证码ICV，并和收到ICV比较，若不符则抛弃所接受数据。

笔者对WEP算法重新进行构造：

模型1 WEP算法：

Encrypt Algorithm $E(M, \mathrm{SK})$

$\mathrm{iv} \xleftarrow{\text{random}} \{0,1\}^{24}$

$K_i \leftarrow \mathrm{iv} \| \mathrm{SK}$

$\mathrm{ICV} \leftarrow \mathrm{CRC32}(M)$

$P \leftarrow M \| \mathrm{ICV}$

$C \leftarrow P \oplus \mathrm{RC4}(K_i)$

$\mathrm{out} \leftarrow \mathrm{iv} \| C$

Return (out, SK)

Decrypt Algorithm $D(C, \mathrm{iv}, \mathrm{SK})$

$K_i \leftarrow \mathrm{iv} \| \mathrm{SK}$

$P' \leftarrow C \oplus \mathrm{RC4}(K_i)$

$M' \| \mathrm{ICV}' \leftarrow P'$

if $\mathrm{CRC32}(M') = \mathrm{ICV}'$ then Return (M')

else Return (failed)

Key-hopping和TKIP协议比较类似，它们都用一个会话密钥生成算法替代了原有WEP的$K_i = \mathrm{iv} \| \mathrm{SK}$。Key-hopping使用HMAC-MD5算法，iv为128 b。TKIP协议担心现有的算法运算速度较慢，因此它使用了自己设计的密钥混合函数，该函数从一临时密钥、48 b的iv以及传送端的MAC地址中导出WEP seed。接收者从收到的MPDU中得到iv，用同样的密钥混合函数推得WEP seed进行解密。因此，这2个解决方案除了使用得生成函数不一样和iv的空间大小不一样外，机制的构造是相同的。因此，可以构造一个模型来描述这2个机制。

模型2 加密增强机制

Enhanced Encrypt Algorithm $\mathrm{Enc}(M, \langle \mathrm{SK}, i \rangle)$

$\mathrm{iv} = i$

$K \leftarrow \mathrm{Algorithm}(\mathrm{SK}, \mathrm{iv})$

$\mathrm{ICV} \leftarrow \mathrm{CRC32}(M)$

$P \leftarrow M \| \mathrm{ICV}$

$C \leftarrow P \oplus \mathrm{RC4}(K_i)$

$\mathrm{out} \leftarrow \mathrm{iv} \| C$

Return $(\mathrm{out}, \langle \mathrm{SK}, i+1 \rangle)$

Enhanced Decrypt Algorithm $\mathrm{Dec}(C, \mathrm{iv}, \langle \mathrm{SK}, i \rangle)$

$\mathrm{iv}' = i$

if $\mathrm{iv} \neq \mathrm{iv}'$ Return (failed)

else

K_i Algorithm(SK, iv)

$P' \leftarrow C \oplus \mathrm{RC4}(K_i)$

$M' \| \mathrm{ICV}' \leftarrow P'$

if $\mathrm{CRC32}(M') = \mathrm{ICV}'$ then Return $(M', \langle \mathrm{SK}, i+1 \rangle)$

else Return (failed)

增强机制的主要思路是每次会话使用的密钥K_i由主密钥SK和状态计数器i通过混合算法导出，第i个消息用K_i通过RC4进行加密。SK为接受方和发送方共享的秘密信息，接受方和发送方的状态计数器在建立连接时均初始化为零，每加密一次，状态计数器递增1次，其值即为iv。iv的长度为n位，以明文的形式随着密文数据帧C发往接收方。这里，iv不再用于生成K，而是作为状态标识来保持双方的同步。接受方通过比较本地iv′和接收iv来确定双方是否同步。如果两者一致，则接收方确定双方同步，并由SK和状态计数器i通过混合算法导出K_i进行解密。由于每个MPDU都有1个唯一的iv与之对应，因此还可利用iv为标志建立重放保护机制。

这种增强机制的优点在于提供了用于提高安全性能的密钥更新模块，对原有WEP协议的加密模块没有改动，可以非常方便地在主机上通过软件实现，无需改动硬件就可以提供高强度的安全性能，对现有的802.11/11b网卡是一个有效的升级方法。

4　安全性能分析

很明显，在模型 2 中通过密钥更新模块生成子密钥，同时扩大了 iv 的空间，大大延长了 SK 的生存周期，从而提高了原有 WEP 机制的安全性能。但对原有的 WEP 安全性能有多少提高，下面利用文献[13]提供的安全性能分析方法对模型 2 进行定量分析。

从结构上看，模型 1 实际上是模型 2 的特例，它们都是先通过某一机制由 SK 生成子密钥，再使用子密钥运用 RC4 算法生成加密使用的序列。因此可以一起进行分析。模型 1 的混合函数实际上为

$\text{Algorithm}_{\text{WEP}}(\text{SK}, \text{iv})$，

$\text{iv} \xleftarrow{\text{random}} \{0,1\}^{24}$，

$K_i \leftarrow \text{iv} \| \text{SK}$。

4.1　相关定理及其证明

模型 2 实际上可以分为 2 个相对独立的模块：子密钥生成模块和加密模块。

整个子密钥的生成过程可以看成一个伪随机数生成状态机 G，因此可以用伪随机性作为分析安全性能的评判标准[13]。用一优势函数 $\text{Adv}(t)$ 来量化输出的伪随机性，该函数表示在时间 t 内攻击者把 n 个输出块与等长的随机数列区分开来的最大概率。

构造 1　伪随机数生成状态机 $G=(\text{SK}, N)$

Algorithm SK，

$\text{SK} \xleftarrow{\text{random}} \{0,1\}^k$，

Return$\langle 0, \text{SK}\rangle$

Algorithm $N(\langle i, \text{SK}\rangle)$

$K_i \leftarrow \text{PRF}(\text{SK}, i)$

Return $(K_i, \langle i+1, \text{SK}\rangle)$

伪随机数生成状态机 G 为二元组。它由随机密钥生成算法 SK 生成状态机的初始状态 $\langle 0, \text{SK}\rangle$。迭代算法 N 把当前状态作为输入，输出 1 个新状态 $\langle i+1, \text{SK}\rangle$ 和一个子密钥，新状态用于下次调用。子密钥和 SK 的长度相等，均为 k 位。

令 $S=(K, \text{RC4})$ 为使用的加密机制，由密钥生成 K，RC4 算法组成，输出 n 字节比特流。则整个数学模型可以如下表述：

$$S'[S, G]=(K', \text{RC4}') \tag{2}$$

这是一个包含状态的加密模型，初始状态包含伪随机数生成状态机 G 的初始状态：$St_0 \leftarrow -K_G$。加密过程被分为多个阶段，在第 i 个阶段，由 G 生成第 i 个密钥用于 RC4 加密，$(K_i, St_i) < N(St_{i-1})$。用状态计数器标明现在的状态，每输出 l 字节比特流就进入下一个状态位。

伪随机数生成状态机 G 优势函数的定义[14]：

定义 1　$G=(\text{SK}, N)$ 为伪随机数生成状态机，密钥长度为 k，n 为状态数，A 为一种攻击，对 G 的输出序列和以相同长度的随机序列进行分析和攻击，攻击成功返回 1。

攻击 A 和伪随机数生成状态机 G 的优势函数分别为：

$$\text{Adv}_{G,n}(A)=\Pr[\text{Attack}_{G,n}(A)=1]-\Pr[\text{Attack}_{\text{random},n}(A)=1] \tag{3}$$

$$\text{Adv}_{\text{G}}(t, n)=\max_A\{\text{Adv}_{G,n}(A)\} \tag{4}$$

伪随机位生成机 G 的优势函数为时间 t 和 n 的函数，表示在时间 t 内检索 n 个输出序列被攻击者攻破的最大可能性。时间 t 是指整个操作需要的时间，而不仅是执行攻击 A 所需的时间。

伪随机函数优势函数的定义。

定义 2　PRF F 为伪随机函数，R^k 为所有从 $\{0,1\}^k$ 映射到 $\{0,1\}^k$ 间均匀分布的函数集合。D 为一种攻击，D 的优势函数为

$$\text{Adv}_{\text{F}}(D)=\Pr[D(F(K))=1]-\Pr[D(f(\cdot))=1 : f \xleftarrow{\text{random}} R^k] \tag{5}$$

则 F 的优势函数为

$$\text{Adv}_{\text{F}}(t, n)=\max_D\{\text{Adv}_{\text{F}}(D)\} \tag{6}$$

伪随机函数优势函数为时间 t 和 n 的函数，表示在时间 t 内检索 n 字节输出序列被攻击者攻破的最大可能性。

定义 3　$S=(K, \text{RC4})$ 为基本流加密机制，K 为密钥，加密算法为 RC4，输出 n 字节比特流。$S'[S, G]=(K', \text{RC4}')$ 为添加密钥更新的流加密机制，G 为密钥更新模块，更新后的密钥为 K'，第 i 状态输出 l 字节比特流，n 为状态数。A 为 S 的攻击，A' 为 S' 的攻击。

S 的优势函数为

$$\text{Adv}_{S,n}(A)=\Pr[A(\text{RC4}(K))=1]-\Pr[A(f(\cdot))=1 : f \xleftarrow{\text{random}} R^n] \tag{7}$$

$$\text{Adv}_{\text{S}}(t, n)=\max_A \text{Adv}_{S,n}(A) \tag{8}$$

S' 的优势函数为

$$\text{Adv}_{S',l,n}(A')=\Pr[A'(\text{RC4}(K'))=1]-$$

$$\Pr[A'(f(\cdot)) = 1 : f \xleftarrow{\text{random}} R^{ln}] \quad (9)$$

$$\mathrm{Adv}_{S'}(t, ln) = \max_{A'} \mathrm{Adv}_{S', l, n}(A') \quad (10)$$

定理1[16] 伪随机函数的优势函数的值为伪随机数生成状态机 G 优势函数的上限为

$$\mathrm{Adv}_G(t, n) \leqslant \mathrm{Adv}_F(t, n) \quad (11)$$

根据定理1和上述定义，推得如下定理：

定理2 $S=(K, \mathrm{RC4})$为基本RC4加密机制，密钥长度为 k 位，G 为伪随机数生成状态机，密钥长度为 k 位，$S'[S, G]=(K', \mathrm{RC4}')$为增强的加密机制：

$$\mathrm{Adv}_{S'}(t, ln) \leqslant \mathrm{Adv}_F(t, n) + n\,\mathrm{Adv}_S(t, l) \quad (12)$$

证明 令 A' 为1个针对增强加密机制的攻击，t 为攻击所需的最大时间，D 为针对伪随机数生成状态机 G 的攻击，A 为针对RC4加密机制的攻击。有

$$\Pr[\mathrm{Attack}_{G, n}(D) = 1] = \mathrm{Adv}_{S', l, n}(A')^{[16]} \quad (13)$$

构造2 个攻击过程 A' 攻击基本RC4加密机制 S。它对一系列完全随机，互相独立的密钥加密的密文序列进行分析。A 的攻击与 A' 相关，A' 和 A 的攻击构造如下：

Attack $A'(S', j)$

$K_i \xleftarrow{\text{random}} \{0, 1\}^k$; $S \leftarrow \varepsilon$

for $i = 1, \cdots, n$ do

if $i \leqslant j$ then $\mathrm{Out}_i \xleftarrow{\text{random}} \{0, 1\}^i$

else$(\mathrm{Out}_i, K_i) \leftarrow S'(K_i)$

$S \leftarrow S \| \mathrm{Out}_i$

$g \leftarrow A'(S)$

return g

Attack $A(S(K, \mathrm{RC4}))$

$j \xleftarrow{\text{random}} \{1, \cdots, n\}$; $S \leftarrow \varepsilon$

for $i = 1, \cdots, n$ do

if $i < j$ then $\mathrm{Out}_i \xleftarrow{\text{random}} \{0, 1\}^i$

if $i = j$ then $K_i \leftarrow K$; $\mathrm{Out}_i \leftarrow \mathrm{RC4}(K_i)$

if $i > j$ then $K_i \xleftarrow{\text{random}} \{0, 1\}^k$; $\mathrm{Out}_i \leftarrow \mathrm{RC4}(K_i)$

$S \leftarrow S \| \mathrm{Out}_i$

$g \leftarrow A'(S)$

return g

令 P_j 为 $A'(S', j)$ 成功的概率，$j=0, \cdots, n$。则有

$$\Pr[\mathrm{Attack}_{\mathrm{random}, n}(D) = 1] = P_0 - P_n \quad (14)$$

可以看到，当输出序列是由RC4生成时，攻击 A 返回1的概率与 $A'(S', j-1)$ 返回1的概率相等；当输出序列完全随机生成时，攻击 A 返回1的概率与 $A'(S', j)$ 返回1的概率相等。j 是在 $\{1, \cdots, n\}$ 间随机选取的，因此有：

$$\Pr[A(\mathrm{RC4}(K)) = 1] = \frac{1}{n}\sum_{j=1}^{n} P_{j-1} \quad (15)$$

$$\Pr[A(f(\cdot)) = 1 : f \xleftarrow{\text{random}} R^{ln}] = \frac{1}{n}\sum_{j=1}^{n} P_j \quad (16)$$

所以

$$\mathrm{Adv}_{S,1} = \frac{1}{n}\sum_{j=1}^{n} P_{j-1} - \frac{1}{n}\sum_{j=1}^{n} P_j = \frac{P_n - P_0}{n}。$$

由式（14）得

$$\Pr[\mathrm{Attack}_{\mathrm{random}, n}(D) = 1] = n\mathrm{Adv}_{S, 1}(A) \quad (17)$$

由式（12）及式（16）推得：

$\mathrm{Adv}_{S', l, n}(A') = \mathrm{Adv}_{G, n}(D) + n\mathrm{Adv}_{S, 1}(A)$，

即 $\mathrm{Adv}_{S'}(t, ln) = \max_{A'} \mathrm{Adv}_{S', l, n}(A') \leqslant \mathrm{Adv}_G(t, n) + n\,\mathrm{Adv}_S(t, l)$。

4.2 安全分析

利用生日攻击方法按上述方式攻击加密算法时，进行 n 次检索的成功概率为 $n^2/2^k$，k 为密钥长度[19]。

考虑到执行时间与检索次数近似成正比，t 近似等于 n。由定理1，密钥更新模块安全性能的优势函数跟其采用的伪随机序列生成函数有关。Key-hopping使用HMAC－MD5算法，其iv长度为128 b；TKIP协议是用自己的混合函数，假设该函数可以提高足够的安全性能，iv长度为48 b；WEP算法没有规定iv的生成，假设它由普通的伪随机序列生成函数生成，则优势函数分别为：

$$\mathrm{Adv}_{G-\mathrm{WEP}}(n) \approx (n^2 + n)/2^{24} \quad (18)$$

$$\mathrm{Adv}_{G-\mathrm{TKIP}}(n) \approx (n^2 + n)/2^{48} \quad (19)$$

$$\mathrm{Adv}_{G-\mathrm{Key-hopping}}(n) \approx (n^2 + n)/2^{128} \quad (20)$$

RC4基本加密机制优势函数近似为[2]

$$\mathrm{Adv}_S(n) \approx (n^2 + n)/2^k$$

则TKIP的优势函数为

$$\mathrm{Adv}_{\mathrm{TKIP}}(ln) \approx (n^2 + n)/2^{128} + n(l^2 + l)/2^{128} \approx (l^2 n + n^2 + ln + n)/2^{128} \quad (21)$$

Key-hopping的优势函数为

$$\mathrm{Adv}_{\mathrm{Key\text{-}hopping}}(ln) \approx (n^2 + n)/2^{48} +$$

$$n(l^2+l)/2^{128}\approx(n^2+n)/2^{48} \quad (22)$$

WEP 协议的优势函数为

$$\mathrm{Adv}_{\mathrm{WEP}}(ln)\approx(n^2+n)/2^{24}+n(l^2+l)/2^k\approx (n^2+n)/2^{24} \quad (23)$$

使用 RC4 机制输出相同长度序列时的值为

$$\mathrm{Adv}_{\mathrm{RC4}}(ln)\approx(l^2n^2+n)/2^k \quad (24)$$

其中 n 为检索的输出序列数，k 为 128 b，假定一个繁忙的 AP 在一个平均带宽为 5 Mb/s 的信道传输长度 $l=1\ 500$ B 的数据帧。WEP 协议、RC4 加密机制和增强机制优势函数值如图 1 所示。

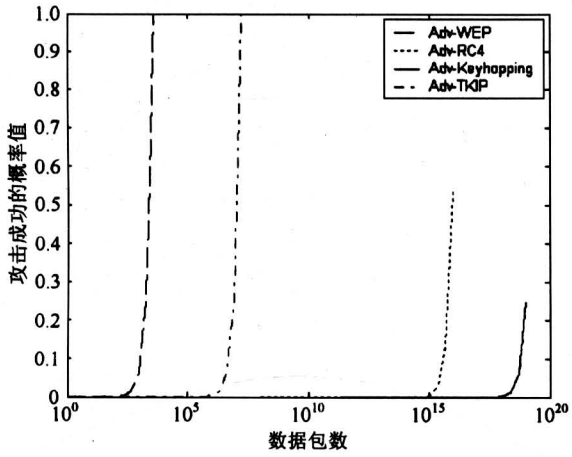

图 1　安全性能比较比较

Fig.1　The comparison of the security

图 1 表示在同样数量的输出数据时是各个机制优势函数的值，y 轴为攻击成功的概率值，数值越高则安全性越低。通过比较看出，WEP 加密机制安全性最差，在输出 4 000 多个数据包时，其被攻破的可能性接近 1，这与文献[3]给出的结果相符；TKIP 协议的安全强度比 WEP 提高约 4 个等量级，但它还是削弱了 RC4 的安全强度，当输出数据包为 10^7 时，被攻破的可能性为 0.6；RC4 加密在输出 10^{16}个数据包时，其被攻破的可能性约为 0.6 左右；Key-hopping 的安全性能最高，在输出 10^{19}个数据包时，其被攻破的可能性约为 0.25 左右，这意味着，一个繁忙的 AP 在一个平均带宽为 5 Mb/s 的信道传输长度为 1 500 B 的数据帧时，TKIP 密钥的生命周期约为 2.4×10^4 h，Key-hopping 密钥的生命周期约为 6.7×10^{12} h，在实际环境中基本上满足需求的。与原有 WEP 相比，TKIP 和 Key-hopping 的安全性能都得到大幅度提高，Key-hopping 的安全强度最高。

5　结论

由定理 2 可以看出，最终加密机制与采用的密钥更新机制有很大的关系，如果密钥更新模块的安全性能近似或大于基本 RC4 流加密机制，密钥更新模块可以起到提高安全性能的作用。若密钥更新模块的安全性能远远低于基本 RC4 流加密机制，由定理 2 推得最终加密机制的安全性能与密钥更新模块的安全性能近似相等，这样安全性能非但不能提高，反而是大大降低了。这就是 WEP 协议失败的原因，由理论推导的结果与实际情况相符。在所有得到应用的无线加密机制中，WEP 的安全性能最低，无法在实际环境中提供安全保护；Key-hopping 的安全性能最高，TKIP 较差。但 TKIP 的运算速度远远高于 Key-hopping。因此，在安全性能要求很高的环境下建议使用 Key-hopping 机制，而在一般环境下还是使用 TKIP 协议就可以满足普通用户对安全的需求。

参考文献

[1] LMSC of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications [S]. IEEE Standard 802.11, 1999

[2] Rivest R L. The RC4 Encryption Algorithm [P]. USA: RSA Data Security, Inc, Mar 12, 1992

[3] Walker J R. Unsafe at Any Key Size; an Analysis of the WEP Encapsulation [S]. IEEE Document 802.11 -00/362, Oct 2000

[4] Simon D, Aboba B, Moore T. IEEE 802.11 Security and 802.1X [S]. IEEE Document 802.11 - 00/034r1, Mar 2000

[5] Dawson E, Nielsen L. Automated cryptanalysis of XOR plaintext strings [J]. Cryptologia, Apr, 1996, (2): 165～181

[6] Fluhrer S, Mantin I, Shamir A. Weaknesses in the key scheduling algorithm of RC4 [R]. Eighth Annual Workshop on Selected Areas in Cryptography, August 2001

[7] Stubblefield A, Ioannidis J, Rubin A. Using the fluhrer, nantin, and shamir attack to break WEP [R]. AT&T Labs Technical Report TD-4ZCPZZ, 2001

[8] 耿　嘉，曹秀英. 无线局域网中基于 RC4 的加密算法的分析与改进[J]. 通信技术，2002，(09)：95～97

[9] LMSC of the IEEE Computer Society. Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security [S]. IEEE STD 802.11i/D3.0, November 2002

[10] Ying Wenping, Key Hopping™ - A Security Enhancement Scheme for IEEE 802.11 WEP Standards [S]. February 2002

[11] Grimm C B. Wi-Fi Protected Access (WPA) Version 1.2 [S]. Wi-Fi Alliance, December 16, 2002

[12] Moore T. Suggested Changes to Robust Security Network (RSN) for IEEE 802.11 [S]. IEEE TGi doc. IEEE 802.11-02/298r4, May 2002

[13] DiÆe W, Oorschot P van, Wiener M. Authentication and authenticated key exchanges [J]. Designs, Codes and Cryptography, 1992, 2(2): 107~125

[14] Biham M, Micall S. How to generate cryptographically strong sequences of pseudo-random bits [J]. SLAM Journal on Computing, 1984, 13(4): 850~864

[15] Bellare M, Desai A, Jokipii E, et al. A conrete security treatment of symmetric encryption: Analysis of the DES modes of operation [A]. Proc of the 38th IEEE FOCS [C]. IEEE, 1997

[16] Abdalla M, Bellare M. Increasing the lifetime of a key: a comparative analysis of the security of re-keying techniques [A]. Okamoto T, editor. Advances in Cryptology-ASIACRYPT 2000, Volume 1976 of Lecture Notes in Computer Science [C]. Springer-Verlag, 2000

[17] Krawczyk H, Bellare M, Canetti R. HMAC: Keyed-Hashing for Message Authentication [S]. RFC2401, February 1997

[18] Rogaway P, Bellare M, Black J, et al. OCB: A Block-Cipher Mode of Operation for Efficient Authenticated Encryption [S]. ACM Conference on Computer and Communications Security, August 3, 2001

[19] Bellare M, Canetti R, Krawczyk H. Keying Hash Funtions for Message Authentication [A]. Koblitz N, edited. Advances in Cryptology - Crypto '96, Lecture Notes in Computer Science Volume 1109 [C]. Springer-Verlag, 1996. 1~15

The Security Analysis for Enhanced Data Encryption Schemes in IEEE802.11/11b WLAN

Song Yubo, Hu Aiqun, Cai Tianyou

(*Research Center of Information Security, Southeast University, Nanjing* 210096, *China*)

[**Abstract**] As an expansion of LAN, the WLAN reduce the cost of building a network infrastructure, to enjoy the mobile, high-quality, multimedia services. The 802.11 standard for wireless networks includes a Wired Equivalent Privacy (WEP) protocol, which is used to protect link-layer communications from eavesdropping and other attacks. Several serious security flaws in this protocol have been discovered and some solutions have been proposed to enhance WEP security. However, it is doubtful whether they can provide enough security as these solutions lack precisely security analysis. In this paper, concrete security analyses of various enhancing mechanisms are given. Results show that these mechanisms indeed increase security and bring significant, provable security gains in WLAN environment. The authors quantify the security as a function of the security of the primitives used, thereby enabling a user to decide how to construct an enhanced mechanism for desired demands.

[**Key words**] WLAN; encryption; WEP; rekey