第3章

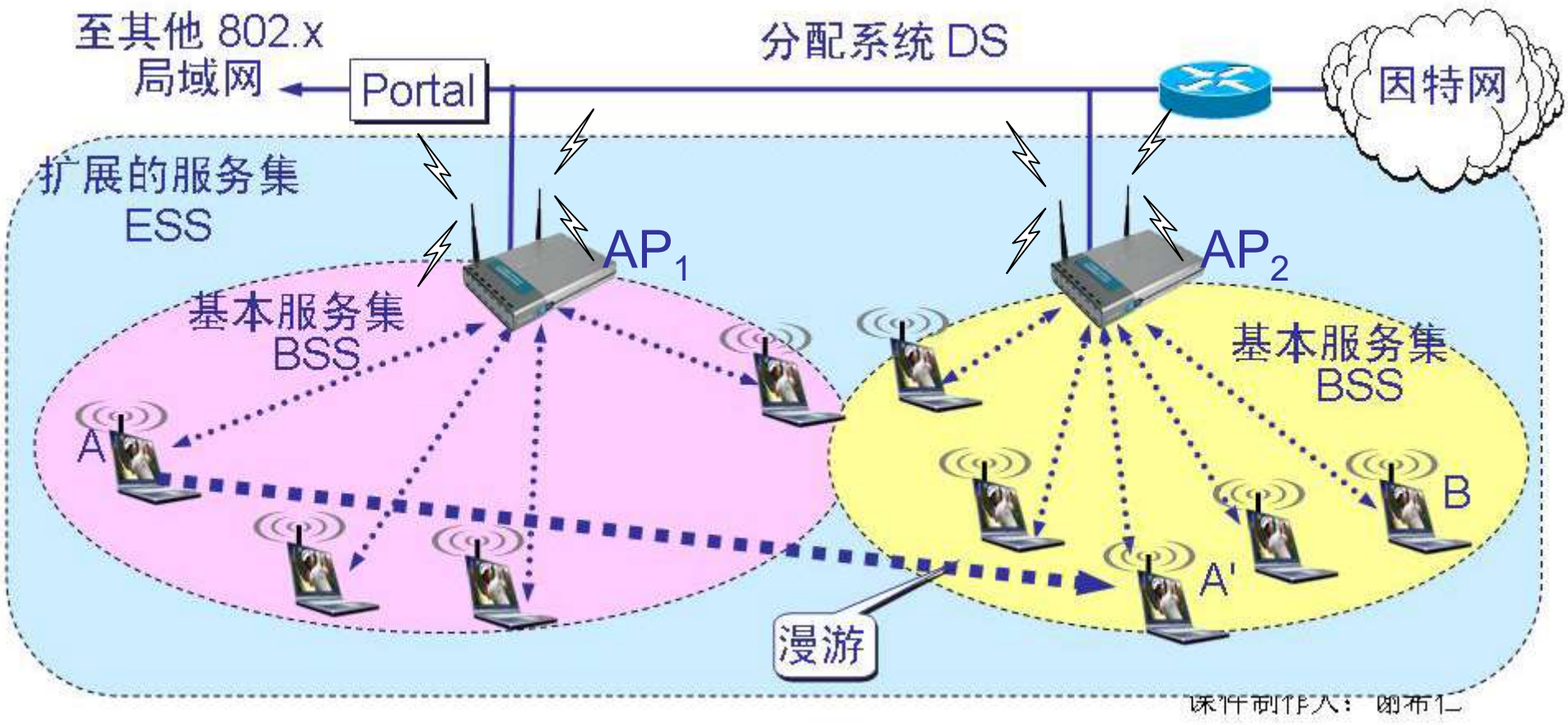
WLAN安全

讨论议题

- **WEP协议**
- **802.1X**
- **802.11i**
- **802.11r 快速切换协议**

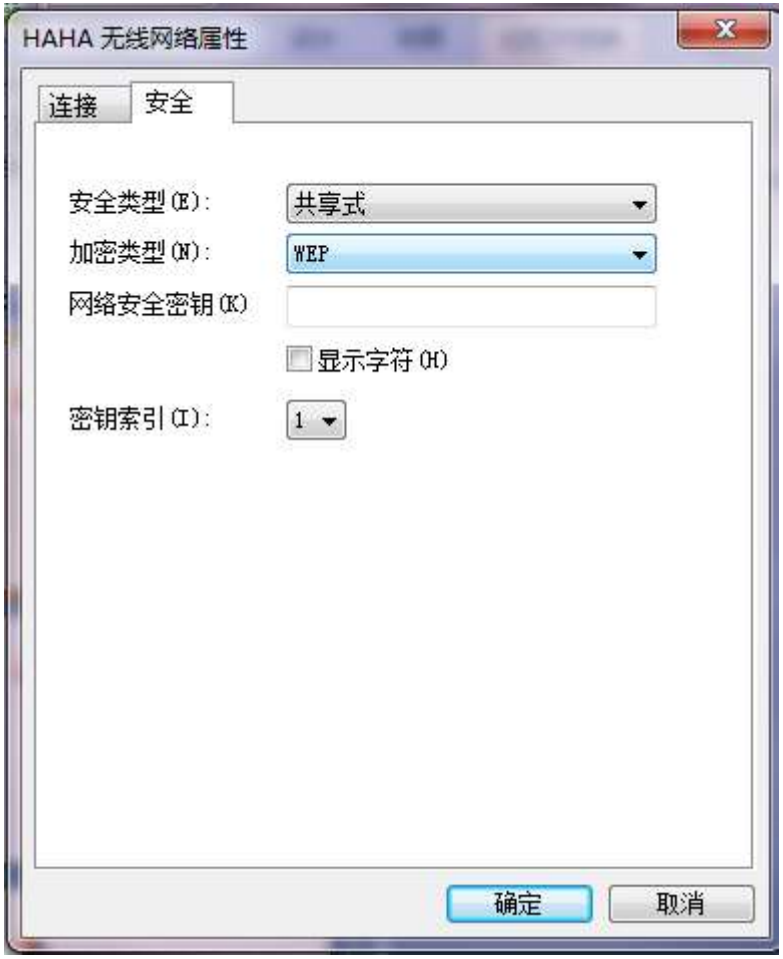
无线局域网的组成

- 有固定基础设施的无线局域网



3.1 WEP认证协议


HAHA 无线网络属性
连接
安全
安全类型(E):
WPA - 个人
加密类型(N):
网络安全密钥(K)
无身份验证(开放式)
共享式
WPA2 - 个人
WPA - 个人
WPA2 - 企业
WPA - 企业
802.1X
确定
取消

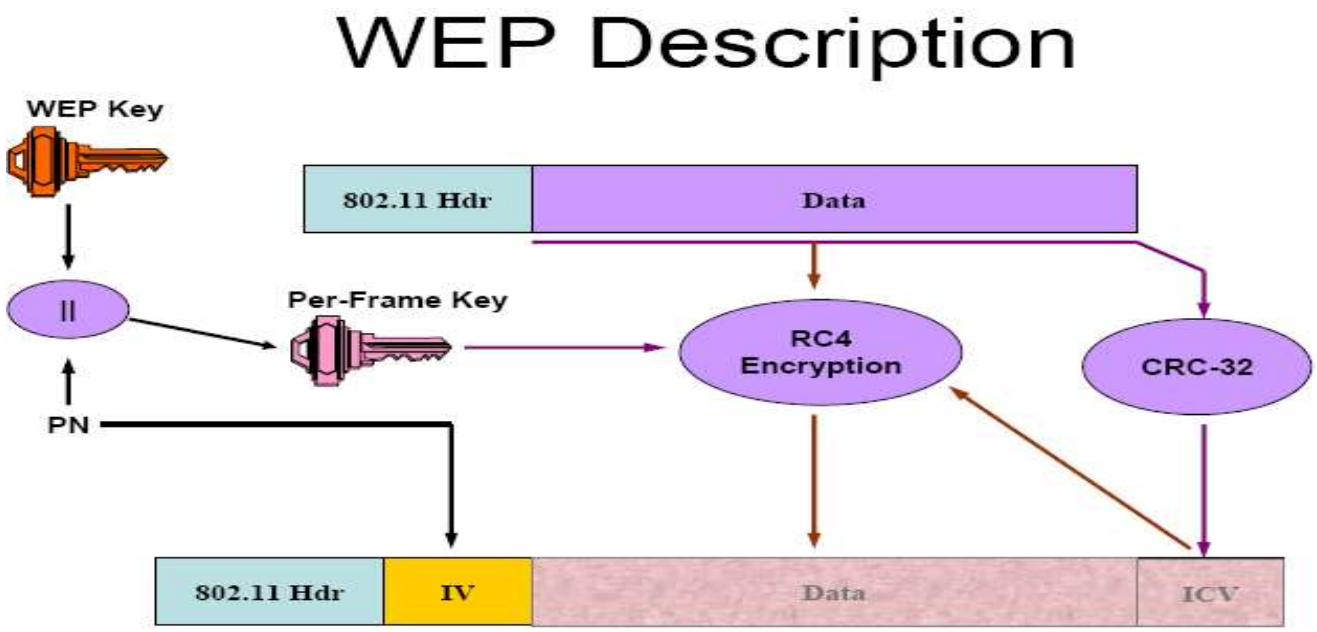

HAHA 无线网络属性
连接
安全
安全类型(E):
共享式
加密类型(N):
WEP
网络安全密钥(K)
显示字符(H)
密钥索引(I):
1
确定
取消

3.1 WEP认证协议

- WEP协议是目前802.11协议中保障数据传输安全的核心部分。
- WEP是Wired Equivalent Privacy的简称，有线等效保密（WEP）协议是对在两台设备间无线传输的数据进行加密的方式，用以防止非法用户窃听或侵入无线网络。
- 2003年被 Wi-Fi Protected Access (WPA) 淘汰
  2004年由IEEE 802.11i 标准（又称 WPA2）所取代

WEP的特点

- 使用共享WEP密钥，长度为40或者104比特
- 使用RC4算法加密
- 使用一个长度为24比特的初始化向量（IV）
- 对原始明文计算CRC-32循环冗余校验得到一个Integrity Check Vector（ICV）



RC4算法

- RC4加密算法是RSA三人组中Ron Rivest在1987年设计的密钥长度可变的流加密算法簇。之所以称其为簇，是由于其核心部分的S-box长度可为任意，但一般为256字节。
- RC4算法的特点是算法简单，运行速度快:速度可以达到DES加密的10倍左右，而且密钥长度是可变的，可变范围为1-256字节(8-2048比特)。完全可以抵抗暴力攻击，如今也没有找到对于128bit密钥长度的RC4加密算法的有效攻击方法。
- RC4有2个主要的算法：密钥调度算法KSA和伪随机数生成算法PRGA
- 解密过程和加密过程完全相同

密钥调度算法KSA算法

- 密钥调度算法的作用是将一个随机密钥k做一个初始变换，打乱状态矢量S

- KSA算法描述如下：

假设S-box长度为N，密钥长度为L。

```
for (i=0; i<N-1; i++)
        s[i]=i;
j=0;
for (i=0; i<N-1; i++)
{
        j=(j+s[i]+k[i mod L])mod N;
        swap(s[i], s[j]);
}
```

返回

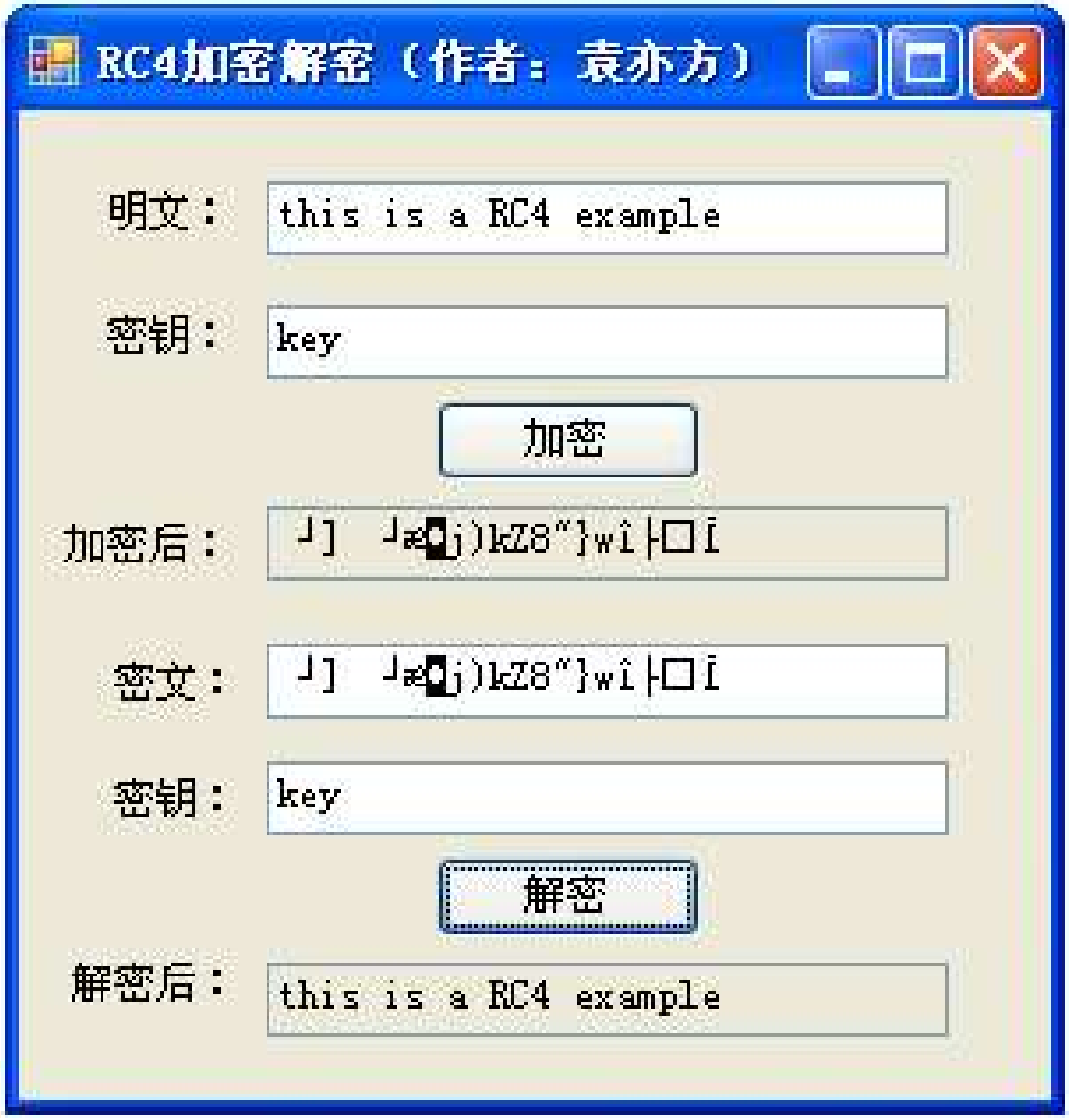
伪随机数生成算法PRGA

- 通过PRGA得到密钥流，得到的密钥流sub_k用以和明文进行xor运算，得到密文

- PRGA算法描述如下：

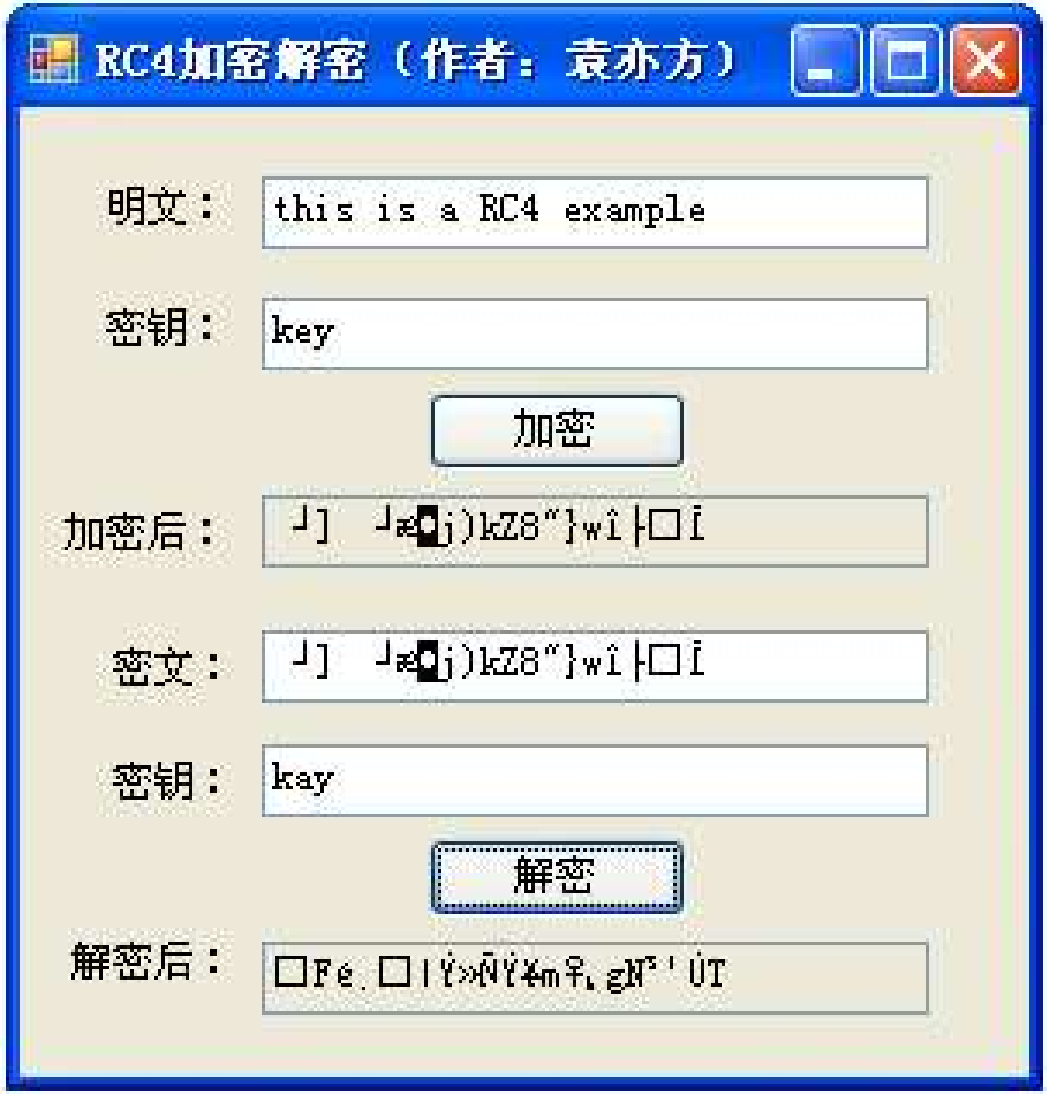
```
i=j=0;
while (明文未结束)
{
        ++i;
        i mod N
        j=(j+s[i]) mod N;
        swap(s[i], s[j]);
        sub_k =s((s[i]+s[j]) mod N);
}
```

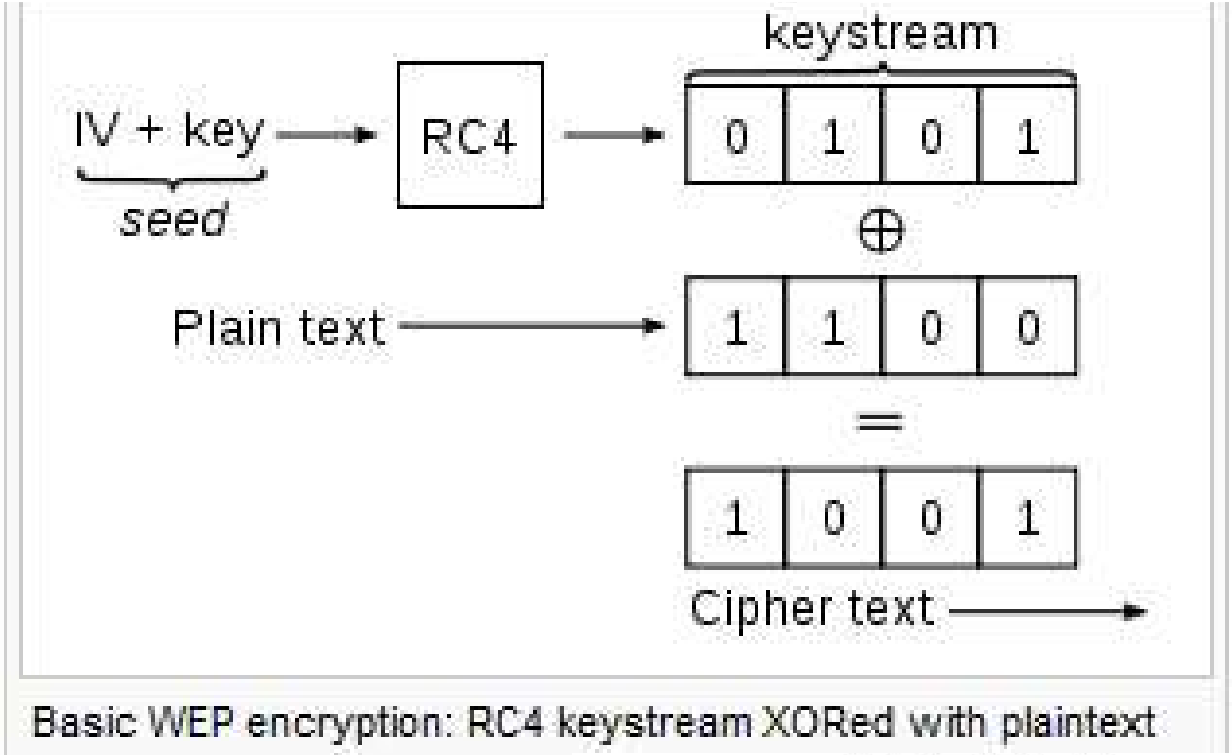

RC4:正确的加密解密


RC4加密解密（作者：袁亦方）
明文：
this is a RC4 example
密钥：
key
加密
加密后：
密文：
密钥：
key
解密
解密后：
this is a RC4 example

RC4:使用错误的密文解密

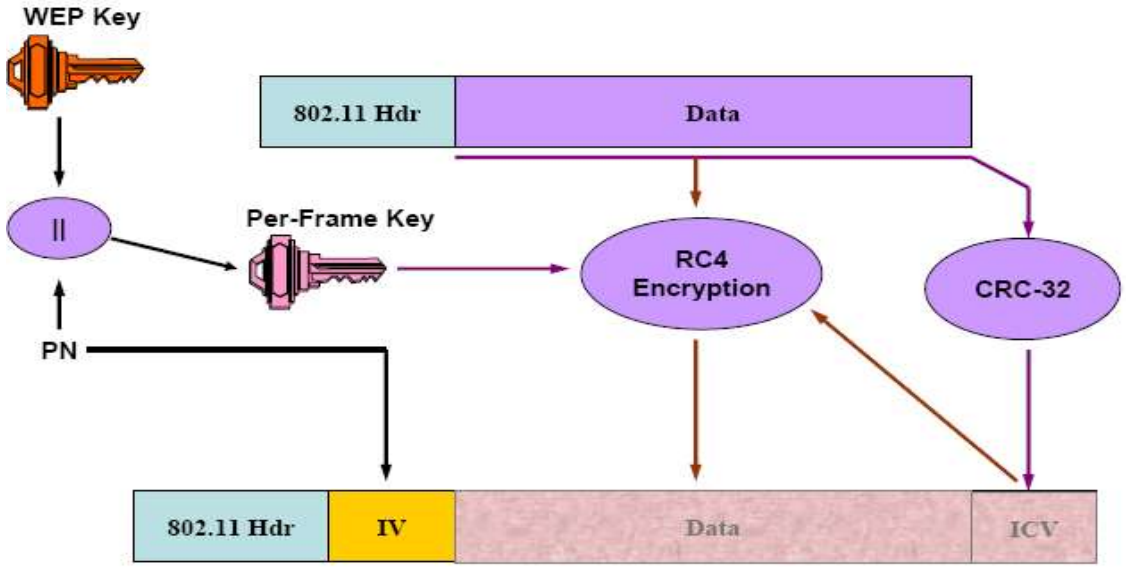
RC4:使用错误的密钥解密

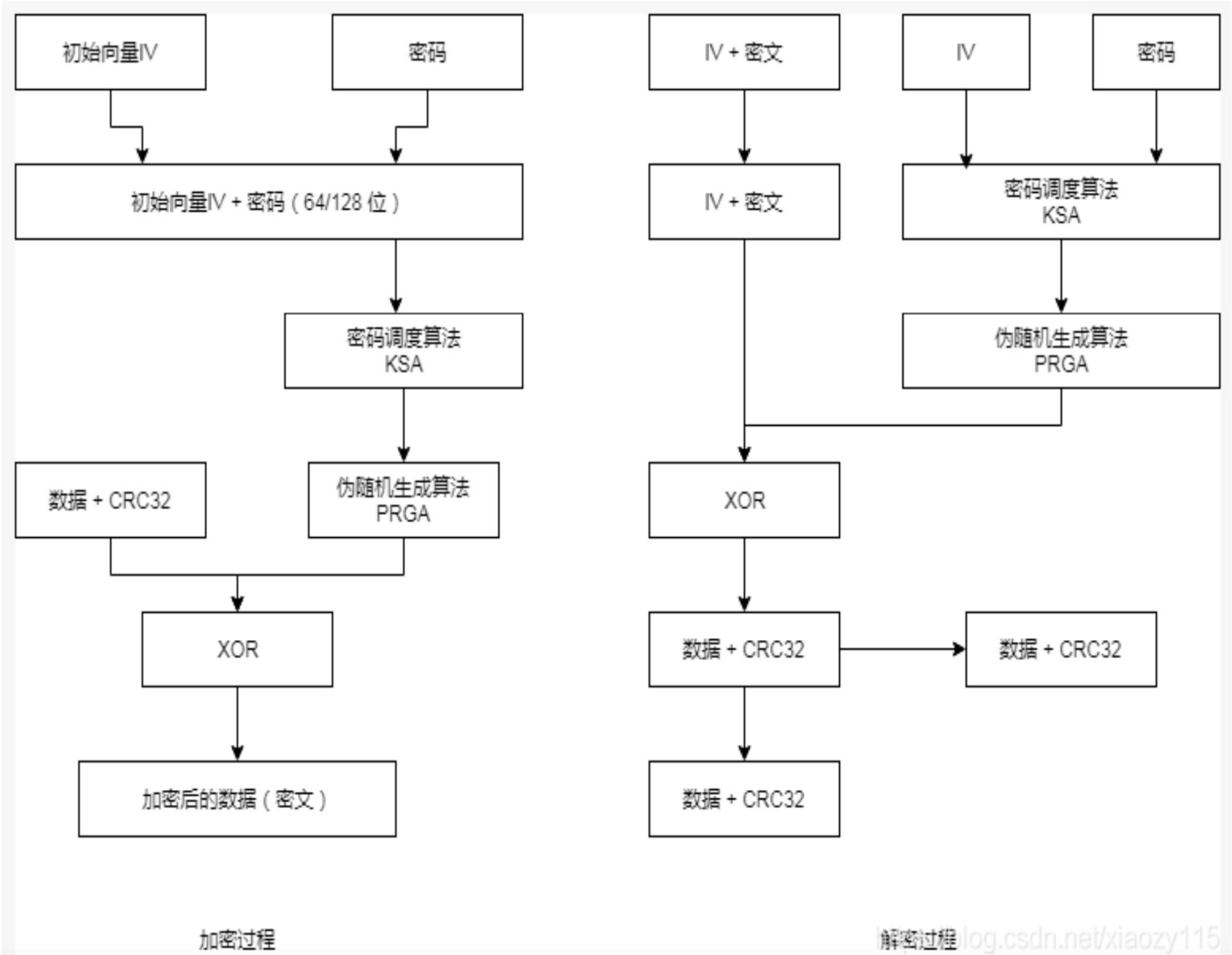




Basic WEP encryption: RC4 keystream XORed with plaintext

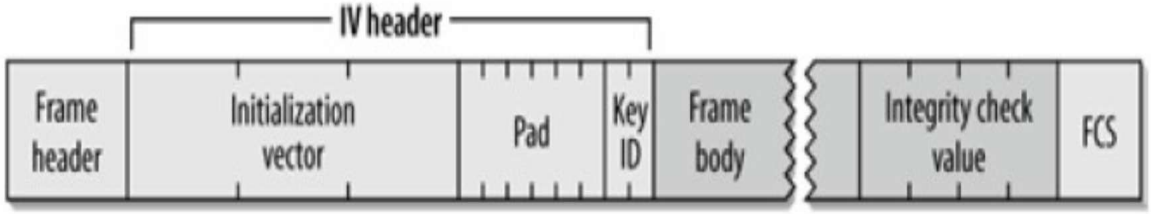
WEP Description




初始向量IV
密码
初始向量IV + 密码（64/128 位）
密码调度算法
KSA
伪随机生成算法
PRGA
数据 + CRC32
XOR
加密后的数据（密文）
加密过程
IV + 密文
IV
密码
IV + 密文
密码调度算法
KSA
伪随机生成算法
PRGA
XOR
数据 + CRC32
数据 + CRC32
数据 + CRC32
解密过程

WEP帧格式

WEP 的帧格式



- **IV header（4字节）**： 作为帧主体的 IV 标头

  前三个字节：表示 24 个bit 的IV

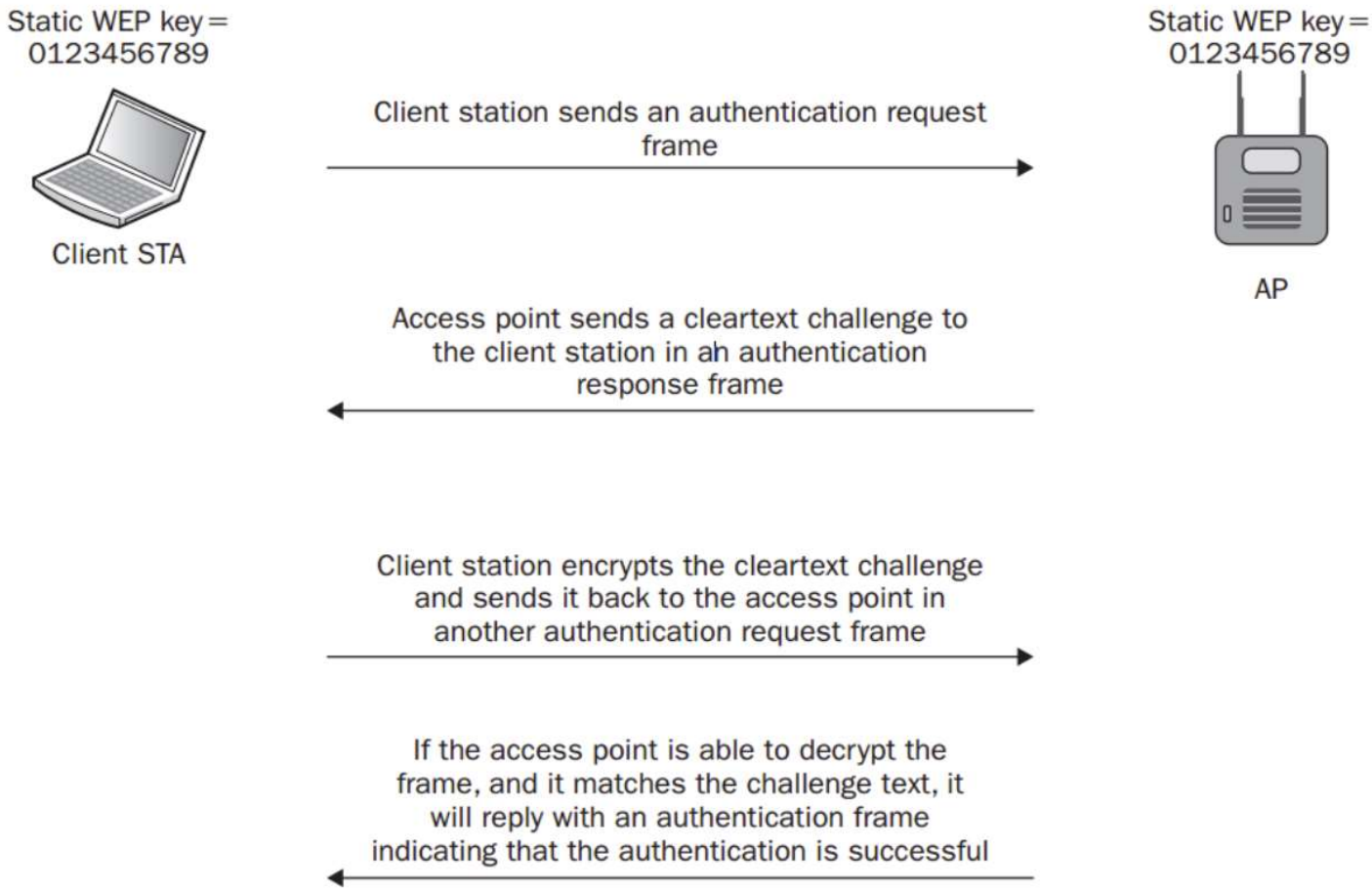
  第4个字节：包含Padding bits（为0）以及密钥识别码。如果使用预设密钥，Key ID 位可用来辨识加密帧的预设密钥。如果使用密钥映射关系，则Key ID 次栏位的值为0。

- **ICV（4字节）**： Integrity Check Value，完整性校验值，作为标尾。

- **FCS**：帧检验序列，32bit 校验码（CRC）提供了完整性的检查，附加于帧主体之后，同时为RC4 所保护。

WEP加密是共享秘钥式

- 共享密钥认证的认证过程为：客户端先向设备发送认证请求，无线设备端会随机产生一个 **Challenge** 包（即一个字符串）发送给客户端；
- 客户端会将接收到字符串拷贝到新的消息中，用密钥加密后再发送给无线设备端；
- 无线设备端接收到该消息后，用密钥将该消息解密，然后对解密后的字符串和最初给客户端的字符串进行比较。
- 如果相同，则说明客户端拥有无线设备端相同的共享密钥，即通过了 **Shared Key**认证；否则 **Shared Key**认证失败。


Static WEP key =
0123456789
Client STA
Client station sends an authentication request frame
Static WEP key =
0123456789
AP
Access point sends a cleartext challenge to the client station in an authentication response frame
Client station encrypts the cleartext challenge and sends it back to the access point in another authentication request frame
If the access point is able to decrypt the frame, and it matches the challenge text, it will reply with an authentication frame indicating that the authentication is successful

WEP机制的安全漏洞

- WEP中秘钥长度过短 40/104bit;
- 802.11协议没有规定WEP中秘密密钥(SK)如何产生和分发。
- 初始向量(IV)空间太小：

1）如果两个相同的IV||SK加密消息

C1⊕C2={P1⊕RC4(IV||SK)}⊕{P2⊕RC4(IV||SK)}=P1⊕P2

C代表密文，P代表明文

2）初始化向量的取值空间如此之小必然会导致相同密钥流的重复使用(key 40bit长，更容易发生。) 对于一个繁忙的接入点, 它不断以11Mbps的速度发送1500字节的数据包, 将在1500 * 8 / (11 * 10^6) * 2^24 = ~18000秒, 或5小时耗尽IV. (时间可能会更少, 因为许多数据包小于1500字节.)

WEP机制的安全漏洞

- 攻击者对消息进行篡改：

根据数据包的位差异计算出它们的CRC-32之间的位差异. 翻转消息中的第n位, 可以明确推算出其CRC-32中必须被翻转的位, 以产生与修改之后的消息对应的校验和. 因为位翻转在RC4解密之后被仍然生效, 这使得攻击者可以任意翻转加密消息中的位, 并正确调整它的校检和, 使最终得到的消息看起来合法.

WEP密钥破解

WepAttack：一款功能强大的WLAN 802.11 WEP密钥测试工具

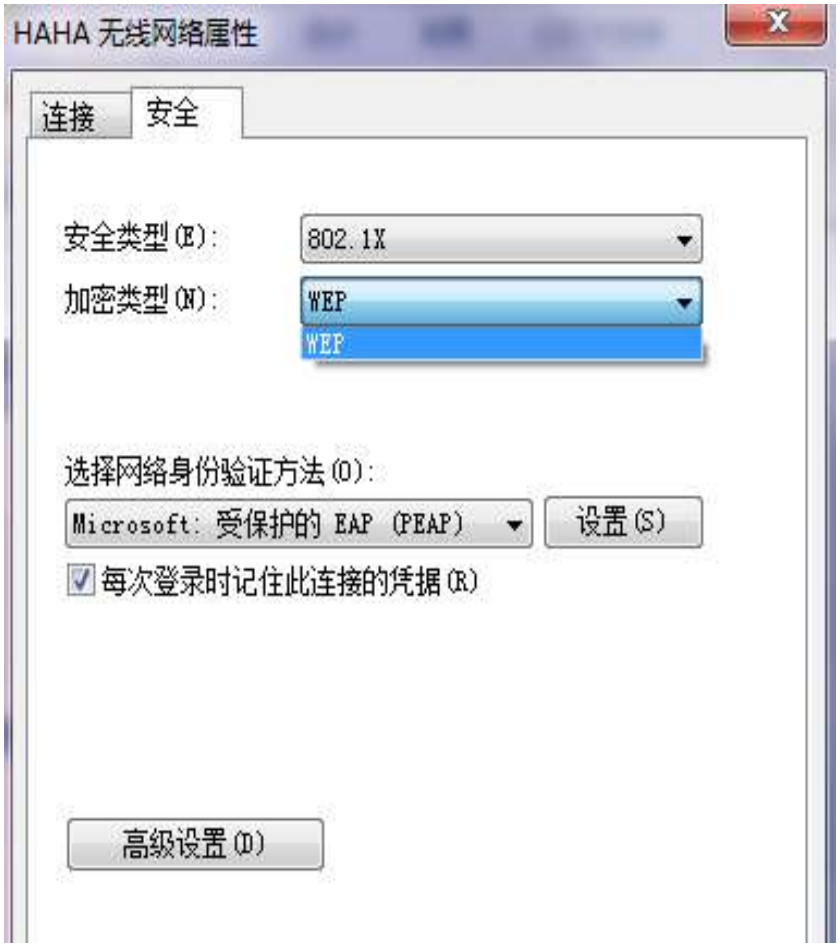
Alpha_h4ck　2018-12-29 15:00:41　203501　6

前言

今天，给大家介绍的是一款名叫WepAttack的开源工具。这是一款基于Linux平台的开源WEP密钥破解工具，它主要针对的是WLAN无线安全领域，可利用基于字典攻击的方式破解802.11 WEP密钥。

3.2 802.1x


HAHA 无线网络属性
连接
安全
安全类型(E):
WPA - 个人
加密类型(N):
网络安全密钥(K)
无身份验证(开放式)
共享式
WPA2 - 个人
WPA - 个人
WPA2 - 企业
WPA - 企业
802.1X
确定
取消


HAHA 无线网络属性
连接
安全
安全类型(E):
802.1X
加密类型(N):
WEP
WEP
选择网络身份验证方法(O):
Microsoft: 受保护的 EAP (PEAP)
设置(S)
每次登录时记住此连接的凭据(R)
高级设置(D)

802.1x简介

IEEE_802.1X

IEEE制定关于用户接入网络的认证标准（注意：此处X是大写），全称是“基于端口的网络接入控制”，属于IEEE 802.1网络协议组的一部分。于2001年标准化，之后为了配合无线网络的接入进行修订改版，于2004年完成。它为想要连接到LAN或WLAN的设备提供了一种认证机制。

使用802.1x的系统为典型的Client/Server体系结构，包括三个实体，分别为：Supplicant system（客户端）、Authenticator system（设备端）Authentication server system

图 1-1 802.1X 认证系统

- 客户端一般为一个用户终端设备，用户可以通过启动客户端软件发起802.1X认证。客户端必须支持局域网上的可扩展认证协议EAPoL（Extensible Authentication Protocol over LANs）。
- 接入设备通常为支持802.1X协议的网络设备，它为客户端提供接入局域网的端口，充当客户端和认证服务器之间的中介，从客户端请求身份信息，并与认证服务器验证该信息。根据客户端的身份验证状态控制其对网络的访问权限。
- 认证服务器用于实现对用户进行认证(Authentication)、授权(Authorization)和计费(Accounting)，通常为RADIUS服务器(Remote Authentication Dial In User Service，远程用户拨号认证系统)

802.1x认证协议

- 802.1X认证系统使用可扩展认证协议EAP（Extensible Authentication Protocol）来实现客户端、设备端和认证服务器之间的信息交互。 EAP协议可以运行在各种底层，包括数据链路层和上层协议（如UDP、 TCP等），而不需要IP地址。因此使用EAP协议的802.1X认证具有良好的灵活。

  1. 在客户端与设备端之间， EAP协议报文使用EAPoL（EAP over LANs）封装格式，直接承载于LAN环境中。

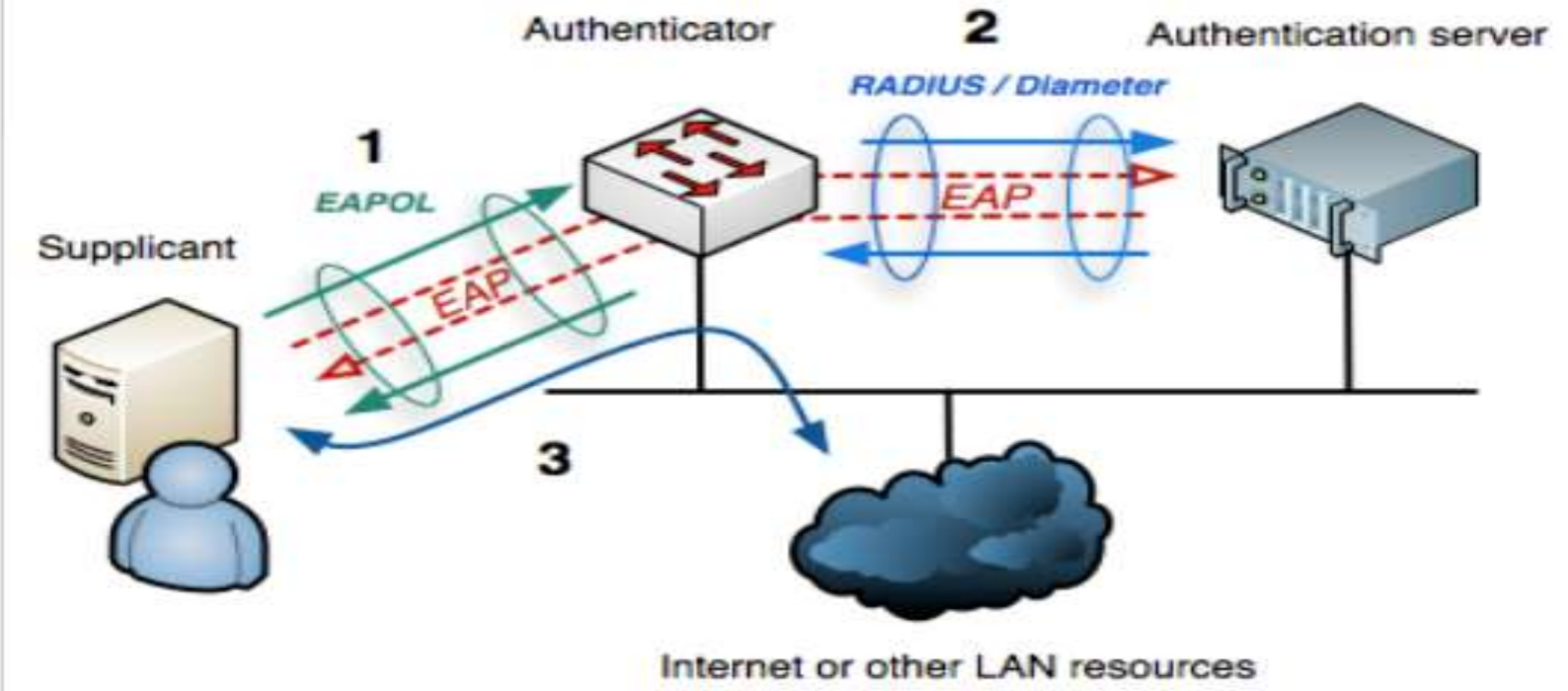
  2. 在设备端与认证服务器之间，用户可以根据客户端支持情况和网络安全要求来决定采用的认证方式。

  – EAP终结方式中， EAP报文在设备端终结并重新封装到RADIUS报文中，利用标准RADIUS协议完成认证、授权和计费。

  – EAP中继方式中， EAP报文被直接封装到RADIUS报文中（EAP over RADIUS，简称为EAPoR），以便穿越复杂的网络到达认证服务器 。

802.1x认证协议

- EAP不仅可以用于无线局域网，而且可以用于有线局域网。EAP是一个认证框架，不是一个特殊的认证机制。
- EAP允许协商所希望的认证机制。这些机制被叫做EAP方法，现在大约有40种不同的方法。RFC中定义的方法包括：EAP-MD5, EAP-OTP, EAP-GTC, EAP-TLS, EAP-SIM，和EAP-AKA, 还包括一些厂商提供的方法和新的建议。
- EAPOL就是(EAP OVER LAN)基于局域网的扩展认证协议。



EAP数据首先被封装在EAPOL帧中，传输于申请者（Supplicant）和验证者（Authenticator）之间。随后又封装在RADIUS或Diameter，传输于验证者和验证服务器（Authentication server）之间。

802.1X的认证过程

1. 申请者向认证者发送EAP-Start帧，启动认证流程；
2. 认证者发出请求，要求申请者提供相关身份信息；
3. 申请者回应认证者的请求，将自己的相关身份信息发送给认证者；
4. 认证者将申请者的身份信息封装至Radius-Access-Request帧中，发送至AS；
5. RADIUS服务器验证申请者身份的合法性，在此期间可能需要多次通过认证者与用户进行信息交换；
6. RADIUS服务器告知认证者认证结果；
7. 认证者向申请者发送认证结果。

图 3-1 EAP 中继认证流程

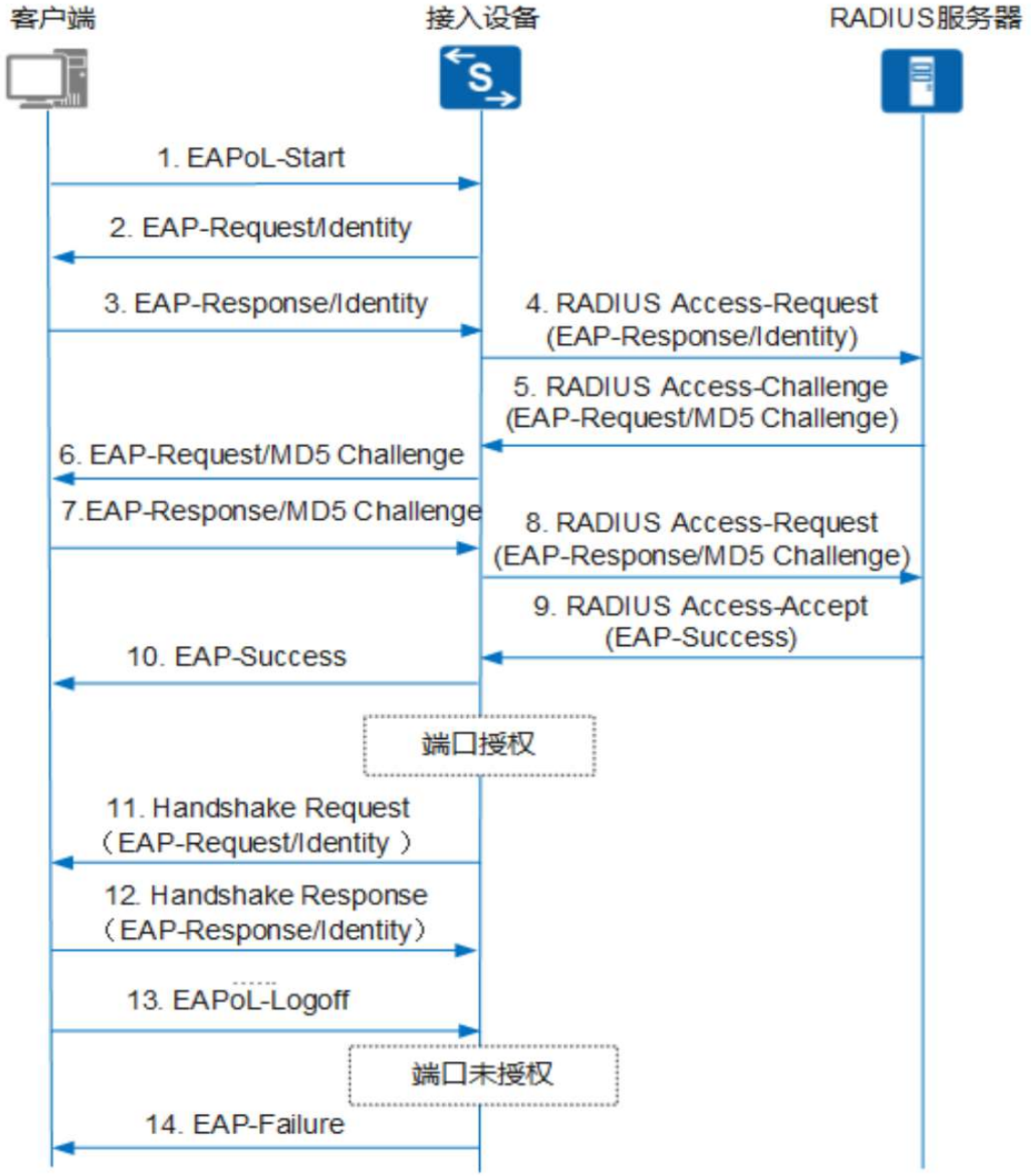
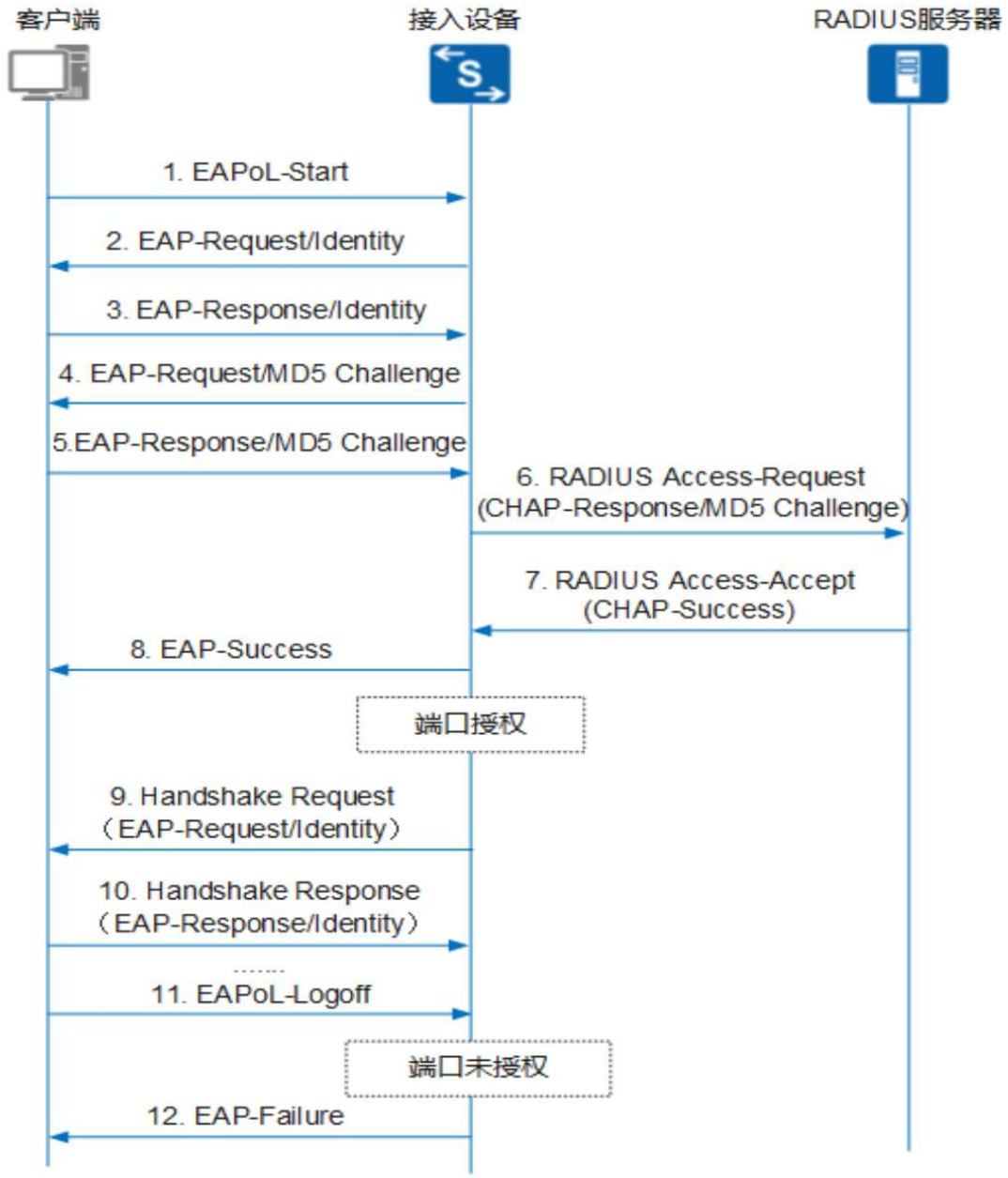


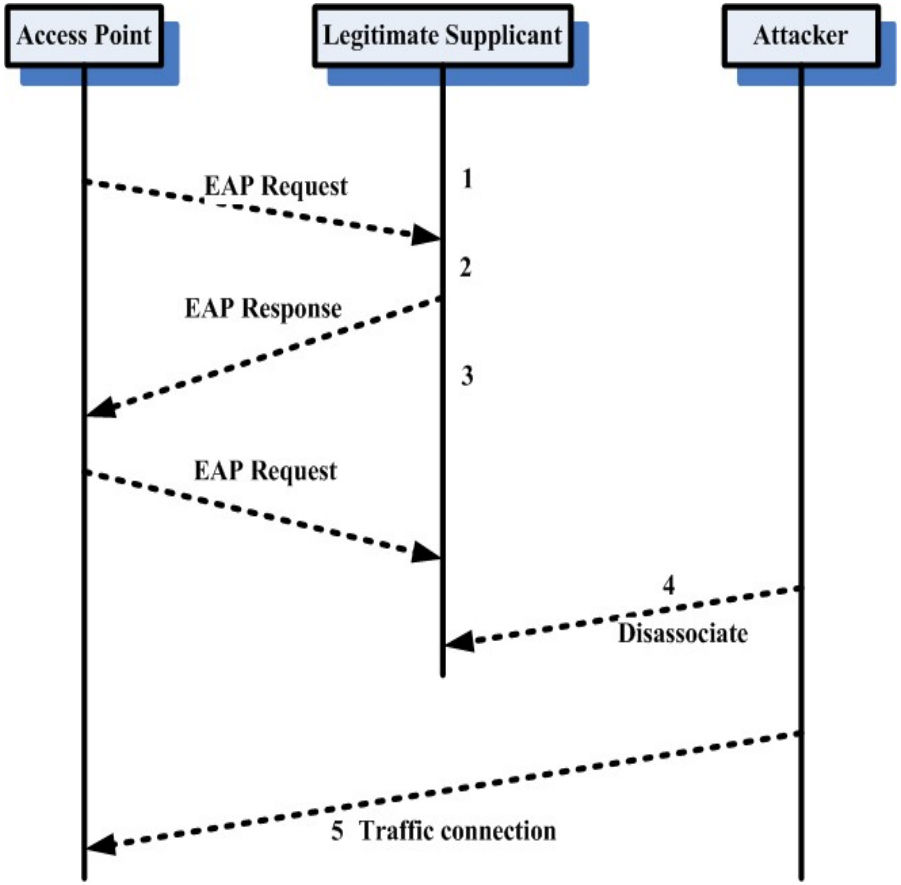
图 3-2 EAP 终结认证流程



802.1x安全分析

- ✓ 申请者和认证者的状态不平等，单向认证；
- ✓ 消息没有完整性保护，攻击者可以伪造这个数据包来冒充认证者实现中间人攻击，如会话劫持攻击。
- ✓ **IEEE802.1x**没有提供**DoS**保护，使得服务器容易耗尽计算资源以及存储资源，导致合法用户无法正常接入。

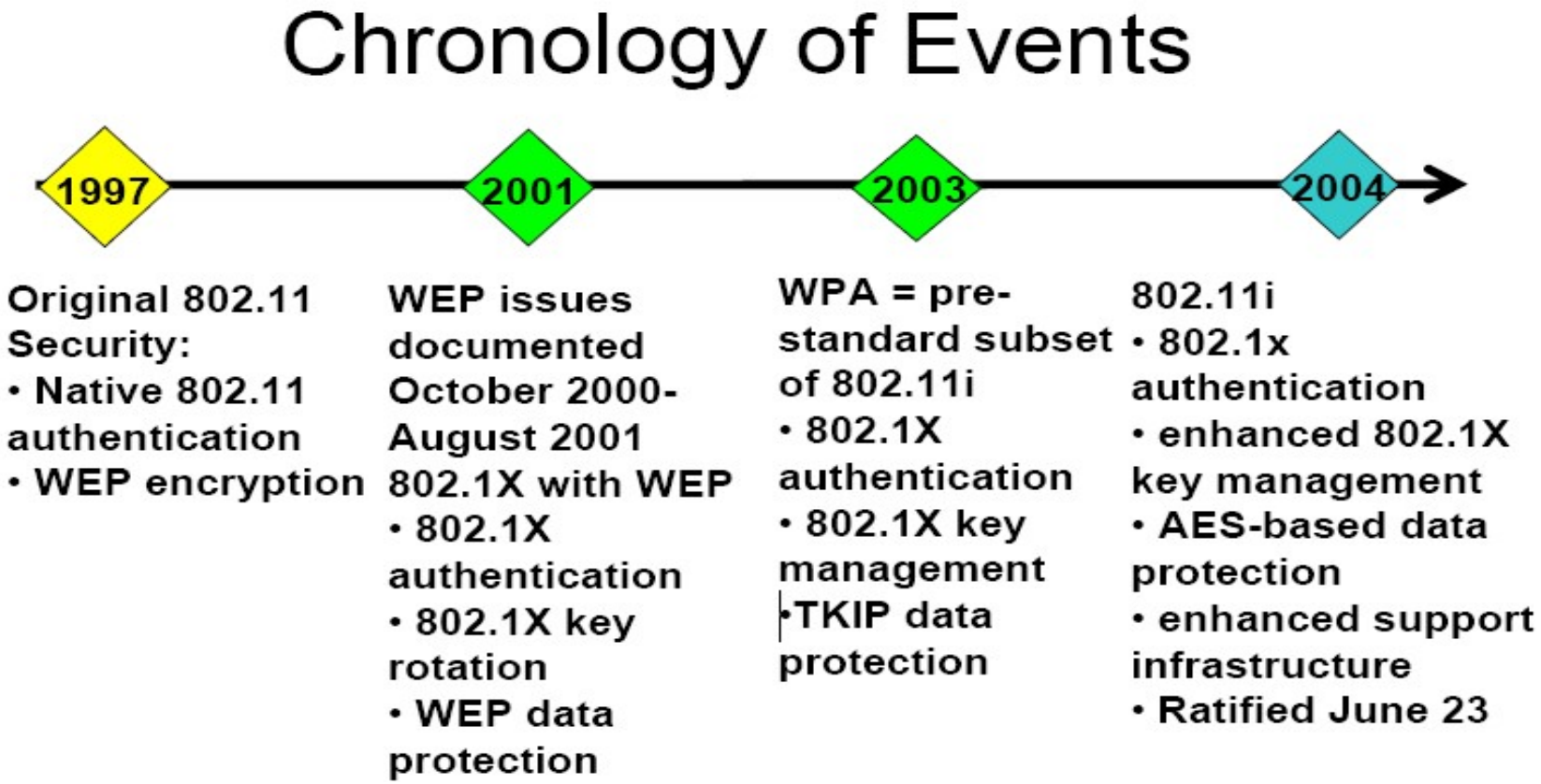
✓ 会话劫持攻击



消息1，2和3：合法的申请者进行认证(假设EAP认证只包含这3条消息，实际的EAP认证多于3条消息)。
消息4：攻击者冒充AP的MAC地址发送一条disassociate管理帧给申请者。这使得申请者的状态为disassociated。
消息5：这时攻击者冒充申请者的MAC地址接入到网络。

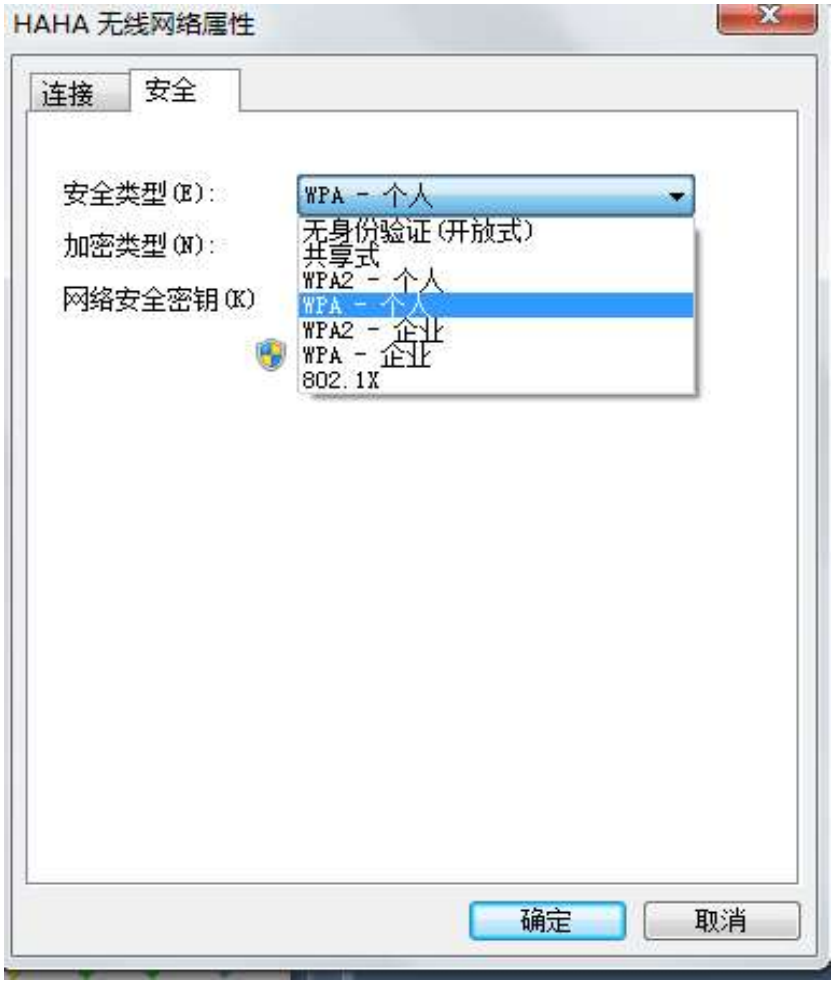
3.3 IEEE 802.11i协议分析

In the beginning …



WPA

全名为Wi-Fi Protected Access，有WPA和WPA2两个标准，是一种保护无线电脑网路（Wi-Fi）安全的系统，它是应研究者在前一代的系统有线等效加密（WEP）中找到的几个严重的弱点而产生的。WPA实作了IEEE 802.11i标准的大部分，是在802.11i完备之前替代WEP的过渡方案。WPA的设计可以用在所有的无线网卡上，但未必能用在第一代的无线取用点上。WPA2具备完整的标准体系，但其不能被应用在某些老旧型号的网卡上。

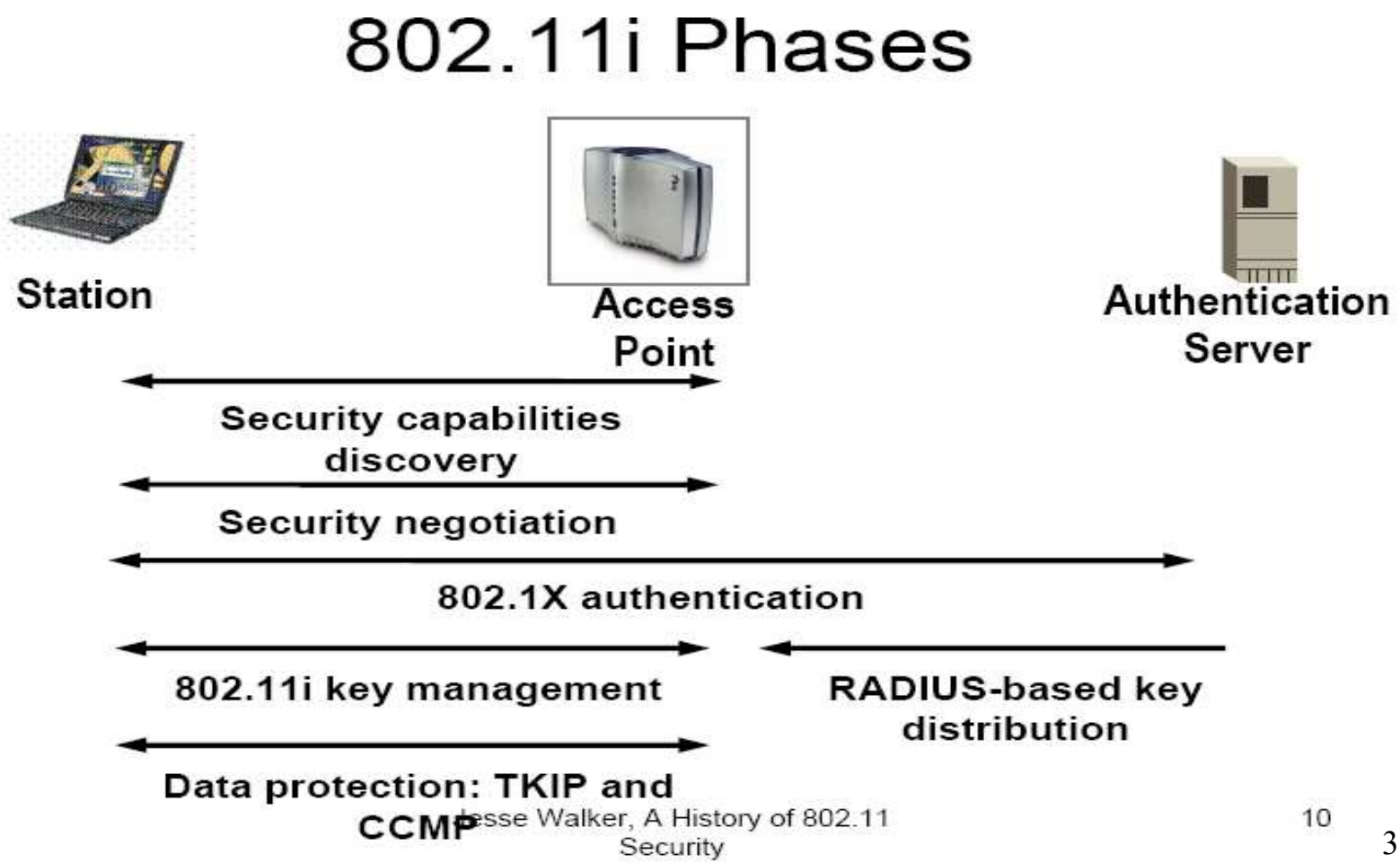


IP 分配:	自动(DHCP)
DNS 服务器分配:	自动(DHCP)
SSID:	Haha
协议:	Wi-Fi 4 (802.11n)
安全类型:	WPA2-个人
制造商:	Intel Corporation
描述:	Intel(R) Wireless-AC 9560 160MHz
驱动程序版本:	22.170.0.3
网络频带:	2.4 GHz
网络通道:	6
链接速度(接收/传输):	144/144 (Mbps)
本地链接 IPv6 地址:	fe80::fde5:32dc:4ee:7e0a%5
IPv4 地址:	192.168.31.60
IPv4 DNS 服务器:	192.168.31.1 (未加密)
物理地址(MAC):	50-E0-85-00-CF-12

WPA是一个中间过渡标准，最终的安全解决标准是802.11i，
WPA=802.11i草案3=802.1x/EAP+WEP(可选)/TKIP
WPA2=802.11i=802.1x/EAP+WEP（可选）/TKIP/CCMP（AES-CCMP）

802.11i流程

Architecture



- **Discovery**
  - –Determine promising parties with whom to communicate
  - –AP advertises network security capabilities to STAs
- **802.1X authentication**
  - –Centralize network admission policy decisions at the AS
  - –STA determines whether it does indeed want to communicate
  - –Mutually authenticate STA and AS
  - –Generate Master Key as a side effect of authentication
  - –Generate PMK as an access authorization token

Master Key(MK)

–MK = symmetric key representing Station's(STA) and Authentication Server's(AS) decision during this session

–Only STA and AS can possess MK

PairwiseMaster Key(PMK)

–PMK is a fresh symmetric key controlling STA's and Access Point's(AP) access to 802.11 channel during this session

–Only STA and AS can manufacture PMK

•PMK derived from MK

•AS distributes PMK to AP

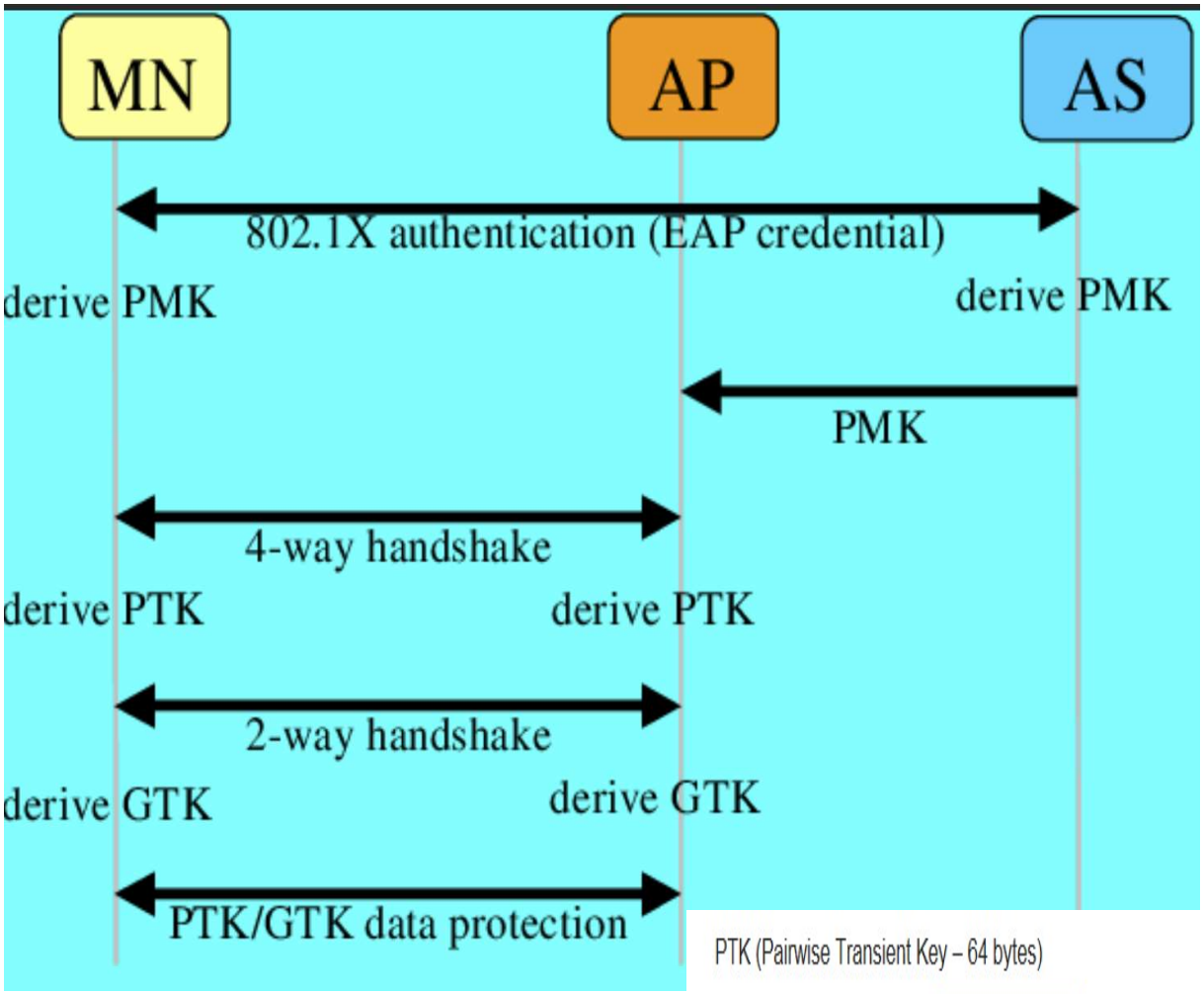
–PMK possession demonstrates authorization to access 802.11 channel during this session

PTK（Pairwise Transient Key，成对临时密钥）

– Prove each peer is live

–Synchronize PTK use

–Distribute GTK

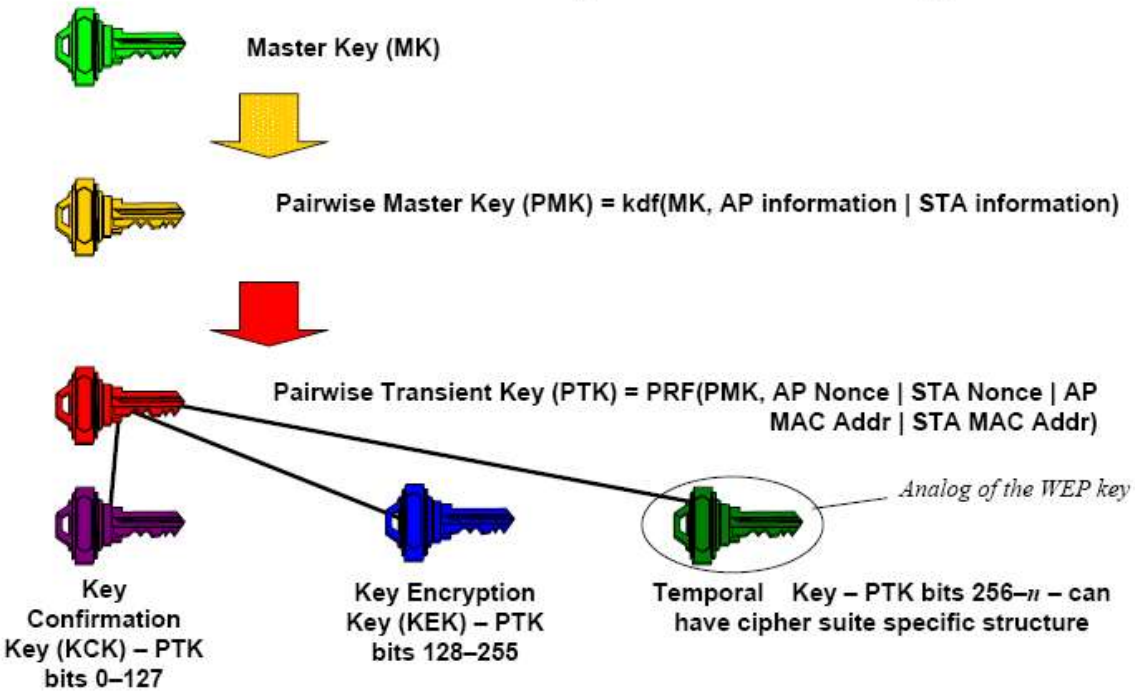


PTK (Pairwise Transient Key – 64 bytes)

1. 16 bytes of EAPOL-Key Confirmation Key (KCK)– Used to compute MIC on WPA EAPOL Key message
2. 16 bytes of EAPOL-Key Encryption Key (KEK) - AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client (for example, the RSN IE or the GTK)
3. 16 bytes of Temporal Key (TK) – Used to encrypt/decrypt Unicast data packets
4. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on unicast data packets transmitted by the AP
5. 8 bytes of Michael MIC Authenticator Rx Key – Used to compute MIC on unicast data packets transmitted by the station

The Michael MIC Authenticator Tx/Rx Keys provided in the handshake are only used if the network is using TKIP to encrypt the data.

802.11i Key Hierarchy

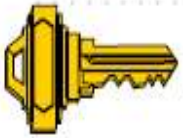


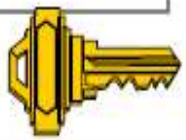
PTK (Pairwise Transient Key – 64 bytes)

1. 16 bytes of EAPOL-Key Confirmation Key (KCK)– Used to compute MIC on WPA EAPOL Key message
2. 16 bytes of EAPOL-Key Encryption Key (KEK) - AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client (for example, the RSN IE or the GTK)
3. 16 bytes of Temporal Key (TK) – Used to encrypt/decrypt Unicast data packets
4. 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on unicast data packets transmitted by the AP
5. 8 bytes of Michael MIC Authenticator Rx Key – Used to compute MIC on unicast data packets transmitted by the station

The Michael MIC Authenticator Tx/Rx Keys provided in the handshake are only used if the network is using TKIP to encrypt the data.

Step 2: 4-Way Handshake





Pick Random ANonce

EAPoL-Key(Reply Required, Unicast, ANonce)

Pick Random SNonce, Derive PTK = EAPoL-PRF(PMK, ANonce | SNonce | AP MAC Addr | STA MAC Addr)

EAPoL-Key(Unicast, SNonce, MIC, STA RSN IE)

Derive PTK

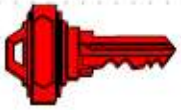
EAPoL-Key(Reply Required, Install PTK, Unicast, ANonce, MIC, AP RSN IE)

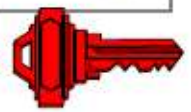
EAPoL-Key(Unicast, MIC)

Install TK

Install TK

Step3: Group Key Handshake





Pick Random GNonce,
Pick Random GTK

Encrypt GTK with KEK

EAPoL-Key(All Keys Installed, ACK, Group Rx,
Key Id, Group , RSC, GNonce, MIC, GTK)

Decrypt GTK

EAPoL-Key(Group, MIC)

unblocked data traffic

unblocked data traffic

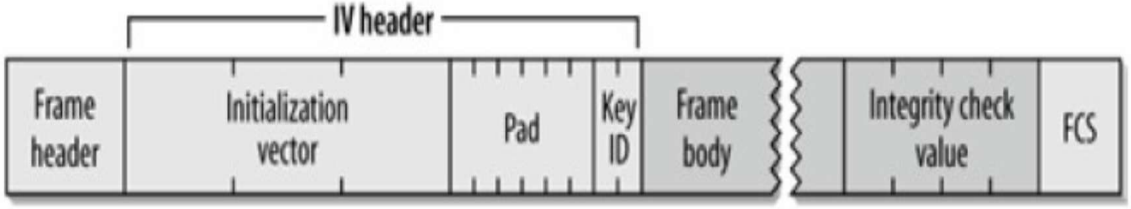
数据保护

- **802.11i提出两种加密机制：TKIP和CCMP**
- **TKIP Temporal Key Integrity Protocol（暂时密钥集成协议）**
- 是一种用于**IEEE 802.11**无线网络标准中的替代性安全协议，由电气电子工程师学会（**IEEE**）**802.11i**任务组和**Wi-Fi**联盟设计，用以在不需要升级硬件的基础上替代有线等效加密（**WEP**）协议。

- **TKIP**是包裹在已有**WEP**密码外围的一层“外壳”。**TKIP**由**WEP**使用的同样的加密引擎和**RC4**算法组成。不过，**TKIP**中密码使用的密钥长度为**128**位。这解决了**WEP**的第一个问题：过短的密钥长度。

- 利用**TKIP**传送的每一个数据包都具有独有的**48**位序列号，这个序列号在每次传送新数据包时递增，并被用作初始化向量和密钥的一部分。将序列号加到密钥中，确保了每个数据包使用不同的密钥。这解决了**WEP**的另一个问题，即所谓的“碰撞攻击”。这种攻击发生在两个不同数据包使用同样的密钥时，由于**48**位序列号需要数千年时间才会出现重复，因此没有人可以重放来自无线连接的老数据包，解决了“重放攻击（**replay attacks**）”

WEP 的帧格式

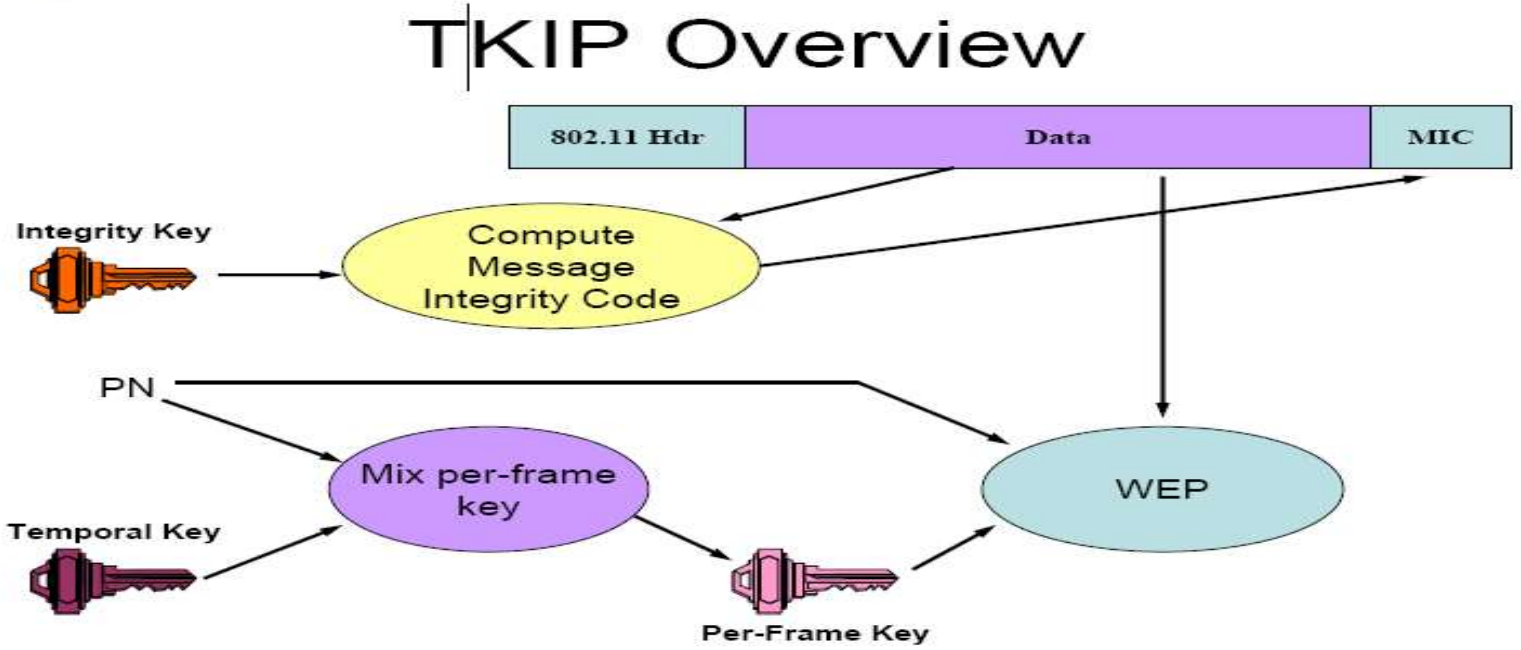


- **IV header（4字节）**： 作为帧主体的 IV 标头

  前三个字节：表示 24 个bit 的IV

  第4个字节：包含Padding bits（为0）以及密钥识别码。如果使用预设密钥，Key ID 位可用来辨识加密帧的预设密钥。如果使用密钥

Data protection



AES-CCMP 技术模式 CBC-MAC协议 (AES-Counter Mode CBC-MAC Protocol）

- ✓ **Definition of:** 是在 **802.11i** 安全协议使用的加密算法。使用 **AES** 块加密算法，但是把密钥的长度限制为 **128** 位。

- ✓ **AES-CCMP** 结合了两种复杂的加密技术**(counter mode** 和 **CBC-MAC)**并把他们应用于以太帧，从而在移动客端和 **AP** 之间提供一种健壮的安全协议。

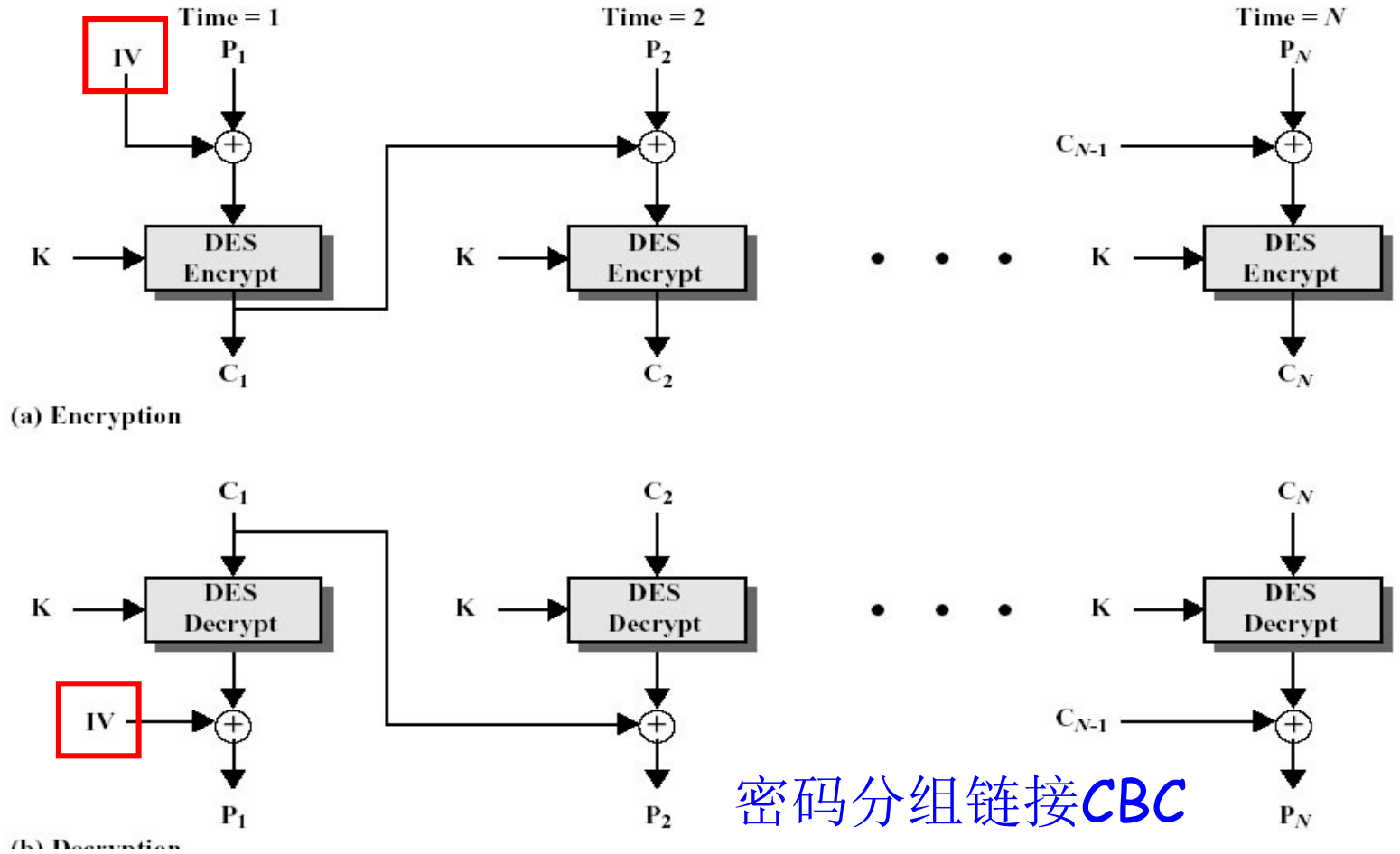
完全废除**wep**

Definition of: counter mode

Counter 模式使用了一个随机数(the counter)，对于每块要加密的信息，这个随机数都会改变。这个 counter is encrypted with the cipher, and the result is XOR'd into ciphertext. Since the counter changes for each block, the problem of repeating ciphertext that results from the electronic code book (ECB) method is avoided.

Cipher Block Chaining Message Authentication Code (CBC-MAC) authentication.

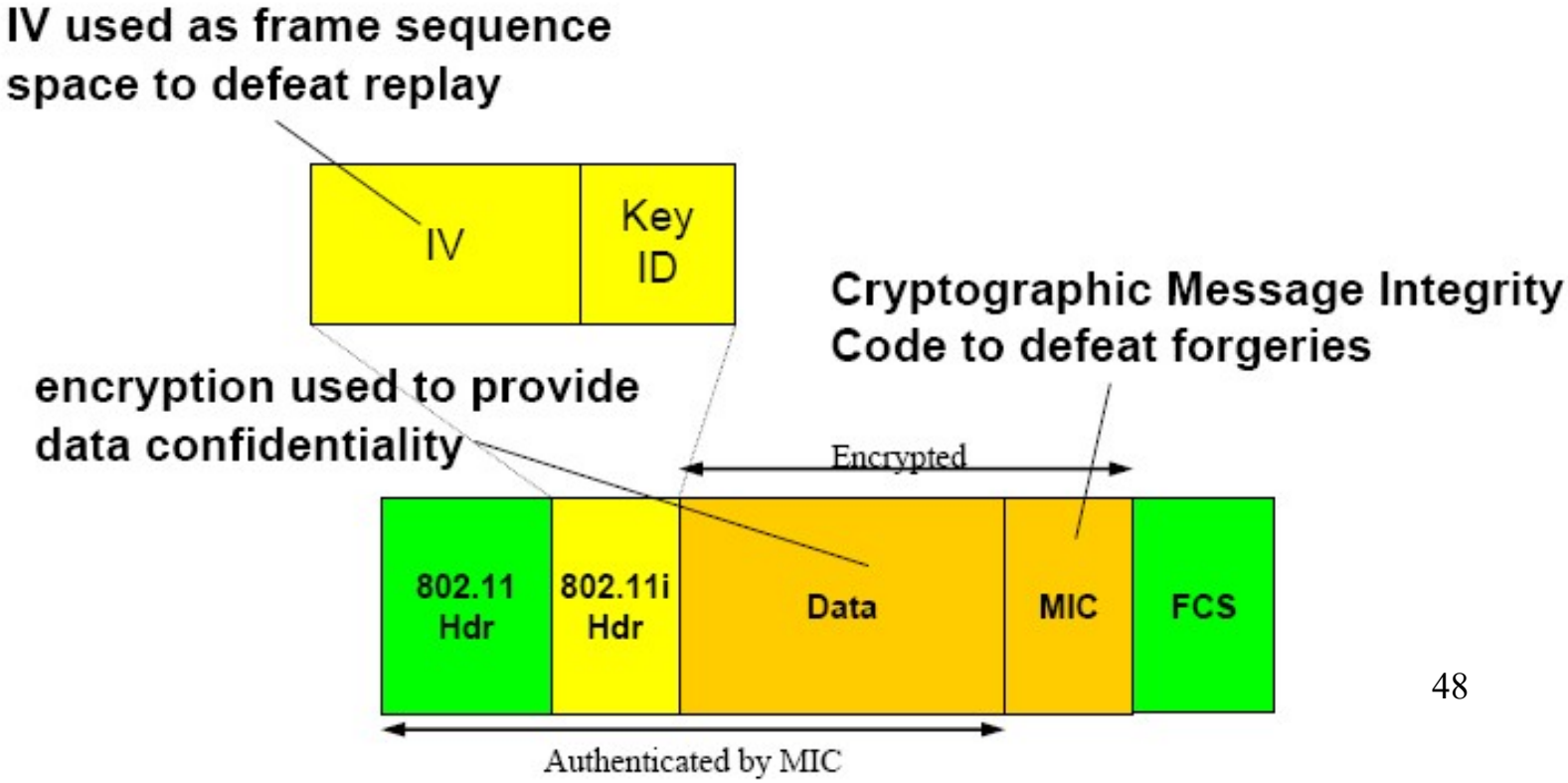
- ✓ Counter(CTR) 模式用于保密，而 CBC-MAC 用于认证和完整性。
- ✓ CCMP 必须使用 AES 算法，采用 128 位密钥和 128 位块大小



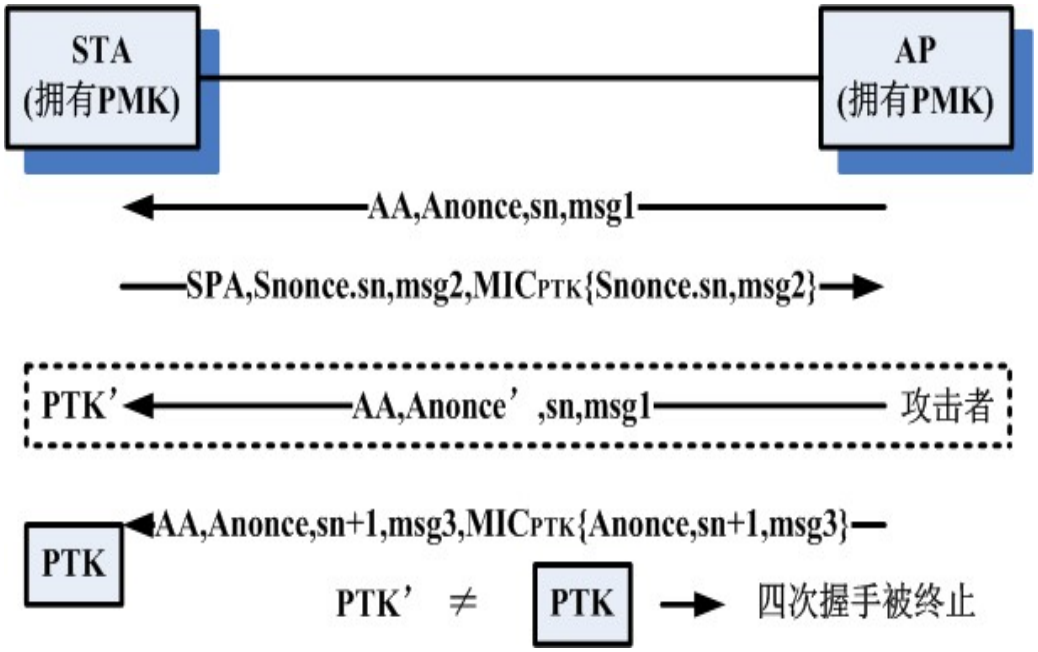
密码分组链接CBC

Data protection

Frame Format



IEEE802.11i安全分析



DoS attack:
数量极大的伪造Messagel必将使STA要存储大量的PTK，从而使得STA的存储器资源耗尽而造成系统瘫痪，无法开始新合法会话，同样造成DoS攻击。

- **攻击者可以在四次握手过程中Message2发送后,冒充AP向STA发送伪造的Messagel'。**
- **STA将根据新的Messagel'中的Anonce'和本身产生的新的Snonce。**
- **重新计算PTK'，而PTK'与认证者收到Message2后产生的PTK显然是不一致的，这样STA收到Message3后无法正确校验，就会导致四次握手过程被终止，造成了DoS攻击。**

- **IEEE 802.1li**工作组为这个问题提供了一种解决方案，对现有的四次握手协议做了部分改进。
- 但是**STA**存储所有可能的**PTK**仍然存在致命的弱点。
- 攻击者可以向请求者发送大量具有不同随机数的**Messagel**，而请求者为了能与合法的认证者完成握手，必须将根据接收的所有随机数计算出的相应的**PTK**存储起来，直到完成握手并得到合法**PTK**。

3.4 快速切换安全协议802.11 R

解決方案

- **Client**可以停留在現有通道，並使用當前的接入點與其他備選接入點通訊。這使**Client**資料流程中斷的可能性降到最小，但客戶無法探測到通過無線電與其他接入點通訊能力的任何細節。

- **Client**也可以直接切換到另一個接入點的通道，這使客戶機可以確定通過無線電與其他接入點通訊的品質，但會造成與當前接入點通訊過程中的一定程度間斷。

802.11 r 概述

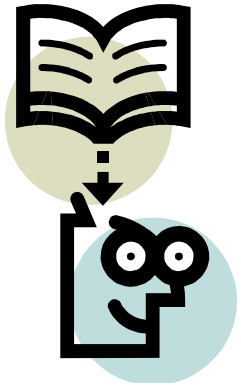
- **802.11r**改善了移動的用戶端設備在**AP**之間移動時的切換過程。協議允許一個無線**AP**在實現切換之前，就建立起與新**AP**之間安全且具備**QoS**的狀態（停留在現有通道）

- **Client**可以將現有的接入點作為通向其他接入點的管道，使由於通道改變所引起的通訊中斷最小化（停留在現有通道）

- **It was published on July 15, 2008.**

802.11 r 概述

- 來自802.11i的PMK緩存技術加快安全連接的速度(20ms～30ms)。這些協議可能實現WLAN連接在AP之間的快速、安全、無縫的切換。



IEEE 802.11 Architecture

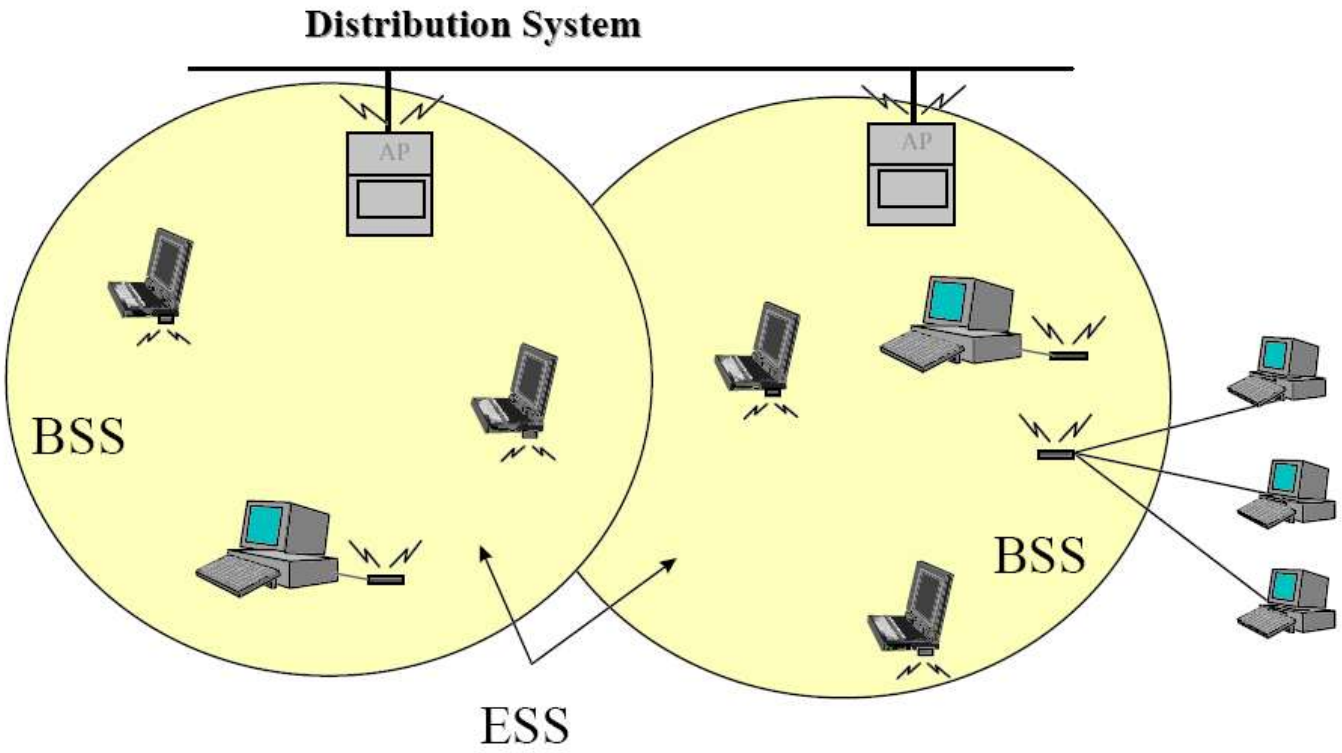


Figure 3: IEEE 802.11 architecture

- From: Pablo Brenner, "A Technical Tutorial on the IEEE 802.11 Protocol"

- BSS: Basic Service Set
- ESS: Extended Service Set
- AP: Access Point
- DS: Distributed System

几个阶段

scanning

802.11 authentication

re-association

PTK derivation - four-way handshake

QoS admission control

- 快速切换过程包括建立新信道的无线连接与新AP建立关联，接着是认证过程(或者是在关联之前实现预认证过程)，然后是密钥管理阶段，最后是确认其他的一些连接参数，例如QoS参数。

Scanning

发现阶段是指当STA发生切换之前，应该通过扫描其他的无线信道发现候选切换的AP以决定目标AP的过程。如果STA的当前连接支持的业务需要一定的资源，那么候选的目标AP则应该能够具备一定的资源支持此业务。 Passive 、 active scanning

802.11authentication/在关联之前实现预认证过程

802.11i中，由802.1x认证引入的时延可以通过PMK(Pairwise Master Key，单播主密钥)的缓存和预认证减少。当STA通过在与新AP关联之前或者预认证阶段缓存了安全关联，STA与新AP关联时无需再进行重新认证，但是还需要通过802.11i规定的4次握手协议实现密钥的管理和分发。

预认证：

- 为了减少漫游时间；
- 利用当前AP作为通信隧道，STA与目标AP进行认证，然后缓存协商好的主密钥PMK，等到客户移动到那个AP的时候，只进行密钥协商。

注意：

- PMK具有存活时间。当AP想对用户重新认证，必须在存活时间内。
- 存活时间由radius服务器告诉AP。而802.11i中AP并不告诉STA关于PMK的超时信息。

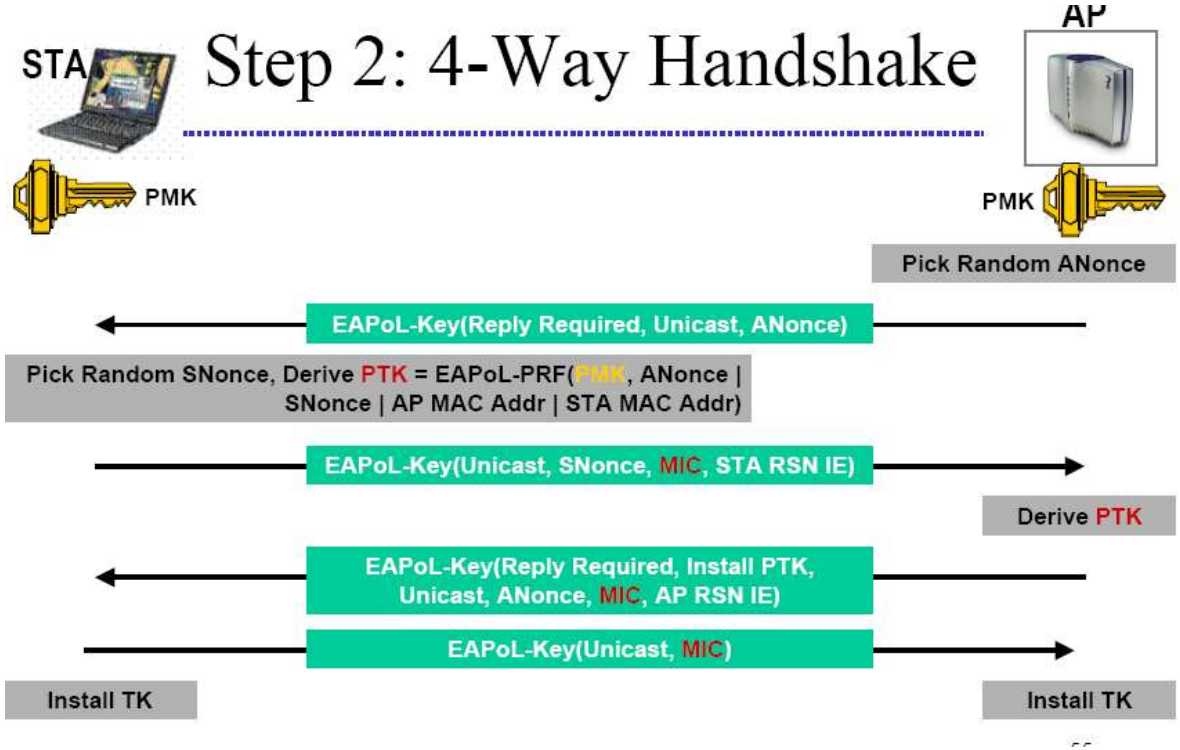
重关联/re-association

- (1)STA暂时断开当前的无线信道，通过其它的无线信道与目标AP2进行通信；
- or
  (2)STA通过当前的AP1转发STA的资源请求与目标AP2进行通信。
- 无论哪种方式，STA和目标AP之间都是通过RRSAP(Resource Request Service Access Point)模块进行资源配置。

QoS admission

- **(1)STA暂时断开当前的无线信道，通过其它的无线信道与目标AP2进行通信；**
- **or**
  (2)STA通过当前的AP1转发STA的资源请求与目标AP2进行通信。
- **无论哪种方式，STA和目标AP之间都是通过RRSAP(Resource Request Service Access Point)模块进行资源配置。**

802.11r安全问题


STA
Step 2: 4-Way Handshake
AP
PMK
PMK
Pick Random ANonce
EAPoL-Key(Reply Required, Unicast, ANonce)
Pick Random SNonce, Derive PTK = EAPoL-PRF(PMK, ANonce | SNonce | AP MAC Addr | STA MAC Addr)
EAPoL-Key(Unicast, SNonce, MIC, STA RSN IE)
Derive PTK
EAPoL-Key(Reply Required, Install PTK, Unicast, ANonce, MIC, AP RSN IE)
EAPoL-Key(Unicast, MIC)
Install TK
Install TK

802.11r安全问题

- **IEEE 802.11r快速切换认证请求帧和快速切换认证响应帧中，缺少对随机数的认证，因此面临比IEEE 802.11i更为严重的DOS攻击。**

(1) 第一类DOS攻击

攻击者可以向AP发送大量快速切换认证请求帧：

- 产生原因：快速切换认证请求帧中的随机数没有经过认证就发送，而AP必须接收该消息并进行相应处理(包括：产生及发送Anouce，预计算PTK以及保持一个连接状态等),有可能会使其内存及计算资源耗尽。
- 解决办法：在快速切换认证请求帧中加入MAC值校验。

802.11r安全问题

(2) 第二类DOS攻击

- STA发送快速切换认证请求帧，其中包含 nonce S ；攻击者假冒AP发送一条篡改的快速切换认证响应帧，其中包含 nonce A’，导致STA和AP计算的PTA不匹配， IEEE 802.11认证确认帧无法通过验证，使STA无法接入网络。
- 产生原因：快速切换认证请求帧没有经过认证就发送，而AP必须接收并进行相应处理。
- 解决办法：在快速切换认证请求帧中加入MAC值校验。

改进认证方案：1 基于 MIC认证解决方案

自阅

- 通过在切换请求消息和切换响应消息中加入MIC（Message Integrity Code）值进行校验，可以有效解决上述安全问题。
- (1) 在快速切换认证请求帧中加入 MIC值校验, MIC 的密钥可以取为 PMK和某一单调增加值的运算式, 克服第一类和第二类 DOS攻击;
- (2) AP在快速切换认证响应帧中加入及 MIC 值校验, 该 MIC的密钥可以取为预计算的 PTK, 解决第三类 DOS攻击。

3.5常见攻击技术介绍

✓嗅探流量

- 实际上，所有的**WiFi**流量都是可以通过监听模式的适配器来嗅探的。嗅探流量是一种被动行为，所以它是不能被检测到的。一定要确保使用了更高层的加密手段。

✓**WiFi**干扰

- 干扰利用故意的无线电干扰，通过使通信介质保持繁忙状态，使发射机在检测到无线介质繁忙或接收机接收到损坏信号时后退，从而危害无线通信。
- 干扰主要针对物理层的攻击，但有时也可能发生跨层攻击
- 干扰的影响：间断连通性或意外断开连接，连接和数据传
延迟，网速迟缓，以及信号强度差。
- 多种干扰机实施。

3.5常见攻击技术介绍

✓流氓热点

- 手机在自动连接至**WiFi**网络时会发生以下两种场景:

1. 手机获取已知**WiFi**网络的**beacon**帧，然后开始与距离最近（信号最强）的热点进行连接。
2. 手机给已知**WiFi**网络发送一个**probe-request**帧，可提供网络服务的接入点将响应一个**probe-response**帧。接下来，你的手机将会跟这个响应接入点进行连接。

- 攻击者可以搭建一个便携式的流氓接入点，这个接入点不仅能够响应（**probe-response**）任何的**probe-request**帧，而且它们还能够给任何的目标网络发送**beacon**帧。

3.5常见攻击技术介绍

✓无线钓鱼

- 用户可以在不知情的情况下连接到他们认为是合法接入点的无线网络，但实际上，是为特别是吸引不知情的受害者设立的蜜罐或开放网络。
- 例如，他们可能在家里有一个被称为“**Linksys**”的网络。因此，他们的笔记本电脑会自动连接到其它任何称为“**Linksys**”的网络。这种内置行为可能会导致偶然关联到一个恶意的无线网路，通常被称为无线网络钓鱼。

总结

- 802.11r通过制定研究新的机制实现快速切换，这些新的机制包括：

(1)通过定义切换能力交换，在STA和AP重关联之前或者重关联过程中实现对资源的配置；

(2)资源预留机制，包括QoS、相关安全参数在内的各种类型的资源，在关联之前通过无线或者通过当前AP和DS实现与目标AP的通信；

(3)新的密钥管理框架，可以实现在STA和AP之间建立惟一的PMKSA；

(4)新的漫游协议，用于在重关联或者是重关联之前推算出PTK。

利用以上策略，802.11r的快速切换可以尽量减少切换带来的连接中断对实时业务的影响，实现宽带无线局域网对VoIP这类实时业务更好的支持。

Thank you!

测试1：根据下面流程设计一个基于第三方的认证协议，单向/双向均可：

（1）说明设计协议的应用场景；

（2）每个节点初始信息，如何获得；例如公钥、随机数等

（3）简介算法整体功能或者目标，包含几个步骤，每个步骤功能；

（4）对每个步骤详细实现加以设计，画出具体消息通信图；