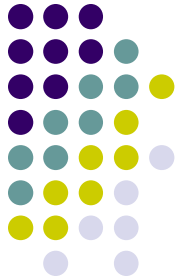


第6章 无线网安全性

Part I

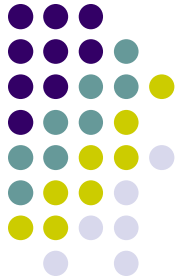
第6章 内容概要

- 6.1 无线通信和802.11 无线局域网标准
- 6.2 有线等价隐私协议
- 6.3 Wi-Fi 访问保护协议
- 6.4 IEEE 802.11i/WPA2
- 6.5 蓝牙安全机制
- 6.6 无线网状网的安全性

概论

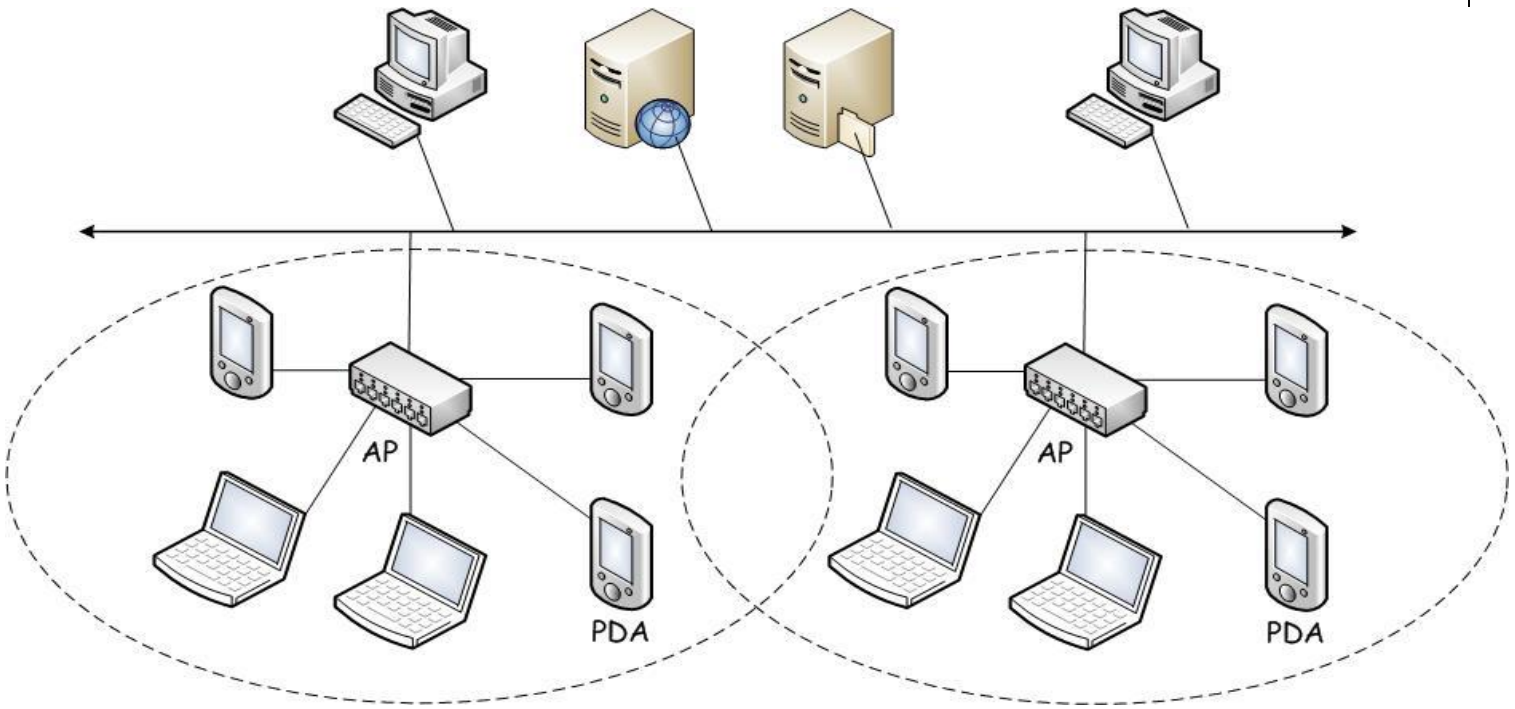
- 无线电通信
- 攻击者，有一个无线的传送和接受装置，与要攻击的无线网使用相同的无线频率，可以做到:
  - 拦截无线网数据
  - 将其计算机连接到一个近处的无线网
  - 对一个现有的无线网络插入数据包
  - 用无线电干扰设备对特定无线网通道实施干扰
- 保密措施
  - 在数据链接层实施加密算法，身份验证算法和完整性检验算法
    - 提供类似有线网媒体访问的隐私保护
    - 高层通信协议和网络应用程序（有线和无线）都无需更改可以照常使用

无线局域网体系结构



- 两种体系结构
  - 固定无线局域网: 可与有线网相连
  - 特定无线局域网(点对点): 不与任何固定的有线网相连
- 含有无线通信设备的装置通常称为移动站STA
  - 根据 IEEE 802.11通信标准，每台STA由一个48比特MAC地址唯一确定
- 无线接入点 (AP)
  - 一端 ：与一个有线局域网建立连接
  - 另一端：在AP和STAs之间建立无线的收、发联系，实现通信
  - 时分复用技术允许多台STA相连
  - 每个AP由一个服务集标识符(SSID)唯一确定，定时向外发送信标

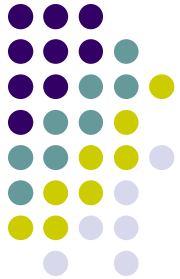
固定局域无线网示意图



- 信标发送：它定时对外公布其SSID及其他信息，为进入其覆盖范围内的STA与其建立连接之用
- 信标扫描：等待信标发送，确定与哪个AP相连，然后对其发出连接请求，继而建立与无线局域网的连接

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

特定无线局域网



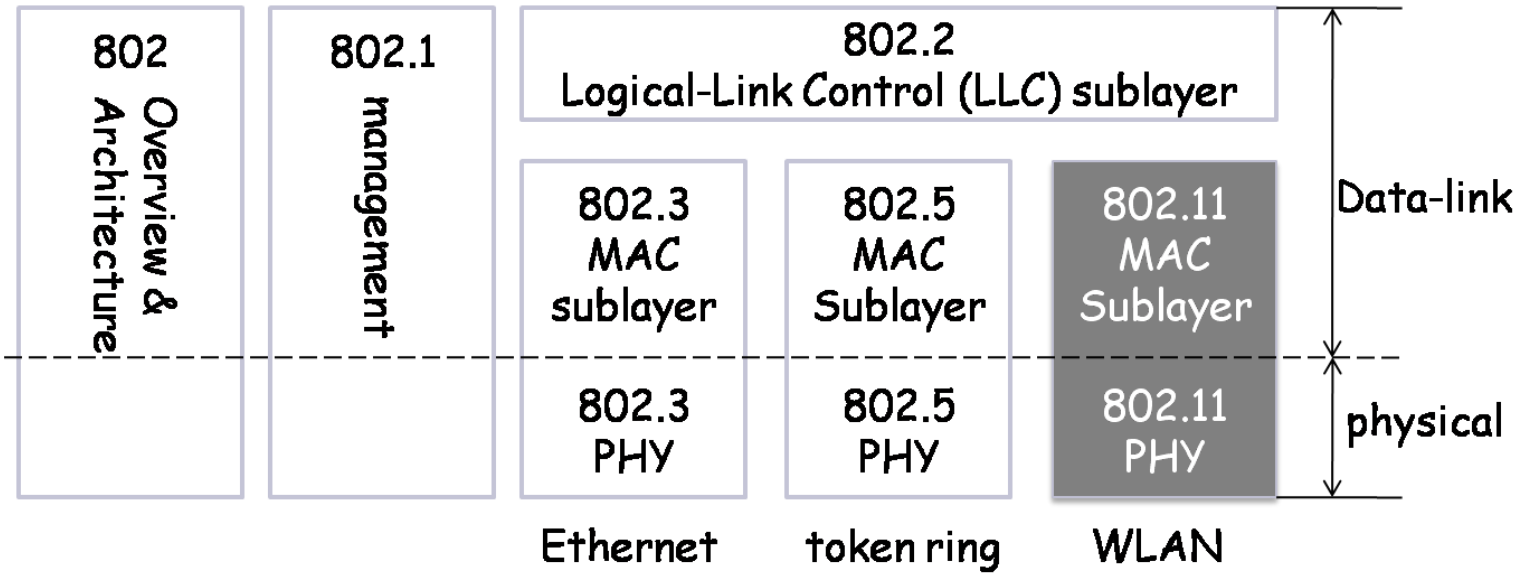
- 不与任何固定的网络基础设施相连
- 不包含APs
- 允许不同的STA直接通信
- 若目标STA不再通信范围内，可根据情况使用若干其他STA作为中转站建立通信路径

802.11 概述

- 802.11是无线局域网通信标准，对应于 802.3 (Ethernet)和802.5 (Token Ring)通信标准
- 它规定了无线局域网在MAC 子层和物理层的通信及安全保护机制
- MAC子层使用媒体访问方式：载波侦听多路访问回避冲突(CSMA/CA)方法
- 通用的子层协议：
  - 802.11a: 5 Ghz
  - 802.11b: 2.4 Ghz, 11Mbps, 室外35m, 室内110m， WEP
  - 802.11g: 2.4 Ghz, 54Mbps , 室外35m, 室内110m
  - 802.11i: WPA2
  - 802.11n: 支持 MIMO（多重输入/多重输出）

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

802局域网通信标准示意图



IEEE 802局域网通信标准示意图

《计算机网络安全的理论与实践（第2版）》．【美】王杰，高等教育出版社，2011年

无线通信的安全性弱点

- 无线通信更易于被侦听
- 无线信号比有线信号更容易受干扰，且在无线媒体中更容易注入无线信号
- 无线计算装置和嵌入式系统的计算功能和电池能源有限，不足以执行复杂运算

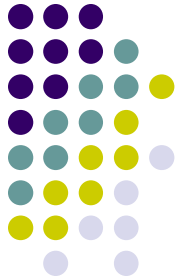
无线通信的安全性弱点

- 易遭受的安全攻击
  - 窃听攻击
  - 服务阻断攻击
  - 消息重放攻击
  - STA-诈骗攻击
  - AP-诈骗攻击

第六章 内容概要

- 6.1 无线通信和802.11 无线局域网标准
- 6.2 有线等价隐私协议
- 6.3 Wi-Fi 访问保护协议
- 6.4 IEEE 802.11i/WPA2
- 6.5 蓝牙安全机制
- 6.6 无线网状网的安全性

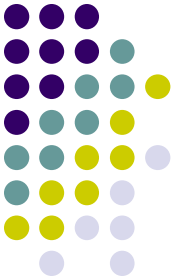
WEP 概述(Wired Equivalent Privacy)



- 发布于1999, WEP是802.11b无线通信标准在数据链接层使用的安全协议
- 要求：同一无线局域网中所有的 STA’s和AP’s都共享同一个密钥 *K* (称之为 *WEP* 密钥)
- WEP 密钥:
  - 40-bit, 104-bit (最通用的), 232-bit
  - WLAN 设备可以共享多个 WEP密钥， 每个WEP密钥通过一个字节长度的ID唯一表示出来，这个ID成为密钥ID
  - WEP 密钥常常有管理员选取（WEP没有规定密钥如何产生和传递）
  - 一般情况下一旦选定， WEP密钥不可改变

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

移动设备认证和访问控制



- WEP 运用挑战与响应的方式认证移动STA
- 为了和AP连网, STA 必须执行以下步骤：
  1. 请求: STA向AP发连接请求
  2. 挑战: AP收到请求后，即产生128位的随机数字符串*cha* 并且发送给 STA

     $cha = a_1 a_2 \ldots a_{16}$ (where each a_i is an 8-bit string)
  3. 响应: STA产生一个24位初始向量 IV，并对 *cha*用 RC4序列加密算法和密钥 *V*||*K*加密，如下计算出 r_i ， res ，并将 res发送给 AP

     $r_i = a_i \oplus k_i$, for i = 1,2,…,16

     $res = V \,||\, r_1 r_2 \ldots r_{16}$
  4. 核实: AP 也对V||K 用RC4 产生相同的子钥序列,并计算 $a_i' = r_i \oplus k_i$ 同时核实是否有 $a_i' = a_i$ 其中， i = 1,2,…,16, 如果是，则STA 被认可为合法用户，并与其相连

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

数据完整性验证

- 目标: 为了确保分组信息没有被修改或没有被非法的STAs侵入
- WEP 用 CRC-32 验证数据完整性，称之为*完整性校验值ICV*
  - CRC-32是一种通用的检测传输错误的技术
- CRC 的简单算法是用 ⊕ 运算和位移操作
  - 可由芯片简单实现
- 获取一个k位的CRC值：
  - M: n位的二进制字符串
  - P: *k阶二元多项式，其系数序列为一个* $(k+1)$位二进制字符串
  - 用生成多项式（二进制数）除以P，得到k位的 $\mathrm{CRC}_k(M)$
- *如果*$M||\mathrm{CRC}_k(M)$ 不能被P除, 意味着M 已被篡改

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年

LLC 网帧加密

- 加密实施在MAC 层，将LLC 网帧加密，分为三个过程
  - 令 M 为一个 LLC网帧:

$$M \,||\, \mathrm{CRC}_{32}(M) = m_1 m_2 \ldots m_l$$

  - 发送方产生一个24位初始向量 V, 用到RC4序列加密算法，以 $V||K$为输入以产生一个8位的子钥序列:

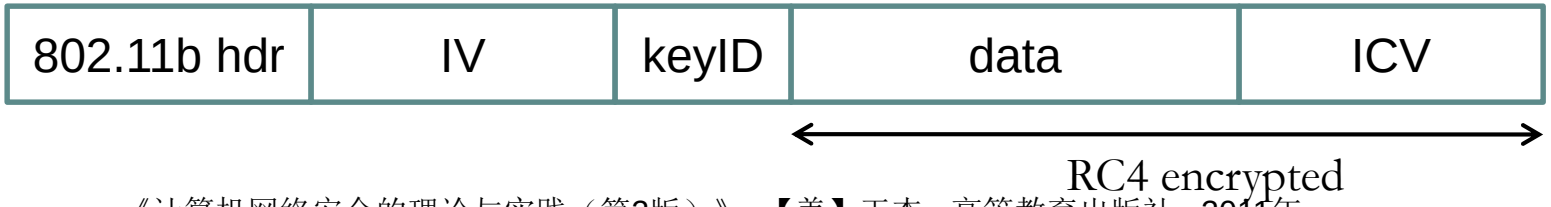
$$c_i = m_i \oplus k_i$$

  - 发送方将MAC 子层增加了载荷文件后发送给接收方

$$V \,||\, \mathrm{KeyID} \,||\, c_1 c_2 \ldots c_l$$

  - 通用加密形式如下:

$$C = ((M \,||\, \mathrm{CRC}_{32}(M)) \oplus \mathrm{RC4}(V||K))$$



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

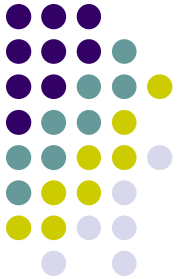
WEP的安全缺陷

认证缺陷:

- 由于WEP采用的挑战-应答机制是一个简单的异或运算，因此很容易受到明文攻击
- 例如:
  - 在AP和合法的STA之间恶意的拦截 (*cha, res*)信息对.
  - 计算$k_i=c_i \oplus r_i$ for i=1,2,…,16
  - 发送连接请求给 AP并等待其发出的挑战信息 *cha'*
  - 用计算出的子钥序列ki和挑战信息运算，产生一个应答信息*res'*，将此信息和截获的*IV一起发给AP*
  - 基于WEP协议， AP 用 RC4 和 IV || K, 产生子钥序列$k_1, k_2, k_3,\ldots k_{16}$, 证实 $k_i \oplus res' = cha'$, 由此，AP认证了攻击者的非法设备，准予其连网

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

WEP的安全缺陷



完整性校验缺陷:

- CRC 弱点
  - CRC具有线性运算性质: $\mathrm{CRC}(x \oplus y) = \mathrm{CRC}(x) \oplus \mathrm{CRC}(y)$
  - 这种线性特征使得攻击者容易篡改数据而不改变CRC值
  - CRC 没有任何密钥，使得攻击者容易向网络注入新的网包
    - 篡改数据
    - 注入信息
    - 碎片攻击

完整性校验缺陷

消息干扰（篡改数据）：

- Alice 发消息给 Bob: $C = (M \| \mathrm{CRC}_{32}(M)) \oplus \mathrm{RC4}(V \| K)$
- 攻击者拦截并修改了消息C 如下， 用另一个网帧Γ，计算得到C':

$$C' = (\Gamma \| \mathrm{CRC}_{32}(\Gamma) \oplus C$$

- Bob接收到一个被篡改的数据 $M' = \Gamma \oplus M$ 和正确的$\mathrm{CRC}_{32}(M')$的完整性校验值 ICV

$$\begin{aligned} C' &= (\Gamma \| \mathrm{CRC}_{32}(\Gamma)) \oplus C \\ &= [(\Gamma \| \mathrm{CRC}_{32}(\Gamma)) \oplus (M \| \mathrm{CRC}_{32}(M))] \oplus \mathrm{RC4}(V \| K) \\ &= [(\Gamma \oplus M) \| (\mathrm{CRC}_{32}(\Gamma) \oplus \mathrm{CRC}_{32}(M))] \oplus \mathrm{RC4}(V \| K) \\ &= [(\Gamma \oplus M) \| (\mathrm{CRC}_{32}(\Gamma \oplus M))] \oplus \mathrm{RC4}(V \| K) \\ &= (M' \| \mathrm{CRC}_{32}(M')) \oplus \mathrm{RC4}(V \| K) \end{aligned}$$

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年

完整性校验缺陷

注入消息:

- 假定 明文-密文对(M,C) 已被获知， V 是一个为产生C的初始向量
- 注意 V 向量是经明文传输
- 然后$(M \oplus C)$运算产生对M加密的子密钥序列， (子密钥产生于RC4$(V||K)$序列加密算法)
- 假定Θ 为一个攻击者试图注入网络的信息，其字节长度<=|M|-4
- 攻击者计算 $CRC_{32}(\Theta)$并将其注入公式，即用算出的子密钥序列来加密

$$V||(\Theta|| \ CRC_{32}(\Theta)) \oplus RC4(V||K)$$

并把它发给其他合法用户，那么以上消息会通过合法认证

完整性校验缺陷

碎片攻击:

- 利用攻击 LLC 网帧首部，将信息注入网络中
  - LLC 网帧首部8个字节为固定值，区分IP包和ARP包
  - 攻击者用XOR算法得到8个子密钥
- 攻击者阴谋:
  - 攻击者将 64字节长的 LLC网帧分割成 16个4字节长的片段
  - 用 *IV* 和前8个子钥$k_1, k_2, \ldots, k_8$ 将4字节长的片段及4字节长的完整性校验值加密
  - 将其封装在MAC包中注入网络, 会获得合法认证

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

安全缺陷

保密缺陷

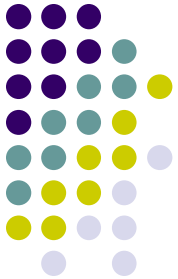
- 重复使用初始向量
  - 一个 24位初始向量 IV，有16,777,216个不同的子密钥序列
  - 依据生日悖论，在处理1.24 $\sqrt{2^{24}} = 5102$个网帧后，至少有一个随机产生的初始向量在之前出现过的概率会 > ½
- 弱密钥
  - 获得初始置换即可破译RC4密码
  - 一些破解 WEP密码的软件工具即是根据FMS攻击原理设计的

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

第六章 概要

- 6.1 无线通信和802.11 无线局域网标准
- 6.2 有线等价隐私协议
- 6.3 Wi-Fi 访问保护协议
- 6.4 IEEE 802.11i/WPA2
- 6.5 蓝牙安全机制
- 6.6 无线网状网的安全性

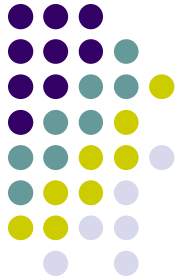
WPA 概论



- 由Wi-Fi 联盟于 2003提出
- 基于早期the IEEE 802.11i 标准（第三稿）而制定
- 三个主要目的:
  - 纠正所有已经发现的WEP中的安全弱点
  - 确保现有WEP硬件也同样能支持WPA
  - 确保WPA与802.11i标准兼容
- 采用 802.1X 协议认证用户设备
- Temporal Key Integrity Protocol (TKIP):
  - 用 *Michael*算法，一种特殊设计的完整性检查算法
  - 用一种新的密钥结构防止旧信重放并使之无法从RC4 密钥获取公有初始向量

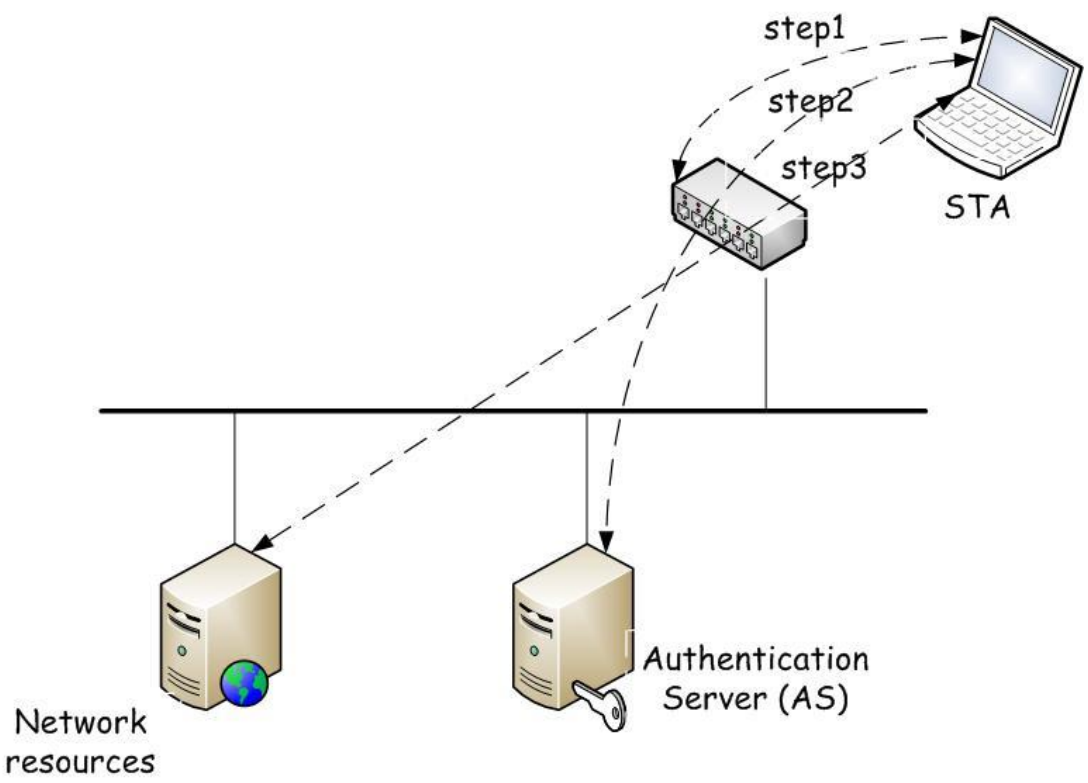
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

用户设备认证和存取控制



- 家庭小型办公组网 WPA:
  - 为家庭或小型办公室
  - 用WEP的预共享密钥
- 企业 WPA:
  - 安全公用的无线局域网
  - 用认证服务器 (AS)
  - 不同的用户与AS使用不同的预共享密钥
  - 预共享密钥以用户密码的形式出现
  - 采用802.1X端口网络访问控制协议认证用户设备STAs

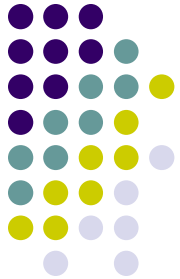
802.1X 概览



1. STA 向AP发连网请求. AP向STA询问认证信息
2. STA 用其与AS共享的密钥给身份签名，向AP发送其身份和签名， AS 核实STA签名告知AP，AP即可根据结果决定是否准许其登录
3. STA 被准予连网

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

TKIP 密钥产生



- AS首先产生一把不同的256位配对主密钥 (PMK)，为每个STA
  - AS 用AS和AP之间的预共享密钥加密后将PMK发送给AP
  - AP 用AP和STA之间的预共享密钥加密后发送PMK给STA
- 然后，基于PMK和其他信息，TKIP产生4把128位的临时配对密钥 (PTK)，用途如下:
  - 数据加密密钥:数据加密用
  - 数据MIC密钥:数据完整性校验
  - *EAPoL*密钥: 局域网扩充认证协议
  - EAPoL MIC密钥: EAPoL完整性校验

4 向握手

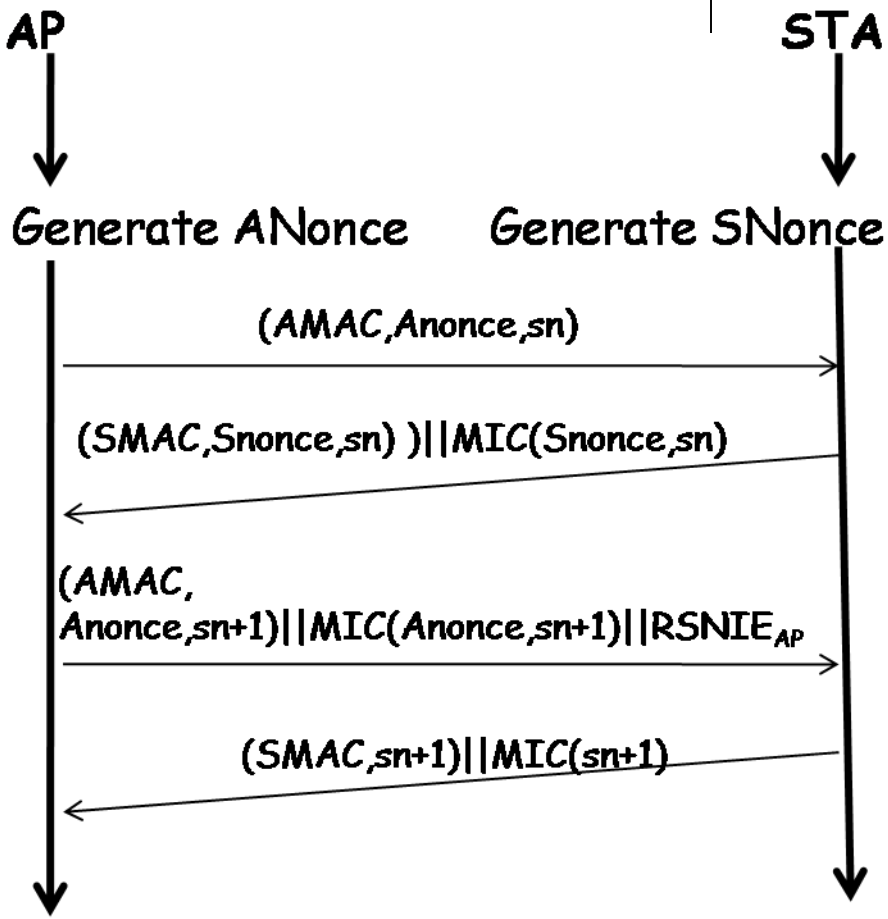
- TKIP用4次握手完成一次交换临时密钥对 (PTK).
  1. AP 发送 ANonce 给STA

     $Message_1$ = (AMAC, Anonce, sn)
  2. STA 发送 SNonce 给 AP

     $Message_2$ = (SMAC,Snonce,sn) || MIC(Snonce,sn) || $RSNIE_{STA}$
  3. AP 发送应答给STA.

     $Message_3$ = (AMAC, Anonce,sn+1) || MIC(Anonce,sn+1) || $RSNIE_{AP}$
  4. STA 发送应答给AP

     $Message_4$ = (SMAC,sn+1) || MIC(sn+1)



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

TKIP 信息完整性码

- 它用到Michael算法产生信息完整性代码(MIC)
- 用64位密钥生成一个 64位信息认证码
- K: 将64位密钥K等分成两部分 K_0 和 K_1
- Michael 算法用密钥K产生MIC:

$$(L_1,R_1) = (K_0,K_1),$$

$$(L_{i+1},R_{i+1}) = F(L_i \text{ XOR } M_i, R_i) \quad i = 1,2,\ldots,n$$

$$MIC = L_{n+1}R_{n+1}$$

其中*F*为Feistel 替换函数

- 如果 F(l,r) 定义如下:

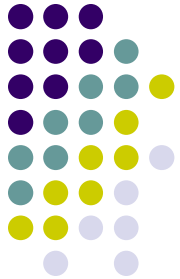
$$r_0 = r.$$
$$l_0 = l,$$
$$r_1 = r_0 \text{ xor } (l_0 <<< 17)$$
$$l_1 = l_0 \text{ xor}_{32} r_1,$$
$$r_2 = r_1 \text{ xor XSWAP}(l_1),$$
$$l_2 = l_1 \text{ xor}_{32} r_2,$$
$$r_3 = r_2 \text{ xor } (l_2 <<< 3),$$
$$l_3 = l_2 \text{ xor}_{32} r_3,$$
$$r_4 = r_3 \text{ xor } (l_2 >>> 2),$$
$$l_4 = l_3 \text{ xor}_{32} r_4,$$
$$F(l, r) = (l_4, r_4)$$

XSWAP(l) 将左边一半l和右边一半l互换

- 比CRC_{32}更安全

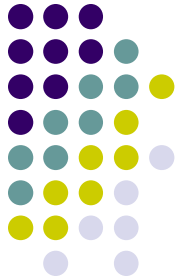
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

Michael 算法的弱点



- 攻击者产生一个消息并且附上一个64位二进制字符串作为 MIC，试图在不知道密钥的情况下找到正确的MIC
  - 尝试所有 2^{64}种可能去找到正确的MIC
  - 用微分密码分析学，只需要尝试攻击 2^{29}次
- 问题解决途径:
  - STA 删除密钥并且解除与AP的连接，如果在一秒钟内有两次失败的连接尝试（消息认证失败），并等待1分钟后再连接

TKIP 密钥混合



- 密钥混合算法为每一个帧产生一个该帧的密钥.
  - 用一个 48比特位的初始向量IV， 将其分割成3个16位的段 V_2, V_1, V_0
  - 密钥混合运算由两部分组成

$$pk_1 = mix_1\ (a^t,\ V_2\ V_1,\ k^t\ ),$$

$$pk_2 = mix_2\ (pk_1,\ V_0,\ k^t\ ),$$

a^t表示发送端设备的48位 MAC地址，k^t 是发送端设备的128位数据加密算法密钥，

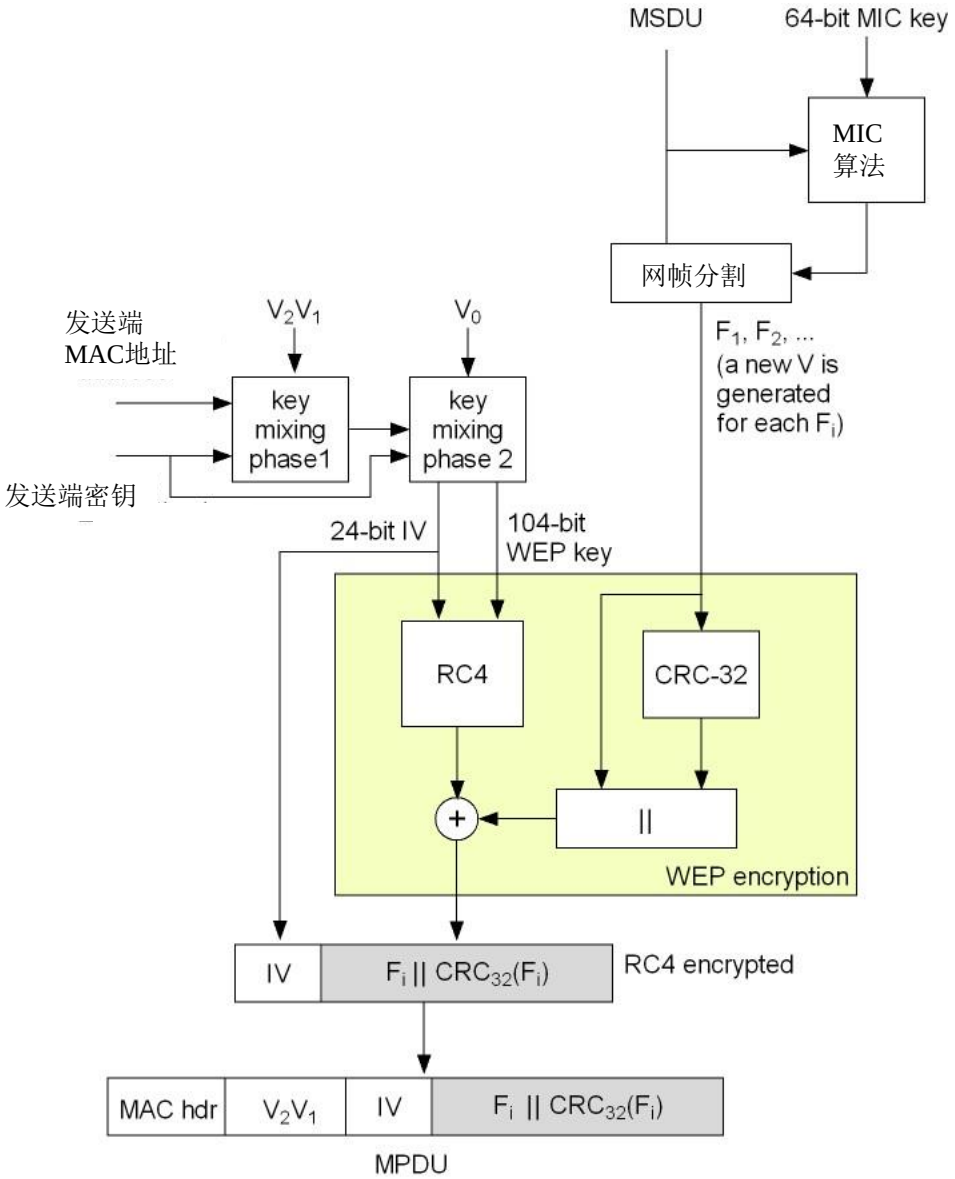
pk_2 is a 128-bit per-frame key for RC4

  - 用两个 S-匣子 S0 和S1 将一个16位二元字符串输入替换成另一个16位字符串作为输出

$$S(X) = S_1(X_1)\ S_0(X_0)\ ,$$

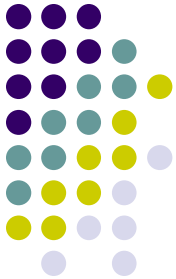
其中 $X = X_1X_0$

WPA加密

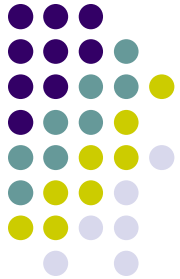


《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

WPA 安全强度和弱点



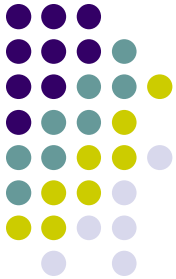
- 优越于 WEP
- 对DoS攻击显得脆弱:
  - WPA计算M 的MIC并将其放入MAC网帧载荷，然后将M || ICV(M)分割成若干块 $F_1, F_2, \ldots$
  - 对每一个F_i, WPA 产生48位初始向量 IV，并产生WEP 密钥
  - 初始向量IV以明文传输，攻击者可能截获一个MAC网帧，并将所包含的初始向量用一个更大值的初始向量取代
  - 由于接收方不能正确的将其解码，只能被清除
  - 由于此初始向量已被使用，导致后面以此值为初始向量的合法网帧也被清除



第6章无线网安全性

Part II

第6章 内容概要



- 6.1 无线通信和802.11 无线局域网标准
- 6.2 有线等价隐私协议
- 6.3 Wi-Fi 访问保护协议
- 6.4 IEEE 802.11i/WPA2
- 6.5 蓝牙安全机制
- 6.6 无线网状网的安全性

WPA 2 概览

- WPA:
  - 为了解决WEP安全问题而仓促设计的安全协议
- WPA2:
  - 基于802.11i (官方版本)
    - 加密并验证MSDUs: 使用AES-128加密算法及计数器模式
    - 认证STAs: 802.1X
  - 没有必要使用明文初始向量去产生子密钥序列
  - 但大多数现有的 Wi-Fi WPA 卡不能在更新后支持 802.11i 标准

密钥生成

- 与WPA一样有分级密钥体系
  - 256位的配对的主密钥 (PMK)
  - 4把128位的临时配对密钥 (PTKs)
  - 每个阶段为CCMP产生一个384位的临时密钥
    - 根据SMAC, SNonce, AMAC, Anonce，由伪随机数发生器产生出来
    - 基于四次握手协议交换信息
    - 密钥被分割为3个128位的临时密钥:
      - 两个用于 STA和AP建立连接
      - 另一个作为为会话密钥

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

CCMP 加密与MIC

- 加密:

$$Ctr = Ctr_0$$

$$C_i = \text{AES-128}_K\,(Ctr + 1) \oplus M_i$$

$$i = 1, 2, \ldots, k$$

- 身份认证与完整性检查:

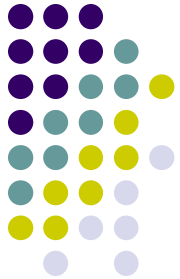
$$C_i = 0^{128}$$

$$C_i = \text{AES-128}_K\,(C_{i-1} \oplus M_i)$$

$$\text{i} = 1, 2, \ldots, k$$

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

802.11i 安全强度和弱点



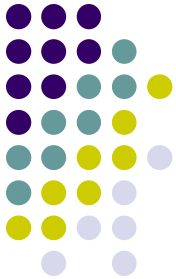
- 密码算法和安全机制均优越于 WPA 和 WEP
- 还是易于遭受DoS攻击:
  - 反转攻击
    - 为支持现有的WEP和WPA设备，802.11i允许RSN设备与没有RSN功能的设备进行通信
    - 攻击者可诱使RSN设备停止使用RSN功能
      - 攻击者冒充合法RSN AP身份宣传自己是一个WEP AP
      - 冒充合法的RSN STA向AP 请求WEP连接

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

802.11i 安全强度和弱点

- RSN IE 投毒攻击
  - 针对四次握手协议
  - 攻击者可能会发起RSN IE投毒攻击，使得STA 和AP的连接遭受中断连接攻击
- 脱网攻击
  - 利用伪造的MAC子层管理网帧将STA和 AP之间已建立的连接切断

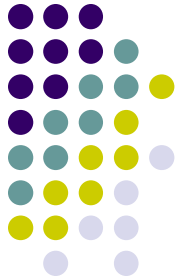
第6章 内容概要



- 6.1 无线通信和802.11 无线局域网标准
- 6.2 有线等价隐私协议
- 6.3 Wi-Fi 访问保护协议
- 6.4 IEEE 802.11i/WPA2
- 6.5 蓝牙安全机制
- 6.6 无线网状网的安全性

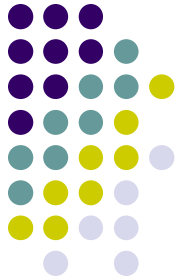
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

概要



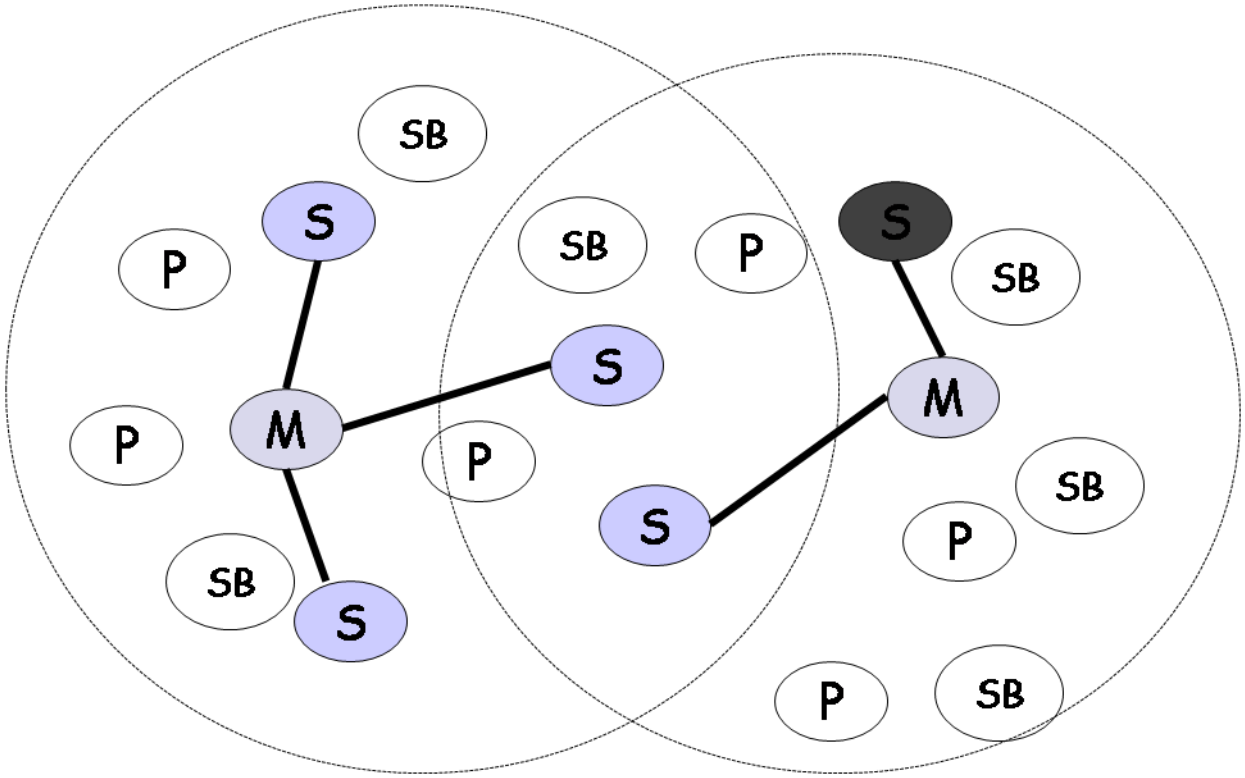
- 作为构造无线个人域网络标准，在 1998提出
- 小范围无线网通信技术，记为WPAN
- IEEE 802.15 标准基于蓝牙技术
- 无线设备支持:
  - 不同的通信设备在不同的操作平台上能够进行无线通信
  - 能耗低，计算量小，适合小型应用
  - 无线个人网络

蓝牙: *个人网*



- 自配置和自组织的动态无线网
- 允许新设备动态加入，网内设备动态离开
  - 支持8台设备使用同一频道通信
  - Pico网内设备都是对等的
  - 设备会动态选出一个设备作为主点
  - 其余设备称为仆点
  - 一个Pico网最多容纳255台设备
  - 节点状态:停泊，活跃，待命
  - 一个蓝牙设备在任何时刻只能加入一个pico网

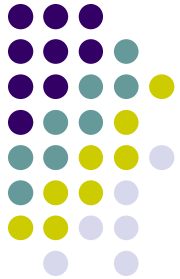
散布网示意图: 重叠的 Pico网



Scatternet (散射网)

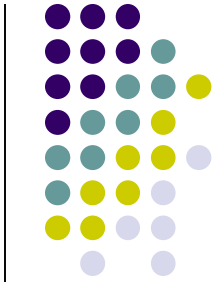
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

安全配对



- 在同一个pico网的节点分享相同的个人标识符PIN
- 节点产生并共享密钥，用于相互认证
  - 蓝牙设备基于用户的PIN码产生128位初始密钥
  - 蓝牙设备又产生一个128位链接密钥(也叫组合密钥)，用以认证设备并产生加密算法密钥
- 使用一个称为 E_0的序列加密算法为网包载荷加密
- 用一个 **SAFER+**分组加密算法 构造三个算法 E1, E21,和 E22去产生子钥和认证设备

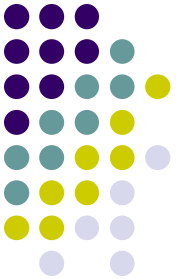
SAFER+分组加密算法



- 认证蓝牙设备
- 是之前 SAFER的增强版 (安全与快速加密程序)
- 是分组大小为128比特位的一种 Fiestel密码体系
- 两个主要成分:
  - 子密钥产生算法
  - 加密解密算法
    - 8轮相同运算(每轮运算两个子密钥)
    - 一个输出转换(一个子密钥)

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

SAFER+ 子密钥



- $K = k_0\ k_1\ \ldots k_{15}$, a 128位加密密钥.

  $k_{16} = k_0 \oplus k_1 \oplus \ldots \oplus k_{15}$
- 17 个128位的子密钥 $K_1, K_2, \ldots, K_{17}$:

$K_1 \leftarrow k_0 k_2 k_3 \ldots k_{15}$
for j = 0,1,…,16 do
  k_j <- LS_3 (k_j)
$K_2 \leftarrow k_1 k_2 k_3 \ldots k_{16}$ xor_8 B_2
for i = 3, 4, …, 17 do
  for j = 0,1,…,16 do
    $k_j \leftarrow LS_3$ (k_j)
  $K_i \leftarrow k_{i-1}\ k_i\ k_{i+1} \ldots k_{16}\ k_0\ k_1 \ldots k_{i-3}$ xor_8 B_{i-3}

B_i: 偏移向量

$B_i[j] = (45^{45^{17i+j+i} \bmod 257}) \bmod 257) \bmod 256$

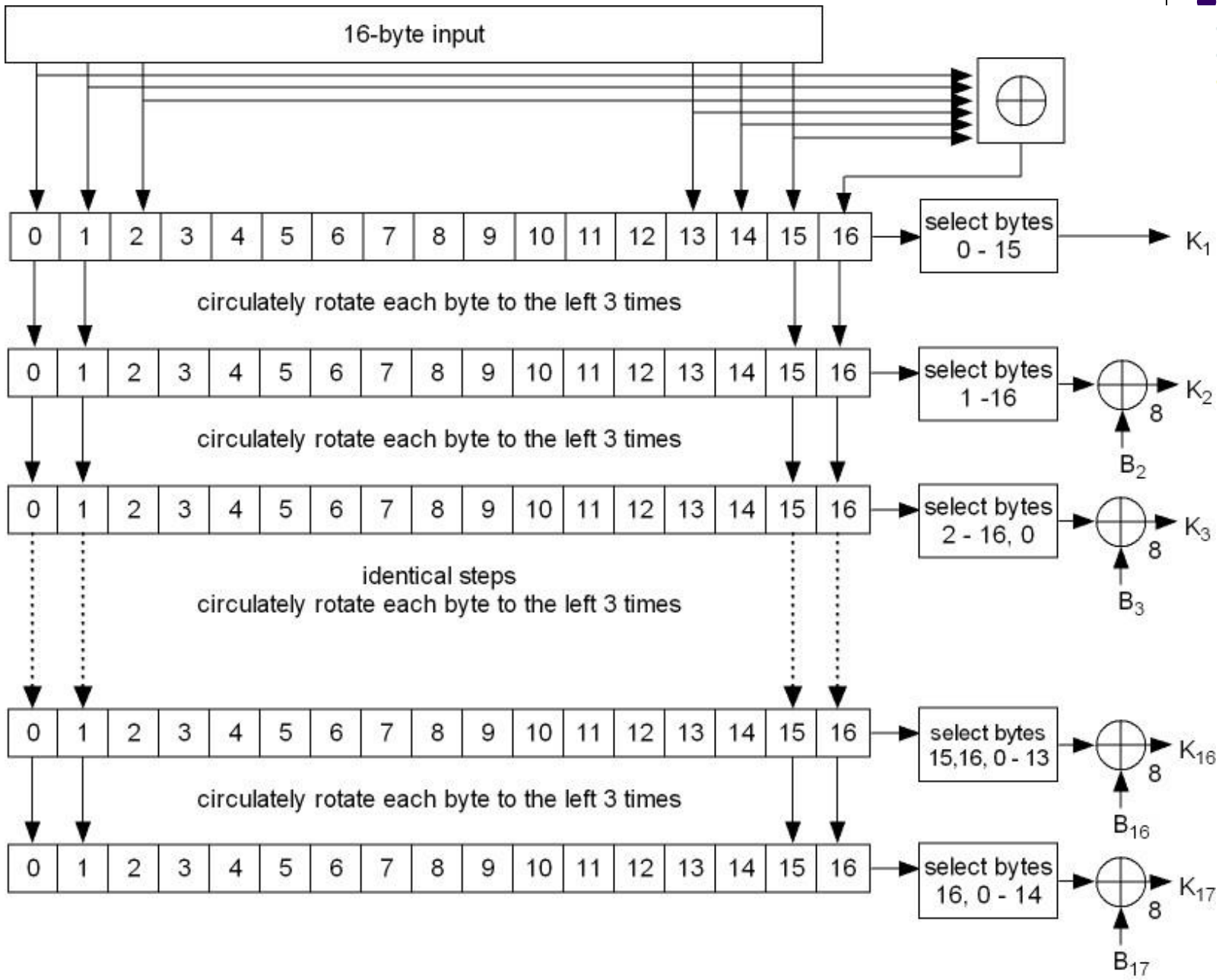
j = 0,1,….,15,

$B_i = B_i[0]\ B_i[1] \ldots B_i[15]$

i = 2,3,….17,

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

SAFER+ 子密钥产生序列图



SAFER+ 加密算法

加密算法轮运算

- 令 $X = x_1x_2\ldots x_{2k-1}x_{2k}$，$x_i$ 为字节
- *Pseudo Hadamard Transform* (PHT):

$$\mathrm{PHT}(X) = \mathrm{PHT}(x_1,x_2)\|\ldots\|\mathrm{PHT}(x_{2k-1}, x_{2k})$$

$$\mathrm{PHT}(x,y) = (2x+y) \bmod 2^8 \,\|\, (x+y) \bmod 2^8$$

- *Armenian Shuffles* (ArS):

$$\mathrm{ArS}(X) = x_8x_{11}x_{12}x_{15}x_2x_1x_6x_5x_{10}x_9x_{14}x_{13}x_0x_7x_4x_3$$

X 是16字节字符串

  - 替换算法使用两个S-匣子 e和 l:

$$e(x) = (45^x \bmod (2^8 + 1)) \bmod 2^8$$

l is e^{-1}: $l(y) = x$ if $e(x) = y$

  - $\oplus$ 和$\oplus_8$ 运算有两个子密钥
  - SAFER+加密的第 i 轮运算：

$$Z_0 = Y_i,$$

$$Z_1[2j-2] = e(Z_0[2j-2] \oplus K_{2i-1}[2j-2]),$$

$$Z_1[2j-1] = l(Z_0[2j-1] \oplus_8 K_{2i-1}[2j-1]),$$

$$Z_1[2j] = l(Z_0[2j] \oplus_8 K_{2i-1}[2j]),$$

$$Z_1[2j+1] = e(Z_0[2j+1] \oplus K_{2i-1}[2j+1]),$$

$$j = 1,3,5,7.$$

$$Z_2[2j-2] = l(Z_1[2j-2] \oplus_8 K_{2i}[2j-2]),$$

$$Z_2[2j-1] = e(Z_1[2j-1] \oplus K_{2i}[2j-1]),$$

$$Z_2[2j] = e(Z_1[2j] \oplus K_{2i}[2j]),$$

$$Z_2[2j+1] = l(Z_1[2j+1] \oplus_8 K_{2i}[2j+1]),$$

$$j = 1,3,5,7.$$

$$Y_{i+1} = PHT\left(ArS\left(PHT\left(ArS\left(PHT\left(ArS(PHT(Z_2))\right)\right)\right)\right)\right).$$

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

- 输出转换：
  - 经过8轮运算后，输出转换运算就像用密钥K_{2i-1}作用于Y_i一样，但不用到S- 匣子。即用密钥K_{17}应用于Y_9，通过以下运算（输出转换运算）得到密文C

$$C[2j-2] = Y_9[2j-2] \oplus K_{17}[2j-2],$$

$$C[2j-1] = Y_9[2j-1] \oplus_8 K_{17}[2j-1],$$

$$C[2j] = Y_9[2j] \oplus_8 K_{17}[2j],$$

$$C[2j+1] = Y_9[2j+1] \oplus K_{17}[2j+1],$$

$$j = 1,3,5,7.$$

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

蓝牙算法 E_1

- E_1 将以下参数作为输入：
  - K: 128-位密钥
  - ρ: 128-位 随机字符串
  - α: 48-位地址

  产生128-位字符串:

$$E_1(K, \rho, \alpha) = A'_r(\tilde{K}, [A_r(K, \rho) \oplus \rho] \oplus_8 E(\alpha))$$

- A_r 是初始 SAFER+加密算法
- A'_r 是修改后的SAFER+加密算法,它将第一轮的输入和第三轮的输入做运算，得到不可逆的算法
- 由密钥K，通过$\oplus$ 和$\oplus_8$ 运算产生 $\tilde{K}$ （书P210）
- $E(\alpha) = \alpha \,||\, \alpha \,||\, \alpha[0{:}3]$

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

蓝牙算法 E21

- E_{21} 将 ρ 和 α 作为输入:

$$E_{21}(\rho, \alpha) = A'_r(\rho', E(\alpha))$$

$$\rho' = \rho[0:14] \| (\rho[15] \oplus 00000110)$$

蓝牙算法E22

E_{22} takes a 16-byte random string ρ, a 6-byte address α, and an ℓ-byte PIN code p as input, where $1 \leq \ell \leq 16$. Let

$$\text{PIN}' = \begin{cases} \text{PIN} \parallel \alpha[0] \parallel \cdots \parallel \alpha[\min\{5, 15-\ell\}], & \text{if } \ell < 16, \\ \text{PIN}, & \text{if } \ell = 16. \end{cases}$$

Let $\ell' = \min\{16, \ell + 6\}$. Let

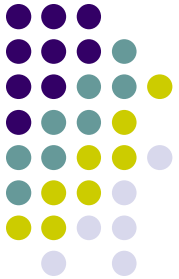
$$\begin{aligned} \kappa &= \begin{cases} \text{PIN}' \parallel \text{PIN}' \parallel \text{PIN}'[0:1], & \text{if } \ell' = 7, \\ \text{PIN}' \parallel \text{PIN}'[0:15-\ell'], & \text{if } 8 \leq \ell' < 16, \\ \rho, & \text{if } \ell' = 16, \end{cases} \\ \rho' &= \rho[0:14] \parallel (\rho[15] \oplus b(\ell')), \end{aligned}$$

where $b(\ell')$ denotes the 8-bit presentation of ℓ'. Then

$$E_{22}(\text{PIN}, \rho, \alpha) = A'_r(\kappa, \rho').$$

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

蓝牙认证



- 初始密钥:

$$K_{init} = E_{22}\,(\mathrm{PIN}, \mathrm{In\_RAND_A}, \mathrm{BD\_ADDR_B})$$

- D_A 和 D_B 产生链接密钥:

D_A sends $(\mathrm{LK\_RAND_A} \oplus K_{init})$ to D_B

D_B sends $(\mathrm{LK\_RAND_B} \oplus K_{init})$ to D_A

$$K_{AB} = E_{21}(\mathrm{LK\_RAND_A}, \mathrm{BD\_ADDR_A}) \oplus E_{21}(\mathrm{LK\_RAND_B}, \mathrm{BD\_ADDR_B})$$

- D_A 认证D_B:

D_A sends $\mathrm{AU\_RAND_A}$ to D_B

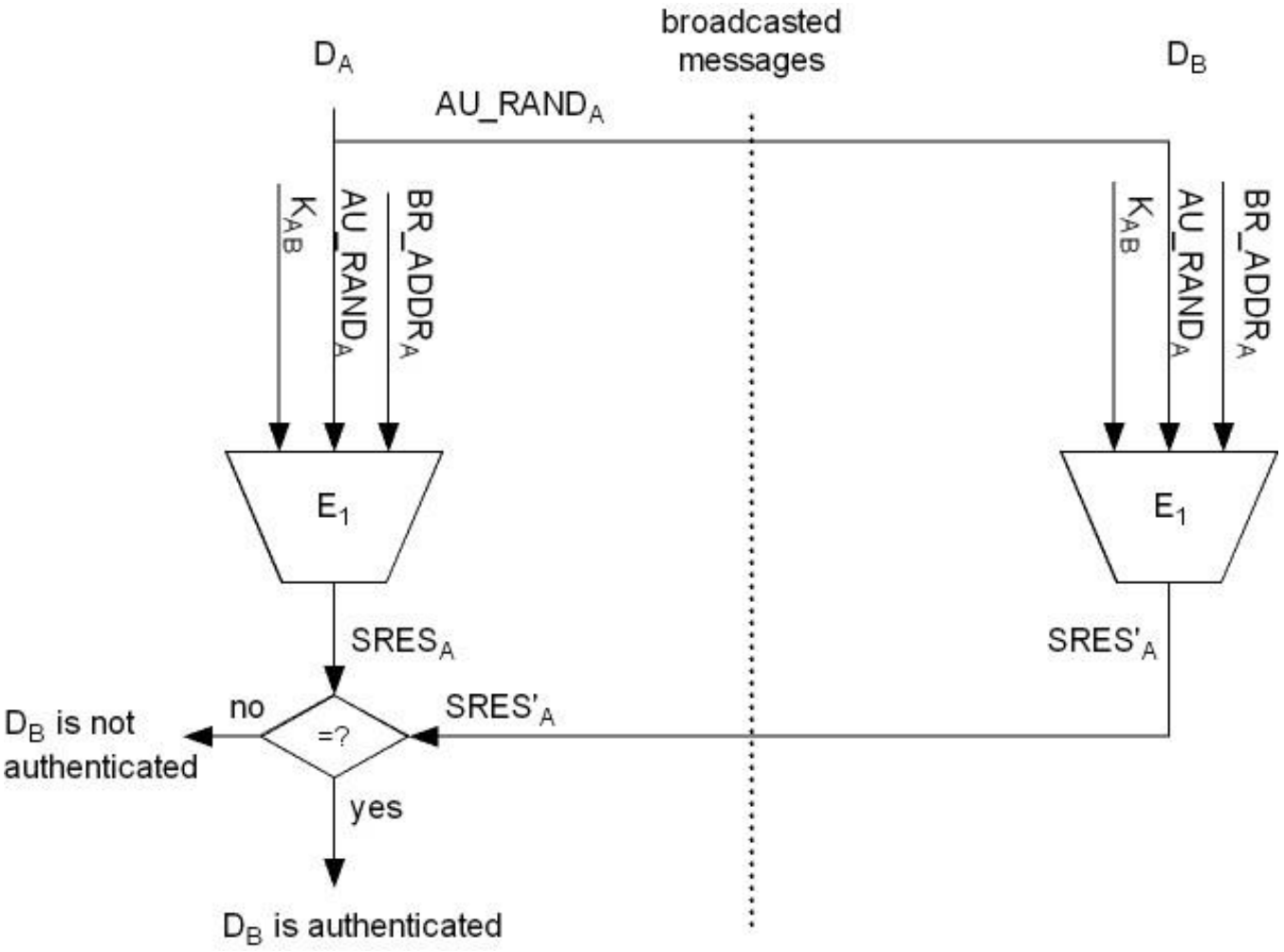
D_B sends $\mathrm{SRES_A}$ to D_A where

$$\mathrm{SRES_A} = E(K_{AB}, \mathrm{AU\_RAND_A}, \mathrm{BD\_ADDR_B})\ [0{:}3]$$

D_A verifies $\mathrm{SRES_A}$

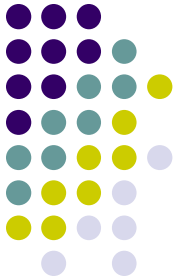
《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

蓝牙设备认证示意图



《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

PIN 码破译攻击



- 攻击者窃听设备D_A 和D_B之间所有的配对和认证通信

message	*source*	*destination*	*data*	*length*	*notes*
1	D_A	D_B	IN_RAND_A	128 bits	plaintext
2	D_A	D_B	$\text{LK\_RAND}_A \oplus K_{init}$	128 bits	
3	D_B	D_A	$\text{LK\_RAND}_B \oplus K_{init}$	128 bits	
4	D_A	D_B	AU_RAND_A	128 bits	plaintext
5	D_B	D_A	SRES_A	32 bits	plaintext
6	D_B	D_A	AU_RAND_B	128 bits	plaintext
7	D_A	D_B	SRES_B	32 bits	plaintext

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年

PIN 码破译攻击

攻击者采用蛮力攻击方法破译PIN码:

- 穷举所有2^{48} 种可能的PIN码
- 获取第一条信息中的IN_RAND_A 及设备D_B的地址 BD_ADDR_B， 计算初始密钥的候选者:

$$K'_{init} = E_{22}(PIN', In\_RAND_A, BD\_ADDR_B)$$

- 用得到的K'_{init} 分别与第二条和第三条信息做异或运算，得到 $LK\_RAND'_A$ 和$LK_RAND'_B$. 然后计算

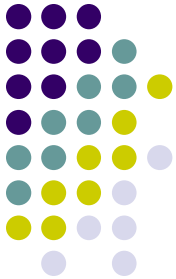
$$K'_{AB} = E_{21}(LK\_RAND'_A, BD\_ADDR_A) \oplus E_{21}(LK\_RAND'_B, BD\_ADDR_B)$$

- 用第四条信息的AU_RAND_A, K'_{AB}, 和BD_ADDR_B 计算

$$SRES'_A = E_1(AU\_RAND_A, K'_{AB}, BD\_ADDR_B)\ [0:3]$$

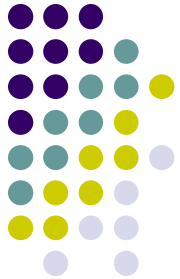
- 验证是否有 $SRES'_A = SRES_A$ （ $SRES_A$ 来自第五条信息）
- 然后用第六条和第七条信息对此PIN码进行确认

蓝牙安全简单配对协议



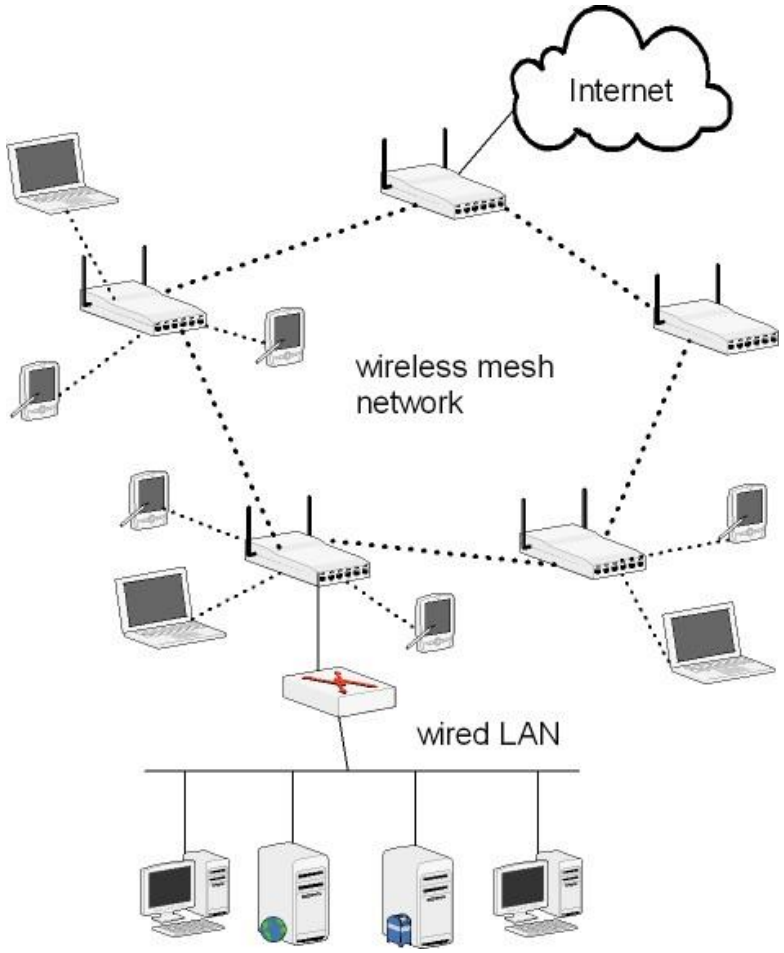
- 为了提高安全性能的新的配对协议
- 安全简单配对协议 (SSP) :
  - 用椭圆曲线Diffie-Hellman (ECDH) 交换算法取代PIN码
    - 抵御 PIN码破译攻击
  - 理想情况，用公钥证书认证公钥拥有者的身份.
    - 防范中间人攻击.
    - 蓝牙通信范围小，在Pico网内实施中间人攻击相对困难。

第六章 内容概要



- 6.1 无线通信和802.11 无线局域网标准
- 6.2 有线等价隐私协议
- 6.3 Wi-Fi 访问保护协议
- 6.4 IEEE 802.11i/WPA2
- 6.5 蓝牙安全机制
- 6.6 无线网状网的安全性

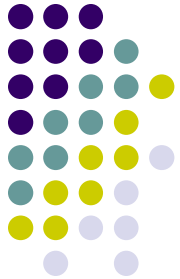
无线网状网(WMN)



- 无线网状网中的AP 可与有线网相连
- 每一个 STA 均与一个 AP相连
- WMNs、 WLANs比较:
  - WLANs: 星型网
  - WMNs: 多跳网络
- 区(region):
  - 一个AP 和所有与其相连的STAs
  - 可视为一个 WLAN
  - 可使用802.11i/WPA2 标准
- AP间也可用802.11i/WPA2保证通信安全

《计算机网络安全的理论与实践（第2版）》. 【美】王杰，高等教育出版社，2011年

WMNs安全漏洞



- 黑洞攻击
  - 假冒合法路由器，清除而不是中转网包
  - 引诱合法用户使用他的路由器
- 虫道攻击
  - 将网包改道传输
- 抢占攻击
  - 根据按需路由协议:
    - 每个路由器必须将第一次收到的路由请求包传播出去，但对之后收到的来自同一设备的路由请求不予理睬，以减少拥堵
  - 抢在合理路由请求包发送之前，发出伪造路由请求，破坏通信
- 路径错误注入攻击
  - 向网络中注入伪造的路径错误包，从而切断通信路径

《计算机网络安全的理论与实践（第2版）》.【美】王杰，高等教育出版社，2011年