哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

本讲主题

无线局域网的安全

WEP的设计目标

- WEP(Wired Equivalent Privacy): 有线等效保密
- 对称密钥加密
  - 机密性
  - 主机认证
  - 数据完整性

- 自同步: 每个分组单独加密
  - 给定加密分组和密钥，便可以解密；即便前序分组丢失，也可以继续成功解密分组(与CBC不同)
- 高效
  - 可以由硬件或软件实现

回顾：对称流密码

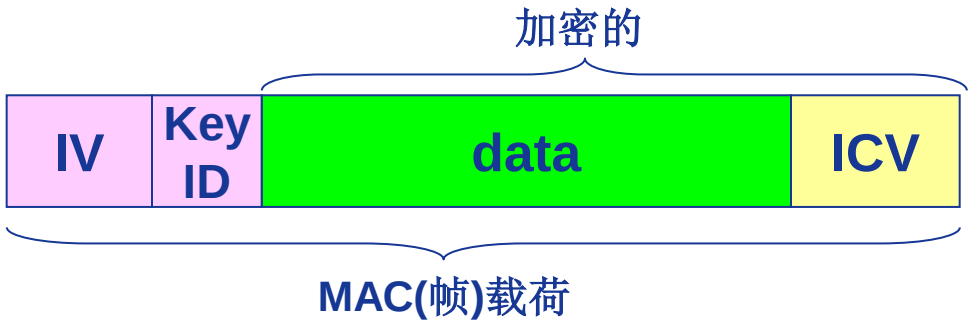
- 将密钥流的每个字节与明文的每个字节进行异或，得到密文：
  - m(i) = 第i个消息单元
  - $k_s(i)$ = 第i个密钥流单元
  - c(i) = 第i个密文单元
  - $c(i) = k_s(i) \oplus m(i)$ ($\oplus$ =异或)
  - $m(i) = k_s(i) \oplus c(i)$
- WEP使用RC4算法

流密码与分组独立性

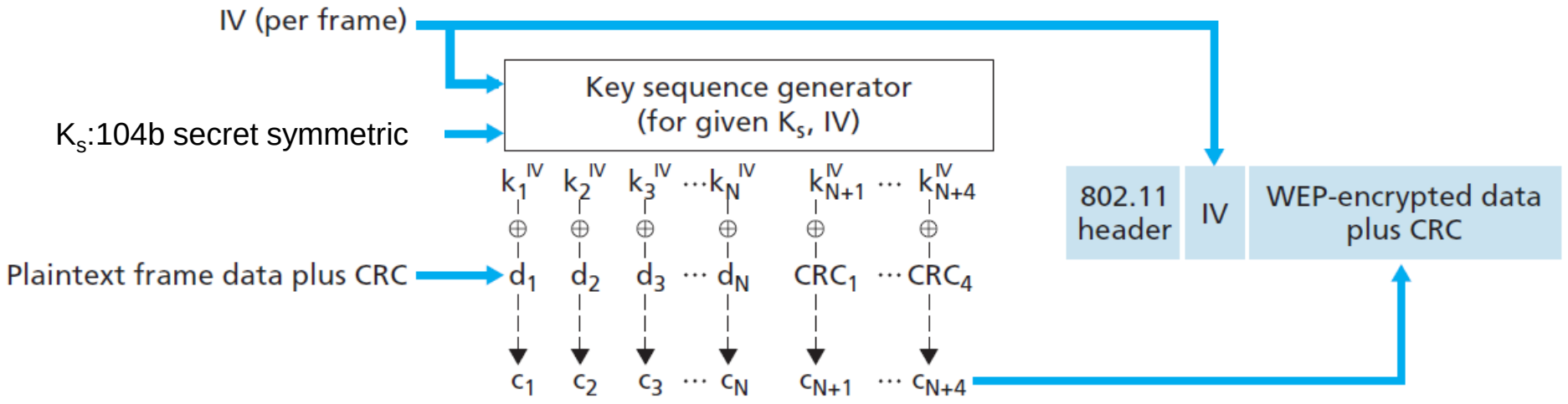
- 回顾WEP设计目标: 每个分组独立加密
- 如果对于n+1号帧使用的密钥流，是在n号帧的密钥流之后，那么每个帧就不是独立加密的
  - 需要知道n号帧使用的密钥流截止到哪里
- WEP的解决方案：初始密钥+针对每个分组的新IV（初始向量），产生针对每个分组的密钥流

WEP加密（1）

- 发送端针对数据(data)计算完整性校验值ICV(Integrity Check Value)
  - 4字节的散列值/CRC，用于数据完整性校验
- 每端有104位的共享密钥
- 发送端生成24位初始向量(IV)，附加到密钥上：得到128位密钥
- 发送端还要附加keyID (8位字段)
- 将128位密钥输入到伪随机数发生器，产生密钥流
- 利用RC4算法对帧中“数据+ICV”进行加密：
  - 将密钥流与“数据+ICV”逐个字节异或(XOR)
  - 将IV和keyID附加到加密数据，构成载荷
  - 将载荷插入到802.11帧中

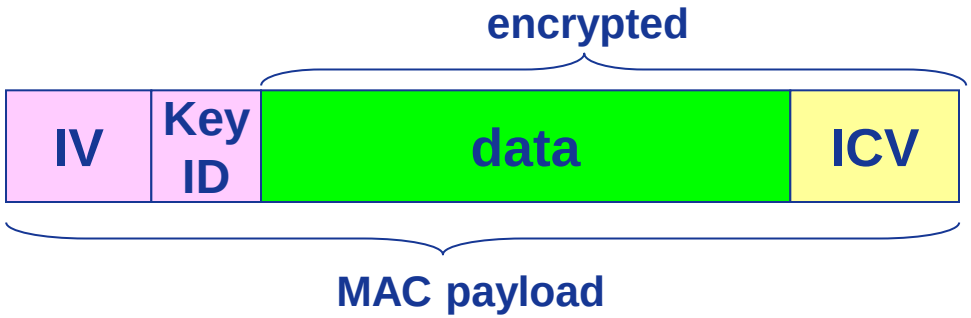


WEP加密(2)



每帧一个新IV

WEP解密概述

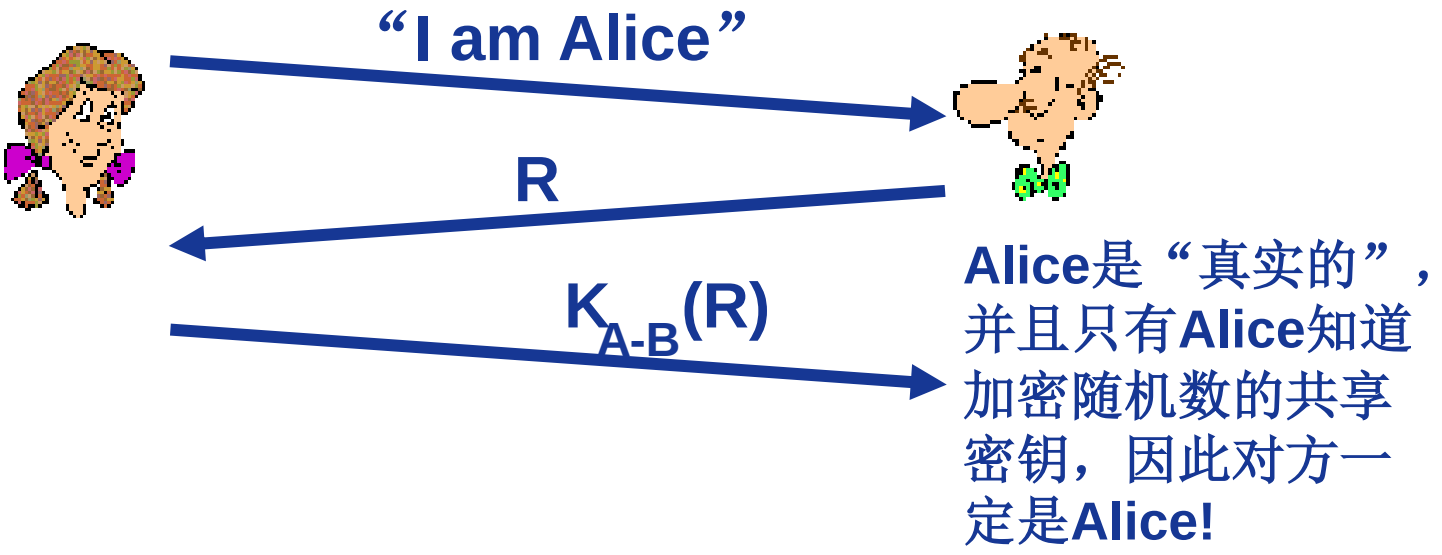


- 接收端提取IV
- 将IV和共享密钥输入伪随机数发生器，得到密钥流
- 将密钥流与加密部分逐个字节异或(XOR)，解密得到数据与ICV
- 利用ICV校验数据完整性
  - 注意: 这里采用的消息完整性验证方法与报文认证码MAC以及数字签名(利用PKI)不同.

利用一次性随机数进行端点认证

一次性随机数(nonce): 一个生命期内只用一次的数R

如何证明Alice是“真实的”： Bob向Alice发送一次性随机数nonceR， Alice必须利用共享密钥加密并返回R。



WEP的身份认证

认证请求

一次数R (128 bytes)

利用共享密钥加密的一次数R

如果解密值与一次数相等，则认证成功

注意:

- 并非所有AP都进行认证，即便使用了WEP
- AP会在信标帧(beacon frame)中指示是否需要认证
- 认证需要在关联前进行

破解802.11WEP加密

安全漏洞:

- 每帧一个24位的IV→IV最终会被重用
- IV以明文传输→重用IV容易被监测

攻击:

- Trudy诱使Alice加密已知明文：$d_1\ d_2\ d_3\ d_4\ \ldots$
- Trudy知道: $c_i = d_i\ \mathrm{XOR}\ k_i^{IV}$
- Trudy已知c_i和d_i，因此可以计算得到k_i^{IV}
- Trudy得到加密密钥序列：$k_1^{IV}\ k_2^{IV}\ k_3^{IV}\ \ldots$
- 下一次IV被重用时，Trudy便可以成功解密！

802.11i: 改进的安全

- 多种（更强的）可选的加密方法
- 提供密钥分发
- 利用独立于AP的认证服务器
- IEEE 802.11i 服务：
  - 认证
  - 访问控制
  - 数据与完整性加密

802.11i: 运行的4个阶段

STA:
客户站点

AP: 访问点

AS:
认证服务器

1 安全能力的发现

2 STA和AS相互认证，共同生成主密钥 (MK).
AP作为“穿越通道”

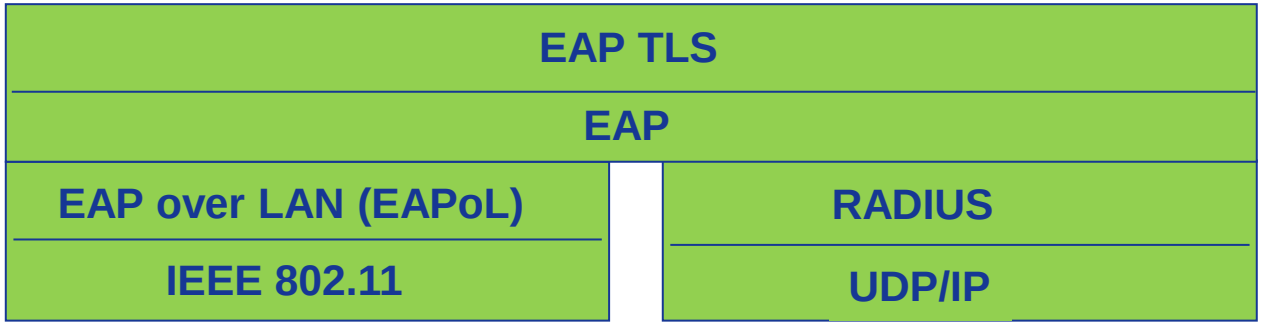
3 STA导出成对主密钥 (PMK)

3 AS导出相同的PMK，
并发送给AP

4 STA、AP使用PMK导出用于
报文加密与完整性的临时密钥(TK)

EAP: 扩展认证协议

- EAP：客户(移动端)与认证服务器间的端-端协议
- EAP运行在两段独立的“链路”上
  - 移动端到AP(EAPoL: EAP over LAN)
  - AP到认证服务器(RADIUS over UDP)



哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！