(2020春季　课程编号：011184)

信息安全导论

第11章 无线网络安全

中国科学技术大学 曾凡平

billzeng@ustc.edu.cn

课程回顾：第10章 Internet安全

10.1 OSI安全体系结构

- 安全攻击，安全服务，安全机制

10.2 IPSec协议

- IPSec体系结构，IPSec工作模式，AH协议

10.3 SSL/TLS协议

- SSL体系结构，SSL记录协议，SSL修改密码规范协议，
- SSL报警协议，SSL握手协议，TLS协议

10.4 安全电子交易

- SET的需求，SET系统构成，双向签名，支付处理

第11章 无线网络安全

- 11.1 IEEE 802.11无线网络安全
  - IEEE 802.11无线网络背景
  - WEP
  - 802.11i
- 11.2 移动通信系统的安全
  - GSM的安全
  - GPRS的安全
  - 第三代移动通信系统(3G)的安全

11.1.1 IEEE 802.11无线网络背景

- **IEEE 802**是一个开发**局域网(LAN)标准**的委员会，**802.11**则是成立于1990年的工作组，负责开发**无线局域网(WLAN)**的协议与传输规范。

- 目前802.11有多种扩展名，一般以后缀字母区分。
- 其中IEEE 802.11是原始标准，规定了无线局域网的**物理层和MAC层**的内容；802.11a、802.11b、802.11g、802.11n、802.11ac等是物理层的相关扩展标准；其余几个重要标准的内容如表11-1所示。

IEEE 802.11系列部分标准

表11-1

标准名称	主要内容
802.11d	在媒体接入控制/链路连接控制 (MAC/LLC) 层面上进行扩展，对应 802.11b 标准，解决不能使用 2.4GHz 频段国家的使用问题
802.11e	在 802.11MAC 层增加 QoS 能力，用时分多址 (TDMA) 方案取代类似以太网的 MAC 层，并对重要的业务增加额外的纠错功能
802.11f	改进 802.11 的切换机制，以使用户能够在两个不同的交换分区 (无线信道) 之间，或在两个不同的网络接入点之间漫游的同时保持连接
802.11h	对 802.11a 的传输功率和无线信道选择增加更好的控制功能，与 802.11e 相结合，适用于欧洲地区
802.11i	消除 802.11 的最明显的缺陷: 安全问题
802.11p	针对汽车通信的特殊环境而制定的标准
802.11v	无线网络管理，面向运营商，致力于增强由 802.11 网络提供的服务

- (1)在无线局域网中，**需要认证技术，以验证节点的身份**。而在有线局域网中，“与网络相连”这个可见行为起了某种程度的认证作用。
- (2)**无线局域网需要隐私保护机制**。而在有线局域网中，“信息的接收节点必须与网络相连”提供了一定程度的隐私性。
- 与有线局域网相比，无线局域网对安全服务和机制有更高的要求。

IEEE 802.11定义的安全机制：数据保密和完整性、身份认证

- 1999年发布的802.11b标准里定义了**WEP(Wired Equivalent Privacy)协议**，为数据提供机密性和完整性保护，并基于WEP协议设计了共享密钥认证机制。
- WEP协议旨在提供和有线局域网同级的安全性，但此后的大量工作证明，WEP存在较大的安全缺陷。因此，IEEE于2001年成立了802.11i任务组，以制定新的安全标准，来增强无线局域网的安全性。但在802.11i完善之前，市场对于WLAN的安全要求十分急迫，为使安全问题不至于成为制约WLAN市场发展的瓶颈，国际Wi-Fi联盟组织(Wi-Fi Alliance)提出了**WPA(Wi-Fi Protected Access)标准**，作为802.11i完备之前替代WEP的过渡方案。WPA以IEEE 802.11i第三版草案为基准，并与之保持前向兼容。
- 2004年6月，完整的802.11i标准通过，Wi-Fi联盟也随即公布了与之相对应的**WPA第二版(WPA 2)**。

11.1.2 WEP

- **有线等效隐私**(wired equivalent privacy，WEP)以为无线局域网提供与有线局域网相同级别的安全保护为目的，广泛应用于保护无线局域网中的数据链路层的数据安全。WEP包含以下三个要素：共享密钥K、初始向量(initialization vector，***IV***)和RC4流密码算法。

1.WEP数据加密及解密

- WEP采用对称加密算法RC4。RC4算法是一种**对称流密码体制**，可以采用64比特或者128比特两种长度的密钥。IEEE 802.11b规定，WEP使用64比特的加密密钥。这64比特长的加密密钥由两部分组成：40比特的WEP用户密钥K和24比特的初始矢量***IV***。

WEP的加密过程

- **(1)数据校验阶段**。对消息M计算完整性校验值(integrity check value，ICV)，使用的算法是CRC32：ICV=CRC32(M)。将ICV与M串接，得到明文P=ICV || M。
- **(2)密钥生成阶段**。选取一个24比特的初始化向量***IV***，将初始化向量***IV***和40比特的用户密钥K串接起来。以***IV*** || K作为伪随机数发生器的种子，应用RC4算法，生成密钥序列(key sequence，KS)，即KS=RC4(***IV*** || K)，这是一个与P等长的伪随机序列。
- **(3)数据加密阶段**。将KS与P作异或运算即可产生密文C=KS ⊕ P。发送时将密文C和初始向量***IV*** 一起传输，即传输***IV*** || C。

WEP数据加密流程

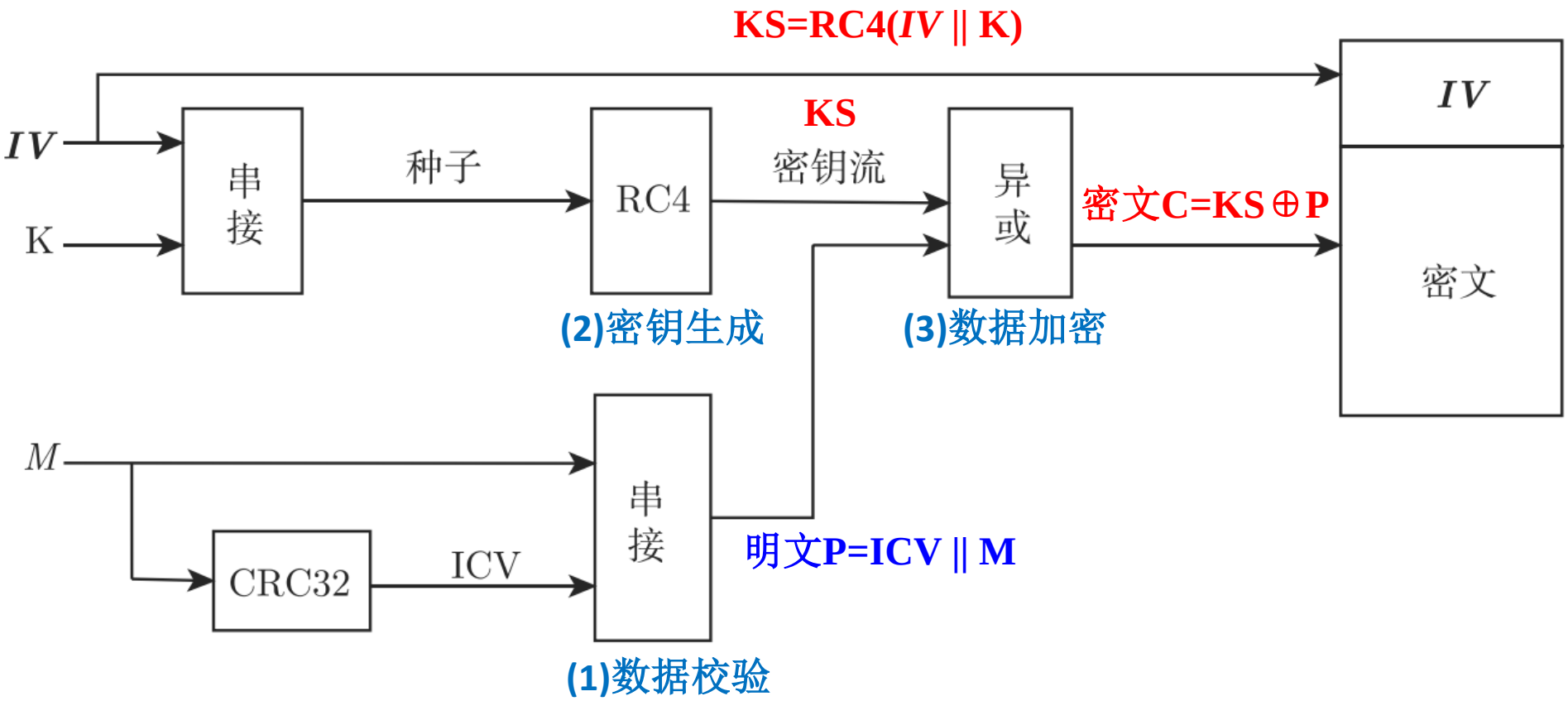


图11-1 WEP数据加密流程

WEP的数据解密过程

(1)提取***IV***和密文C；

(2)将***IV***和密钥K一起送入，采用RC4算法的伪随机数发生器得到解密密钥流；

(3)将解密密钥流与密文相异或，得到明文消息M以及完整性校验值ICV；

(4)对得到的明文进行处理，采用相同的算法计算完整性校验值ICV；

(5)比较两个完整性校验值结果，如果相等则说明协议数据正确。

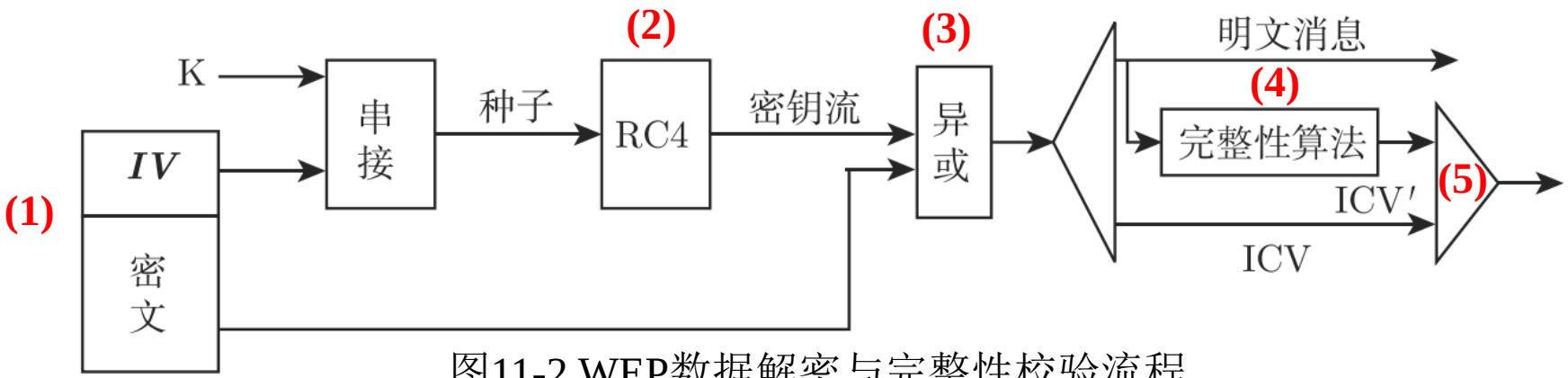


图11-2 WEP数据解密与完整性校验流程

WEP的MPDU
(MAC protocol data unit，MAC协议数据单元)结构

- IEEE 802.11b标准规定无线工作站和接入点可以共享的WEP加密密钥是有限制的，最多为4个。
- 在实际应用中，WEP帧中的Key ID决定具体使用哪个WEP用户密钥。
- WEP的MPDU(MAC protocol data unit，MAC协议数据单元)结构如图11-3所示。

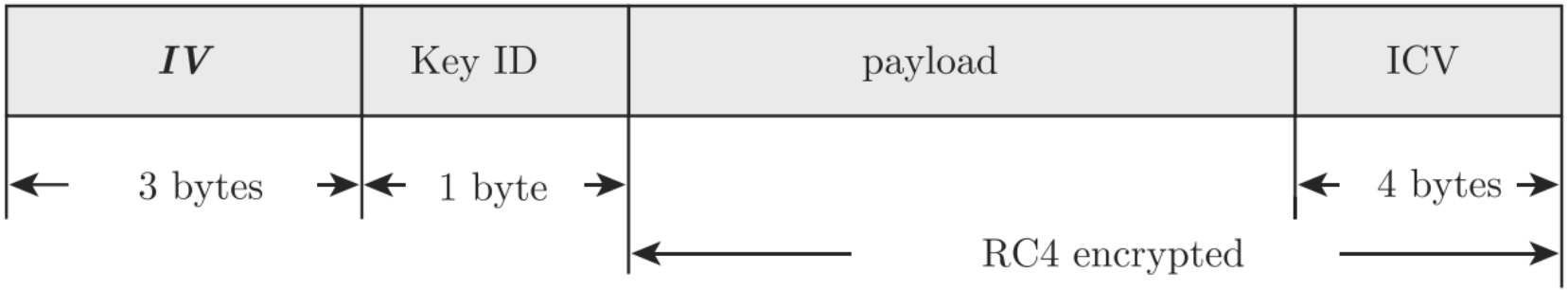


图11-3 WEP MPDU结构

2.WEP认证- 1)开放系统认证

- 开放系统认证是IEEE 802.11的缺省认证方式。这种认证经常被称为“零认证”，因为这种认证方式本质上就是一种空认证机制，认证过程没有采用密码技术，甚至一个空的SSID就可以获得认证。因此，任何符合无线网络MAC地址过滤规定的终端都可以访问这个无线局域网，因而无线局域网的安全性较差。
- 当无需对身份进行认证的时候，一般就采用开放系统认证。整个认证过程以明文方式进行，只有两步：认证请求和认证响应。无线站点发送一个包含自身ID的认证请求，其中未包含涉及认证的任何与客户端相关的信息。若无线接入点的认证算法标识也为开放系统认证，则它返回一个包含认证成功或认证失败的认证响应。当无线站点收到包含认证成功的响应信息后，就表明通信双方相互认证成功。

2.WEP认证- 2)共享密钥认证

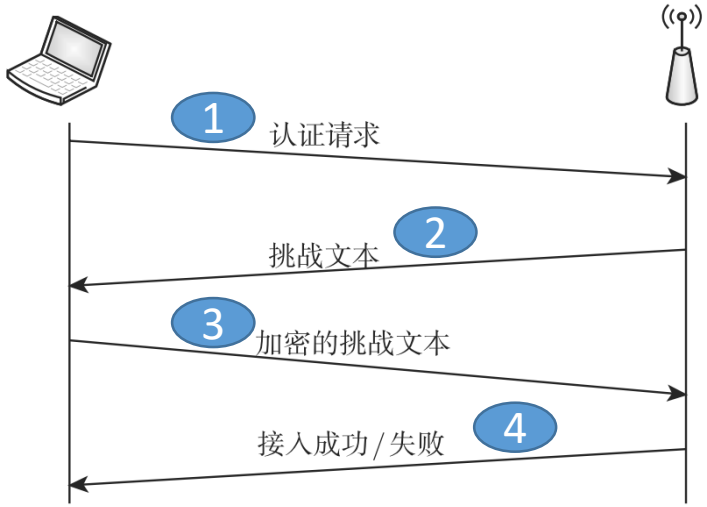


图11-4 共享密钥认证

- 它采用挑战/响应方式，是基于共享密钥的身份认证机制
- 整个认证过程包括如下几个步骤：

(1)无线工作站点搜寻无线接入点，同时向无线接入点发送申请认证的数据帧。

(2)当无线接入点收到认证请求后，会向无线工作站点发送一个认证管理帧作为响应，其中包含一个挑战文本。这个挑战文本由WEP的伪随机数生成器利用某个共享密钥和初始矢量***IV***生成。

(3)当无线工作站点收到接入点发来的挑战文本时，会用相应的共享密钥对挑战文本进行加密，然后将加密之后所得到的密文发回给接入点。

(4)接入点用相同的密钥对接收到的密文进行解密，并将解密结果与之前发送的挑战文本相比较。若二者相同，则接入点向无线工作站点发送一个包含“成功”信息的认证结果；若二者不同，接入点则向无线工作站点发送一个包含“失败”信息的认证结果。

3.WEP密钥

- IEEE 802.11b以手工的方法将密钥输入到每个设备中。
- 现实当中，很多机构在设置了一个初始的WEP共享密钥后就永远不会变了，因为WEP密钥是被无线网络中所有的接入点和用户所共享的。同时因为多数无线网络在设计上允许漫游，所以单一无线网络连接的所有设备必须要拥有同一个WEP密钥，如果有越来越多的设备共享同一密钥，就必然会增加密钥丢失的可能性。这也会增加加密方案被破解的可能。
- IEEE 802.11b允许最多4个密钥存储在每个设备上，每个WEP信息在传送时必须包括密钥编号(key ID)，只有发送设备和接收设备都采用相同的共享密钥，信息才能被正确地传送和解码。可存储多个密钥及利用密钥表编号去指定使用哪一个密钥的功能会带来多种多样的密钥轮换方案，经常改变密钥可提高WEP的安全性，但在4组预先设置的密钥之间不停轮换只提供有限度的改善，更新加密密钥内容会更理想，但这个过程不可避免需要手工执行，因此更新频率受限。

4.WEP的缺陷

1)静态共享密钥和*IV*重用

- WEP没有密钥管理的方法，使用静态共享密钥，通过***IV*** / shared key来生成动态密钥。静态密钥的安全强度是比较低的。
- WEP协议的加密过程可以表示为：
  - **C=P⊕RC4(*IV*，K)**，其中C表示密文，P表示明文，***IV***是初始化向量，K是共享密钥。RC4是一种流密码算法，流密码算法也具有缺陷，比如不能用相同的密码加密多个不同的信息。
  - 如果所有的报文都用相同的***IV***和密钥加密，那么将两个加密报文进行异或运算就能去掉密钥流，得到原始明文的异或形式。

4.WEP的缺陷- 1)静态共享密钥和IV重用

- 例如，假设两组明文p1和p2，用相同的***IV***和密钥加密，对应的密文为c1和c2，则有c1⊕c2=(p1⊕RC4(***IV***，K))⊕(p2⊕RC4(***IV***，K))=p1⊕p2。因此，如果数据在传输途中被截获并对密文进行异或运算，就可以得到原始明文的异或形式。进一步，如果其中的一组明文的内容已知，则很容易就可以得到另一组明文。所以，***IV***的重用会带来机密性的破坏。

- 在WEP中，***IV***的取值空间为[0，2^{24} -1]。当加密的数据包个数超过2^{24}时，***IV***必然发生重复，如果此时没有更换密钥的话，便会出现若干个数据包用来加密的种子密钥发生重复，从而很容易被破解。按照IEEE 802.11b中WLAN的最高传输速率11Mb/s来计算，传输1800字节大小的数据包，6小时后一定会出现重复。

4.WEP的缺陷- 2) CRC-32的漏洞

- 为了保障数据传输的完整性，WEP协议计算32位的循环校验(CRC)作为完整性校验值。但CRC并不是一种真正意义上的信息认证码，实际上满足不了网络对安全的要求。
- CRC算法是线性的，所以CRC校验体现出了很强的数据关联性，违背了密码学的随机性原则，安全性也随之降低。
- 此外，CRC本身是一种简单的算法，加上之前提到的线性原则，攻击者只要在信息流中插入一定比特位后再调整CRC校验与其相符，就可以做到破解密钥。

4.WEP的缺陷- 3)认证的漏洞

- WEP协议中规定的身份认证是单向的，即只包含接入点对无线工作站的认证，而却没有无线工作站对接入点的认证，不能防止假冒接入点的问题。
- WEP协议中规定的共享密钥认证也容易导致认证伪造。因为在认证过程中，接入点发送给无线工作站的“挑战文本”是以明文方式发送的，而无线工作站发回给接入点的消息为加密之后的。如果攻击者同时截获了明文和密文，就很容易根据**RC4(IV，K)=C⊕P**恢复出密钥序列，从而获得认证数据中的有用信息，以此通过接入点的验证而获得网络资源的访问。
- 此外，WEP协议本身没有抗重放保护机制，因此对加密的报文可以随意重放，接收方无法识别该报文是发送方发送的还是攻击者重放的。

11.1.3 802.11i

- 因为WEP协议存在重大安全缺陷，IEEE成立了安全任务组，制定了802.11i安全标准，以解决无线局域网的安全问题。IEEE 802.11i关注无线接入点(access point，AP)和无线工作站点(station，STA)之间的安全通信，引入了健壮安全网络**RSN(robust security network)**的概念，定义了以下安全服务。
  - A. **认证：**定义用户和网络的交互，以提供相互认证，并生成用于STA和AP之间无线通信的短期密钥。
  - B. **访问控制：**对认证功能的增强，能与多种认证协议协同工作。
  - C. **带消息完整性的机密性：**MAC层数据与消息完整性校验码一起加密以提供机密性和完整性。

IEEE 802.11i强安全网络操作的5个阶段

(1)发现阶段：STA和AP建立连接，决定保护通信机密性和完整性的协议、认证方法、密钥管理方法等。

(2)认证阶段：一个STA与一个AP相互认证，目的是只允许授权STA访问网络，并且向STA保证连接的是一个合法网络。STA和AP还产生一个共享的主密钥。

(3)密钥管理阶段：AP和STA执行一系列操作，由认证阶段生成的主密钥来产生各种密钥并保存于AP和STA。

(4)安全通信阶段：AP和STA交换数据帧，交换的数据得到安全保护，以保证机密性和完整性。

(5)连接终止阶段：AP和STA拆除安全连接。

802.11i协议结构

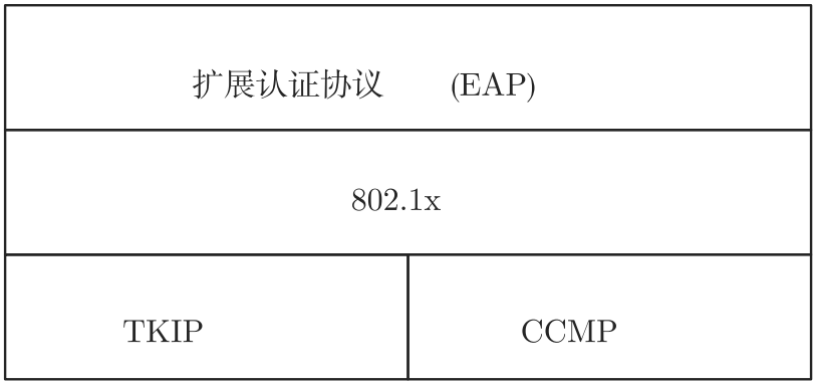


图11-5 IEEE 802.11i协议结构

IEEE802.11i规定使用802.1x认证和密钥管理方式，定义了**TKIP(temporal key integrity protocol)**和**CCMP(counter-mode/CBC-MAC protocol)**两种**数据加密机制**，增强了WLAN中的数据加密和认证性能，从而大幅度提升了网络的安全性。

IEEE 802.11i支持的安全协议：

① 加强的加密算法CCMP或TKIP，其中必须实现基于AES的CCMP。

② 动态的会话密钥。

③ 具有密钥管理算法。

④ 基于802.1x的、无线接入点和无线工作站点的双向增强认证机制。

⑤ 支持快速漫游和预认证。

⑥ 支持独立基本服务集(independent basic service set，IBSS)。

WPA (Wi-Fi Protected Access)只是802.11i的子集

- WPA是由产业界的Wi-Fi联盟提出的、802.11i标准成熟之前的过渡方案。WPA基于802.11i草案中的稳定部分构成，Wi-Fi联盟要求兼容WPA的设备能够在802.11i获批准后升级至与802.11i兼容。
- WPA支持以下安全协议：
  ① 加强的加密算法TKIP。
  ② 动态的会话密钥。
  ③ 具有密钥管理算法。
  ④ 基于802.1x的双向增强认证机制。
- 可以看出，WPA只是802.11i的子集。

802.11i — 1.数据加密和完整性

- TKIP(temporal key integrity protocol)是一种对传统设备上的WEP算法进行加强的协议，目的是在不更新硬件设备的情况下，提升系统的安全性。作为一种过渡算法，虽然其所能提供的安全措施有限，但它能使各种攻击变得比较困难。

- TKIP与WEP 一样基于RC4加密算法，但相比WEP算法，**将密钥的长度由40位增加到128位，初始化向量的长度由24位增加到48位，解决了WEP密钥长度太短的问题。**并对WEP进行了改进，引入了四种新机制以提高加密强度。

TKIP引入了四种新机制以提高加密强度

(1)每包一密钥(per-packet key)： 每个MAC数据包使用不同的密钥加密，该加密密钥通过将多种因素混合在一起而生成，安全强度大大提高。

(2)消息完整性校验码(message integrity code，MIC)： TKIP实现了一个64位的消息完整性检查(MIC)，防止伪造的数据包被接受。

(3)具有序列功能的初始化向量*IV*： 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，确保了每个数据包使用不同的密钥。

(4)密钥生成及定期更新功能： 解决了密钥管理的问题。

TKIP的加密过程

(1) MPDU(MAC protocol data unit，MAC协议数据单元)的生成

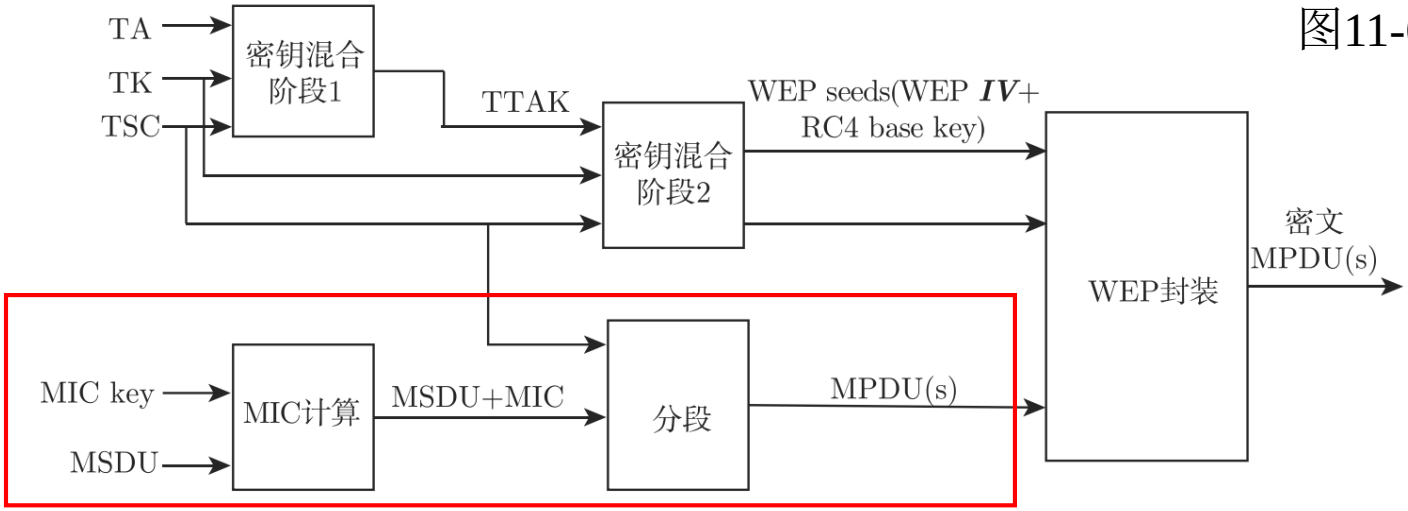


图11-6 TKIP加密

- 包括MIC (message integrity check，消息完整性校验码)的产生和MSDU(MAC service data unit，MAC服务数据单元)的分段。
- 发送方针对明文MSDU计算Hash值，将此Hash值作为MIC串接到MSDU后面。如果有必要的话，发送方将串接的MIC和MSDU分成一个或多个明文MPDU，并给每个MPDU分配一个单调增加的TSC(TKIP sequence counter，TKIP序列计数器)，所有来自同一个MSDU的MPDU所使用的TSC值来自相同的计数空间。这些MPDU将作为 WEP算法的输入。

TKIP的加密过程：(2) WEP种子(WEP seeds)生成

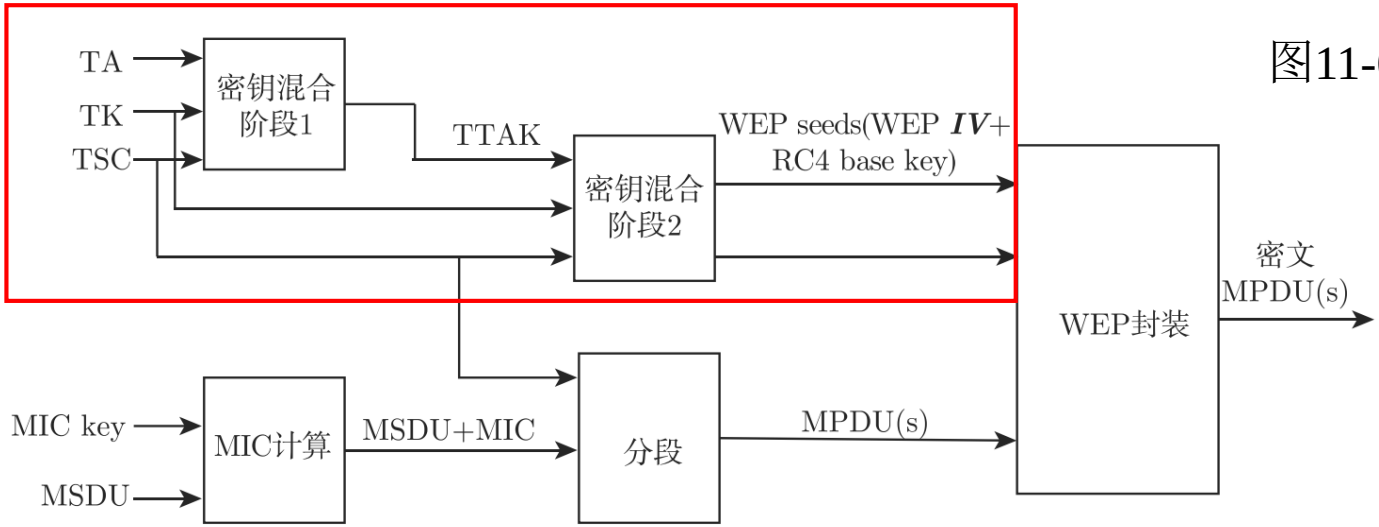
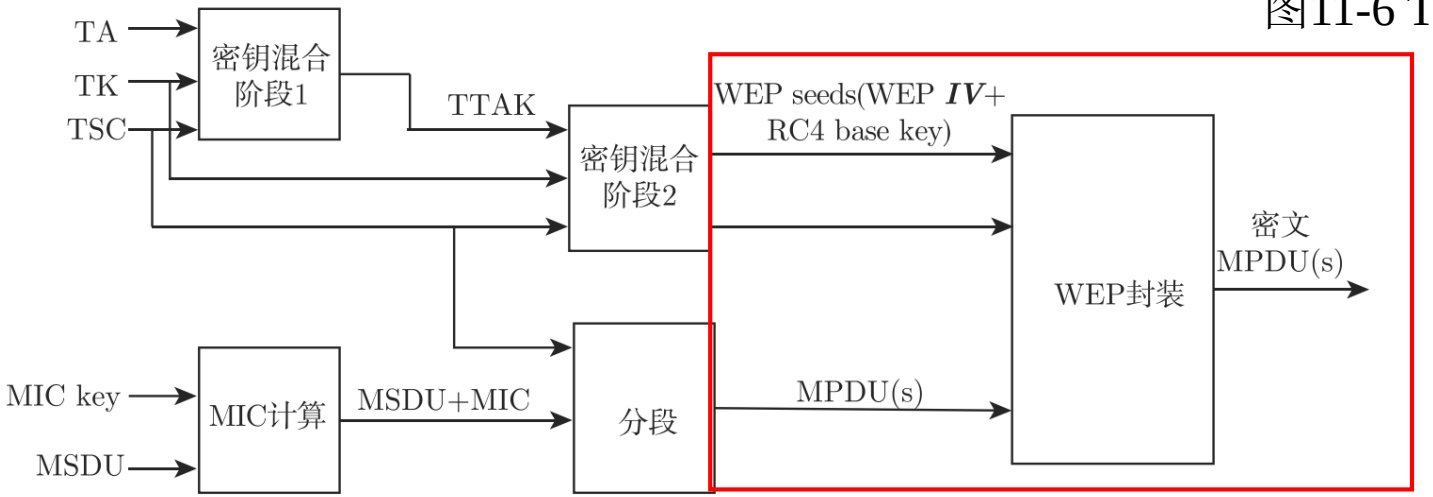


图11-6 TKIP加密

- 这一步是为了弥补WEP静态共享密钥的缺陷。
- 对于每个MPDU，TKIP都将计算出相应的WEP seed，也就是per-packet key(RC4 key)。WEP seed的生成主要包括两个密钥混合过程：第一阶段的密钥混合基于临时密钥(temporary key，TK)生成一个临时的混合密钥(TTAK)。利用TTAK、TK和TSC作为第二阶段混合的输入即可得到用于WEP加密的WEP seed。

TKIP的加密过程：(3)WEP封装

图11-6 TKIP加密



TKIP把经过两次混合产生的种子密钥WEP seed分解成WEP ***IV***和 RC4 base key，然后和MPDU 一起传给WEP进行加密。TK对应的key ID会被编入WEP的***IV***域中。

总的来看，加密时的输入有TK、MIC key，明文MSDU、TSC和TA。其中，TK、TSC和TA参与第一阶段的混合，生成TTAK; TTAK、TSC和TK经过第二阶段的混合生成 WEP seed，供RC4调用生成密钥流。同时，明文MSDU和MIC key经过Hash运算生成 MIC，然后明文MSDU和MIC串接并分段得到多个MPDU，每一个MPDU对应一个特定的TSC。MPDU作为WEP输入，和密钥流异或得到密文。

TKIP的MPDU结构

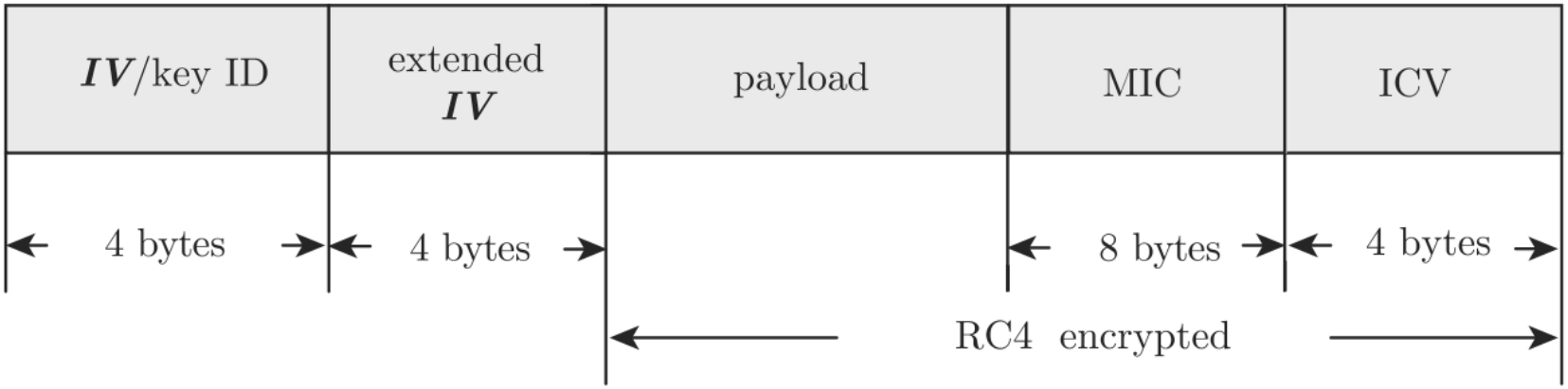


图11-7 TKIP MPDU结构

- TKIP重用了WEP的MPDU格式，但扩展了4个字节，用作扩展***IV***字段，同时增加了8字节的MIC字段。
- MSDU-MIC可以封装在一个单一的MPDU，如果不行，则被分段，成为适当大小的多个MPDU，MIC可能只在最后的MPDU中出现。

TKIP解密过程

- TKIP解密过程与加密过程相反，包括以下步骤。

(1)在WEP解封一个收到的MPDU前，TKIP从***IV***中提取TSC和key ID。如果 TSC超出了重放窗口，则该MPDU被丢弃；否则，根据key ID定位TK，通过两个阶段的混合函数计算出WEP seed，计算过程和加密过程中的完全相同，不再赘述。

(2) TKIP把WEP seed分解成WEP ***IV***和RC4 base key的形式，把它们和MPDU 一起送入WEP解密器进行解密。

(3)检查ICV，如果结果正确，则该MPDU将被组装入MSDU。

(4)如果MSDU重组完毕，则检查MIC。如果MIC检查正确，TKIP把MSDU送交上一层；否则，MSDU将被丢弃。

TKIP从如下几个方面加强了WEP协议

(1) WEP缺少防止消息伪造和其他主动攻击的机制，TKIP中设计MIC以保证MSDU数据单元的完整性，从而可以有效抵抗这类攻击。

(2) TKIP中使用两个阶段的混合加密函数计算得到WEP seed。这个种子包括了WEPIV，与TSC一一对应。同WEP中的静态密钥和24位的***IV***相比较，混合函数把密钥和数据包的属性结合起来，可以有效地抵抗重放攻击，使密钥更安全。

(3) TKIP使用TSC给它所发送的MPDU来排序，接收者会丢掉那些不符合序列的 MPDU。这提供了一种较弱的抵抗重放攻击的方法。

- 因为TKIP的总体安全性仍是取决于WEP核心机制，而WEP算法的安全漏洞是由于机制本身引起的，因此，TKIP只是一种过渡算法。

2.CCMP协议

- CCMP基于AES算法和CCM模式，由两个部分组成：加密模式(CTR counter mode)，用于保证数据的私密性；CBC-MAC(cipher block chaining message authentication code)模式，用于数据完整性校验。CCMP是802.11i强制使用的加密方式，为WLAN提供了加密、认证、完整性和抗重放攻击的能力，**能解决WEP中出现的所有问题。**

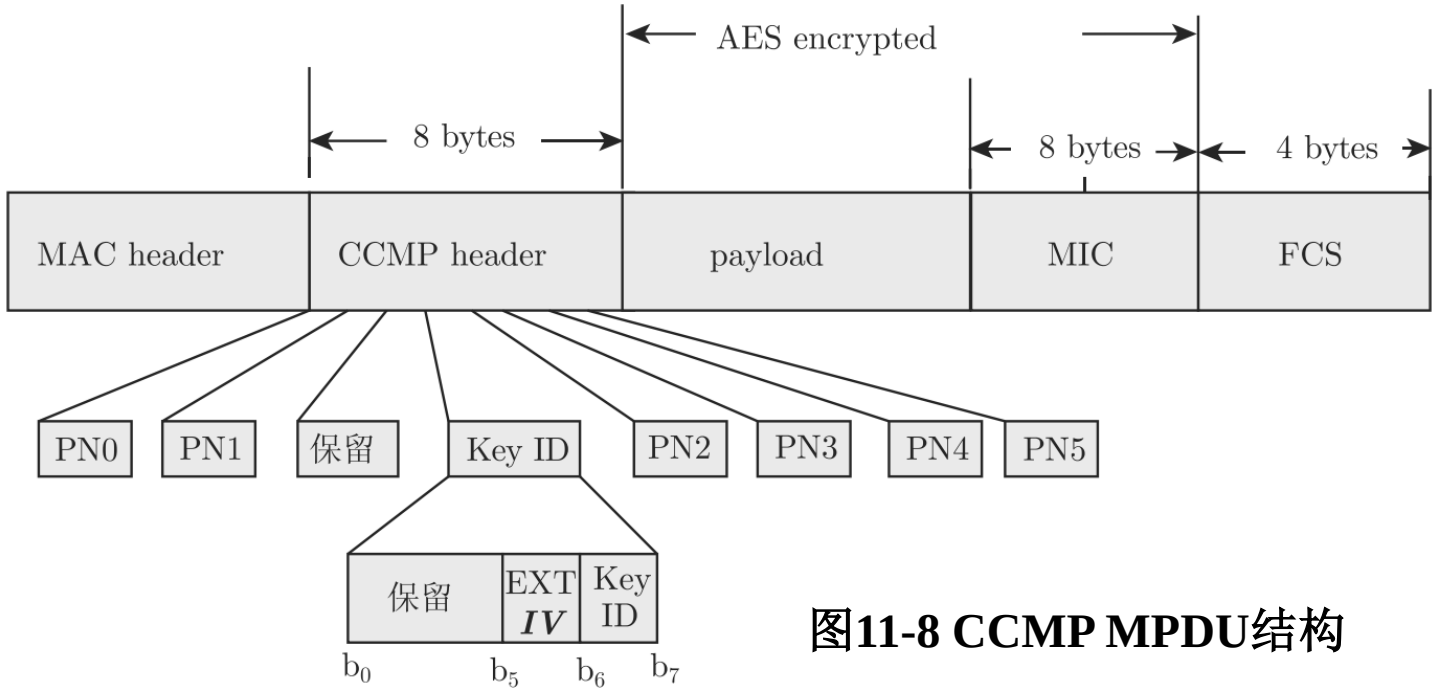


图11-8 CCMP MPDU结构

CCMP的正向封装过程实现了MPDU的加密和认证

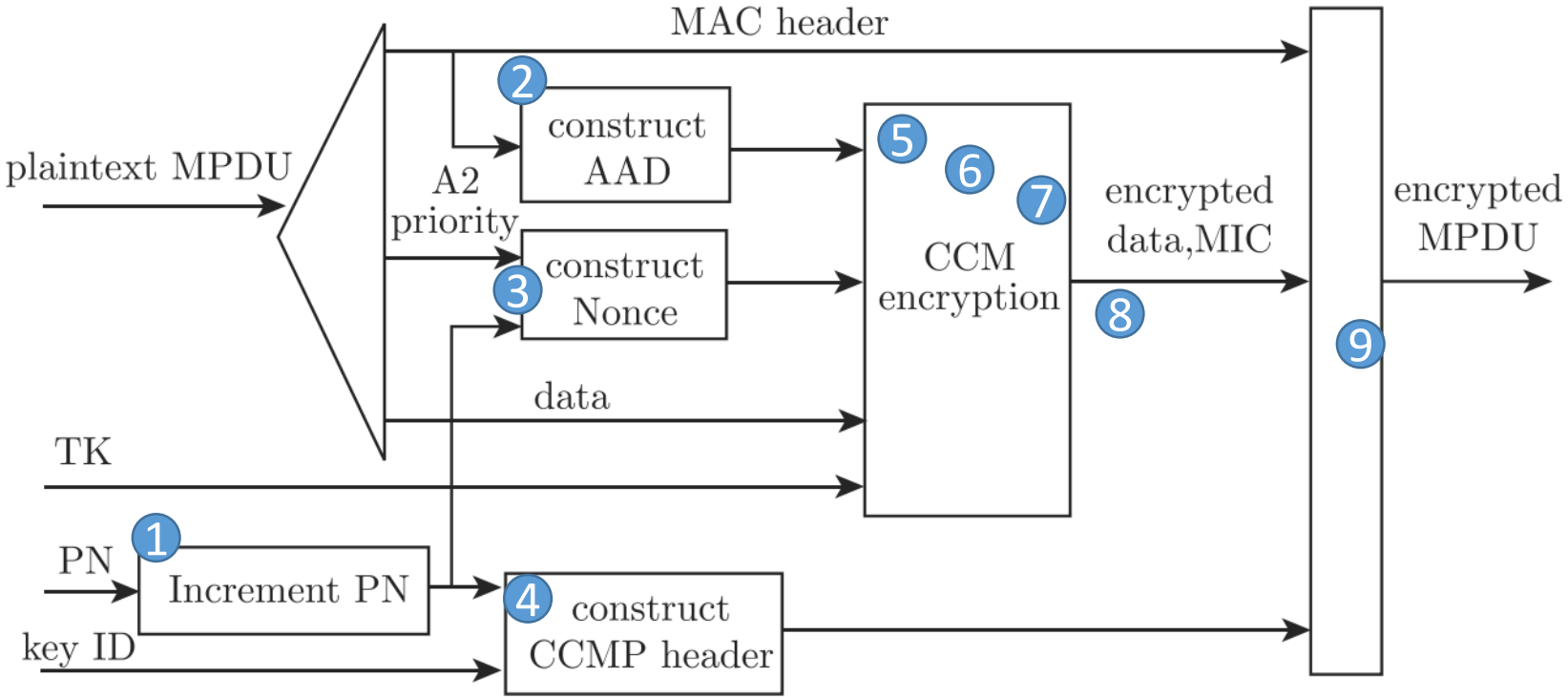


图11-9 CCMP封装过程

CCMP的封装过程包括以下几个步骤：

- (1)增加PN，保证对每个MPDU有一个新鲜的PN;
- (2)用MAC头构造CCM的附加认证数据(additional authentication data，AAD)，CCM算法也为AAD提供完整性保护；
- (3)利用PN、MPDL的发送地址和优先级域计算CCM nonce;
- (4)把PN和kev ID编入CCMP头部；
- (5)利用MPDU和Nonce构造CCM-MAC的IV;
- (6)使用该IV，CCMP在CCM-MAC下使用AES计算出MIC，将MIC截为64位，添加在MPDU数据后面；
- (7)利用PN和MPDU TA构造CTR模式的counter;
- (8)使用该counter，CCMP在CTR模式下使用AES加密MPDU数据和MIC;
- (9)最后，由原MAC帧头、CCMP header和密文组合形成CCMP MPDU。

CCMP MPDU的解封装

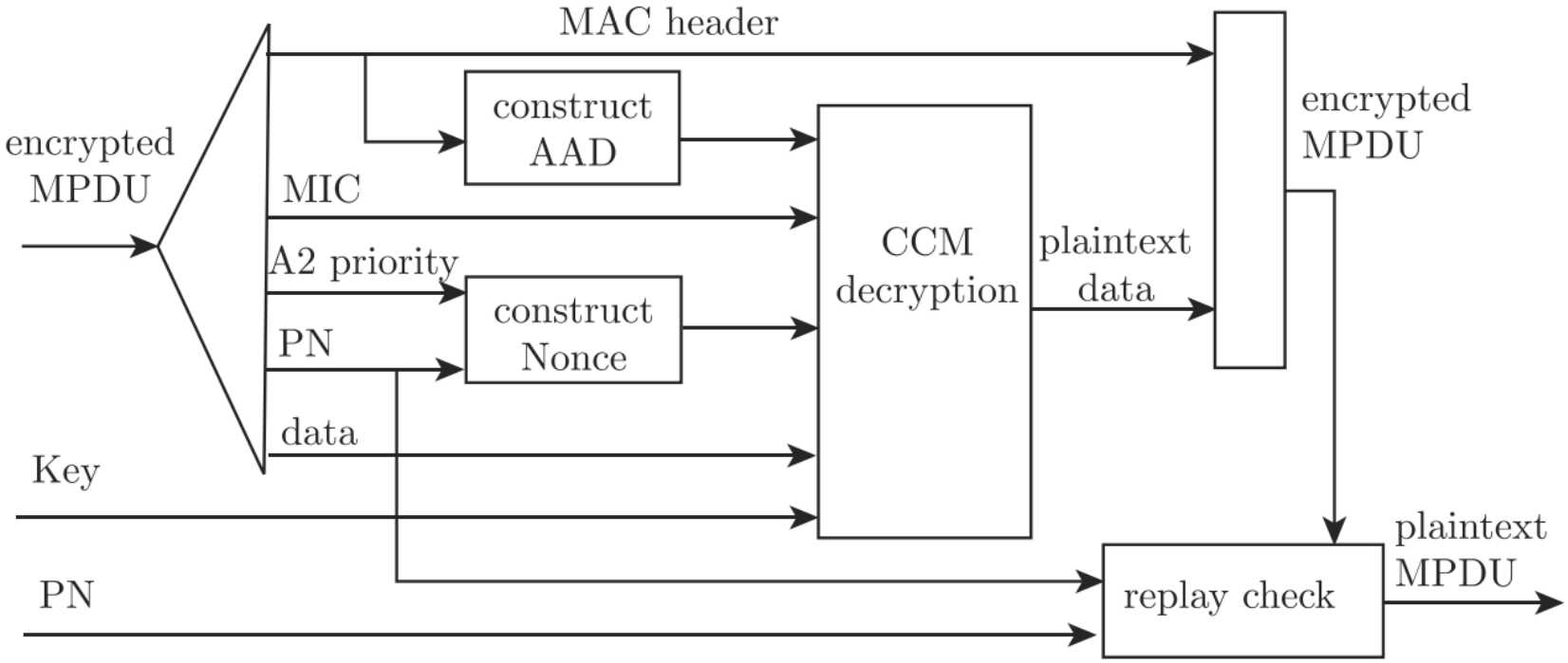


图11-10 CCMP解封装过程

CCMP MPDU的解封装

解封装包括以下几个步骤：

(1)获取PN，进行重放检查，若为重放则抛弃该帧；

(2)以Olen、TA、PN为输入，构建初始分组，其输出同样记为MIC_IV;

(3)以PN、MPDU TA为输入，构建用于CTR解密的计数器；

(4)在TK的控制下，对包含了MIC的密文MPDU通过CTR解密；

(5)以解密后的明文MPDU、MIC_IV以及packet number为输入，在临时密钥TK的作用下，通过CBC-MAC重新计算得MIC;

(6)将MIC与接收到的MIC比较，若不同则视为遭到篡改攻击，抛弃当前接收数据，并记入日志。

3.认证协议

- 802.11i中的认证、授权和接入控制主要是由三个部分配合完成的，分别是802.1x标准、EAP协议和RADIUS协议。

1) 802.1x

- 802.1x是基于端口的网络访问控制标准，其初衷是对有线网络提供接入控制。虽然802.1x并非专门针对WLAN设计，但它提供了可靠的用户认证和密钥分发框架，因此也可对802.11无线网络的用户进行身份验证和访问控制。
- 802.1x的认证模型包含三个实体：请求者(supplicant)、认证者(authenticator)和认证服务器(authentication server，AS)。在802.11无线局域网的上下文中，前两者分别对应STA和AP。AS通常是网络中的一个有线连接的独立设备，但是也可以集成到AP中。

1) 802.1x

- 在认证成功之前，无线接入点AP会阻塞STA和AS之间的非认证流量。但AP并不参与认证交互过程，仅仅发送AS和STA之间的通信。认证的目的是只允许授权STA使用网络，并向STA保证它连接的是一个合法网络。一旦请求者被认证且授予其密钥，认证者可以发送来自请求者的数据。
- 请求者和认证服务器之间通过EAP协议进行认证，EAP协议包中封装认证数据。请求者和认证者之间交换的EAP数据包采用EAPoL(EAP over Lan)协议封装，认证者则将 EAP协议封装到其他高层协议中，如RADIUS，以便EAP协议穿越复杂的网络到达认证服务器。

802.1x认证结构

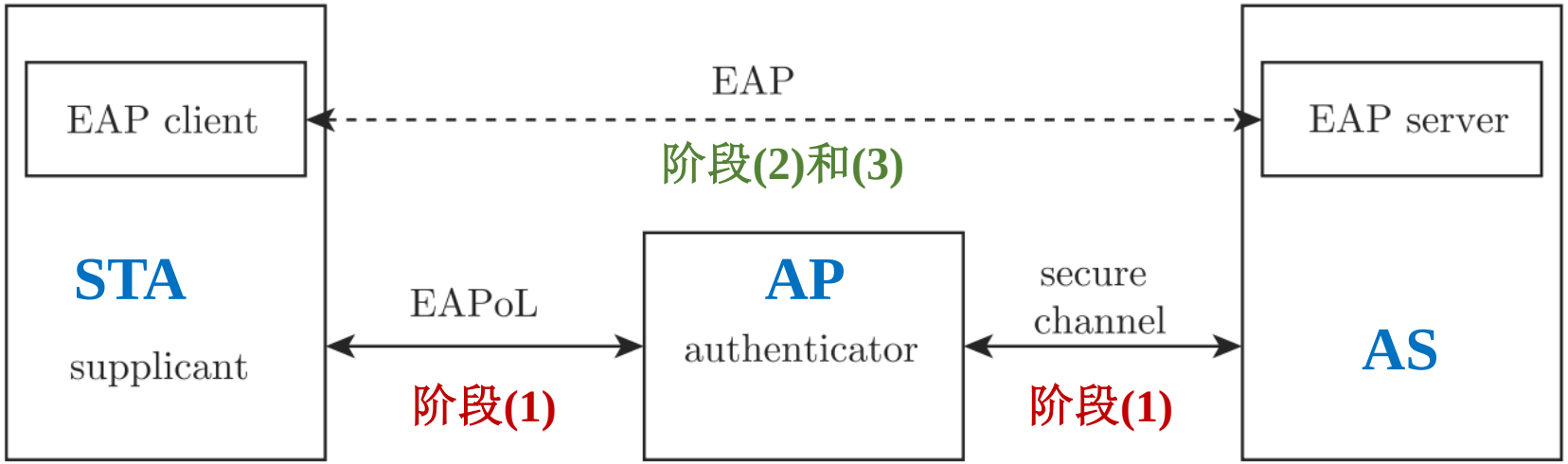


图11-11 802.1x认证结构

可以认为，802.11i的认证过程包括三个阶段

- (1)**连接到AS**：STA向它的AP发送一个请求以连接到AS。AP识别这个请求并给AS发送一个访问请求。
- (2) **EAP交换**：这个交换让STA和AS相互授权。
- (3)**安全密钥分发**：一旦认证完成，AS和STA产生一个主会话密钥(master session key，MSK)，此密钥也被称为AAA密钥(authentication、authorization、accounting)。STA和AP进行安全通信所需的加密密钥都从MSK产生。

2) EAP

- **可扩展认证协议(extensible authentication protocol，EAP)**最初是针对点对点协议(PPP)设计的，然而“可扩展”意味着我们可以在最初定义的认证方法以外设计新的认证方法。现在 IETF标准中已经有几十种EAP认证协议，如LEAP、EAP-FAST、EAP-TLS、EAP-TTLS等。因此，本质上EAP协议只是定义了认证框架，**实质的认证过程取决于框架内填充的认证方法**。
- EAP可以和802.1x很好地配合使用，因为802.1x专门定义了在LAN上运行EAP的报文格式EAPoL。EAPoL在原有的EAP报文外面增加了一层封装，使得EAP报文适合在局域网传输。**802.11i**并没有限制采用哪些协议作为上层认证协议，但规定了高层认证协议必须满足双向认证的要求，并**推荐采用EAP-TLS方法**。
- **EAP-TLS是一种基于TLS的认证方式**，认证服务器与请求者采用TLS协议协商会话密钥，该协议要求双方都要有公钥证书。

无线局域网环境下EAP-TLS认证过程

(1) STA发出EAP start消息给AP，请求认证；

(2) AP发出EAP请求消息，要求STA输入用户名；

(3) STA回复EAP响应消息，其中包含自己的用户名信息；

(4) AP将STA的用户名信息重新封装成RADIUS access request消息，并发送给RA- DIUS服务器；

(5)服务器回复STA 一个EAP-TLS开始消息；

(6) STA给服务器发送SSL client_hello消息；

(7) 服务器将server certificate、client certificate request、server-hello和可选的server key exchange消息发送给STA;

无线局域网环境下EAP-TLS认证过程

(8) STA校验服务器证书和finished消息，并向服务器回复client certificate、client key、change cipher SPE和finished消息；

(9)服务器校验client证书，回复change cipher SPE和finished消息；

(10) client校验finished消息，并回复服务器；

(11) 服务器和STA推导出主会话密钥；

(12) 服务器给AP发送RADIUS ACCEPT消息，其中包含client的主会话密钥和认证成功的指示；

(13) AP向STA转发EAP success消息，认证成功。

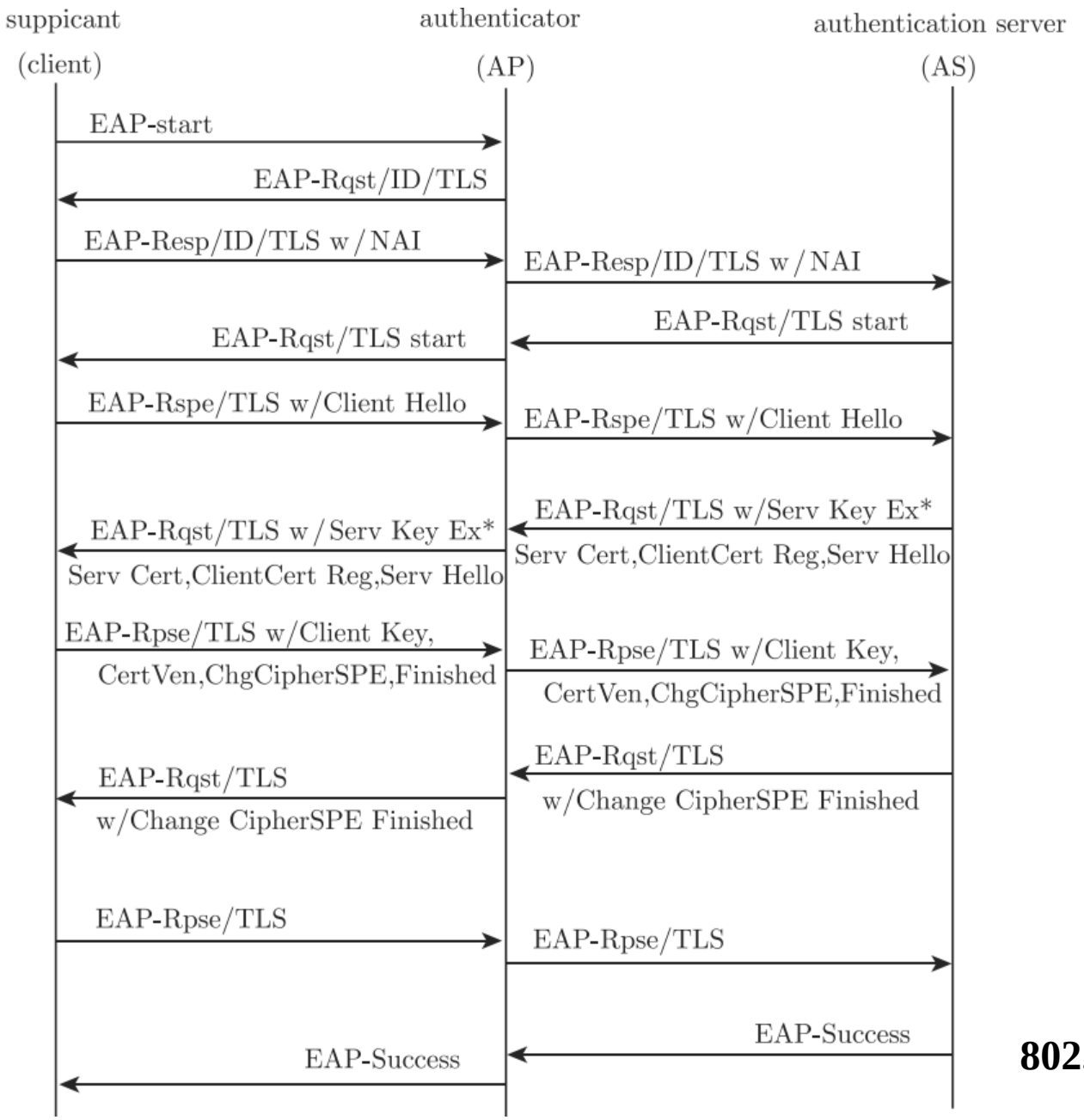


图11-12
802.1x认证结构

3) RADIUS

- RADIUS协议是一个应用普遍的AAA协议，最初为拨号网络设计，基于IP网络。AP与AS之间的交互协议不是802.11i关注的重点，在此不再详述。

- 缺乏自动有效的密钥管理是802.11的一大安全缺陷。人工配置密钥的方法烦琐而低效，并且以口令作为密钥还容易受到字典攻击。因此，密钥管理机制的设计也是802.11i的一个重点。当STA和AS成功地相互认证(比如，通过EAP-TLS)，并产生一个主密钥后，就进入密钥管理流程。

4.密钥管理

1)密钥层次

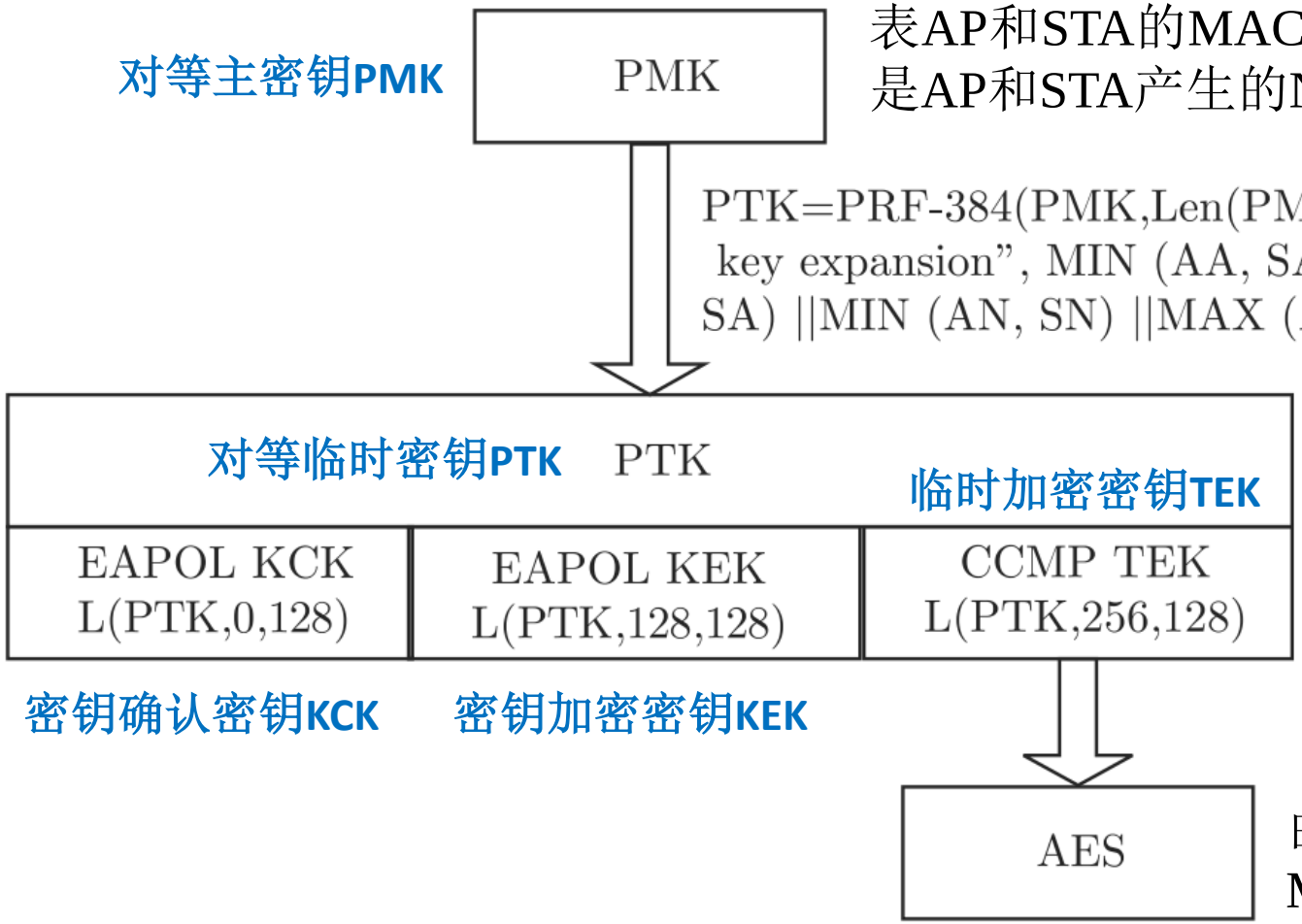
- 在802.11i中，存在多个层次的密钥。
- 认证成功后，无线工作站STA和认证服务器AS各自生成32字节的**对等主密钥(pairwise master key，PMK)**。PMK生成的方法与认证方式相关。如果是EAP认证，则由认证过程得到EAP主密钥(主会话密钥MSK)，再由MSK派生出对等主密钥PMK(通常是取MSK前面若干长度的比特组成PMK)。认证服务器AS将密钥材料安全地传送到认证者AP，从而使AP生成相同的PMK。
- **PMK处于密钥层次的第一级。**

4.密钥管理— 1)密钥层次

- 802.11无线网络中，单播密钥是在某个STA和AP之间使用的，在802.11i中被称为**对等临时密钥(pairwise temporary key，PTK)**。多播（组播和广播）密钥是在同一个AP覆盖的小区内使用的，在802.11i中叫做**组临时密钥(group temporary key，GTK)**。PTK根据PMK计算生成，进而可以根据PTK得到加密所需的其他各种密钥。GTK则由**组主密钥(group master key，GMK)**生成，通常是AP生成的随机数。
- 802.11i支持TKIP和AES两种加密算法，这两种算法都需要多个密钥。以AES为例，其密钥导出层次如图11-13所示。

4.密钥管理— 1)密钥层次：AES密钥导出层次

Len()是求长度函数，AA和SA分别代表AP和STA的MAC地址，AN和SN则是AP和STA产生的Nonce(伪随机数)



由 TEK 根 据 CBC-MAC算法导出AES加密密钥

图11-13 AES密钥导出层次

4.密钥管理— 2)四步握手

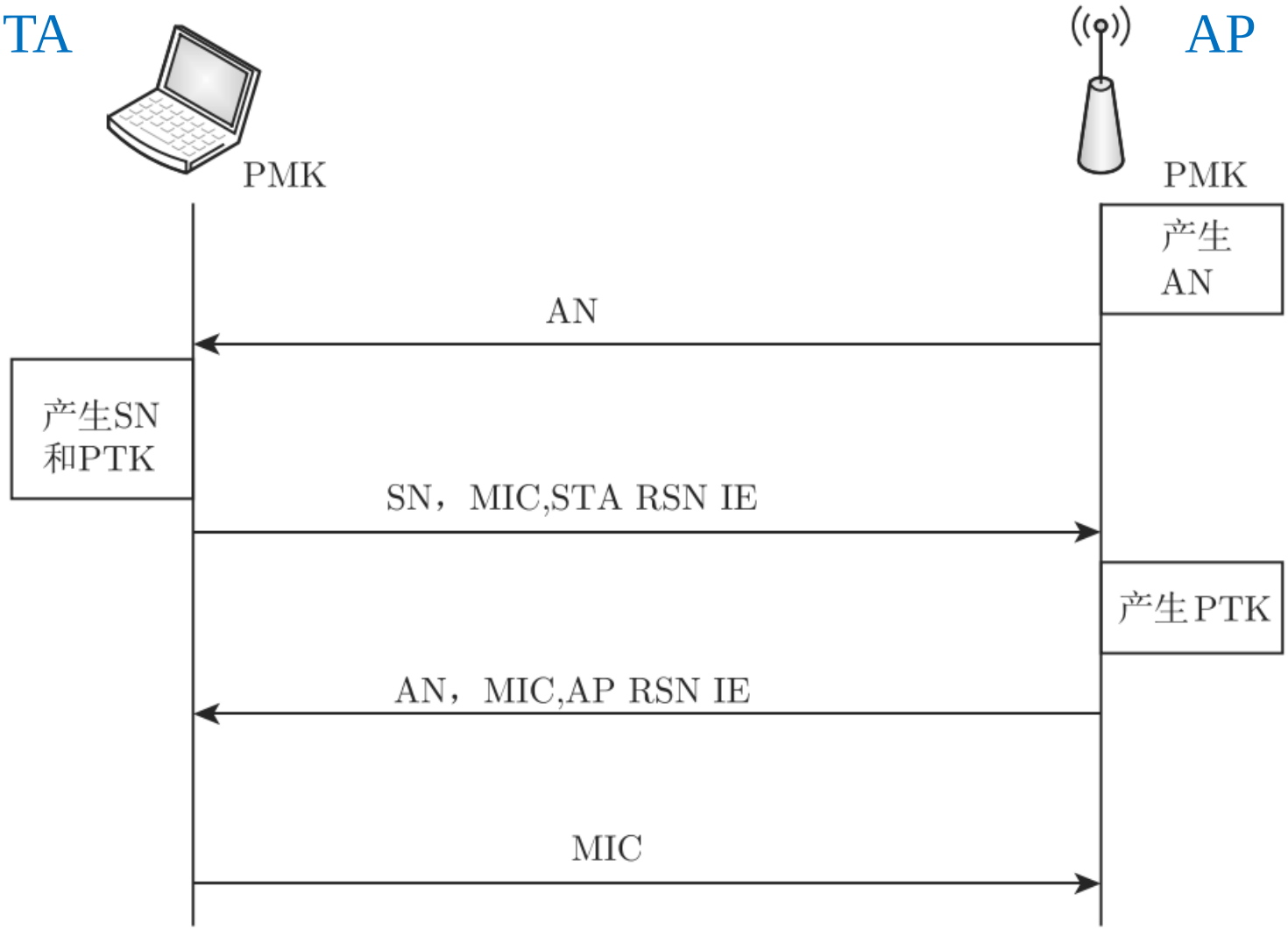


图11-14 四步握手流程图

4.密钥管理— 3)组密钥更新

图11-15 组密钥更新流程图

5.RSNA建立过程

- IEEE 802.11i的**强安全网络连接(robust security network association，RSNA)**建立过程包含三个实体：申请者(STA)、认证者(AP)和认证服务器（如Radius服务器）。
- 通常一个成功的认证意味着STA和AS互相证实对方的身份，并为下一步的密钥管理过程产生一个共享密钥，在这个共享密钥的基础上，密钥管理协议计算并分发用于数据传输的密钥。

大体上，RSNA建立过程可分成6个阶段。

- (1)**网络和安全能力发现**：一方面，AP在某一特定信道以发送信标帧(beacon)的方式周期性地向外广播它的安全性能，这些安全性能信息包含在RSN信息单元中。另一方面，AP也会发送探询应答帧来响应无线工作站的探询请求。

- (2) **802.11认证和连接**：STA从可用的AP列表中选择一个AP，与该AP进行认证和连接。然而这种认证是很脆弱的，必须在以后的阶段加以强化。经过这一阶段后，802.1x端口还处于关闭状态，还不能进行数据包的交换。
- (3) **EAP/802.1x/RADIUS认证**：STA与AS执行双向认证协议(如EAP-TLS)，AP扮演数据中转站的角色。经过这一阶段以后，STA与AS互相进行认证并生成共享密钥，即主会话密钥(MSK)。STA由MSK派生出对等主密钥(PMK)，AS将密钥材料安全地传送到 AP，从而使AP可以生成相同的PMK。
- (4) **四步握手**：申请者与认证者通过四步握手机制来确认PMK的存在，核实所选用的加密套件，并生成PTK用于后面的数据传送。经过这一阶段，认证者与申请者共享一个新的PTK，802.1x端口也会开通进行数据的交换。
- (5) **组密钥握手**：当存在多播应用时，AP会生成一个新的GTK，并将这一 GTK发送到每一个STA。
- (6) **安全数据传输**：利用PTK或者是GTK，以及前面所协商的加密组件，申请者与认证者就可以依照数据加密协议，传送受到保护的数据。

一个例子：华为路由器WS5200

11.2 移动通信系统的安全

- 当前，移动互联网已经深入到人们生产生活的方方面面，极大地方便了人们的生活。
- 移动互联网包括了以下几个要素：**无线移动通信网络**，包括2G、3G和4G等，提供接入服务；**公众互联网**，即Internet，提供内容服务；**移动通信终端**，包括手机和PDA等。

- 移动互联网十分严格地强调对用户隐私和用户行为的保护，比传统互联网具有更高的安全性要求。

11.2.1 GSM的安全(2G)

- 移动通信系统首先必须解决两个问题：

① **第一，对用户进行认证，防止未注册用户的欺骗性接入；**

② **第二，对无线路径加密，以防止第三方窃听。**

- 此外，移动台的位置更新过程也将成为系统的安全薄弱环节，因为这意味着即使是在非通话期间，也有可能对用户位置进行跟踪。因此，**移动通信系统还应能提供用户身份保护，防止用户位置泄露。**

GSM安全性的提升

- GSM作为第二代蜂窝移动通信网的典范，与第一代的模拟蜂窝系统相比，安全性有很大提升：

✓GSM在无线接口上采用的数字语音编码算法，GMSK(高斯最小移频键控)调制方式，慢速跳频技术以及复杂的TDMA时隙结构，使得无论是无线信号的截收、同步还是解码都更加困难；

✓另一方面，GSM利用密码学方法引入的认证与加密技术更为保护用户的隐私，为防止欺骗性接入提供了进一步的防范措施，很好地解决了上述三方面的问题。

1.GSM安全机制

- GSM的安全机制包括了以下几个方面的功能：用户身份认证、用户身份保密、用户数据保密以及信令数据保密。
- 每个GSM用户用**国际移动用户识别码IMSI**唯一标识，并由网络统一分配**用户认证密钥Ki**。**IMSI和Ki**一起构成了网络**籍以鉴别用户**的重要**“身份证件”**。而GSM认证与加密方案的一个设计要点就是保证这一“身份证件”永远无需在无线路径上传输（除非是在网络数据库故障之类的特殊场合）。
- 网络对用户的认证采用“问——答”机制，对无线路径的加密则使用临时随机产生的会话密钥K_C。
- 一般情况下，移动台也仅使用网络临时分配的临时移动用户标识TMSI，以进一步防止用户真实身份IMSI的泄露。

GSM安全机制

- GSM安全性管理涉及的主要部件是移动台一侧的**SIM卡**和网络一侧的**鉴权中心AUC**，它们是存储用户认证密钥K_i的地方。需注意的是，它们并不传送K_i，而是各自独立完成**A3和A8**算法。根据**随机数RAND**，计算签名回答SRES=A3(RAND，K_i)，会话密钥 K_C=A8(RAND，K_i)。
- 所不同的是，AUC的计算是根据随机选择的RAND事先完成的，并将其计算结果(RAND，SRES，K_i)三元组在归属位置寄存器HLR和访问位置寄存器VLR处分别存储。SIM卡的计算则在当网络端要求进行用户认证时，根据网络端送来的RAND临时计算，并将结果SRES发送回网络以供比较，从而得出用户是否合法。

- 图11-16总结了有关安全信息在整个系统中的分布情况。

安全信息在整个系统中的分布情况

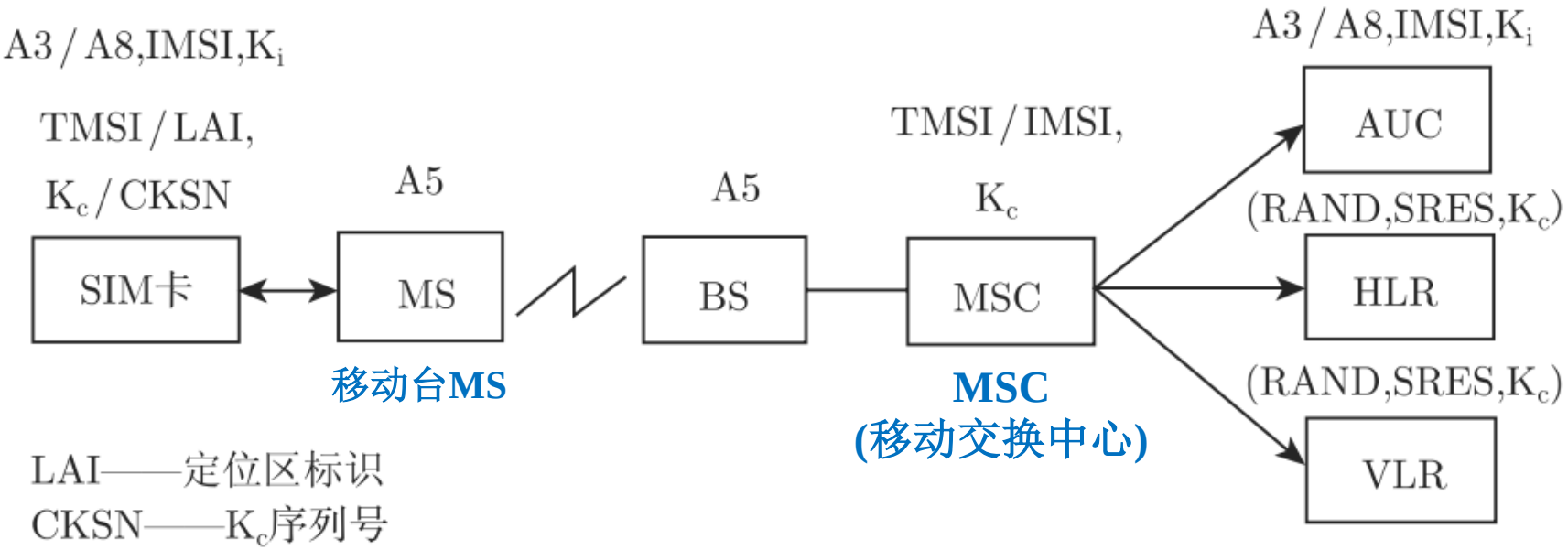


图11-16 安全信息在整个系统中的分布情况

- GSM在无线路径上的传输是以突发脉冲为传输单位的。一个普通突发脉冲包含114比特的用户数据，因此，在无线路径两端的加 / 解密操作都是在一个突发脉冲的114比特的基础上进行的。

A3/A8和A5算法的外部规范。

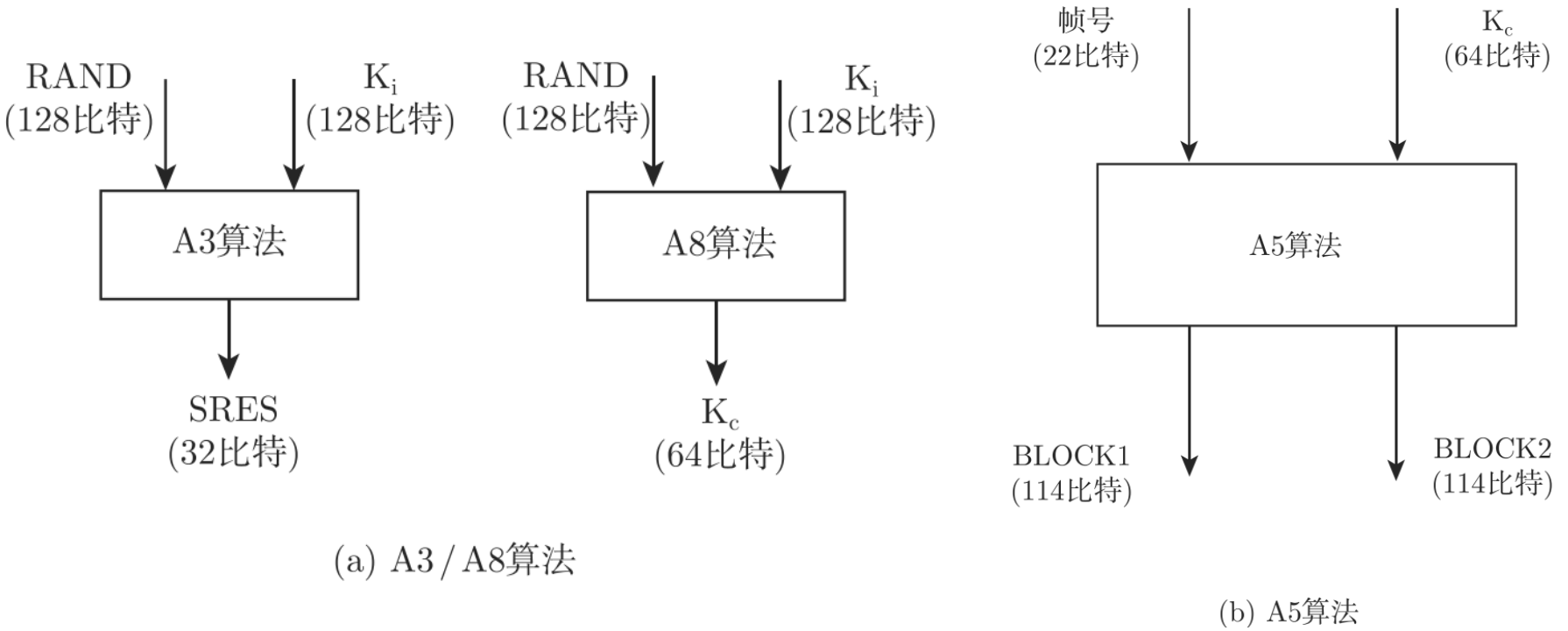


图11-17 A3/A8和A5算法外部规范

1.GSM安全机制— 1)用户身份认证

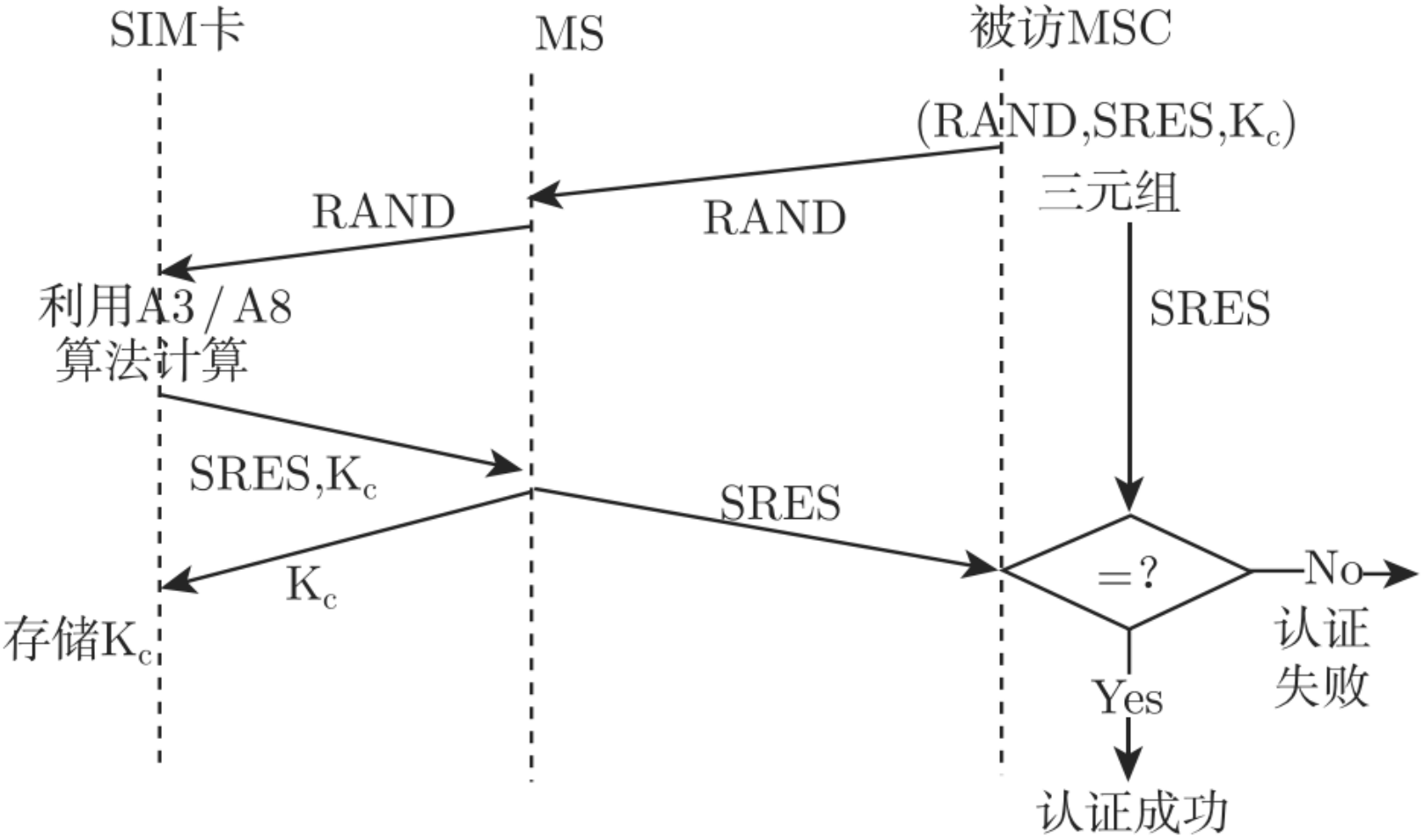


图11-18 GSM用户认证与密钥生成

1.GSM安全机制— 2)信令及数据保密

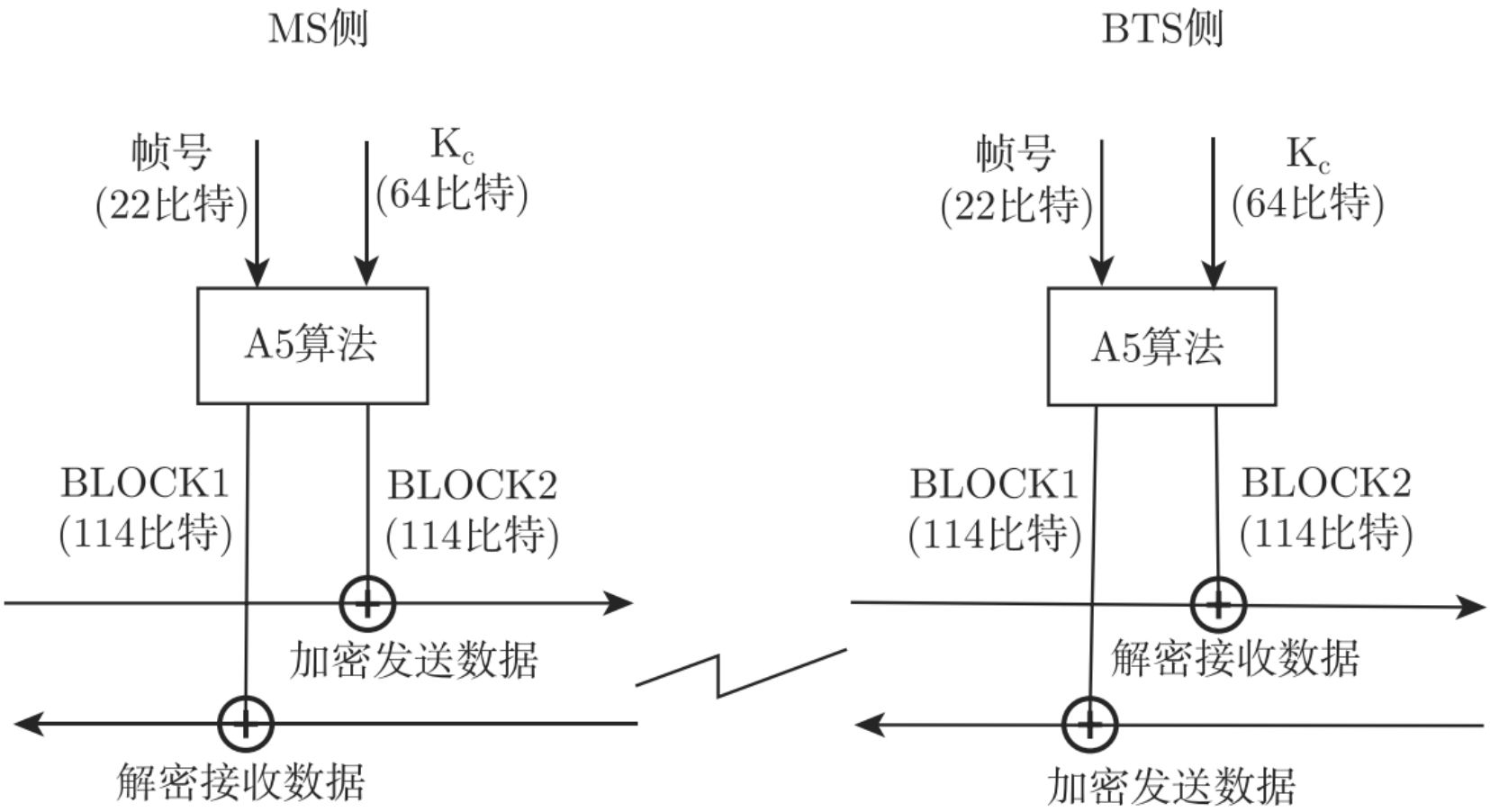


图11-19 GSM加密模式传输

1.GSM安全机制— 3)用户身份保密

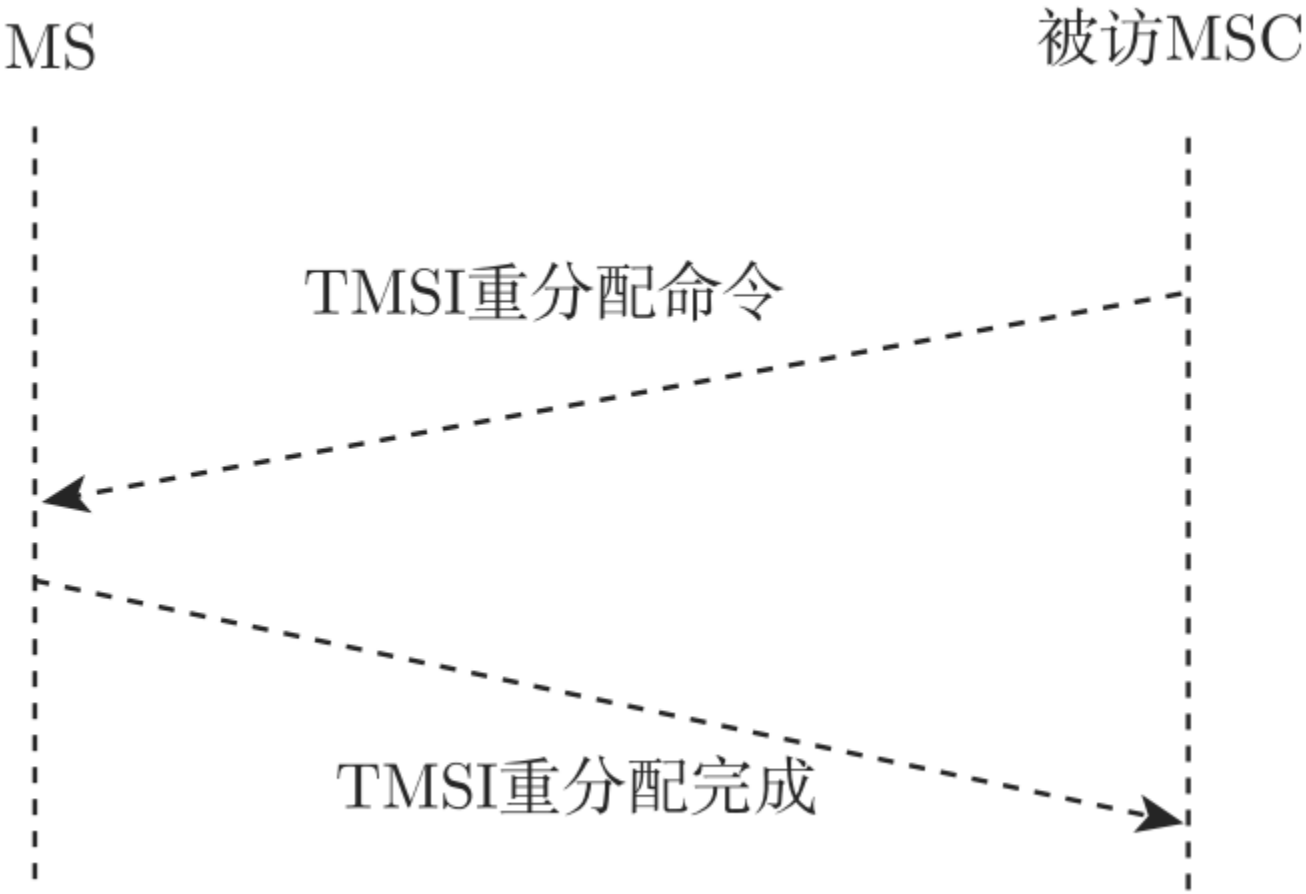


图11-20 TMSI的分配

2.认证方案

- GSM的认证方案采用了单钥体制，其认证协议为典型的“问—答”机制，并只对用户进行单向认证。
- 由于公钥体制具有较高的安全性，且更易于密钥的管理，较单钥体制有许多优点。目前限制公钥体制应用的主要因素是其计算量大。但随着公钥密码算法的发展（例如，算法所需计算量在通信双方的分布更加不均匀）以及移动台本身计算能力的提高，在未来的数字移动通信网（个人无线通信网）中，采用双钥体制将会是一种趋势。
- 通过采用更复杂的认证协议，双向认证也将成为可能。

3.加密算法A5

- 目前，所有国家都使用一种A5算法，该算法属于GSM MoU(理解备忘录)的财产，受版权保护。由于保密原因，只有其外部规范是公开的，A5算法也因此成了众多密码学者研究分析的对象。以下是收集到的一些有关A5算法的信息。

  (1) A5算法为基于三个钟控LFSR(线性反馈移位寄存器)的流密码，三个LFSR的阶数分别为19、22和23。

  (2)钟控信号分别来自于三个LFSR“中间”比特位的开关函数。

  (3)三个LFSR的总阶数为64，因此，64比特的会话密钥K_C被用于初始化LFSR的内容。

  (4) 22比特的TDMA帧号被依次移入LFSR。

  (5)输出为两个114比特的密钥流序列。

  (6)据说A5算法的有效密钥长度最多为40比特。

- 考虑到出口限制，A5算法还有A5/1和A5/2不同的版本，其中A5/2算法的强度稍弱些，可以理解为密钥长度自效位数的减少。但即使是不采用任何A5算法，GSM也远比模拟蜂窝系统安全。

4.密钥长度

- 一个密码算法的密钥长度是衡量该算法抗穷举攻击的重要尺度。密钥越长，则搜索整个密钥空间以找到正确密钥所需的计算量也将以2的指数增加。
- 随着近年来计算机的普及，以及其处理能力的提高，认为“安全”的密钥长度的概念也在改变。目前普遍的看法是采用128比特的密钥，像国际数据加密算法IDEA的密钥即为128比特，密钥长度为56比特的DES因此极有可能在不久后遭到淘汰。
- 相对而言，A5算法的密钥长度只为64比特，并且如果其有效密钥长度果真仅为40比特的话，则只能在短时间内对信息提供保护。
- **一般认为，普通蜂窝电话的内容受保护的时间应该在星期这个数量级上，因此在现阶段A5算法应该还是能胜任的。**

11.2.2 GPRS的安全

- 随着无线数据业务的迅速发展，移动数据业务已经从传统的电路交换方式发展为分组交换方式。**通用分组无线业务(GPRS)**是一种新的数据业务，它可以在现有GSM网络基础上，通过增加一些网络节点给移动用户提供无线分组接入服务。

- GPRS的安全机制在GSM的基础上得到了加强，包括身份保密、身份认证、用户数据加密、信令数据加密以及其他由GPRS系统提供的GSM标准之外的安全机制。在GPRS的标准规范中提供的一些安全特征，运营商可以有选择地使用。除此之外，还可以使用其他组织提供的安全特征。但是，GPRS也存在一些安全缺陷，下面首先简单介绍GPRS网络结构，然后分析其安全机制。

1.GPRS网络结构

- GPRS网络是在现有GSM网络中增加分组控制单元(PCU)、服务GPRS支持节点(SGSN)和网关GPRS支持节点(GGSN)而实现的，使得用户能够在端到端分组方式下发送和接收数据。其系统结构如图11- 21所示。

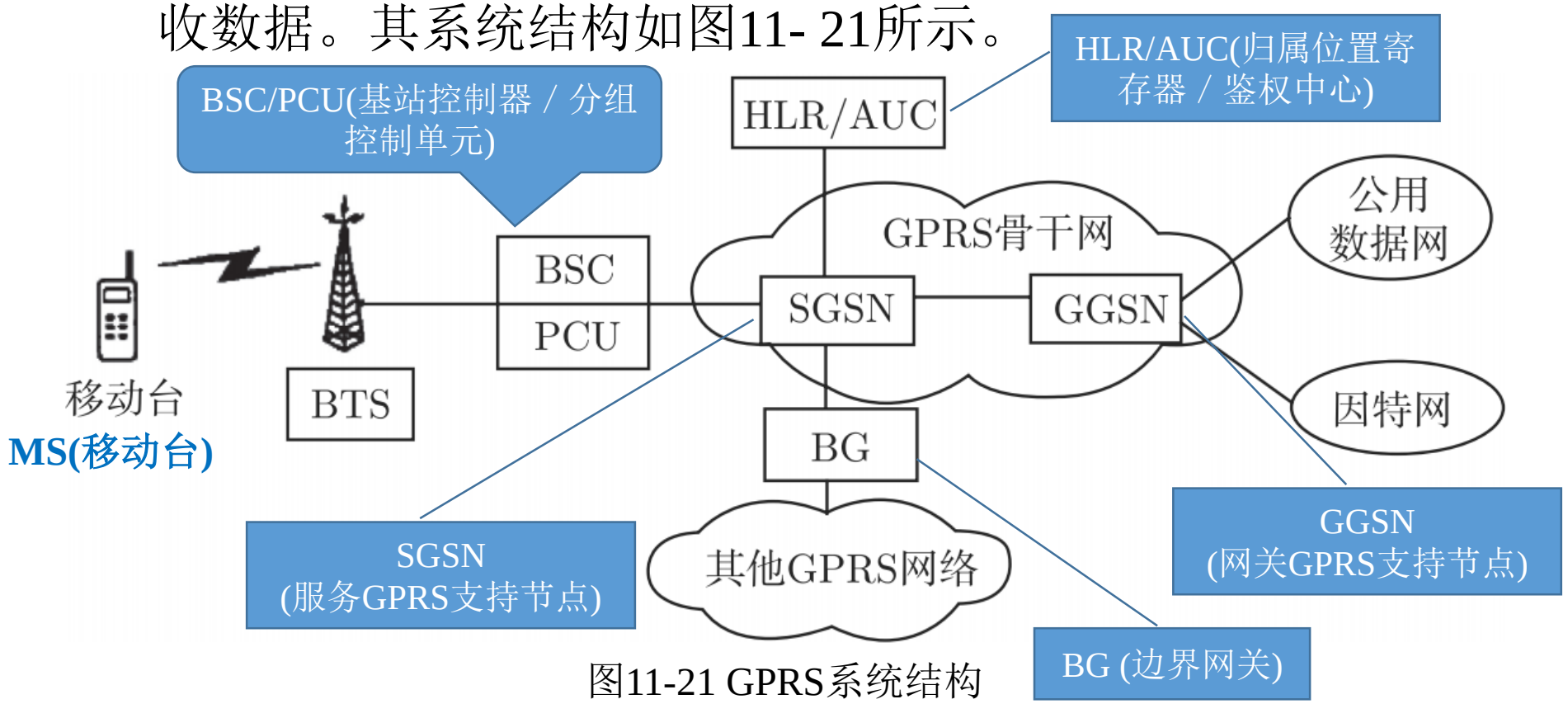


图11-21 GPRS系统结构

GPRS系统包括下述功能单元

- MS(移动台)：支持GPRS的手机。
- BSC/PCU(基站控制器 / 分组控制单元)：主要用于完成无线链路控制，并且实现与 SGSN的通信接口。
- HLR/AUC(归属位置寄存器 / 鉴权中心)：存放包括用户私钥在内的用户签约数据，产生认证消息及会话密钥。
- SGSN(服务GPRS支持节点)：SGSN是GPRS网络的主要组成部分，与MSC(移动交换中心)处于网络体系的同一层，执行移动台注册、移动性管理、安全功能、接入控制及路由选择功能。
- GGSN(网关GPRS支持节点)：GGSN是连接GPRS网络和外部分组交换数据网的网关。GGSN与SGSN的通信是通过基于IP协议的GPRS骨干网进行的。GGSN可以把 GPRS网中的GPRS分组数据包进行协议转换，从而可以把这些分组数据包传送到远端的 TCP/IP或X.25网络。另外，GGSN还提供必要的网间安全机制（如防火墙）。
- BG（边界网关）：边界网关用于不同GPRS骨干网的互联，执行运营商之间的漫游协定，并具有基本的安全功能。

GPRS业务的基本流程

- 电脑或其他数据设备通过串行或无线方式连接到GPRS移动台上；
- GPRS移动台与基站通信，但与电路交换式数据呼叫不同，GPRS分组是从基站经分组控制单元处理后发送到SGSN，而不是通过移动交换中心连接到语音网络上；
- SGSN与 GGSN进行通信，GGSN对分组数据进行相应的处理，再发送到目的网络，如因特网或X.25网络；来自因特网且标识有移动台地址的IP包，由GGSN接收，再转发到SGSN，继而传送到移动台上。

2.GPRS网络的安全机制

- GPRS提供的安全特征与GSM非常类似，包括身份标识保密、身份认证、用户数据加密、信令数据加密以及利用硬件存储用户的私钥。由于GPRS的骨干网是IP网，因此GPRS的骨干网可以利用GSM标准之外的安全机制。

1) GPRS网络的安全机制

- GPRS系统的身份认证由移动台、SGSN和HLR/AUC共同完成，认证是基于移动台和 HLR/AUC之间的共享密钥K_i。
- 认证过程如图11-22所示。

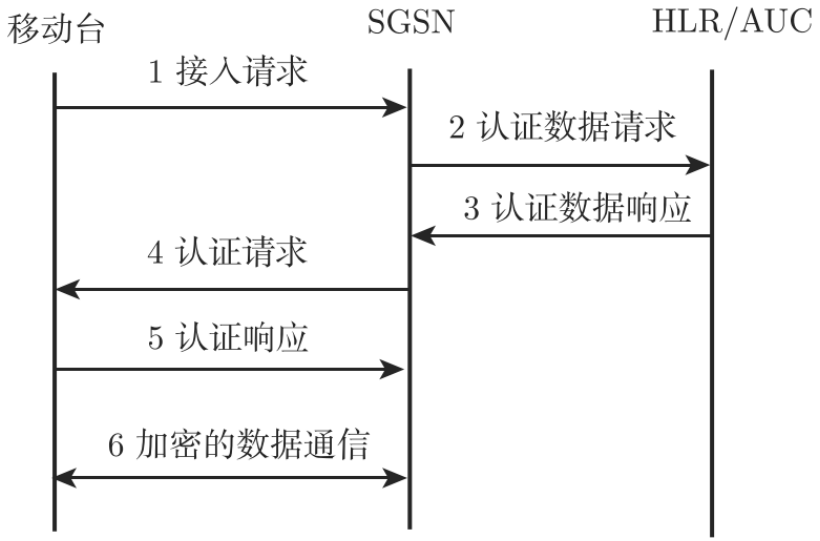


图11-22 GPRS系统的认证过程

2.GPRS网络的安全机制—2)信令数据和用户数据加密

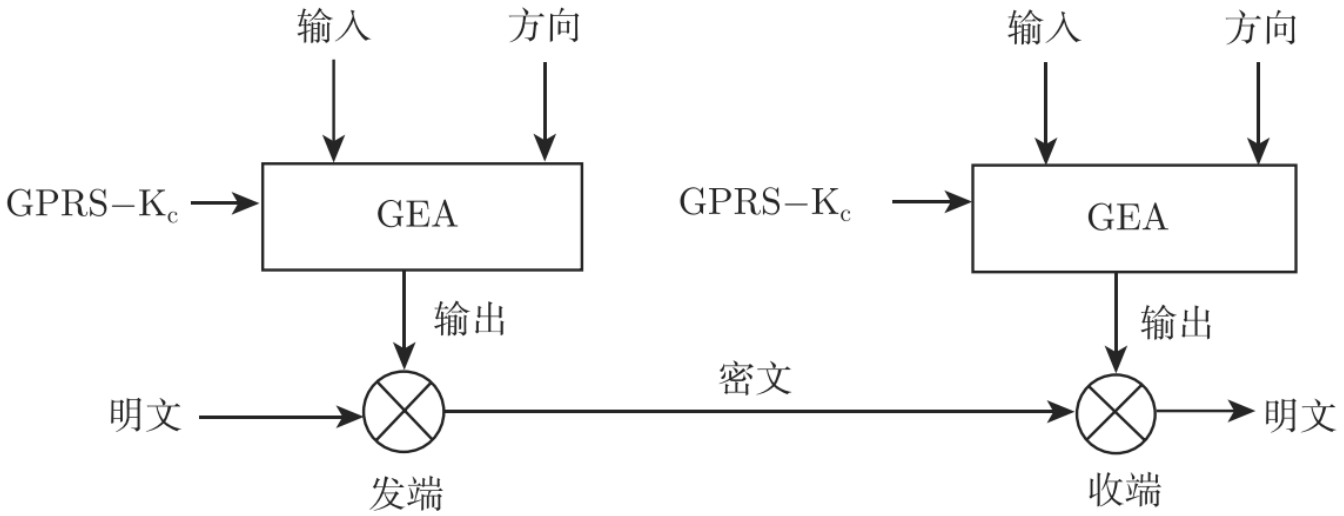


图11-23 加密和解密流程

- 发送端通过GEA算法产生密钥流，密钥流与要发送的明文消息逐比特异或产生密文，完成加密过程。密文传到接收端后，由接收端先通过GEA算法产生密钥流，然后与接收到的密文逐比特异或产生明文，完成解密过程。GPRS规范中定义的加密算法有两个：GEA1和GEA2，都是保密的。

2.GPRS网络的安全机制— 3)身份保密

- 身份保密的目的是保护用户的隐私，使攻击者不能根据手机到基站的无线链路上的数据或从基站到SGSN的数据链路上的数据识别出用户。

- 作为用户标识的国际移动用户标识码(IMSI)应尽量少用，而以临时逻辑链路标识(TLLI)代替。TLLI与路由区域标识(RAI)一起使用，可以唯一确定用户。
- TLLI与IMSI的关系由SGSN中的数据库保存。

2.GPRS网络的安全机制— 4) SIM卡的使用

- GPRS系统的用户终端利用SIM卡保存用户信息，包括用户的密钥K_i及国际移动用户标识IMSI。
- **SIM卡实质上是一个智能卡，卡中实现了A3、A8和GEA算法**，与安全相关的运算都在SIM卡中进行，以防止密钥的泄露。
- 认证中心在用户注册时，将用户的密钥K_i和IMSI分配给用户并装入到SIM卡中，并同时存入AUC的数据库中。
- K_i只在SIM卡和 AUC中使用，永远不会在网络中传输，可以有效避免密钥的泄露。

3.安全缺陷分析

1)身份认证问题

- 通过SGSN对移动用户的认证，可以保证GPRS网络资源不被非授权用户使用，保护了运营商的利益。
- 但是**认证过程是单向的**，即只是网络对移动用户认证，用户对SGSN不做认证。因而可能存在攻击者利用**假的SGSN对用户进行欺骗**，让用户以为连接到了真正的GPRS网络上，这样可能使用户的敏感信息被窃取或无法正常地访问网络资源。

2)信令及数据加密问题

- GPRS系统中的加密范围是从移动台到SGSN，不提供端到端的加密。对于需要端到端安全的应用来说，必须考虑到这个因素，不能仅依赖GPRS系统的安全性，而应该在系统设计时增加端到端的安全功能。
- GPRS的安全算法也存在问题。加密算法GEA密钥长度太短，只有64比特，无法抵抗穷举攻击。
- 在电信安全领域，开放性对于加密算法的完善来说是至关重要的。然而GPRS设计委员会却将所有安全规范保密，使别的专家无法对算法进行分析评估，以及时发现其缺陷并进行修正。

3) SIM卡问题

- GSM及GPRS系统的安全性都是基于私钥密码，用户存储在SIM卡中的私钥K_i是系统安全的根本。如果SIM卡中的数据可以被复制或通过别的途径被获取，则非授权用户可以以授权用户的身份使用网络资源提供的服务，而费用却算在该授权用户的账上，这将使系统的安全性受到破坏。
- 最近，IBM的研究人员发现了SIM卡的一个漏洞，运用一种称为分割攻击的方法，可以获取SIM卡中的密钥。这种方法通过监视边信道（即加密硬件进行加密运算时，可以被监测到的与加密运算相关的信息），如电能消耗及电磁辐射，**攻击者可以在几分钟内获得SIM卡中的密钥信息**，这比攻击SIM卡中的算法或从芯片中提取密钥更简单。在此之前最有效的攻击SIM卡的方法是对卡内的算法进行密码分析，大约需要8小时。
- 当前人们正在开发基于SIM卡的应用，如电话银行和股票交易等，在这些应用中，个人信息都存放在SIM卡中，所以应用系统的开发必须考虑防止各种攻击，包括分割攻击。
- **从终端用户的角度来说，要防止别人获得自己的终端。**

4)其他安全问题

由于GPRS系统的骨干网是基于IP的网络，所以IP网络的所有安全问题在GPRS网络中仍然存在，包括来自内部的安全攻击和来自于GPRS网络相连的外部数据网络及其他 GPRS网络的威胁。

5)结论

- GPRS网络继承了GSM网络有效的安全特征，如采用身份认证、用户数据和信令数据的加密以及利用硬件存储用户的密钥等。同时GPRS网络在安全方面比GSM网络有所提高，表现在其用户数据和信令数据的加密范围比GSM网络大，降低了明文传输的范围。
- 但是GPRS网络毕竟是在GSM网络基础上通过增加特定的网络设备构建起来的，所以必然存在GSM网络在安全方面的一些缺陷，如认证是单向的，加密密钥太短。所以在利用GPRS进行安全通信时，不能只依靠GPRS系统本身的安全机制，还应在应用层上加强安全保护。在未来移动通信系统的研究和设计中，应该继承GSM、GPRS网络中有效的安全特征，并克服和改进其不足。

11.2.3 第三代移动通信系统(3G)的安全

- 3G系统的安全体系主要有两个系列：**3GPP(WCDMA)&3GPP2(cdma2000)**。

- 本节基于3GPP体制探讨3G的安全体制，重点分析3G认证与密钥分配协议和加密与完整性保护。
- 3GPP2的认证协议也采用了“请求—响应”的形式，整个认证方式与3GPP类似，但其认证是以基站为核心的，只有其增强认证和加密模式才可提供用户和网络的相互认证。

1. 3GPP安全体制的总体结构

3GPP安全体制的总体结构如图11-24所示，可分为三个层面五个部分。

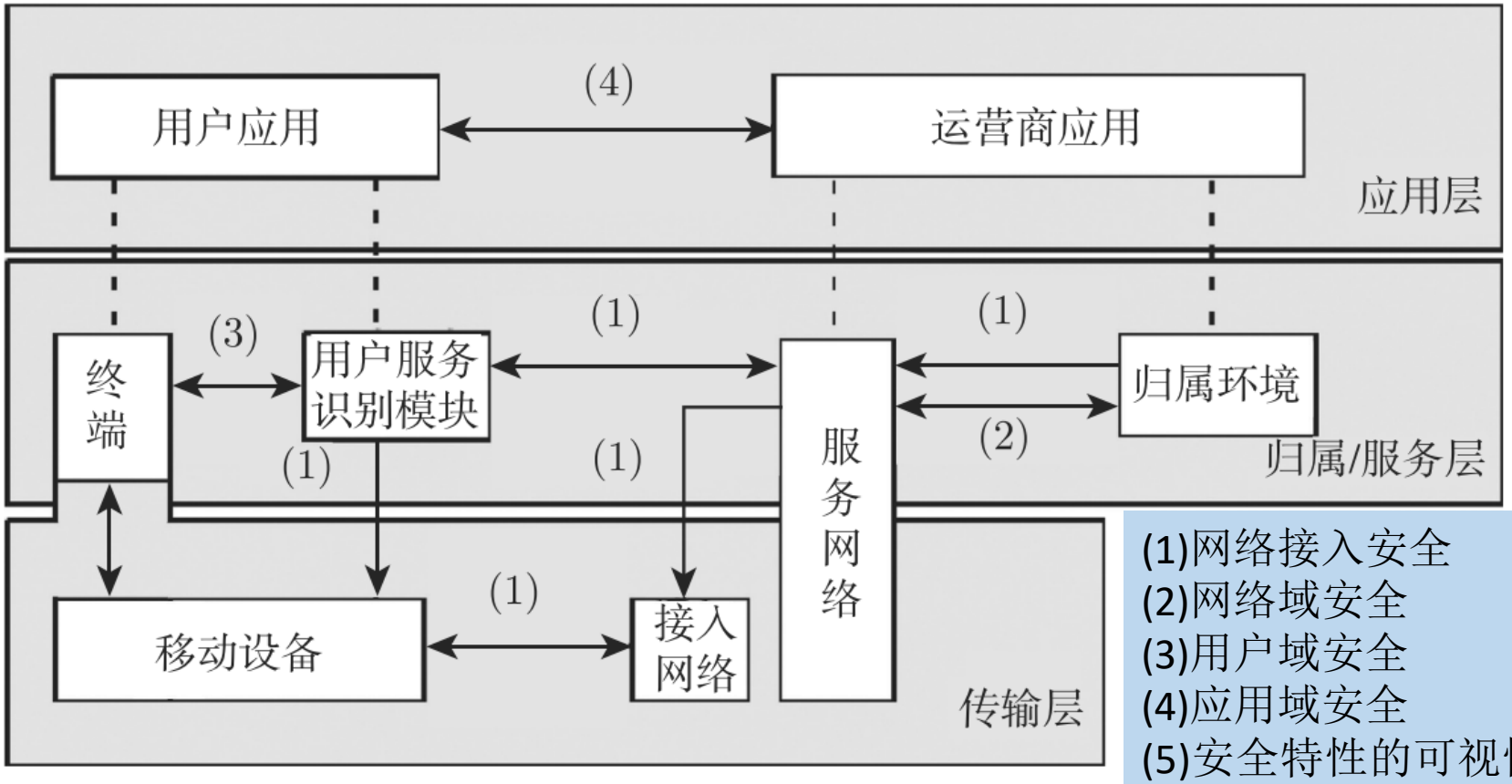


图11-24 3GPP安全体制总体结构

(1)网络接入安全
(2)网络域安全
(3)用户域安全
(4)应用域安全
(5)安全特性的可视性及可配置能力

3GPP安全体制的三个层面五个部分

- (1)**网络接入安全**：提供安全接入3G服务网的机制并抵御对无线链路的攻击。空中接口的安全性最为重要，因为无线链路最易遭受各种攻击。这一部分的功能包括：用户身份保密、认证和密钥分配、数据加密和完整性等。其中，认证和密钥分配是基于USIM和HE/AuC共享秘密信息K的相互认证。认证过程中也融合了加密、完整性保护等措施。
- (2)**网络域安全**：保证网内信令的安全传送并抵御对有线网络（核心网部分）的攻击。
- (3)**用户域安全**：主要保证对移动台的安全接入。包括用户与智能卡间的认证，智能卡与终端间的认证及其链路的保护。
- (4)**应用域安全**：使用户域与服务提供商的应用程序间能够安全地交换信息。
- (5)**安全特性的可视性及可配置能力**：主要指用户能获知安全特性是否在使用以及服务提供商提供的服务是否需要以安全服务为基础。

2.认证与密钥分配(AKA)协议

1) AKA协议过程： AKA参与方由三部分构成，即MS、VLR/SGSN、HLR。其认证与密钥分过程包括以下几个步骤：

(1)认证过程由VLR发起。首先VLR收到MS的注册请求后，向MS的HLR发送该用户的IMSI，请求对该用户进行认证。

(2)HLR收到VLR的认证请求后，生成SQN和RAND，计算认证向量***AV***，并发送给 VLR。

(3)VLR收到认证向量后，将RAND || AUTN发给MS，请求MS产生认证数据。

(4)MS接收到认证请求后，先计算XMAC并与AUTN中的MAC比较，若不同，则向 VLR发送拒绝认证消息并放弃该过程。

(5)同时MS验证接收到的SQN是否在有效的范围内，若不在有效的范围内，MS则向 VLR发送“同步失败”消息，并放弃该过程。

(6)上述两项验证通过后，MS计算RES=$f2_k$(RAND)、CK和IK，并将RES发送给 VLR。

(7) VLR接收到来自MS的RES后，将RES与认证向量***AV***中的XRES进行比较，相同则认证成功，否则认证失败。

2) AKA安全性分析

- 用户与网络之间的相互认证依赖于MS与HLR共享的秘密密钥K。AKA应达如下目标。

➢ (1)VLR对MS的认证及MS对HLR的认证：AKA第(3)步中VLR收到来自HLR的 ***AV***中包含了期望MS产生的XRES。若MS是合法用户应能正确地计算RES=$f2_k$(RAND)且RES=XRES。MS对HLR的认证是通过MAC实现的。MS收到VLR转发的来自HLR的MAC，计算XMAC=f1k(SQN || RAND || MODE)，若MAC=XMAC，则认证成功。

➢ (2)MS与VLR之间的密钥分配：AKA第(3)步中VLR收到来自HLR的AV中包含了CK_{HLR}与IK_{HLR}，合法用户在收到正确的RAND后，能正确产生CK_{m5}与IK_{m5}，且 CK_{HLR}=CK_{m5}，IK_{HLR}=IK_{m5}。CK与IK将用于其后的保密通信，而CK与IK没有在空中接口中传输，确保了密钥的安全性。

➢ (3)确保MS与VLR之间密钥的新鲜性：由于每次通信前的认证选择了不同的***AV***，保证了每次通信采用的CK与IK是由不同的RAND计算得到。而每次使用的MAC是由不断递增的SQN作为其输入变量之一，从而确保密钥的新鲜性，有效地防止了重放攻击。

3)本地认证

- AKA是基于认证向量的在USIM和HE之间的认证，适用于用户第一次登录时的情况。
- 在线用户发出服务请求、位置更新或剥离网络请求时常使用另一种认证：本地认证。它使用了AKA中产生的CK与IK，认证只在USIM和VLR之间，可为用户数据提供完整性保护。
- 这样做的好处是即使HE/AUC的链路不稳定，VLR/SGSN也可为用户提供安全服务。

3.加密和完整性保护

- 认证成功后，3G系统允许对空中接口的数据进行加密和完整性保护。加密和完整性算法分别采用了KA5UMI算法中的f8和f9算法。
- 通过f8算法产生密码流分组对原始数据进行加密。若构成无线承载(radio bear)的RLC层采用非透明模式，则加密由RLC层实施；若RLC层采用透明模式，则加密由MAC层实施。
- f9算法的输入参数包括：IK、完整性序列号COUNT-1、随机数FRESH、方向比特DIRECTION和信令消息MESSAGE。
- 发送方利用f9算法计算出MAC-1，随消息一起发送出去，接收方计算XMAC-1并与收到的MAC-1相比较以验证消息的完整性。

第11章 作业

- 作业
  - 2.WEP共享密钥认证包括哪些主要步骤？
  - 5.简述CCMP的封装过程。
  - 6. 802.11i的认证过程包括哪些阶段？
  - 8.GSM安全包括哪些安全功能？
  - 9.简述3GPP安全总体结构。

- 实践（自己研究，不考核）
  - 修改无线路由器的接入密码。