第3章 无线安全通信

CHAPTER 3

由于无线通信信道具有广播特性与开放性，授权用户和非法用户都可接收到通信信号。因此，个人隐私、工业数据和商业机密等敏感信息在无线传输过程中可能受到窃听、数据篡改和干扰等攻击，导致信息泄露等严重后果，对个人、企业甚至国家造成严重损失。研究无线通信安全技术确保传输数据的保密性和可靠性，防止敏感信息被窃取和恶意干扰，能够有效维护通信网络的稳定性和安全性。

本章首先介绍了无线通信中主动和被动窃听攻击，给出典型的窃听模型，分析其对数据隐私泄露的潜在威胁。特别地，主动窃听者可以在窃听信号的同时，通过发射干扰噪声，造成合法链路的通信质量下降，甚至导致通信链路中断，进而诱使发射机进一步提高发射功率，造成更严重的数据泄露，极大地损害了通信的可靠性和安全性。此外，本章分别介绍了基于对称密钥和公钥的无线通信加密技术，阐述其在无线通信系统中应用的优缺点和适用条件。例如，对称密钥无线通信加密技术依赖于发送和接收双方共享相同的密钥来加解密通信数据，即使窃听者拦截了传输的密文，也很难在没有密钥的情况下正确提取出明文。当前常用对称加密算法主要包括数据加密标准(Data Encryption Standard，DES)和高级加密标准(Advanced Encryption Standard，AES)等，具有高效、快速的特点，适用于无线资源和处理能力有限的无线通信设备。然而，无线通信系统需要采用合适的密钥管理机制来保证密钥管理和分发的有效性和安全性，特别是在面对大规模无线网络和动态拓扑结构时，需要重点考虑密钥分发和管理所带来的网络开销。

然后，重点讨论了无线通信系统中常见的加密协议。这些协议基于复杂的加密算法以及数字签名等技术，以保护数据的真实性、机密性、完整性和可用性。加密协议设计和实现需要考虑到多种因素，包括安全性、性能、复杂性和资源消耗等。常见的加密协议包括WPA2、WPA3以及5G认证密钥协商协议。WPA2通过改进的密码保护等手段提升无线网络的安全性；WPA3在此基础上进一步增强了密码和用户隐私保护；5G认证密钥协商协议则通过先进的身份验证和密钥协商机制，确保移动通信中的数据安全和隐私保护。这些协议在安全性、性能、复杂性和资源消耗等方面各具特点，为无线通信系统提供了全面的保护。

接着，本章介绍了密钥管理的重要性以及分类，以随机性密钥管理和确定性密钥管理为例，简要说明了密钥生成、存储、更新和使用等过程，探讨了密钥管理方法应用在不同场景中的优势和缺陷。例如，在随机密钥管理中，节点通常从密钥池中随机选取一部分密钥，存储

在本地用于匹配其他节点的密钥，其特点是分配机制简单，但通常具有盲目性，且需要消耗较大的存储空间。

最后，探讨了物理层加密技术，并简要介绍了基于友好干扰和人工噪声的无线抗窃听技术。物理层安全技术作为上层加密算法的补充，具有诸多优势。一方面，密钥可以在通信双方直接生成，无须密钥管理及分发过程，降低了密钥泄露风险。另一方面，物理层密钥利用无线通信信道天然的随机特性，有效降低了密钥生成的计算复杂度。此外，信道的互易性与时变性可用于高效生成“一次一密”的动态密钥，提高无线通信的安全性能。

本章节需要重点掌握以下几个技术内容：

(1) 掌握基于对称密钥的无线通信加密技术。

(2) 了解基于公钥的无线通信加密技术及其原理。

(3) 了解无线通信加密协议的种类、特点和应用场景。

(4) 掌握无线通信中密钥管理的重要性和相关技术。

(5) 了解物理层加密技术和基于友好干扰的无线抗窃听技术的原理和应用。

3.1　无线通信中的窃听威胁

无线通信的窃听攻击是指未经授权的用户，通过截取、拦截或监听无线通信信号，以获取敏感信息或进行其他恶意活动的行为，分为被动窃听和主动窃听。一旦窃听者成功截取到通信信号，可以利用截获的通信信号发起信息篡改和恶意软件注入等恶意活动，造成用户数据(如通信内容和位置信息)泄露等安全风险。以无线传感器网络为例，窃听者可先截获传感器设备向控制中心反馈的环境监测数据，并进一步发送篡改后的数据，导致错误的监测数据和系统控制决策。图 3-1 所示的窃听模型中包括一对合法的发射端(Alice)和接收端(Bob)以及窃听者(Eve)。其中，发射端(Alice)将 K 比特的消息 $\boldsymbol{w}=[w(n)]_{1\leqslant n\leqslant K}$ 编码为 N 个码字 $\boldsymbol{X}=[X(i)]_{1\leqslant i\leqslant N}$，则接收端(Bob)接收到的信号为

$$Y(i)=G_m(i)X(i)+N_m(i) \tag{3-1}$$

而窃听者(Eve)接收到的信号则为

$$Z(i)=G_e(i)X(i)+N_e(i) \tag{3-2}$$

其中，G_m 和 G_e 表示发射端分别到接收端和窃听者的信道增益，N_m 和 N_e 表示零均值，方差分别为 σ_m^2 和 σ_e^2 的高斯白噪声。

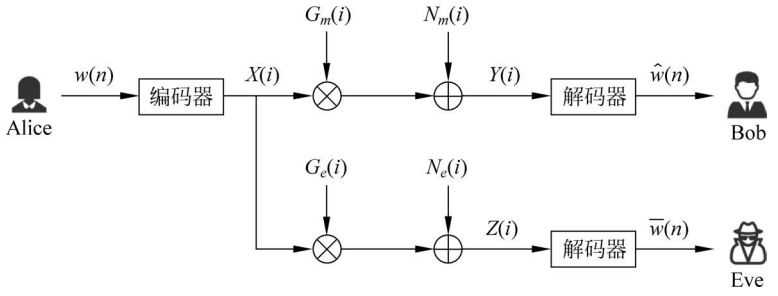

图 3-1　窃听模型

3.1.1 被动窃听

被动窃听是一种在无线通信中常见的威胁，它只对通信内容进行窃听，不会主动发起攻击。具体来说，攻击者可以在通信双方之间设置监听设备，在通信双方不知晓的情况下窃取传输的数据，隐蔽性较高。其目的是在不影响用户消息接收性能的情况下，拦截正在进行的数据传输，窃取合法通信信息。此外，被动窃听可以采用流量分析来推断通信模式和用户位置等隐私信息，并通过跟踪通信模式以促进其他形式的攻击例如重放攻击和位置追踪等。

为了有效应对被动窃听的潜在威胁，可以采取一系列解决方案。首先，利用加密技术对通信数据进行端到端加密，即使攻击者窃听无线传输过程，数据也将以加密形式呈现。因此，无法正确解码，使得敏感信息不被泄露。其次，为确保双方身份真实性和通信完整性，可以引入认证机制验证通信双方的身份，并确保通信过程未受到中间人攻击等恶意行为的影响。此外，定期对通信环境进行监测和审查，发现异常行为并及时采取应对措施也是一种有效的防御手段。

3.1.2 主动窃听

主动窃听的特点在于，攻击者不仅可以监听合法的通信内容，也可以通过发送干扰信号引诱节点执行非法操作，例如诱使目标节点提高发射功率等。与被动窃听相比，主动窃听具有更高的侵入性和破坏性，可能导致通信中断和数据篡改等严重后果。智能化的主动窃听者更可以采用多种手段先发起干扰攻击，例如采用强化学习优化其干扰的信号功率和信道，以中断合法的通信传输链路，旨在以更低的攻击成本提高合法设备的发射功率，加剧了合法通信的数据泄露，从而窃取更多数据辅助推断用户的隐私信息。

为了应对主动窃听的威胁，可以采取一系列的解决方案。首先，可以采用加密技术，防止通信数据被篡改或窃取。其次，可以进行主动窃听行为预测，具体措施包括使用频谱感知技术和信号检测机制，实时监测通信频谱中的异常信号，分析信号特征，及时发现潜在的窃听活动。最后，加强身份认证和访问控制，限制未经授权的设备接入，防止攻击者利用恶意设备进行攻击。

3.2 基于对称密钥的无线通信加密技术

基于对称密钥的无线通信加密技术是一种常见且有效的保护无线通信安全的方法，其基本原理是通信的合法双方使用相同的密钥对通信数据进行加解密。密钥的共享和管理至关重要，因为只有合法的通信双方持有相同的密钥时，才能够正常地加密和解密通信数据。

如图 3-2 所示，对称密钥加密技术是指在发射端和接收端秘密地选择共同的密钥，对消息进行加解密。加密技术能够保证进行无线通信的双方能以窃听者无法理解的方式进行数据传输。其中，Alice 在未加密的状态下传输给 Bob 的数据流通常称为明文(Plaintext)，如文字、数据或其他符号等。为了保护这些信息在传输过程中不被未授权的第三方窃取或篡改，Alice 和 Bob 共享同一把预先设定的密钥，将传输的信息转换为密文(Ciphertext)的形式，并将密文发送给 Bob。加密过程可能涉及各种算法，如对称或非对称密钥加密，这取决

于所选用的具体加密技术和协议。Eve 可以通过窃听获得 Alice 发送的密文信息，但却无法从密文中恢复出明文信息。Bob 可以使用预先设定的密钥成功解密密文，恢复出明文信息。该加解密过程可确保信息传输的机密性和安全性。

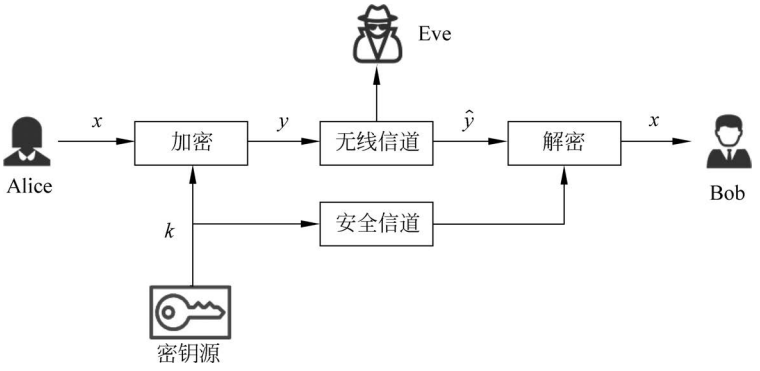

图 3-2　基于对称密钥的无线通信加密技术

基于对称密钥的技术广泛应用在无线网络标准中的数据加密领域，以保护用户数据的隐私。本节将以 AES 算法为例，介绍基于对称密钥加密算法流程。首先，AES 算法将用户数据分成长度为 128 比特的组，并在组内使用相同的密钥进行加密和解密。作为一种迭代型加密算法，AES 的可选加密轮数 R 为 10、12、14 轮，分别对应三种不同的密钥长度 128、192、256 位。具体来讲，AES 加密的迭代过程如图 3-3 所示，分为初始轮、轮函数和结尾轮。

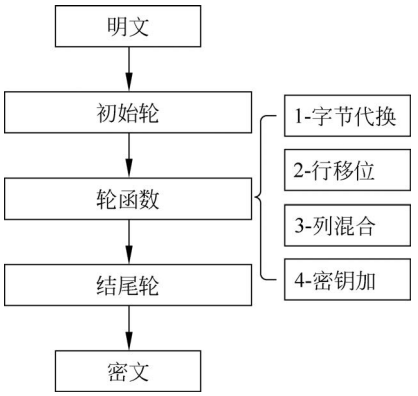

图 3-3　AES 加密过程

（1）初始轮：将数据分为大小为 128 位（16 字节）的明文块，并与轮密钥进行异或运算，轮密钥由种子密钥根据密钥编排算法得到，包含密钥扩展和轮密钥选取两个部分。

（2）轮函数：轮函数根据不同的密钥长度分别运行 $R-1$ 轮。该部分由四个不同操作过程组成，包括字节代换、行移位、列混合和密钥加。其中，字节代换操作是一种非线性变换，使用 S 盒对输入的 16 字节状态阵列进行一对一代换；行移位操作是对状态阵列的各行进行循环移位，状态阵列的行数 i 向左移位 $i-1$ 个字节；列混合操作对状态阵列的每一列进行操作，每一列都视为在 $GF(2^8)$ 上的多项式，再与多项式 $c(x)=03x^3+01x^2+01x+02$ 进行模 x^4+1 乘法；密钥加操作则是将状态阵列与轮密钥进行异或。

（3）结尾轮：该操作与轮函数部分的字节代换、行移位、密钥加一致，没有列混合操作。

总的来说，AES 加密算法通过复杂的多轮加密操作（包括字节代换、行移位、列混合和密钥加）并支持 128 位、192 位和 256 位密钥长度，确保数据难以被破解。AES 在软件和硬件实现中都非常高效，适用于低功耗设备，能快速加解密数据。AES 加密算法灵活性强，支持多种密钥长度，适应不同的安全需求，对差分和线性攻击具有强大抵抗力，可采用以下几种工作模式以适应不同场景的加密需求：

（1）电子密码本模式：将明文分成固定大小的分组（例如 128 位），然后使用相同的密钥

对每个分组进行加密。但是，该方案存在一个很严重的缺陷，在同一密钥下，相同的明文分组会生成相同的密文分组，这使得电子密码本模式不适合加密长数据或重复性高的数据。如果明文为全 0 或 1，那么电子密码本模式其实是失效的。

（2）密码分组链接模式：每个明文分组在加密前先与前一个密文分组进行异或操作，第一个明文分组使用与明文长度相同的初始向量相异或。可以看出，密码分组链接模式中前后密文的加密是存在链式关系的。具体而言，改变当前明文分组，会导致当前密文分组和之后所有密文分组发生改变，这也表明密码分组链接模式可用于产生消息认证码，使得消息接收者 Bob 可以验证传输的信息是来自发送者 Alice 且未经过篡改。也就是说可以使用密码分组链接模式保护消息的完整性。此外，密码分组链接模式中初始向量需要被保护，必须为收发双方共享，且不能被第三方预测到。

（3）输出反馈模式：在电子密码本模式中，明文分组是使用相同的密钥异或进行加密的；另一种常用的方法是使用密钥流来加密明文分组。在输出反馈模式中，当前的加密密钥由前一个加密密钥使用加密函数计算得出，然后再由加密密钥与明文异或得到密文。需要注意的是，所有的加密和解密过程都使用相同的加密函数。

3.3 基于公钥的无线通信加密技术

密钥的传输，分发和管理限制了基于对称密钥的无线通信加密技术的发展。因此，基于公钥的无线通信加密技术使用加入非对称加密算法，采用公钥和私钥用于数据的加解密过程，解决密钥分配和管理困难及开销大等的问题。其中，公钥可以公开传播，而私钥则只属于密钥的持有者。任何发送端都可以使用接收方提供的公钥来加密数据，但只有拥有相对应私钥的接收方才能正确解密数据，保证通信的机密性。

如图 3-4 所示，与基于对称密钥的加密技术相比，基于公钥的加密技术无需使用安全信道进行密钥分发，它允许通信双方进行双向通信，并用于区分窃听者和合法接收者。基于公钥的加密技术有分别用于加密和解密的两个密钥。任何用户都可以使用公钥对发送的消息进行加密，但只有持有私钥的合法接收者才能解密消息。目前主要的公钥加密体制分为：椭圆曲线密码学（Elliptic Curve Cryptography，ECC）、基于配对的密码学（Pairing-Based Cryptography，PBC）、基于大整数分解难题的 RSA 算法（由 Ron Rivest、Adi Shamir 和 Leonard Adleman 提出，RSA）和 Rabin 算法等及基于格理论的 NTRU 加密算法（Number Theory Research Unit，NTRU）等，如表 3-1 所示。其中，RSA 算法的破解难度取决于大整数分解的计算量，即将一个大的合数分解为其素数因子。随着密钥长度增加，RSA 算法被

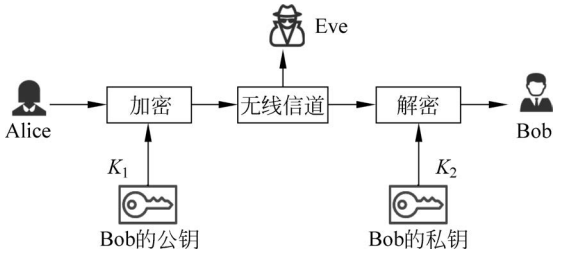

图 3-4 基于公钥的无线通信加密技术

破解的概率急剧降低，但同时也带来更多的加解密计算开销。

表 3-1　主要公钥加密体制对照表

加密体制	理论基础	速　度	主要运算
RSA	大数模余环	慢	模幂、模乘
ECC	椭圆曲线群	快	标量乘、点映射
Rabin	大数模余环	加密快	模平方
NTRU	格理论	最快	卷积
PBC	双线性对映射	最慢	对运算、点映射

3.3.1　基于大整数分解难题的加解密算法

RSA 算法由 Ron Rivest、Adi Shamir 和 Leonard Adleman 在 1977 年共同提出，RSA 的名字取自他们三人姓氏的首字母，是目前应用最广泛的公钥加密技术之一，用于保护通信安全。RSA 基于数论的加密算法，其安全性依赖于大数分解的困难性。

1. 密钥生成

选择两个大质数 p 和 q：这两个质数需要足够大，以确保 RSA 的安全性。计算两个质数的乘积 $n=p\times q$，以及 n 的欧拉值函数 $\varphi(n)=(p-1)(q-1)$。选择一整数 e，满足 $1<e<\varphi(n)$，且 $\varphi(n)$和 e 的最大公因子为 1。计算 d，满足 $d\cdot e=1 \bmod \varphi(n)$。以$\{e,n\}$为公钥，$\{d,n\}$为私钥。

2. 加密

首先将明文进行分组，使得每个分组长度小于 $\log_2 n$，然后对每个明文分组 m，计算 $c=m^e \bmod n$。

3. 解密

解密过程使用私钥$\{d,n\}$将密文 c 还原为明文 m：

$$m=c^d \bmod n$$

以质数 $p=7$ 和 $q=17$ 为例，RSA 算法的加解密流程为：首先计算 $n=p\times q$ 可得 $n=119$，$\varphi(n)=96$，选择 $e=5$，确保 e 与 $\varphi(n)$互质。根据 $d\times 17=1 \bmod 3120$，得到 $d=77$，因此公钥为$\{5,119\}$、私钥为$\{77,119\}$。当明文 $m=19$ 时，则密文为 $c=19^5 \bmod 119=66$，解密的过程为 $m=66^{77} \bmod 119=19$。

此外，RSA 也广泛应用在安全协议之中，以下将介绍其在安全套接层(Secure Sockets Layer，SSL)中的应用。安全套接层是使用最广泛的安全协议之一，提供了数据加密、源等服务身份验证和完整性保护，可以适应用于密钥协商、加密和散列的不同加密算法(这些算法的特定组合则称为密码套件)，其主要组件是握手协议和记录层协议。其中，握手协议允许客户端和服务器协商通用密码套件、相互验证并使用公钥算法建立和共享主密钥。记录层从主密钥中派生对称密钥，并将其与更快的对称密钥算法一起使用，从而进行应用程序数据的批量加密和身份验证。由于公钥操作的计算成本很高，协议设计者重用了客户端和服务器先前建立的主密钥能力，此功能也称为“会话恢复”“会话重用”或“会话缓存”。由此而产生的简短握手不涉及任何公钥加密，并且需要更少和更短的消息。

基于 RSA 的握手操作流程如下：首先，客户端和服务器交换随机数(用于重放保护)，并使用 ClientHello 和 ServerHello 消息协商密码套件。接着，服务器在服务器证书消息

(Server certificate message)中发送其签名的 RSA 公钥。客户端验证服务器的 RSA 密钥，并使用它来加密随机生成的 48 字节数字(预主密钥)，加密结果在客户端密钥交换消息中发送。服务器使用其 RSA 私钥来解密预主密钥。最后，两个端点使用预主密钥创建一个主密钥，与之前交换的随机数一起用于派生密钥、初始化向量和 MAC(消息认证码)密钥，以便记录层进行批量加密和身份验证。

3.3.2 椭圆曲线密码学

与 RSA 相比，ECC 在提供同等级别安全性的同时使用的秘钥大小更小，从而实现更快的计算。与 RSA 算法不同，ECC 对有限域上定义的椭圆曲线上的一组点进行运算。其主要加密运算是标量点乘法，计算公式为 $Q=kP$(P 点乘以整数 k 得到曲线上的另一个点 Q)。标量乘法通过点加法和点倍增法的组合来执行。例如，$11P$ 可以表示为 $11P=(2((2(2P))+P))+P$。ECC 的安全性依赖于解决椭圆曲线离散对数问题的难度，该问题指出，对于给定 P 和 Q，很难找到 k，使得 $Q=kP$。除了曲线方程之外，椭圆曲线的一个重要参数是基点 G，它对于每条曲线都是固定的。在 ECC 中，以一个较大的随机整数 k 作为私钥，而将私钥 k 与曲线基点 G 相乘的结果作为相应的公钥。

文献[13]的结果表明，使用 ECC 加解密算法可以减少服务器为新 SSL 连接处理请求的时间。对于 70 KB 的页面大小，将 ECC-160 与 RSA-1024 相比，处理时间减少了 29%；对于 10 KB 的文件大小，将 ECC-224 与 RSA-2048 相比，处理时间减少了 85%。

并非所有椭圆曲线都具有强大的安全性，对于某些曲线，椭圆曲线离散对数问题可以有效解决。由于曲线选择不当可能会危及安全性，美国国家标准与技术研究院和高效密码学标准小组等标准组织发布了一组具有必要安全属性的曲线，并建议使用这些曲线作为促进安全协议不同实现之间互操作性的一种手段。和对称密钥加密技术一样，如果密钥太短，基于公钥的加密技术也易受到穷搜索攻击。因此，密钥必须足够长才能对抗穷搜索攻击。然而，又由于公钥密码体制的计算复杂性与密钥长度常常不是呈线性关系，而是增加得更快。因此密钥太长会使得加解密运算太慢而不实用。

3.4 无线通信加密协议

无线信号传输容易受到窃听、篡改和重放攻击等威胁。加密协议可保证未经授权的个体无法获取或篡改通信内容。这些协议通常基于对称和非对称加密算法以及数字签名等技术，保护数据的真实性、保密性、完整性和可用性。无线通信加密协议的设计和实现需要考虑到多种因素，包括安全性、性能、复杂性、资源消耗等。同时，随着无线通信技术的不断发展，加密协议也需要不断升级和改进，以应对新型安全威胁和攻击手段。因此，理解和掌握无线通信加密协议的原理和应用至关重要，对于确保无线通信数据的安全性具有重要意义。

3.4.1 Wi-Fi 网络安全接入协议

有线等效加密(Wired Equivalent Privacy，WEP)由 IEEE 802.11 标准于 1997 年制定并发布，使用静态密钥来加密数据传输，并采用 CRC32 校验和初始化向量(Initialization Vector，IV)来保护传输数据的完整性。但是，WEP 存在严重的安全缺陷，如静态密钥易破

解、重用漏洞和弱加密算法等问题，使得加密的数据容易受到攻击和破解，安全性差。Wi-Fi联盟于2003年推出了WPA协议，作为对WEP的改进和替代，旨在提供更强大的加密和认证机制，以解决WEP存在的安全问题。其核心原理包括临时密钥完整性协议（Temporal Key Integrity Protocol，TKIP）、动态密钥生成、802.1X认证和消息完整性校验码（Message Integrity Code，MIC）。其中，临时密钥完整性协议采用临时密钥对数据进行加密，提高了通信的保密性；动态密钥生成机制定期更新会话密钥，增加了破解的难度，从而提高了网络的安全性；消息完整性校验码可以确保数据在传输过程中不被篡改，保证了通信的完整性。

2006年，Wi-Fi联盟进一步推出WPA2（Wi-Fi Protected Access Ⅱ）加密方案，采用更强的加密算法和协议，显著提升了无线网络的安全性。WPA2协议允许请求者（如笔记本电脑和智能手机等终端设备）与认证者（例如路由器等无线接入点）建立加密密钥，包括成对临时密钥（Pairwise Transient Key，PTK）和组临时密钥（Group Temporal Key，GTK），以便对通过网络交换的消息进行加密。在典型情况下，成对临时密钥用于保护请求者的Wi-Fi流量，组临时密钥用于保护认证者到其请求者的广播消息安全，如IP多播流量等。

WPA2密钥的建立依赖于请求者和认证者的四次握手协议：双方相互共享各自生成的随机数，并分别将两个随机数与预共享密钥相结合，以得出其成对临时密钥。认证者派生出成对临时密钥后，会与请求者共享组临时密钥。WPA2协议中区分了密钥的派生和安装：一方派生出密钥后，它就知道该密钥，但可能尚未准备好使用该密钥加密消息；只有当一方安装密钥时，该方才能使用该密钥加密消息。具体而言，在收到组临时密钥后，请求者会安装两个密钥并向认证者发送确认，认证者在收到确认后也会安装成对临时密钥。四次握手的具体执行如下：

如图3-5所示，认证者首先生成一个随机数（称为ANonce），并将其与重放计数器一起发送给请求者。请求者生成自己的新随机数SNonce，并使用密钥派生函数从预共享密钥和两个随机数中派生成对临时密钥。然后，请求者将其在消息1中收到的SNonce和重放计数器发送给认证者。为了使认证者可验证消息的完整性，消息交互过程附加了使用成对临时密钥计算的消息完整性代码。当收到消息2后，认证者会派生临时密钥并检查其消息完

图3-5　WPA2协议中四次握手示意图

整性代码，并生成加密组临时密钥，将其与递增的重放计数器和消息完整性代码一起发送给请求者。

当请求者收到消息 3 时，需要先验证消息完整性代码：如果验证成功，它会安装组临时密钥和成对临时密钥，并将成对临时密钥的随机数设置为 0 作为初始化向量。当请求者的身份验证器确认已成功安装密钥，则使用临时密钥为消息 3 的重放计数器计算消息完整性校验码，并将重放计数器和消息完整性校验码发送回身份验证器。最后，认证者安装临时密钥，握手完成。

然而 Vanhoef 和 Piessens 在 2017 年发现 WPA2 的四次握手过程很容易遭受密钥重装攻击(Key-Reinstallation Attacks，KRACK)的安全漏洞，是一种中间人攻击，这利用了最关键的四次握手协议本身，通过巧妙利用 WPA2 机制(如消息重传)，迫使一方重新使用随机数。如前所述，在未遭受攻击的四次握手中，认证者和请求者首先交换随机数，然后认证者将组临时密钥传输给请求者。然后，请求者安装成对临时密钥和组临时密钥，并向认证者确认安装，认证者反过来也会安装成对临时密钥。但如果认证者没有收到请求者的安装确认，就会出现问题。这时就需要重新传输消息：如果认证者在一定时间内没有收到安装确认，它会认为请求者没有收到上一条消息，因此会向请求者重新传输消息 3。但如果请求者确实收到了上一条消息，已经安装了密钥，在这种情况下，请求者在再次收到消息 3 后重新安装这两个密钥，从而将成对临时密钥的随机数重置为 0。如果请求者在重新安装之前使用成对临时密钥发送了加密消息，则随机数重置将导致在第二次安装后加密其他消息时重复使用随机数。因此，中间人攻击只需诱骗认证者，让其相信请求者未安装密钥，即攻击者只需阻止请求者的安装确认到达认证者即可。当认证者随后重新传输消息 3 时，攻击者会将其转发给请求者，请求者将重新安装密钥。实际上，攻击在实现上可能没有那么简单。这是因为某些请求者仅在安装了成对临时密钥后才接受加密消息，而攻击者拦截的消息 3 仍然未加密。

在密钥重装攻击出现之后，Wi-Fi 联盟进一步发布了 WPA3(Wi-Fi Protected Access 3)协议作为升级版。需要注意的是，WPA3 并没有定义新的协议。相反，它是一种认证，定义设备必须支持哪些现有协议，并且使用对等实体同时验证(Simultaneous Authentication of Equals，SAE)协议取代了 WPA2 个人版的预共享密钥认证方式来提供前向保密性和对字典攻击的抵抗力，即使攻击者知道了网络中的密码，也不能解密获取到的流量，显著提升了无线网络的安全性能。

为了兼容不同的设备，协议规定使用相同的密码同时支持两种协议，使得无线网络可以在过渡模式下运行。在此模式下，无线接入点将管理帧保护设置为可选。然后，较旧的客户端使用不带管理帧的 WPA2 进行连接，而较新的设备终端使用启用了管理帧的 WPA3 对等实体同时验证协议进行连接，但必须使用对管理帧。

由于对等实体同时验证协议握手使用了大量的复杂算法，如果攻击者不停使用大量不同的消息认证码来发送 SAE 报文，这将会频繁触发协议握手过程，耗费大量计算资源，从而达到拒绝服务攻击的目的。针对这种方式的攻击，SAE 协议规定交互报文的并发量达到一定阈值后，如果有新的握手过程，则必须同时验证协议的报文中所携带的 token 用于标示用户的唯一 MAC，否则，就拒绝协议交互，从而达到防止攻击的作用。此外，字典攻击和降级攻击将严重影响协议的安全性和可靠性，其中，字典攻击是通过捕获握手数

据并使用预生成的密码列表来猜测用户密码，特别是当无线用户使用弱密码时。降级攻击则是强制设备使用较低级别的安全协议，从而利用其已知漏洞进行攻击，这一过程主要包括：

(1) 攻击过渡模式。

在该模式下攻击者通过降级攻击修改信标诱使用户终端认为接入点仅支持 WPA2，虽然可以通过四次握手检测出来，但往往攻击者已经捕获了足够的数据来进一步执行字典攻击(只需捕获一条经过身份验证的四次握手消息就可以进一步执行字典攻击)。当攻击者获取网络的 SSID 且靠近用户终端，即可使用给定的 SSID 广播仅支持 WPA2 的网络，使得用户终端采用较低级别的安全协议连接到恶意接入点。此时，攻击者可以伪造四次握手的第一条未经身份验证的消息。作为响应，用户终端会传输经过身份验证的第二条消息。基于该握手消息，则可以成功发起字典攻击，使得用户数据泄露。

(2) 攻击 SAE 协议的协商过程。

SAE 协议握手可以使用不同的椭圆曲线或乘法组来运行，IEEE 802.11 标准允许接入点按照用户可配置的顺序进行优先排序，以提供灵活性，但用于协商所需组的机制很容易受到攻击。原因在于，用户终端需要与接入点协商用于加密所需的组，当接入点不支持该组，则用户终端需要不断与接入点协商，直到选择双方都支持的椭圆曲线加密算法。然而这一过程没有提供检测机制验证该过程是否有受到干扰，使得攻击者可以伪造接入点的协商帧，强制用户设备使用低级别加密的组，进一步发起降级攻击。

为了减轻降级攻击和字典攻击的风险，用户端设备应该记录网络是否支持 SAE 协议，当通过协议验证成功连接网络后，客户端绝不能再使用较弱的握手过程连接到该网络，例如，Linux 系统的 NetworkManager 组件和 Google Pixel 3 已经采用了类似的防御。如果客户端注意到网络不再支持 SAE 协议，应提示用户输入网络的密码，用于防止自动降级攻击，同时允许用户通过重新输入密码来增强防御。对于部分仅支持 WPA3 的无线接入点，可以在协商帧中添加数据位标志，以指示支持不同协议的设备，表明该网络无法防御降级攻击。另一种防御方法是部署单独的支持不同协议的网络并使用不同的密码，通过在四次握手期间将受支持组的信息包含在协商帧中，可以缓解降级攻击的风险。

3.4.2　蜂窝移动通信网络安全协议

LTE 是第四代移动通信网络标准，旨在提供无缝覆盖、高数据速率和低延迟的蜂窝无线通信服务。为了促进用户终端(User Equipment，UE)和分组核心网(Evolved Packet Core，EPC)之间的安全数据包交换，LTE 蜂窝网提出了演进分组系统认证及密钥协商协议，用于保护网络免受重定向攻击、流氓基站攻击和中间人攻击。在该协议中，用户终端和分组核心网之间调用了双向身份验证过程，负责生成加密密钥(Ciphering Key，CK)和完整性密钥(Integrity Key，IK)。加密密钥和完整性密钥都用于数据加密和完整性检查，以增强 LTE 传输的机密性和完整性。图 3-6 显示了采用演进分组系统认证及密钥协商协议的 LTE 双向身份验证过程，用户终端和 LTE 网络应验证彼此的身份。

具体来说，分组核心网中的移动性管理实体首先向用户终端发送用户身份请求，用户终端回复其唯一的国际移动用户识别码。接着，移动性管理实体向归属用户服务器发送认证数据请求，其中包括用户终端的国际移动用户识别码和服务网络的身份。归属用户服务器

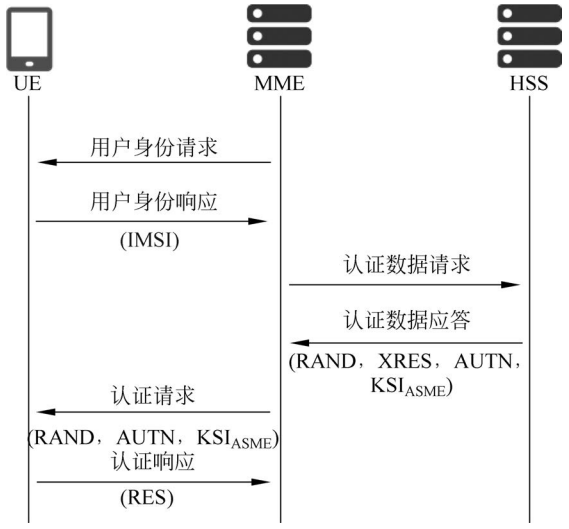

图 3-6　使用 EPS-AKA 协议在 LTE 中进行双向身份验证

收到请求后，通过返回包含输入随机参数 RAND、认证算法在 LTE 网络侧的输出 XRES、网络授权机构的标识 AUTN、接入安全管理实体的密钥集标识 KSI_{ASME} 的演进分组系统认证向量来响应移动性管理实体，然后，移动性管理实体向用户终端发送包含输入随机参数、网络授权机构的标识和接入安全管理实体的密钥集标识的认证请求。用户终端检查其接收到的参数以验证 LTE 网络，如果网络认证成功，则用户终端生成响应 RES 并发送给移动性管理实体。移动性管理实体将认证算法在 LTE 网络侧的输出与用户终端生成响应进行比较，如果相同则意味着用户终端也通过了认证。

第五代(5G)移动通信系统的认证密钥协商协议(Authentication and Key Agreement，AKA)引入了公钥加密隐藏订阅永久标识符，从而增强移动用户的隐私保护。然而，认证密钥协商协议仅在被动攻击者存在的情况下才能够保护隐私，并且仍然容易受到主动攻击者的链接攻击。主动攻击者可以通过执行这些攻击来跟踪目标手机，这会危及用户的隐私安全。因此，3GPP 更新了认证密钥协商协议，使用户终端和归属网络能够相互身份验证，并为后续程序建立锚密钥。

与之前的协议相比，5G 认证密钥协商协议在保护用户隐私方面取得了进展，例如禁止以不安全的明文形式传输用户永久标识符。当订阅永久标识符通过无线电发送时，必须使用归属网络的公钥通过椭圆曲线集成加密算法加密订阅永久标识符，使得只能监控无线流量的窃听攻击者既无法以明文形式访问订阅永久标识符，也无法通过订阅永久标识符在认证密钥协商协议会话中跟踪用户终端。然而，最近的研究发现协议仍然容易受到流氓基站等主动攻击，造成严重的隐私泄露。具体来说，攻击者通过重放来自其先前参加的认证密钥协商协议会话的消息，将目标用户终端与其先前的认证密钥协商协议会话链接起来，以达到监视或跟踪目标用户终端的目的，甚至可以推断出用户的真实身份。

此外，攻击者可以在不同代的移动通信协议跟踪目标用户终端。例如，在 5G 中将目标用户终端与其 4G 认证密钥协商协议的会话关联起来。更具体地说，跨协议可链接性攻击首先捕获目标用户终端的 4G 认证密钥协商协议会话，包括其订阅永久标识符等，然后对攻击区域内的所有用户终端发起可链接性攻击，并通过其独特的响应来区分目标用户终端，使

得攻击者能够跟踪高价值目标用户(例如大使馆官员和记者),并造成 5G 认证密钥协商协议会话的订阅永久标识符泄露。

提高 5G 认证密钥协商协议的隐私性并非易事,主要原因有以下几点:首先,存在多种类型的可链接性攻击,需要"一次性"解决所有问题,所提升的效果才能令人满意。其次,提议的修复方案必须与 3GPP 当前的 5G 网络规范(如 TS 31.102 定义的 SIM 卡命令)兼容。最后,除了修改所有相关标准的努力之外,不兼容的方案还需要通信提供商为所有用户更换 SIM 卡,并要求所有服务网络相应地修改其实现,这将导致过高的迁移成本,使得在实际部署中非常麻烦。

3.5　无线通信秘钥管理

无线通信中的密钥管理过程涉及密钥的生成、存储、使用、备份、恢复、更新、撤销和销毁等,为用户提供身份验证、可追溯、保密性、不可否认性和数据保护等多方面的安全服务。通常,密钥管理机制需充分考虑通信节点的可用带宽、传输距离、电池寿命、计算能力以及部署环境等约束条件,满足可用性、完整性、保密性、可拓展性、有效性、连接性和抗毁性等要求。当前,根据无线网络中的密钥对称性、节点类型、网络结构以及动态性等特征,可以将密钥管理的方案分为对称和非对称密钥管理、同构和异构密钥管理、分布式和集中式密钥管理、静态和动态密钥管理以及随机和确定密钥管理。本节以随机和确定密钥管理为例,介绍密钥管理机制的基本原理。

3.5.1　随机密钥管理

在随机密钥管理中,节点通常从密钥池中随机选取一部分密钥,其特点是分配机制简单,但通常具有盲目性且需要消耗较大的存储空间。具体来说,随机密钥管理通常包括以下几个阶段:

(1) 密钥预分配阶段:每个传感器节点从一个密钥池中随机选择一定数量的密钥,并将其存储在内存中。这些密钥构成了节点的密钥环。密钥池的大小选择使得任意两个随机子集之间以一定概率共享至少一个密钥。

(2) 共享密钥发现阶段:部署后,每个节点广播其携带的密钥索引,以便邻近节点发现是否存在共享的密钥。如果存在共享密钥,则使用该密钥来保护与广播节点的通信。

(3) 路径密钥建立阶段:如果两个邻近节点没有共享密钥,它们可以通过安全的方式协商一个共同的密钥。此过程利用了已经建立的安全链接来传递密钥信息。此外,在实际的无线传感器网络中,随机密钥的分发与管理可以根据节点位置、网络拓扑和节点分组管理等信息进一步提高网络连接性并降低资源开销。例如,在无线传感器网络的部署过程中,节点的最终驻留位置可能遵循某种概率分布(如高斯或泊松分布等)。因此,可以预测节点之间的距离和连通概率,从而在密钥选择阶段提高邻近节点分配相同共享密钥的概率,增强网络的整体连接性。

最经典的随机密钥管理方案是由 Eschenauer L. 和 Gligor V. 在 2002 年提出的随机密钥预分配方案(E-G 方案)。在无线传感器网络中,为了确保节点之间的安全通信,通常采用预生成包含 K 个不同的密钥的密钥池。每个节点从密钥池中随机选择 k 个密钥(k 远小于

K），形成个体密钥集。当邻居节点发现彼此的密钥集有相同的密钥时，则共有密钥可作为双方的配对密钥，直接建立加密通信。当两个节点各自的密钥集中找不到可以直接共享的密钥，它们将尝试建立一个由多个中间节点组成的通信链路来进行通信，其中每一跳的链路都依赖于连续节点间的配对密钥。根据随机图理论，若任意两个节点之间至少存在一个相同密钥的概率为 p，则其与随机选取的密钥数量 k 和密钥总量 K 之间存在如下关系：

$$p = 1 - \frac{((K-k)!)^2}{(K-2k)!K!} \tag{3-3}$$

由此可见，网络的安全连通概率会受到几个因素的影响：首先是密钥池的大小，这决定了可供选择的密钥数量；其次是每个节点选择的密钥集的大小，即节点拥有的密钥数量；最后是网络的规模，也就是网络中节点的数量。

随机密钥管理增强了网络灵活性、可拓展性和安全性，即使在节点间不存在共享密钥的情况下，也可建立间接安全路径。此外，在分布式无线网络中，每个节点通过存储一定量的密钥也能够获得较高的安全连通概率。例如，从包含一万个密钥的密钥池中随机选取 75 个密钥，就可以确保任意两个节点间的安全连通概率达到 50%。此外，根据节点连接概率、密钥路径建立以及节点部署分布等先验信息，在 E-G 方案的基础上，又分别提出了 RKPS、q-Composite、CPKS 等密钥管理机制，进一步提升密钥管理效率和加密性能。

3.5.2 确定密钥管理

确定密钥管理机制通过在任意两个节点间建立起安全通信链路，保证节点间的高连通概率，相比于随机密钥管理提高了网络的安全性。特别地，针对无线传感器网络的存储空间、计算资源和能量受限等特征，基于密钥预分发机制在网络部署之前将密钥信息分发到所有传感器节点，以确保节点在无需网络拓扑知识的条件下安全通信，减少密钥存储和计算开销。然而，该机制可能存在部署灵活性低、网络可拓展性差以及抗毁能力弱等问题。

基于组合理论的确定密钥管理机制根据无线传感器网络的节点规模 N，将密钥分配视为一个组合设计问题，并采用平衡不完全区块设计（Balanced incomplete block design，BIBD）和广义角（Generalized Quadrangles，GQ）等方案使得每个传感器节点能够以均匀的方式共享密钥，从而提高任意两个节点之间共享密钥的概率。具体而言，首先确定一个满足 $n^2+n+1>N$ 的质数 n，然后生成 $n-1$ 个 n 阶的正交拉丁方矩阵。在该矩阵中，恰有 n 种不同的元素且同一行或同一列里只出现一次，该结构确保了元素的均匀分布和唯一性。然后，节点之间利用正交拉丁方矩阵中的行和列找到共享的密钥，从而实现直接的密钥共享。最后，通过 GQ 理论中的邻接结构、环结构、对称性，以及冗余连接等特性，为大规模传感器网络提供额外的连接路径和提高网络的结构复杂性来增强网络中节点之间的连通性。该方案可以保证网络中任意两个节点之间的连通概率为 1，提高密钥共享的概率和降低平均密钥路径长度。

此外，基于可信分发中心的密钥分发机制可采用伪随机数、主密钥和消息认证码等方式，为网络节点建立密钥配对以保证数据的保密性。具体来说，可信分发中心作为高度可信任的实体，负责密钥的生成、存储和分发，该过程通常依赖于严格的认证和授权流程，只有经过授权的用户或设备才能获得密钥，确保全过程的安全性和可靠性。其核心优势在于集中管理，从而简化了密钥的生命周期管理，提高了整体的效率和可控性。例如可信分发中心负责密钥的更新和撤销，在密钥过期或泄露时生成新的密钥，并更新相关记录，以防止

旧密钥的继续使用。为了确保所有操作的可追溯性，可信分发中心通常会记录详细的审计日志。

3.6　无线通信物理层加密技术

物理层加密技术作为上层加密算法的补充，具有诸多优势。首先，物理层密钥可以在通信双方直接生成，无需密钥管理及分发过程，降低了密钥泄露的风险。其次，物理层密钥利用无线信道天然的随机特性，降低了密钥生成的计算复杂度。最后，信道的互易性与时变性可用于高效生成“一次一密”的动态密钥，提高无线通信的安全性能。

Maurer 提出通过提取通信信道的共有信息生成加密密钥的方法。根据信道的短时互易性，通信双方在同一时刻测得的信道特征相同，可以作为生成密钥的随机源。进一步，利用无线信道的时变性自动更新密钥，从而降低被窃听的概率。具体来说，无线通信信道具有很好的随机性和互易性，即通信双方在同时同频工作时，上下行信道在短时间内具有相同的信道特性（信道相干时间），且随着发射机或接收机的位置而改变。而窃听者只有在非常接近合法接收者的位置（相干距离）时，才能获得相近的信道特性，这在实际系统中难以达到。当把无线信道的随机性转化为加密密钥，该密钥就具有近似“一次一密”的安全特性。另外，由于上下行通信信道的互易性，通信双方由信道特性转化出的密钥通常具有对称性，因而无需给通信双方分发对称密钥。因此，利用无线收发信机之间的多径信道特性的密钥生成方法，可以构造安全的无线保密通信系统，保护空中接口的安全。

如图 3-7 所示，基于无线信道随机性的物理层加密密钥生成技术通常包括以下 5 个步骤。

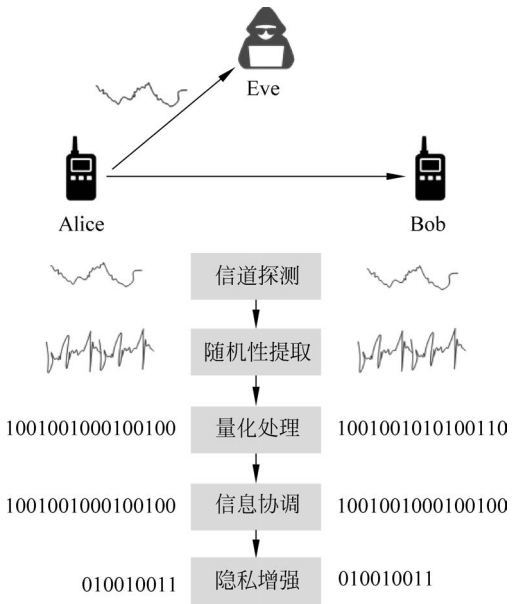

图 3-7　基于无线信道随机性的物理层密钥生成

（1）信道探测：用于测量通信双方的信道状态信息、接收信号强度或相位等信息。由于信道的互易性，通信双方在相干时间内会探测到高度相关的接收信号。

（2）随机性提取：从信道衰落中提取出随机性并去除确定性的部分，如由通信距离引起的路损，用来生成共享密钥。通常可以采用移动窗口平均法提取信道小尺度衰落随机性。

（3）量化处理：将提取的随机性信息离散化处理，便于处理和存储。

（4）信息协调：通信双方之间进行的一种纠错方式，目的是确保双方分别生成的密钥是相同的。由于无线信道的不完全互易性，量化后双方提取的比特通常不完全相同。

（5）隐私增强：用于消除关于密钥和量化比特之间的相关性的方法，该部分信息可能在信道探测或信息协调时被窃听。

3.7 基于友好干扰和人工噪声的无线抗窃听技术

无线通信的广播特性使得合法的数据传输极易受到窃听攻击，存在用户隐私泄露风险。基于友好干扰和人工噪声的抗窃听技术通过人为产生噪声信号，阻止窃听节点截获合法传输信号，从而降低数据泄露风险，增强系统的安全性。抗窃听系统的安全性一般由保密速率衡量，定义为合法传输速率和窃听速率的差值。1949 年，克劳德·香农为秘密通信的研究奠定了理论基础，其研究表明，如果窃听者可以访问与接收者完全相同的信息（除了加密密钥），只有当密钥长度至少与保密信息一样大时，才能实现完美的保密。Csiszár 等则进一步证明了如果窃听者的信道容量小于收发机之间的信道容量，则保密通信是可实现的。但是，如果窃听者拥有比接收机更好的信道条件，例如窃听者比接收机更靠近发射机，则保密能力可能为零，但这并不意味着不能实现保密通信。例如，发射机可以通过发送人工噪声来降低窃听者截获到的数据质量。

3.7.1 友好干扰

友好干扰技术通过向窃听者发射干扰信号以降低其接收信号质量，从而降低其对合法信号的解码概率，因此可以增强通信系统的安全性能。在无线通信系统中，窃听者可以截获发射机和接收机之间传输的信号，而系统中的友好干扰机则发射一串随机信号对窃听者造成干扰，以降低被截获信号的信干噪比，提高通信的隐蔽性。该随机码字可以被合法的接收者解码，并从接收到的信号中减去，但窃听者没有预先知识，因此无法解码。抗窃听系统的安全容量定义为合法信道容量和窃听信道容量的差值。虽然干扰信号会同时影响到窃听者和合法用户，但是主信道容量和窃听信道容量之间的差值可能会增大，因此可以有效提高通信的安全性。

在多用户正交频分多址保密通信系统中，可通过联合优化友好干扰的信道和发射机的功率，降低窃听者的检测性能，实现隐蔽通信。在准静态信道条件下，即信道变化缓慢且信道系数在一次传输过程中保持不变，在存在多接收器的情况下，由于在某单个频段增大传输功率会提高窃听者的检测概率，因此需要在满足隐蔽性约束的条件下分配发射机的传输功率以实现在不同频段的最佳保密通信速率。而在高动态信道状态下，即信道变化快且在一次传输过程中信道系数可能会发生多次变化，还需要进一步考虑优化用于信道估计的导频序列长度，以平衡信道估计和数据传输时间，从而在满足隐蔽性约束的条件下最大化保密通信速率。此外，友好干扰机和窃听者之间的交互过程可采用非零和博弈模型描述，其中，友好干扰机分配各个信道的干扰功率以提升网络的保密容量，而窃听者则通过选择攻击的信

道以最大化其窃听速率。该抗窃听博弈的纳什均衡表明友好干扰机和窃听者都将选择在窃听容量最高的信道上进行功率分配和攻击，而当可用的通信信道多于窃听信道时，友好干扰机可以选择攻击具有最大窃听容量的信道，以提高系统的保密速率。

为了提高友好干扰的能量效率和成功概率，干扰信号的波形设计应该考虑到实际通信系统的协议配置，如通信带宽、调制编码方式和信号的时频域结构，使干扰信号的时频带宽与发射信号的时频带宽基本匹配。特别是，当发射信号不是严格平稳的情况下，使用普通高斯噪声或自由匹配噪声作为干扰信号，干扰效率相对较低。在实际系统中，由于干扰信号的随机结构和同步偏移，往往难以实现完美的时频带宽匹配，因此，在设计干扰信号波形时可以将信号分段，并分别分析每个段的频谱特征以设计相应的匹配波形结构。例如，信号频谱的中间部分通常具有较窄的带宽，如正交振幅调制或相位键控信号中包含的同相和正交分量，可以采用平坦的电压噪声覆盖这些关键信息，增加窃听者解码的难度。而边缘部分则具有较宽的带宽可以使用高斯白噪声，在多个频率上均匀分布能量，窃听者在尝试解码时，可能会将这些噪声视为背景噪声，从而无法有效提取出有用的信号信息。

然而，友好干扰技术也存在一些难点和挑战，有待进一步研究和解决。例如，接收机的干扰信号在实际情况中通常难以被完美消除，因此同样会降低接收信号的信干噪比，导致合法通信链路的误码率增加。此外，产生干扰信号也会消耗功率资源，带来额外的系统开销。因此，通信的安全性、可靠性和系统开销之间的折中是个重要的研究问题。

3.7.2　人工噪声

基于人工噪声的物理层安全技术通过在信道中引入特定的噪声信号，以降低窃听者的接收信号质量。如图 3-8 所示，通过引入噪声信号，使得窃听者难以获取有效信息，从而保护通信内容的机密性。一般而言，噪声信号是由发送端动态生成的，并且在通信过程中不断更新，以确保安全性。具体来说，发送端生成具有随机性和复杂性的噪声信号，并将原始信息与生成的噪声信号混合后发出。接收端通过相应的解码算法将噪声信号分离出来，还原出原始信息内容。由于噪声信号的引入，即使窃听者拦截到混合了噪声的通信信号，也很难还原出有效的原始信息。

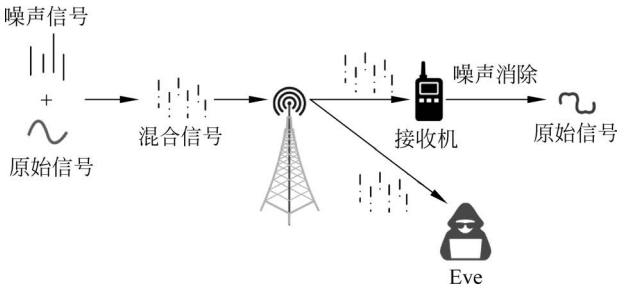

图 3-8　基于人工噪声的物理层安全技术

Goel 等研究了基于人工噪声的多天线通信系统，实现了窃听场景中的保密通信。其结果表明，当发射天线的总数超过窃听者的天线数时，无论窃听者的位置如何，即使窃听者距离发送端比接收端更近，系统均存在非零的保密速率。而在单天线通信系统中，可以通过中继节点的天线来产生人工噪声，从而提升系统安全性。具体而言，假设发射端有 N_T 个天

线，接收端有 N_R 个天线，窃听者有 N_E 个天线，$\boldsymbol{H}_k$ 表示接收端信道矩阵，$\boldsymbol{G}_k$ 是窃听者信道矩阵，则在第 k 时隙，接收端和窃听者接收到的信号分别为 $\boldsymbol{z}_k=\boldsymbol{H}_k\boldsymbol{x}_k+\boldsymbol{n}_k$ 和 $\boldsymbol{y}_k=\boldsymbol{G}_k\boldsymbol{x}_k+\boldsymbol{e}_k$，其中，$\boldsymbol{x}_k$ 是发射信号，$\boldsymbol{n}_k$ 和 $\boldsymbol{e}_k$ 分别是接收端和窃听者的高斯白噪声。

在发射端，传输的信号 $\boldsymbol{x}_k$ 是信息信号 $\boldsymbol{s}_k$ 和人工噪声 $\boldsymbol{w}_k$ 的组合，即 $\boldsymbol{x}_k=\boldsymbol{s}_k+\boldsymbol{w}_k$，其中，$\boldsymbol{s}_k$ 和 $\boldsymbol{w}_k$ 都是复高斯向量。为了确保人工噪声不会影响接收端，选择位于接收端信道 $\boldsymbol{H}_k$ 的零空间中的 $\boldsymbol{w}_k$，即 $\boldsymbol{H}_k\boldsymbol{w}_k=\boldsymbol{0}$。此时，接收端和窃听者接收到的信号分别为

$$\boldsymbol{z}_k=\boldsymbol{H}_k\boldsymbol{s}_k+\boldsymbol{n}_k \tag{3-4}$$

$$\boldsymbol{y}_k=\boldsymbol{G}_k\boldsymbol{s}_k+\boldsymbol{G}_k\boldsymbol{w}_k+\boldsymbol{e}_k \tag{3-5}$$

只有窃听者会受到人工噪声的干扰，因此，在发射端设计人工噪声信号时，需要保证接收端可以正确地消除噪声信号的影响，因此

$$\boldsymbol{x}_k=\boldsymbol{p}_k\boldsymbol{s}_k+\boldsymbol{Z}_k\boldsymbol{v}_k \tag{3-6}$$

其中，$\boldsymbol{Z}_k$ 是 $\boldsymbol{H}_k$ 零空间的正交基，则 $\boldsymbol{w}_k=\boldsymbol{Z}_k\boldsymbol{v}_k$ 即是产生的人工噪声，$\boldsymbol{p}_k$ 为权重向量。为了最大化保密容量，发射端需要进一步优化选择 $\boldsymbol{p}_k$ 使得 $\boldsymbol{H}_k\boldsymbol{p}_k\neq 0$ 且 $|\boldsymbol{p}_k|=1$。

保密容量的下界由发射端与接收端和发射端与窃听者之间的互信息差值给出

$$C_{\text{sec}}\geqslant C_{\text{sec}}^{a}=I(z;u)-I(y;u) \tag{3-7}$$

因此，可以在保证接收端通信质量的前提下，有效地干扰窃听者的信道，从而提高通信系统的保密性。进一步地，Zhou 等研究了多用户多窃听者场景，若窃听者之间是非协作的，用户间采用平均功率分配是一种简单且接近最优的策略。当窃听者的数量增加时，需要相应地提高功率来产生人工噪声。此外，当收发机之间不能准确获得完全信道状态信息时，制造更多的人工噪声来混淆窃听者比增加接收方的信号强度更高效。然而，噪声的生成会额外增加通信系统的复杂性和成本，因此需要合理设计算法和参数，以平衡安全性和性能。

3.8 本章小结

本章深入探讨了无线通信的窃听威胁和安全技术，包括加密技术、密钥管理、加密协议和物理层加密技术等方面。通过本章的学习，读者可以对无线通信安全有全面的了解，为实际应用和研究提供基础和指导。面对窃听威胁，从被动窃听到主动窃听，无线通信系统需要采取一系列措施来确保通信的安全性。对称密钥加密技术以其加密解密速度优势而受到青睐，但需要解决密钥分发和管理的复杂性；相反，基于公钥的加密技术克服了密钥分发问题，但密钥长度较长，导致处理大数据量时效率下降。此外，针对不同的无线通信协议，如 Wi-Fi 和蜂窝网络，都有专门设计的加密协议以确保其通信安全，但也存在一些劣势。例如，WEP 中静态密钥容易被破解，传输数据很容易被窃取。WPA2 提供了稳定的安全性和强大的加密性能，但其容易受到密钥重装攻击。WPA3 在此基础上加强了安全保护，采用 SAE 防止密钥重装攻击，增加了数据安全性。密钥管理方面，随机密钥管理分配机制简单，但需要较大的存储空间；确定密钥管理则提供了一种更为便捷的方法，但是该机制带来的通信和计算开销较大。物理层加密技术利用信号的物理特性来保护通信安全，虽然更难以破解，但实现复杂且可能影响通信性能。最后，基于友好干扰和人工噪声的抗窃听技术为防御窃听攻击提供了有效手段，然而也可能对通信质量和通信开销造成一定影响。在选择安全技术时，需要全面考虑各种因素，以确保无线通信系统的安全性。

习题

3-1　简要描述窃听的概念以及分类。

3-2　简要描述 AES 加密的工作原理。

3-3　相比对称密钥加密技术，公钥加密技术有何优点？

3-4　简要描述 WEP 技术的原理和缺点，以及 WPA 针对这些缺点所做的改进。

3-5　简要描述 LTE 中进行双向身份验证的过程。

3-6　简要描述 5G 认证密钥协商协议的过程。

3-7　请简述随机密钥管理的特点、优势和不足。

3-8　无线通信物理层加密技术的核心原理是什么？

3-9　多用户多天线通信系统中，基于人工噪声实现保密通信的核心前提是什么？

3-10　人工噪声的基本含义是什么？其核心设计思想是什么？

参考文献

[1] Lu. X, Xiao. L, Li. P et al. Reinforcement learning-based physical cross-layer security and privacy in 6G [J]. IEEE Communications Surveys & Tutorials. 2023, 25(1): 425-466.

[2] Douglasr. S. 密码学原理与实践[M]. 冯登国等译. 第 3 版. 北京：电子工业出版社，2016.

[3] Zou Y, Zhu J, Wang X, et al. A survey on wireless security: Technical challenges, recent advances, and future trends[J]. Proceedings of the IEEE, 2016, 104(9): 1727-1765.

[4] Smid M E, Branstad D K. Data encryption standard: Past and future[J]. Proceedings of the IEEE, 1988, 76(5): 550-559.

[5] Borisov N, Goldberg I, Wagner D. Intercepting mobile communications: The insecurity of 802.11[C]//Proceedings of the 7th Annual International Conference on Mobile Computing and Networking (MobiCom), July 16-21, 2001, Rome, Italy. New York: ACM press, 2001: 180-189.

[6] Hellman M E. An overview of public key cryptography[J]. IEEE Communications Magazine, 2002, 40(5): 42-49.

[7] Hellman M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[8] 何炎祥，孙发军，李清安，等. 无线传感器网络中公钥机制研究综述[J]. 计算机学报，2020，43(03)：381-408.

[9] 陈晓峰，王育民. 公钥密码体制研究与进展[J]. 通信学报，2004，25(8)：109-118.

[10] Boneh D. Twenty years of attacks on the RSA cryptosystem[J]. Notices of the AMS, 1999, 46(2): 203-213.

[11] 侯整风，李岚. 椭圆曲线密码系统(ECC)整体算法设计及优化研究[J]. 电子学报，2004(11)：1904-1906.

[12] Mark Stamp. 信息安全原理与实践[M]. 杜瑞颖，等译. 北京：电子工业出版社，2007.

[13] Gupta V, Stebila D, Fung S, et al. Speeding up secure web transactions using elliptic curve cryptography[C]//Proceedings of the 11th Annual Network and Distributed System Security Symposium (NDSS), California, USA. San Diego: Internet Soceity, 2004: 231-239.

[14] IEEE standard for wireless lan medium access control (MAC) and physical layer (PHY) specifications, IEEE STD 802[S]. 11-1997, +. 1-445, 1997.

[15] Cremers C, Kiesl B, Medinger N. A formal analysis of IEEE 802.11's WPA2: Countering the KRACKS caused by cracking the counters [C]//Proceedings of the 29th USENIX Security Symposium (USENIX Security 20). August 12-14, 2020, Boston, MA, USA, 2020: 1-17.

[16] Vanhoef M, Ronen E. Dragonblood: Analyzing the dragonfly handshake of WPA3 and EAP-pwd [C]//2020 IEEE Symposium on Security and Privacy (SP). IEEE, 2020: 517-533.

[17] Pinkas B, Sander T. Securing passwords against dictionary attacks[C]//Proceedings of the 9th ACM Conference on Computer and Communications Security. 2002: 161-170.

[18] Zhang Y, Weng J, Dey R, et al. Breaking secure pairing of bluetooth low energy using downgrade attacks[C]//29th USENIX Security Symposium (USENIX Security 20). 2020: 37-54.

[19] Cao J, Ma M, Li H, et al. A survey on security aspects for LTE and LTE-A networks[J]. IEEE Communications Surveys & Tutorials, 2013, 16(1): 283-302.

[20] Wang Y, Zhang Z, Xie Y. {Privacy-Preserving} and {Standard-Compatible}{AKA} Protocol for 5G [C]//30th USENIX Security Symposium (USENIX Security 21). 2021: 3595-3612.

[21] 刘彩霞，胡鑫鑫，刘树新，等. 基于 Lowe 分类法的 5G 网络 EAP-AKA'协议安全性分析[J]. 电子与信息学报，2019，41(8)：1800-1807.

[22] Basin D, Dreier J, Hirschi L, et al. A formal analysis of 5G authentication[C]//Proceedings of the 2018 ACM SIGSAC conference on computer and communications security. 2018: 1383-1396.

[23] Arapinis M, Mancini L, Ritter E, et al. New privacy issues in mobile telephony: Fix and verification [C]//Proceedings of the 2012 ACM conference on Computer and communications security. 2012: 205-216.

[24] 张国印，孙瑞华，马春光，等. 无线传感网络密钥管理及认证综述[J]. 计算机科学，2010，37(02)：1-6+11.

[25] 苏忠，林闯，封富君，等. 无线传感器网络密钥管理的方案和协议[J]. 软件学报，2007(05)：1218-1231.

[26] Hegland A M, Winjum E, Mjolsnes S F, et al. A survey of key management in ad hoc networks[J]. IEEE Communications Surveys & Tutorials, 2006, 8(3): 48-66.

[27] Xiao Y, Rayi V K, Sun B, et al. A survey of key management schemes in wireless sensor networks [J]. Computer Communications, 2007, 30(11): 2314-2341.

[28] Du W, Deng J, Han YS, et al. A key management scheme for wireless sensor networks using deployment knowledge[C]//Proceedings of the 23th IEEE International Conference on Computing and Commununications (INFOCOM), March 07-11, 2004, Hong Kong, China. Piscataway: IEEE Press, 2004. 586-597.

[29] Eschenauer L, Gligor V. A key management scheme for distributed sensor networks [C]// Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS), November 18-22, 2002, Washington DC, USA. New York: ACM press, 2002: 41-47.

[30] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks [C]// Proceedings 2003 Symposium on Security and Privacy (SP), May 11-14, 2003, California, USA. Washington: IEEE Computer Society, 2003: 197-213.

[31] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks[C]//Proceedings of the 10th ACM Conference on Computer and Communications Security (CCS), October 27-30, 2003, Washington DC, USA. New York: ACM press, 2003: 52-61.

[32] Camtepe S A, Blent Y. Combinatorial design of key distribution mechanisms for wireless sensor networks[J]. IEEE/ACM Transactions on Networking, 2007, (15)2: 346-358.

[33] Perrig A, Szewczyk R, Tygar J, et al. SPINS: Security protocols for sensor networks. [C]// Proceedings of the 7th Annual International Conference on Mobile Computing and Networking

(MobiCom), July 16-21, 2001, Rome, Italy. New York: ACM press, 2001: 189-199.

[34] 黄开枝,金梁,陈亚军,等.无线物理层密钥生成技术发展及新的挑战[J].电子与信息学报,2020,42(10):2330-2341.

[35] MAURER U M. Secret key agreement by public discussion from common information[J]. IEEE Transactions on Information Theory, 1993, 39(3): 733-742.

[36] Zeng K. Physical layer key generation in wireless networks: Challenges and opportunities[J]. IEEE Communications Magazine, 2015, 53(6): 33-39.

[37] Shannon C E. Communication theory of secrecy systems[J]. Bell System Technology Journal, 1949, 28: 656-715.

[38] Csiszár I, Korner J. Broadcast channels with confidential messages [J]. IEEE Transactions on Information Theory, 1978, 24(3): 339-348.

[39] Chen X, An J, Xiong Z, et al. Covert communications: A comprehensive survey [J]. IEEE Communications Surveys & Tutorials, 2023, 25(2): 1173-1198.

[40] Huang K W, Deng H and Wang H M. Jamming aided covert communication with multiple receivers [J]. IEEE Transactions on Wireless Communications, 2021, 20(7): 4480-4494.

[41] Xu Z, Baykal-Gürsoy M. Power allocation for cooperative jamming against a strategic eavesdropper over parallel channels [J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 846-858.

[42] Jin R, Zeng K, Zhang K, A Reassessment on Friendly Jamming Efficiency[J], IEEE Transactions on Mobile Computing, 2021, 20(1): 32-47.

[43] Goel S, Negi R. Guaranteeing secrecy using artificial noise [J]. IEEE Transactions on Wireless Communications, 2008, 7(6): 2180-2189.

[44] Zhou X, McKay M R. Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation [J]. IEEE Transactions on Vehicular Technology, 2010, 59 (8): 3831-3842.

参考答案

3-1 简要描述窃听的概念以及分类。

答：无线通信的窃听威胁指未经授权的个人或实体截取或监听无线信号以获取敏感信息或进行恶意活动。窃听分为被动和主动两种方式。被动窃听仅监听通信内容，不修改数据；主动窃听则通过发送干扰信号或引诱受害者进行恶意操作，不仅监听还可能导致通信中断和数据篡改，具有更高的侵入性和破坏性。

3-2 简要描述 AES 加密的工作原理。

答：首先，明文被分成 128 位(16 字节)块，并使用长度为 128、192 或 256 位的密钥进行密钥加，即将明文与密钥进行异或运算。然后，进入主要的加密轮次，这些轮次包括字节代换，即通过固定的 S 盒对每个字节进行非线性替换；行移位，将每行字节循环左移不同的位数；列混合，将每列数据通过固定的矩阵进行线性混淆；以及密钥加，再次将当前块与本轮密钥异或。根据密钥长度，AES-128 执行 10 轮，AES-192 执行 12 轮，AES-256 执行 14 轮，最后一轮省略列混合步骤。

3-3 相比对称密钥加密技术，公钥加密技术有何优点？

答：密钥的传输与分发限制了基于对称密钥的无线通信加密技术的发展，基于公钥的

加密技术无需使用安全信道进行密钥分发，通信双方允许双向通信用于区分窃听者和合法接收者。

3-4　简要描述 WEP 技术的原理和缺点，以及 WPA 针对这些缺点所做的改进。

答：有线等效加密（WEP）使用静态密钥、CRC 校验和初始化向量（IV）来保护数据传输，但存在严重的安全漏洞。主要问题包括静态密钥易被破解、IV 重用漏洞以及 RC4 加密算法的已知安全缺陷，这些使得攻击者可以轻松解密数据和窃取信息。

WPA 通过更强大的加密和认证机制解决了 WEP 的安全问题。其核心原理包括临时密钥完整性协议、消息完整性校验码和动态密钥生成。临时密钥完整性协议用于临时密钥加密数据，增强通信保密性；消息完整性校验码确保数据未被篡改，保障通信完整性；动态密钥生成定期更新会话密钥，提高网络安全性。

3-5　简要描述 LTE 中进行双向身份验证的过程。

答：首先，移动性管理实体向用户终端发送用户身份请求，用户终端回复其国际移动用户识别码。接着，移动性管理实体向归属用户服务器请求认证数据，该数据包含用户终端的国际移动用户识别码和服务网络身份。归属用户服务器返回包含输入随机参数 RAND、认证算法在 LTE 网络侧的输出 XRES、网络授权机构的标识 AUTN、接入安全管理实体的密钥集标识 KSI_{ASME} 的演进分组系统认证向量。然后，移动性管理实体将输入随机参数、网络授权机构的标识和接入安全管理实体的密钥集标识发送给用户终端，用户终端验证以确认网络，生成响应 RES 并发送给移动性管理实体。最后，移动性管理实体比较 LTE 网络侧的输出和用户终端生成响应，如果一致，用户终端认证通过。

3-6　简要描述 5G 认证密钥协商协议的过程。

答：在注册阶段，用户终端使用椭圆曲线集成加密算法用归属网络的公钥加密订阅永久标识符，并通过基站使用无线电信道发送用户隐藏标识符给归属网络。在 challenge-response 阶段，归属网络选择一个随机 challenge（即 RAND），并计算 AUTN。具体来说，AUTN 包含消息认证码和隐藏的归属网络序列。用户终端使用消息认证码来验证 RAND 的真实性和完整性（为简单起见，我们也说用户终端使用消息认证码来验证 RAND 的有效性），并使用归属网络序列检查 RAND。在收到（RAND，AUTN）后，用户终端首先检查消息的有效性，如果此检查失败，则返回 MAC_Failure 消息。然后，它通过比较归属网络序列和用户终端序列来检查消息，如果检查失败，则返回（Sync_Failure，AUTS）消息，其中用户终端使用 AUTS 与归属网络重新同步。当所有检查都通过后，用户终端为 RAND 生成响应，计算后续过程的锚密钥材料（K_{seaf}），并将响应发送给归属网络。当用户终端无法直接与其归属网络通信（如在漫游场景中归属网络的基站不可用）时，它可以连接到提供本地移动通信服务的服务网络。在这种情况下，通信消息是在服务网络的帮助下传输的，其中用户终端通过无线信道与服务网络的基站通信，服务网络通过 5G 核心网络提供的有线信道与归属网络通信。

3-7　请简述随机密钥管理的特点、优势和不足。

答：在随机密钥管理中，节点通常从密钥池中随机选取一部分密钥，具有分配机制简单的优势，但需要消耗较大的存储空间。随机密钥管理的特点在于通过随机生成和分配密钥来保护通信安全，这种方法具有高随机性和动态性，密钥可以定期更换，从而增强了系统的安全性和抗攻击能力。由于密钥是随机生成的，攻击者很难预测或破解，因此适用于各种网

络结构，包括集中式和分布式网络。然而，这种方法的不足之处在于管理大量随机密钥需要复杂的算法和大量计算资源，增加了系统的复杂性和通信开销。频繁更换密钥虽然提高了安全性，但也需要额外的通信来分发新密钥，增加了网络负担。同时，在分布式系统中，确保所有节点同步使用正确的密钥是一项挑战，可能导致通信中断或安全漏洞。尽管如此，随机密钥管理在提升网络安全性方面的优势仍然显著，但在实施过程中需要克服其固有的复杂性和同步问题。

3-8　无线通信物理层加密技术的核心原理是什么？

答：利用无线通信信道天然的随机特性，降低密钥生成的计算复杂度。特别是信道的互易性与时变性，可用于高效生成“一次一密”的动态密钥，提高无线通信的安全性能。具体来说，收发双方利用无线信道的独特特性，如多路径效应、衰减和噪声，生成和分配加密密钥。这种方法依赖于发送端和接收端所共享的信道状态信息，只有在同一信道内的合法通信双方才能正确解密。

3-9　多用户多天线通信系统中，基于人工噪声实现保密通信的核心前提是什么？

答：在多用户多天线通信系统中，基于人工噪声实现保密通信的核心前提是利用发射端的多天线优势，通过在信号传输过程中同时发送有用信息和人工噪声来干扰潜在的窃听者。具体而言，发射端将人工噪声投射到与合法接收者信道正交的空间，使得合法接收者能够通过其特定的信道矩阵有效地解码有用信息，而窃听者由于无法区分有用信号和人工噪声，其接收到的信号中包含大量无法消除的干扰，从而难以正确解码或理解信息。

3-10　人工噪声的基本含义是什么？其核心设计思想是什么？

答：人工噪声指的是在发射端生成具有随机性和复杂性的噪声信号，并将原始信息与生成的噪声信号混合后发出。接收端通过相应的解码算法将噪声信号分离出来，还原出原始信息内容。由于噪声信号的引入，即使窃听者拦截到混合了噪声的通信信号，也很难还原出有效的原始信息。

其核心设计思想是使产生的人工噪声位于接收机信道矩阵的零空间内，使得接收端可以完美消除噪声信号，而窃听者往往由于不满足信道矩阵的零空间的约束而无法消除噪声信号，从而达到保密通信的目的。