第5章 无人系统通信网络安全

在无人系统领域，通信网络作为连接各系统部件的生命线与核心脉络，承载着维持系统运转的重任，但这些不可或缺的信息通道正遭受持续的安全威胁。近年来，电信巨头AT&T公司被曝出数据泄露案，其中大约7300万用户的敏感数据（如账户和密码）不仅被非法泄露，而且被秘密销售多年。该事件像一颗重磅炸弹，震惊了科技界，这也提醒了我们，即便是规模庞大、技术先进的通信企业的安全防线也并非无懈可击。此外，2010年的震网蠕虫病毒攻击也是一个典型例子，它不仅针对伊朗核设施的控制系统，还对该国整体核计划的约五分之一造成了重大损害，也可通过网络传播来感染和控制网络中的各类无人设备，将传统战争的火药味带入了数字世界。因此，在设计和部署无人系统时，通信网络的安全性成为不可忽视的核心议题。这不仅仅是为了防御黑客的侵袭，更是为了保护系统的隐私、确保关键基础设施的稳定运行。在本章中，我们将详细探讨无人系统通信网络所面临的各种安全威胁，并讨论当前可行的防护措施。

本章要点

- 无人系统中通信网络的类型、典型威胁和安全挑战。
- 面向无人系统通信网络的安全认证机制与访问控制策略。
- 面向无人系统通信网络的物理层安全技术。
- 面向无人系统通信网络的入侵检测方法、系统和典型应用。

5.1 无人系统通信网络安全现状概述

5.1.1 无人系统通信网络类型

无人系统多样化的应用场景需要采用不同的通信网络结构和方案，每种通信网络类型都有其独特优势，选择合适的通信网络类型可以有效地提升系统性能和可靠性。表5-1提供了无人系统中不同类型通信网络的比较，具体介绍如下。

表 5-1 无人系统通信网络类型对比

网络类型	覆盖范围	传输速度与延迟	适用场景	优势与局限性
卫星通信网络	广泛，包括偏远和海洋区域	高速，但受信号延迟和天气影响	远程控制、长距离数据传输	覆盖广泛，但受环境影响大

续表

网络类型	覆盖范围	传输速度与延迟	适用场景	优势与局限性
Ad Hoc网络	临时部署，覆盖范围受限于节点分布	可变，依赖于节点间的连接质量	灾难救援、军事行动	灵活、自组织，但覆盖有限
移动通信网络	广泛，依赖基站分布	高速，低延迟（5G/6G）	协作无人驾驶、工业智联网	高速、低延迟，但需基础设施支持
Mesh网络	灵活，随节点增减调整	中等至高速，低延迟	无人机群编队、应急通信	自愈、可靠，但初期部署复杂
专用通信网络	根据设计定制，可高度专业化	可定制，满足特定需求	军事系统、关键基础设施	高度定制、安全，成本可能较高
地面对空通信网络	地空通信专用，覆盖范围有限	中等至高速，低延迟	无人机监测、农业监控	特定于地空，高度可靠

- 卫星通信网络：其利用地球轨道上的卫星进行信号传输，提供广泛的覆盖范围，甚至可达偏远或海洋区域。这种网络对于实现远程控制和监视、长距离数据传输至关重要，尤其适用于跨越大陆和海洋的无人系统操作。卫星通信网络可以支持高速数据传输和实时控制，但受限于卫星信号的延迟和天气条件的影响。
- Ad Hoc网络： Ad Hoc网络的灵活性和自组织特性使其成为临时或动态环境中理想的通信解决方案。不同于传统通信网络依赖固定的网络基础设施，这种网络依靠无人系统中智能体之间的直接通信，可在没有固定基础设施支持下快速建立通信，非常适合灾难救援、军事行动、野外搜寻等需要快速部署通信系统的场景。
- 移动通信网络：随着移动通信技术的迅猛发展，5G和6G可以为无人系统提供更快数据传输速度、更低传输延迟和更广网络覆盖的通信服务，能够满足如协作无人驾驶、工业智联网等针对实时数据传输和处理的无人系统应用。此外，该类网络通常具备更强的抗干扰能力和更广泛的设备兼容性。
- Mesh网络：该网络通过节点之间相互连接来提供高度稳定、可靠的数据传输服务，这对于需要在动态或不确定环境中稳定运行的无人系统尤为重要，例如无人机群的编队飞行和灾区场景下的应急通信。此外，Mesh网络的自愈特性能够确保即使部分节点失效，网络也能稳定运行。
- 专用通信网络：与公共网络不同，专用通信网络可以根据特定需求进行定制化设计，如对特定区域进行网络覆盖、为特定智能体在组织、管理等环节提供可靠的通信服务的专业网络。通常来说，该网络是为特定的任务或应用量身定制的，通过为无人系统提供定制化的功能和增强的安全性来满足如军事无人系统和关键基础设施等特定领域需求。
- 地面对空通信网络：该网络主要用于地面控制站与空中无人系统（如无人机）之间的通信，可以在空中摄影、农业监测、交通监控等领域发挥关键作用。但这类网络通常需要高度可靠和低延迟的通信链路，以确保空中无人系统实时数据交换和无人机操作安全。

5.1.2 通信网络安全威胁

无人系统通信网络中存在多种安全威胁，其可能严重影响系统正常运行和数据安全，本节主要讨论无人系统通信网络中潜在的安全威胁。

- 信息窃取与监听：这种威胁涉及未授权的第三方通过各种手段截获和监听通信数据。攻击者可能利用窃听到的信息进行间谍活动、竞争情报收集或其他恶意目的。信息窃取、干扰攻击对无人系统的机密性构成严重威胁，特别是在涉及敏感或机密数据的军事和商业应用中。
- 拒绝服务攻击：该攻击目标在于使目标网络资源无法正常访问或使用，通常通过淹没系统服务与基础设施的处理能力，导致出现过载状况。在无人系统内，此类攻击可能致使无人系统的关键通信链路中断，引发任务执行的中断甚至在关键时刻失去指挥与控制能力，从而严重威胁到操作安全与任务成功。
- 未经授权访问：未经授权的访问是指未授权的用户或系统获得对网络资源的访问权限，实现未授权控制无人系统或访问敏感数据，进而导致数据泄露、系统损害或操作失误。
- 篡改和伪造：数据篡改和伪造涉及对正在传输的数据进行未授权的修改或创建假冒通信。这种攻击可能导致无人系统做出基于错误信息的决策，引发安全事故或操作失误。
- 恶意软件：攻击者可将病毒、蠕虫、木马等恶意软件植入无人系统的通信网络中，破坏系统的正常运作。恶意软件通过创建假的通信节点或数据，以误导系统或隐藏恶意活动。这些威胁可能导致系统瘫痪、数据损失或其他严重后果。

5.1.3 通信网络安全挑战

无人系统通信网络在确保其数据及操作的安全性方面面临诸多挑战，这些挑战不仅仅局限于技术层面，还包括环境、政策规划等多方面因素。本节主要从网络安全漏洞、隐私泄露威胁、复杂多变环境、技术限制与标准化、持续威胁演进五方面来说明其面临的安全挑战。

- 网络安全漏洞：在网络设计、实施、配置阶段出现不当操作会产生未察觉的安全漏洞、弱点，这些漏洞是系统最薄弱的一环，可以被恶意攻击者所利用来实施攻击，例如数据窃取、拒绝服务攻击或更为严重的破坏性攻击行为。
- 隐私泄露威胁：无人系统成为关键性技术设施，通常需要去传输、处理大量敏感数据，包括个人信息、财务数据、甚至国家机密文件。如黑客通过发动未经授权的访问、信道窃听、隐私推理等攻击会导致严重的隐私泄露。
- 复杂多变环境：无人系统通常需要在如灾后救援、战场、极地等多变极端环境中运行，这些环境中的物理障碍、电磁干扰及不稳定的网络连接等因素，均可能对通信网络造成严重的威胁。
- 技术限制与标准化：随着技术的快速演进，新的通信技术不断涌现，然而这些新技术的安全性尚未完全被验证，同时缺少统一的安全标准。这不仅对无人系统的通信网络带来新的安全挑战，也使得设备和系统的兼容性成为一个问题。

- 持续威胁演进：网络安全的威胁是不断变化和进化的，黑客和攻击者持续开发新的攻击方法，例如高级持续性威胁、零日攻击等。这些高级威胁往往难以检测和防范，需要持续的安全监控、智能威胁分析和快速响应策略。

接下来，将详细介绍常见的无人系统通信网络安全防御措施，囊括了安全认证与访问控制、物理层安全传输、入侵检测的基本原理和技术细节。

5.2 安全认证与访问控制

安全认证与访问控制的主要目的在于保护无人系统和资源免受未经授权的访问和损害，并确保只有授权智能体能够获取所需的资源或信息，以防止未授权的访问、数据泄露和恶意攻击。具体来说，① 安全认证是确认智能体身份的过程，确保其合法性和真实性，无人系统通常通过密码、数字证书、生物特征识别等方式验证实体身份，通过认证后的智能体才能获得对系统、应用、数据的访问权限。② 访问控制是指认证成功后根据实体身份、权限等因素来管理资源的访问，以确保数据和系统的安全性。它涉及智能体可以访问哪些资源、以什么方式访问及访问资源的时间等方面的控制。在本节中，我们分别介绍针对无人系统的安全认证和访问控制的基本原理及机制设计，图5-1展示了无人系统中的安全认证与访问控制的分类。

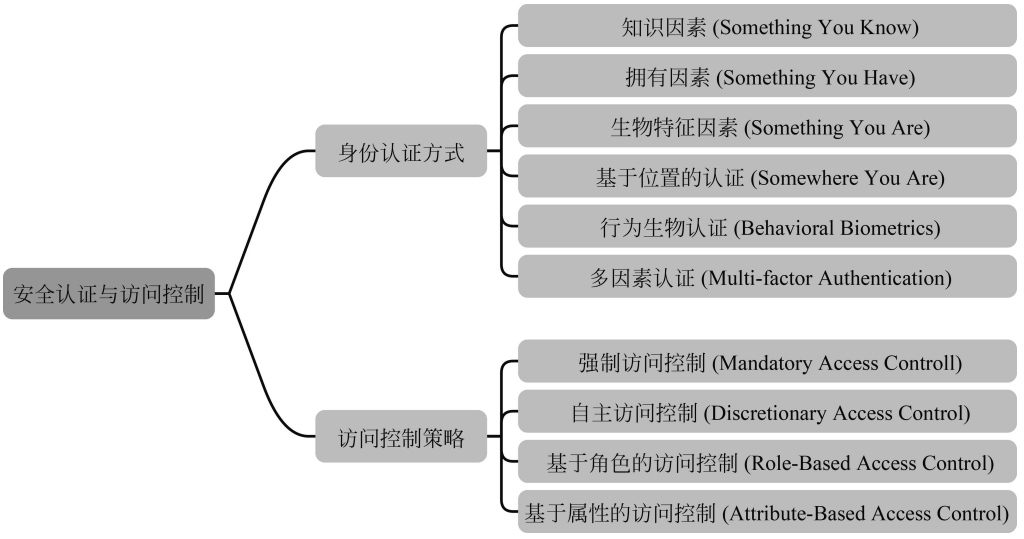


图 5-1　无人系统安全认证与访问控制分类

5.2.1 安全认证与访问控制概述

随着无人系统技术的发展，机器对人类操作的依赖正在逐步减少，智能体能够根据环境信息自主执行任务。例如，智能家居系统会自动侦测房间的温度并调整空调设定以维持舒适度，智能灌溉装置则能监测土壤湿度并据此自动进行灌溉。在这一背景下，确保无人系统中的自主行为在适当的访问控制下进行，以确保这些系统的传输安全、操作安全、数据保密性和防止未授权的访问，已成为无人系统安全领域研究的重要课题。在这个背景下，安全

认证和访问控制成了保障这些系统安全的关键技术，其中安全认证旨在确认通信双方的可信性、保障信息传输的安全及验证消息的完整性，实施身份验证、数据加密和完整性校验的措施，有效防止了信息的篡改、窃听或伪造。同时，访问控制机制通过限制对系统资源的访问，确保只有授权用户才能访问特定的数据和操作，进而提升系统的安全性和操作可靠性。无人系统可能承载着如商业机密或军事情报等敏感数据，防止未授权访问对避免这些信息泄露至关重要。引入安全认证和访问控制不仅保护了这些敏感信息和系统资源，还有效防止了恶意攻击者修改控制指令或操作逻辑，从而保障系统不被非法使用或破坏，同时减少了因误操作造成的安全事故风险。

然而，实现无人系统中的安全认证和访问控制面临诸多挑战，这些挑战源于无人系统的特性，包括系统的高度自主性、动态变化的操作环境、设备资源的限制、严格的时延要求及对灵活互操作性的需求。系统的自主性要求安全机制能在无人工干预的情况下自动执行，需要依赖于复杂的决策逻辑和自适应算法实现自主安全管理。其次，无人系统经常在动态变化的环境中运作，要求认证和访问控制机制能够适应网络拓扑和连接质量的变化，同时保持高效和可靠。此外，尤其是对于小型无人机或传感器网络而言，其计算能力、存储空间和能量供应受限，对安全认证和访问控制机制的复杂度提出了限制。另外，严格的实时性要求意味着安全认证和访问控制过程不能引入过多延迟，以免影响系统的响应速度和操作安全。最终，无人系统技术的快速发展超前于安全标准和协议的制定，不同制造商和系统采用的不同安全技术可能导致兼容性和互操作性问题，增加了实施统一安全策略的难度。

因此，设计和实施无人系统的安全认证和访问控制策略需综合考虑多种安全技术和策略，以应对不断变化的安全威胁和挑战。这要求从系统设计的初期阶段开始就将安全性作为关注的一部分，采用全面的安全架构和分层防御策略，确保无人系统在各种场景下的安全性和可靠性。

5.2.2 身份认证机制

身份认证是信息安全领域的核心技术，用来验证个体身份，确保通信或访问请求者的真实性。在网络环境中，身份认证的核心在于确认通信双方或系统中的个体（无论是人、物体还是智能体）的真实性。简单地说，身份认证旨在确保通信双方能够准确识别与其通信的另一方的身份。当在网络上进行通信时，通常需要传递一定的身份信息来识别彼此。然而，这种身份信息本身只具有识别作用，并不能直接证明信息的真实性，因为在公开网络（如互联网）上传输时，这些信息可能会遭受恶意篡改。因此，尽管无法完全阻止恶意篡改的发生，仍可以采取措施确保一旦身份信息被篡改，接收方能够轻易地发现。为了鉴别身份信息的真伪，首先必须建立对真实身份的“认识”。在网络通信中，我们可能会与陌生的实体进行交互。如何判断其身份的真伪呢？这里引入一个关键概念：信任。在网络环境下，信任并不仅仅是对某个实体可靠性的认可，而是基于双方共享的秘密信息（如密钥信息）的了解。例如，如果 Alice 和 Bob 之间共享了一个密钥，并且这个密钥的安全性得到了保证，那么它们之间就建立了相互信任的关系。如果 Alice 确信它拥有 Bob 的公钥，那么可以说 Alice 对 Bob 建立了信任，但这并不自动意味着 Bob 对 Alice 的信任。换句话说，在没有任何信任基础的情况下，通过网络建立新的信任关系是不可靠的。

对于无人系统来说，这一原理同样适用，当无人系统在执行任务时，无论是智能体之间

还是与其他无人系统进行通信，都需要通过安全的认证机制来确保通信的真实性和安全性。这通常涉及使用加密技术和密钥管理策略来建立和维护信任关系，确保无人系统能够在复杂且可能不安全的网络环境中安全高效地运行。通过这种方式，无人系统不仅能够保护自身免受未授权访问和篡改，还能够确保数据的保密性和完整性，从而提高整个系统的可靠性和效率。

安全认证技术的演进是与密码学的发展紧密相连的历史进程，从古代的简单密码学应用，经过机械加密时代的创新，到数字加密技术的兴起，再到现代复杂的认证协议和系统的建立，每一步都体现了对通信安全需求的响应和技术的进步。最初，古代密码学通过简单的替换和置换技术实现通信的保密，如凯撒密码在军事和政治通信中的应用。进入20世纪，机械加密设备的出现，例如恩尼格玛机，通过复杂的机械转轮提高了加密通信的安全性。20世纪70年代，随着计算机技术的发展，迪菲-赫尔曼密钥交换协议和RSA算法的提出标志着公钥密码学的诞生，为安全通信和认证开辟了新的途径。20世纪80年代至90年代，互联网的普及带来了对网络安全和认证协议的需求，如Kerberos、SSL和TLS等协议应运而生，提供了身份验证、密钥交换和数据加密等功能，以保护在线通信安全。进入21世纪，随着网络安全威胁的日益复杂化，现代安全认证技术如多因素认证、生物识别、基于证书的认证、单点登录和基于区块链的认证机制等被开发，以提供更高的安全性和更优的用户体验。此外，物理层安全认证技术的发展，例如基于信道特性的密钥生成技术，展示了安全认证领域向利用物理层属性进行身份验证和密钥协商方法的探索。这一发展历程不仅展示了技术进步对安全认证方法的推动，也反映了随着通信技术的演进，安全需求如何不断驱动认证技术向更高层次的发展。

认证方法可根据验证属性的差异划分为多个常见类别，包括知识要素、持有要素、生物特征要素、地理位置依赖、行为特征识别，以及多因素认证等，具体如下。

- 知识因素（Something You Know）：这类认证方法基于用户所知道的信息，如密码、PIN码或安全问题的答案，它是最传统且广泛使用的认证方式，优点在于用户容易理解和使用，并且成本低廉。然而，其安全性相对较低，因为密码和答案可能被猜测、窃听或通过社会工程学手段获得，用户还可能忘记密码，或倾向于使用简单且易于破解的密码。
- 拥有因素（Something You Have）：这种认证方式基于用户所持有的物理或数字对象，如安全令牌（如USB密钥或一次性密码生成器等物理设备）、智能卡（带有存储用户身份信息和密钥的嵌入式芯片）或基于手机的一次性密码。拥有因素提供了比知识因素更高的安全性，因为物理或数字对象更难被盗用或复制。同时，物理设备的管理和发放可以由组织控制，减少用户管理密码的负担。但是需要分发和管理物理设备，可能增加成本和用户负担，且有丢失或损坏的风险。
- 生物特征因素（Something You Are）：生物特征认证是基于用户的生理或行为特征来验证身份的方法，这些特征包括指纹、面部识别、虹膜扫描、声纹识别等生物识别信息。另外，设备指纹（识别和分析设备的特定硬件和软件配置）虽然通常不归类为生物特征，但在无人系统中可用于识别和验证设备的身份。这些特征独一无二、难以被复制或模仿，提供了高安全性的认证方式。同时生物特征绑定于个体，无法轻易转让给他人，用户也不需要记忆密码或携带物理令牌。但是生物识别数据的收集和存

储可能引发隐私问题，而且需要特定的传感器和高级算法来捕捉和分析生物特征，另外可能受动态的环境条件或变化的个体特性（如被涂装的外表）的影响。

- 基于位置的认证（Somewhere You Are）：根据用户或设备的地理位置信息来进行身份验证的方法，通过定义安全区域的虚拟边界，确认请求发起者处于特定的、预定义的安全区域内时，才允许访问系统或数据。这可以通过GPS信号确定智能体的精确位置。在室内或GPS信号不佳的环境中，也可以通过Wi-Fi接入点或蜂窝网络基站来估计位置。该方法通过结合物理位置信息，为认证过程增加了一层安全保护，同时兼具灵活性，支持定义多个安全区域以适用于不同的安全需求和场景。但可能存在位置伪造的风险，并依赖于外部服务的准确性和可用性，另外，收集和使用地理位置信息可能引发用户的隐私顾虑。
- 行为生物特征（Behavioral Biometrics）：基于用户的行为模式进行认证，包括键盘打字节奏（如分析用户在键盘上输入文字时的节奏和习惯）、鼠标移动习惯（分析用户使用鼠标时的节奏和习惯）、行走模式（如无人配送车辆中，通过识别操作员或目标接收者的步态进行身份确认）等。与传统的生物识别技术不同，行为生物特征关注于个体行为的微妙差异，提供了一种连续和动态（整个会话期间不断验证）的身份验证方法，由于每个实体的行为模式都是独特的，因而难以被他人准确复制。然而，行为模式可能受环境（如所持设备方式）等因素影响，且分析这些模式需要高度复杂的算法。
- 多因素认证（Multi-Factor Authentication，MFA）：多因素认证是一种安全机制，如图5-2所示，通过结合两个或多个不同类型的认证方法来验证用户身份，以此来提供比单一认证方法更高的安全性。例如，结合密码和手机令牌。用户首先输入密码（知识因素），然后使用手机上的认证应用生成一次性密码（拥有因素），或者指纹结合动态口令、面部识别结合行为分析等。多因素认证的优势在于，即使其中一个因素被破解，其他因素仍然可以保护系统的安全，然而，多重认证可能影响用户体验（操作复杂性）并增加实施和维护的成本。

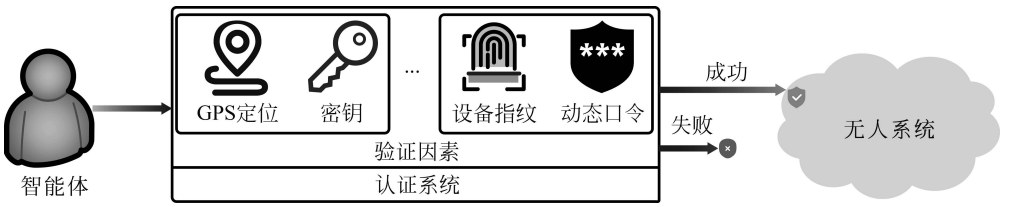


图 5-2　无人系统通信网络中多因素认证示意图

5.2.3　访问控制及其策略

无人系统中的智能体依赖于高度安全和可靠的通信网络来执行任务和交换信息，确保通信网络的安全不受未授权访问的威胁至关重要。访问控制是无人系统中数据管理中的核心组成部分，旨在保护系统资源免受未授权访问，同时确保授权用户能够访问所需资源。访问控制策略定义了谁可以访问什么资源，以及在什么条件下可以访问。通过提供灵活、高效且智能化的解决方案，访问控制技术不仅可以保护关键资源和信息系统，还能适应无人系统通信网络的特定安全需求和挑战，确保其安全运营和数据保密性。

访问控制技术的发展紧跟信息技术和网络安全的步伐，从20世纪70年代起，访问控制技术便开始从基本的自主访问控制（Discretionary Access Control，DAC）和强制访问控制（Mandatory Access Control，MAC）模型发展起来，这两种模型分别依据资源所有者的决定和预设的安全策略来执行访问权限，为早期的安全需求奠定了基础。20世纪90年代，基于角色的访问控制（Role-Based Access Control，RBAC）通过角色分配简化了权限管理，并增加了灵活性。进入21世纪，基于属性的访问控制（Attribute-Based Access Control，ABAC）通过属性和策略引入了更为动态的访问控制机制，实现精细的权限配置。

随着互联网和云计算技术的普及，访问控制技术面临新的挑战，如跨域认证和远程访问控制，促成了联邦身份管理和基于云的访问控制服务的发展，为云应用和服务提供有效的访问控制方案。最新的趋势是向智能化和自适应访问控制转变，其中人工智能和机器学习技术的集成，使系统能够基于实时的风险评估动态调整访问权限。这一转变引入了自适应访问控制和基于风险的访问控制（Risk-Based Access Control，RBAC），为应对复杂的安全威胁和满足业务需求提供了先进的解决方案。

根据访问控制决策的依据和实施机制来进行的，可以将典型的访问控制策略划分为强制访问控制、自主访问控制、基于角色的访问控制及基于属性的访问控制四个主要类别。表5-2对比了上述四类访问控制策略，具体介绍如下。

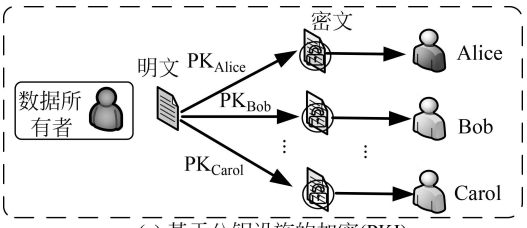
表 5-2　常见访问控制策略对比

访问控制策略	定　义	优　势	劣　势
强制访问控制	系统级安全访问策略控制，不允许无授权变更访问权限	高度安全性和机密性	灵活性低且管理复杂
自主访问控制	资源所有者或创建者控制访问权限	易于实施、灵活度高	安全依赖于个体决策、易受恶意行为影响
基于角色的访问控制	访问权基于用户的角色，角色定义了对应的权限	管理便捷、易于扩展和维护	依赖角色划分、易出现权限不合理或不精细划分
基于属性的访问控制	访问权限基于用户、资源、操作的属性和环境条件	细粒度控制、灵活度高、易于扩展及审计	策略复杂度、配置开销、维护成本高

- 强制访问控制：强制访问控制是一种由系统级安全策略控制的访问控制机制，它不允许拥有者或用户在没有管理者授权的情况下更改访问权限。在该模型中，每个实体（无人系统的设备、文件等）都被分配一个敏感度级别（如机密、秘密等），而访问这些实体的能力是基于实体的安全级别和主体（用户、程序）的访问权限来决定的。在无人系统通信网络中，强制访问策略可以通过实施集中式的安全策略，为无人机、无人车等设备分配统一的安全标签，并根据这些标签控制设备对网络资源的访问，例如只有被授权的无人机才能访问特定的导航数据或执行任务指令。由于是基于预定义的策略，强制访问控制能够有效防止未授权访问，增加系统的安全性，并且通过严格的安全标签和分类，可以防止敏感信息泄露给低安全级别的实体。但是其策略的严格性可能限制了其在快速变化的无人系统中的适应性，同时该策略需要精确管理和

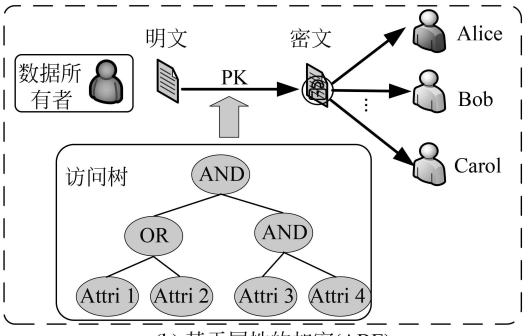
配置安全标签和策略，增加了管理的负担。

- 自主访问控制：该方式允许资源的所有者或创建者基于他们的判断自主管理、分配或撤销对资源的访问权限。例如，无人机的操作者可以决定哪些数据可以被其他无人机访问，或者哪些控制命令可以由地面站执行。在自主访问控制模型中，访问控制是通过访问控制列表实现的，其中列出了谁可以访问资源及他们可以执行的操作。相比于强制访问控制，自主访问控制更容易在多种系统和环境中实施，同时模型提供了高度的灵活性，允许用户根据需要轻松分享资源。但是，自主访问控制依赖于个体的决策（可能基于片面观察得到），可能会由于配置错误导致安全漏洞，同时资源所有者可能因不恰当地分配权限而导致不必要的访问权限扩散。
- 基于角色的访问控制：该策略涉及将访问权赋予定义明确的角色，用户通过承担一个或若干角色间接享有这些权限。例如，可以设定“飞行控制员”角色，赋予其操作无人机飞行的权限，而“数据分析师”角色则可能只有分析收集数据的权限。这样，当一个智能体被指定为某一角色时，它就自动获得了该角色对应的所有访问权限。这种模型将访问权限与角色关联起来，其依据的是用户的职责和任务，而非直接与个人身份关联。例如，文献[91]引入了基于角色的加密方法进行访问控制，只有授权用户才能解密数据。这包括高效的用户撤销和外包解密，减少计算负载。通过角色的抽象，基于角色的访问控制模型有效简化了权限的分配和管理过程，特别是在用户数量众多时。同时，通过精确定义角色和权限，可以最小化不必要的访问权限，并易于添加新角色和调整现有角色权限。但是，在复杂的无人系统中，可能需要定义大量的角色以覆盖所有访问需求，导致角色管理变得复杂，角色的泛化可能导致某些用户获得不必要的权限。
- 基于属性的访问控制：图5-3展示了基于公钥设施（Public Key Infrastructure，PKI）的加密和基于属性的加密（Attribute-Based Encryption，ABE）的区别。基于属性的访问控制根据属性和策略来控制访问，这些属性可以是用户属性、资源属性、操作属性或环境条件。该模型允许创建基于多个维度的复杂访问控制策略，提供了高度灵活和细粒度的访问控制。在无人系统中，基于属性的访问控制可以实现基于设备状态、地理位置、时间或任务类型等条件的动态访问控制。例如，只有当无人机位于特定飞行区域且在指定时间内，才允许其访问特定的导航数据。该模型具有高度灵活和动态、细粒度控制、适应性强等多个优势。具体来说，可以根据广泛的上下文信息动态调整访问权限，并允许基于复杂的规则和条件实现细粒度访问控制，同时能够适应多变的环境和需求，适用于需要高度个性化访问控制的场景。但是出于性能考虑，在每次访问决策中评估复杂的属性和规则可能影响系统性能。



(a) 基于公钥设施的加密(PKI)

图 5-3　基于 PKI 的加密和基于 ABE 的加密



(b) 基于属性的加密(ABE)

图 5-3　(续)

对于无人系统通信网络而言，选择合适的访问控制策略是确保系统安全的关键。不同的访问控制模型提供了不同层级的安全保护和灵活性。在实际应用中，可能需要根据无人系统的具体需求和安全策略，结合使用多种访问控制方法，以实现最优的安全性和操作效率。

5.3　物理层安全

构建可靠、安全的物理层传输技术是整个无人系统通信安全体系的基础，是实现通信和安全一体化的重要手段。建立在信息论基础上，物理层安全技术利用无线信道的随机性、多样性(如噪声、衰落和干扰等)来保护数据在通信介质上的传输，以防止传输过程中被未经授权者访问、篡改、截获或干扰等，其主要包括物理层安全传输、物理层密钥协商、物理层身份认证等技术手段。

5.3.1　物理层安全概述

由于无线信道的开放性和广播特性，通信网络面临着广泛且多样的安全威胁，攻击者试图截获、篡改或阻断信息传输，对通信安全构成严重挑战。为应对这类威胁，无线通信网络需满足保密性和认证两个基本的安全需求，其中保密性确保未授权者无法获取机密信息的内容，而认证则使得消息接收方能够验证信息来源的真实性，防止攻击者冒充信息源。物理层安全技术（Physical Layer Security，PLS）是基于信息论的安全理念，其利用物理层传输介质的随机性和不对称性为无人系统通信网络提供保密、可认证的数据传输。这种技术在无线通信领域，特别是在资源受限和对安全性要求极高的场景中，展现出了极大的潜力和优势。

与传统的（如对称加密和非对称加密算法等）安全措施相比，物理层安全技术具有多种优势。① 简化密钥管理：物理层安全技术不依赖于传统的密钥交换和密钥管理机制。在对称和非对称加密算法中，密钥的管理和安全交换是一个复杂和具有挑战性的问题，尤其是在动态变化的无人系统网络中。物理层安全通过利用通信信道的随机性和不可预测性来保证数据的安全性，从而避免了密钥管理的需求。② 增强安全性：物理层安全技术利用信道的不对称性（例如信道衰落和环境噪声），只有合法的接收方在特定的位置和时间才能够正确解码发送的信息。随着算力的不断提高，传统加密方法面临着窃听者利用无限计算资源进

行暴力破解或分析攻击的风险，这对任何加密系统来说都是极大的威胁。而基于物理层随机属性的安全机制，使得即使攻击者能够拦截到通信信号，也无法从中提取有用信息，因为攻击者的信道条件与合法接收方不同。③ 提升兼容性：物理层安全技术可以与传统的加密技术结合使用，提供多层次安全保护机制，该机制使得无人系统可针对具体应用和安全需求对安全技术进行定制和优化，显著增强无人系统通信网络的安全性。④ 适应动态环境：由于无人系统通常操作在动态变化的环境中，物理层安全技术能够利用这种环境的变化（如移动引起的信道变化）来增加系统的安全性。这种适应性是传统加密方法难以实现的，因为它们通常依赖于静态的、预先共享的密钥。⑤ 提升资源效率：由于物理层安全技术不依赖于复杂的加密算法，因此在处理能力有限的无人系统（如小型无人机和传感器网络）中部署时，可以减少计算资源的消耗，延长设备的运行时间。更重要的是，物理层认证能够在信号解调和解码前迅速确认合法节点，避免了对非目标传输信号的无效处理。

物理层安全作为一种关键性保障无线通信安全的方法，其研究起源和发展可以追溯到1949年，Claude Shannon在其开创性工作《通信的数学理论》[92]中提出的基于信息论的保密系统理论。他指出，安全级别取决于窃听者所掌握的信息量，当窃听者除了随机猜测之外对传输的信息一无所知时，便可实现完美的保密。尽管Shannon的工作主要集中在密码学上，但他的理论为后续的物理层安全研究奠定了基础。接着，Aaron D. Wyner在1975年[93]提出了离散无记忆窃听信道（Discrete Memoryless Wiretap Channel，DMWC）模型，该模型是物理层安全领域的基础模型之一，他的研究首次在理论上证明了，在存在窃听者的情况下也可以实现安全通信，对后续的研究产生了深远的影响。Wyner的窃听信道模型开启了利用信道编码来提高无线通信系统安全性的研究领域，激发了对广播信道、高斯信道等其他通信场景下物理层安全性能研究的广泛兴趣。20世纪80年代到21世纪初，物理层安全理论得到了进一步扩展，Imre Csiszár 和 János Körner于1983年发展了Wyner的理论，提出了更一般化的窃听信道模型，即Csiszár-Körner模型，扩展了物理层安全的理论基础。接着，Ueli Maurer等在秘密共享和公开讨论的基础上，于1993年提出了基于公共信道的密钥协商理论，这些研究为利用物理层特性进行密钥生成和安全通信提供了理论依据。21世纪初期，随着无线通信技术的迅猛发展，物理层安全开始从理论走向实践，研究者开始探索如何在实际无线网络中实现物理层安全机制，如基于信道特性的密钥生成、人工噪声干扰、波束成形技术等。2010年前后，物理层安全技术在多输入多输出（MIMO）系统、认知无线电网络、无线传感器网络等领域得到了广泛应用和研究，研究重点包括提高安全容量、设计抵抗窃听的通信策略、实现低复杂度的安全机制等。近年来，随着无人车、无人机等无人系统的蓬勃发展，物理层安全面临新的挑战和机遇，学术界和工业界仍在探索新的物理层安全机制，以适应更加复杂多变的通信环境和更高的安全需求。

当前，物理层安全的研究分为两大主流方向，分别是Wyner引导的无密钥安全模型及Maurer引导的基于无线信道的密钥机制，前者最初是由Wyner于1975年提出，这是信息论与通信安全交叉的重要里程碑。如图5-4所示，Wyner的模型考虑了一个简化三节点通信场景：发送者Alice，合法接收者Bob，以及窃听者Eve，其中Alice希望向Bob发送保密信息，而Eve试图窃听这些信息。在传输过程中存在两个信道：从Alice到Bob的主信道和从Alice到Eve的窃听信道，均假定为离散无记忆信道。

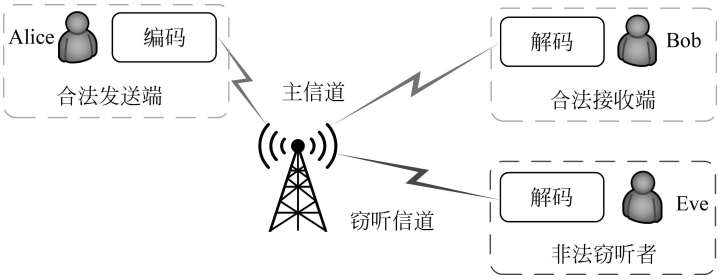


图 5-4　Wyner 窃听信道模型示意图

Wyner 的核心发现是，在某些条件下，即便 Eve 的信道条件比 Bob 更优，Alice 仍能安全地向 Bob 传输信息，无须依赖传统加密技术。此外，Wyner 引入了保密容量的概念，用以量化在确保窃听者获得的信息量趋近于零的条件下，发送者和接收者之间可以安全传输信息的最大速率。在 Wyner 的离散无记忆窃听信道模型中，保密容量 C_s 可以用以下公式来表示：

$$C_s = \max_{P_X(x)} [I(X;Y) - I(X;Z)] \tag{5.1}$$

其中，$I(X;Y)$ 表示发送者和合法接收者之间的互信息，而 $I(X;Z)$ 表示发送者和窃听者之间的互信息，分别定义为

$$I(X;Y) = \sum_{x,y} P_X(x) P_{Y|X}(y|x) \log \frac{P_{Y|X}(y|x)}{P_Y(y)} \tag{5.2}$$

$$I(X;Z) = \sum_{x,z} P_X(x) P_{Z|X}(z|x) \log \frac{P_{Z|X}(z|x)}{P_Z(z)} \tag{5.3}$$

这里，$P_Y(y)$ 和 $P_Z(z)$ 分别是合法接收者和窃听者接收到信号的边缘概率分布，它们可以通过对 $P_X(x)$ 和相应的条件概率分布进行积分或求和来计算。保密容量的推导揭示了，在保证窃听者无法获取有效信息的前提下，通过优化发送信号的概率分布 $P_X(x)$，可以最大化发送者和合法接收者之间的保密容量 C_s。

另一研究方向由 Ueli Maurer 于 1993 年提出[94]，关注的是如何在公开信道上交换信息以生成一个只有通信双方知晓的共享密钥。Maurer 的理论模型基于这样的观点：即使在公开信道上，通信双方也能通过利用信道的随机性产生共享的、对第三方保密的信息，进而生成密钥。这两大研究方向为物理层安全提供了坚实的理论基础，Wyner 的模型揭示了，即使在潜在窃听者存在的情况下也能保证通信的安全性，而 Maurer 的模型则提供了一种在公开信道上利用信道随机性和互易性的密钥生成方法，为物理层安全通信开辟了新的途径。

5.3.2　物理层通信典型攻击

由于无线信道的开放性和广播特性，使得物理层通信面临攻击多样且广泛的威胁（包括被截获、篡改或信息传输阻断等）。以下是一些物理层面临的典型攻击。

- 窃听攻击：信道窃听是最直接的物理层攻击方式之一，攻击者试图监听无线通信系统中的信号来获取传输中的敏感信息。由于无线传输的广播特性，窃听相比其他攻击实施起来更容易，同时任何处于信号传播范围内的设备理论上都能成为窃听者。另外，窃听通常不会对通信系统造成直接影响，因此攻击者可以在不被发现的情况下长时

间进行监听。

- 干扰辅助窃听：干扰辅助窃听是一种更为主动的攻击方式，攻击者旨在通过发送干扰信号来最小化保密容量，进而提高窃听能力。这种攻击融合了干扰攻击和窃听攻击，使得攻击更加隐蔽、有效。如图5-5所示，窃听者首先通过发送干扰信号来降低通信链路的质量，迫使合法通信双方采用更低的数据传输速率或者更简单的加密算法重新发送消息，从而降低通信的安全性，在这种窃听条件下，窃听者可能更容易窃听和解码通信内容。
- 假冒攻击：攻击者可能伪造大量假身份（例如女巫攻击），或通过身份盗取伪装成合法的通信实体去欺骗接收方或网络。在物理层中，这种攻击通常涉及信号的伪造（如伪造无线接入点的信号），使得用户的设备连接到攻击者控制的网络中。攻击者通过假冒身份可以实施中间人攻击、数据拦截和信息窃取等，特别是在没有介质访问控制和IP/IPv6协议的物理层，其开放性信道的使用可能导致用户更容易受到此类攻击。
- 消息伪造攻击：消息伪造攻击涉及生成和发送伪造的通信消息，目的是在不被授权的情况下影响系统的行为或获取敏感信息。在物理层，这可能涉及模拟信号或数据包的特征使其看起来像是来自合法源，在伪造的控制信号或数据的影响下，攻击者可以误导接收方执行非预期的操作或泄露敏感信息。
- 旁路攻击：该攻击也可称为侧信道攻击，其不直接针对通信信号本身，而是通过分析设备在执行加密操作时产生的物理副产品（如电磁泄漏、功耗、声音等）来获取敏感信息。这类攻击可以非常精细，甚至能够从加密设备中提取出密钥信息，这对于设计高安全性的加密算法和硬件设备提出了挑战。

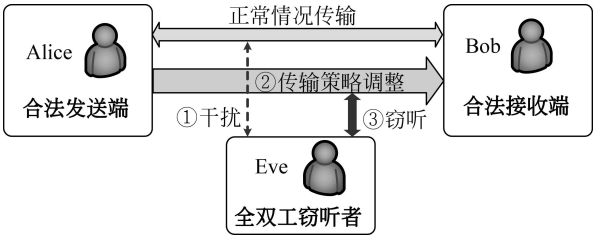


图 5-5　干扰辅助窃听攻击示意图

为应对这些威胁，物理层安全技术基于信息论理论，利用信道的随机性和不对称性为无人系统通信网络提供保密和可认证的数据传输。下面将从物理安全预编码、物理层密钥技术、物理层身份认证出发，介绍其具体防御措施。

5.3.3　物理层安全预编码技术

安全预编码技术是一种在多天线通信系统中广泛使用的信号处理技术，旨在实现多天线窃听信道的保密容量上界，其关键在于扩大合法接收者Bob和窃听者Eve之间的信号强度差异，能在有效提高信号传输的效率和质量的同时降低多用户干扰和增强信号的安全性。预编码技术利用无线信道的不对称性和随机性，基于信道状态信息来设计预编码矩阵，进而调整发射信号的传输参数（如幅度、相位和方向）。通过有意设计信号的传播路径，能确保合法接收端具有最佳的接收信号质量，同时使未授权用户（窃听者）难以接收、解码信号，从而在不依赖于传统加密算法的情况下实现通信的安全性。

根据数学处理方法的不同，可以将安全预编码技术分为线性预编码和非线性预编码两大类，如图5-6所示。

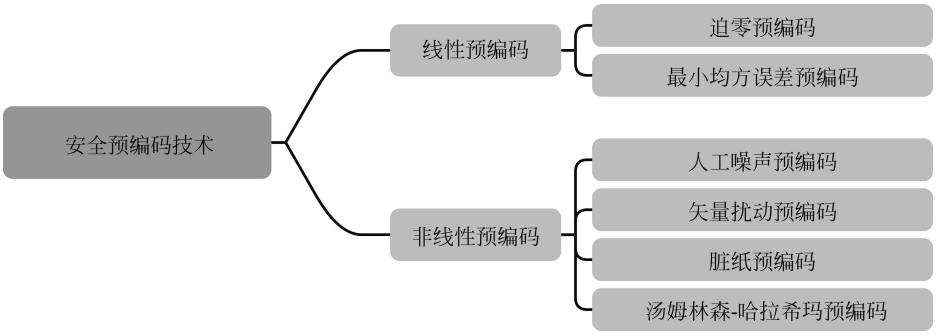


图 5-6　物理层安全预编码技术分类

（1）线性预编码技术。线性预编码是一种使用线性变换对信号进行处理的技术，在这类方法中，发送信号通过一个线性预编码矩阵进行处理，该矩阵基于信道状态信息进行设计。线性预编码的主要优点是其简单性和计算效率，特别适合于需要实时通信和大规模MIMO系统的多无人系统。代表性的线性预编码包括迫零（Zero Forcing，ZF）预编码和最小均方误差（Minimum Mean Square Error，MMSE）预编码两类。

- 迫零预编码：它通过发送端预处理信号来消除接收端信号之间的干扰，尤其是在多用户环境中。它直接反转信道矩阵，使得每个用户接收到的信号仅包含为其设计的信号成分，从而“迫使”其他用户的信号干扰为零。迫零预编码的优势在于简单直观，能够有效消除多用户干扰，但其对信道估计误差很敏感，同时可能因为信道条件不佳而放大噪声。
- 最小均方误差预编码：它旨在最小化由于噪声和干扰导致的误差平方和，这种方法在设计预编码矩阵时综合考虑了信道条件和噪声水平，以优化信号的整体性能。相比迫零预编码，最小均方误差预编码提供了更好的性能——噪声和干扰的影响能够被更有效地管理，其缺点在于计算复杂度相对迫零预编码稍高，需要更精确的信道和噪声估计。

（2）非线性预编码技术。非线性预编码采用更复杂的数学处理对信号进行预处理，能够更加有效地利用信道特性，通常提供比线性预编码更好的性能，尤其是在信号干扰和信道不确定性方面。非线性预编码方法主要包括人工噪声（Artificial Noise，AN）预编码、矢量扰动预编码（Vector Perturbation precoding，VP）、脏纸预编码（Dirty Paper Coding，DPC）、汤姆林森-哈拉希玛预编码（Tomlinson-Harashima Precoding，THP）。

- 人工噪声预编码：通过在发送信号中添加人工噪声，干扰非法接收者的信号接收，而合法接收者可以通过预先共享的信息从接收信号中去除这些噪声。人工噪声通常被添加到信号空间的一个子空间，该子空间对合法接收者是正交的，但对窃听者则不是。该方法有效地增强了通信保密性，特别是在窃听者的信道状态未知或部分未知的情况下。即使在窃听者知道预编码策略的情况下也难以解码信号。但是要求发送者有合法接收者的精确信道信息和对窃听者信道的部分知识，同时在设计阶段需要精确控制噪声的功率和分布，以免影响合法用户的信号质量。

- 矢量扰动预编码：此技术通过在发送信号中加入一个优化过的扰动向量来提升通信性能，尤其是在多用户环境中减少干扰。通常来说，扰动向量的选择是通过解决一个非线性最小化的优化问题来完成，其目标是找到一个最优的扰动向量，使得在满足功率或速率约束下，能最小化总的传输功率或最大化系统容量。这种方法能在不显著增加系统总功率的情况下，有效减少多用户干扰并提升系统容量，然而用户数量增多时，优化过程的计算复杂性也相应增加。
- 脏纸预编码：这种技术的名称来源于一个比喻，即使在已经被墨水弄脏的纸上写字，知道哪里有墨迹的人也能写出清晰的信息，不被墨迹干扰。它是一种高度非线性的编码技术，允许发送者在已知未来干扰的情况下编码信号，发送者可以预先抵消这些干扰（包括由于多用户引起的干扰和潜在的窃听者信号），从而在接收端实现无干扰的接收。这要求发送者对信道干扰有精确的知识，包括合法用户的干扰和可能的窃听者干扰。在理论上，脏纸编码能够完全抵消已知干扰，达到信道容量的上限，但其实际应用受限于较高的计算复杂度。
- 汤姆林森-哈拉希玛预编码：它是脏纸编码的扩展应用，主要用于减少或消除多用户通信系统之间的干扰，提高通信效率和安全性。该预编码的工作原理基于模块化和反馈策略，发送端在发送信号之前，先对信号进行模块化操作，通过引入一定的非线性处理来抵消或减少由于信道条件引起的干扰。这种预失真处理使得接收端更容易从叠加的信号中恢复出各自的数据流，从而提高了通信的可靠性和效率。通过减少干扰，该技术可以支持更多的用户同时通信，从而增加了系统的容量和频谱效率，但是非线性预失真处理增加了发送端的计算复杂度，同时需要有效的信道估计和反馈机制以得到准确的信道状态信息。

在通信系统设计中，选择预编码技术是优化信号质量和减少干扰的关键决策。线性预编码以其简单算法和低计算复杂度易于实现，适合计算资源受限或需快速响应的场景。相比之下，非线性预编码虽计算复杂度高，但在高信噪比环境下能显著提升性能，适用于追求高性能的应用。因此，根据系统的性能要求和计算资源可用性，合理选择预编码技术是实现性能与资源利用平衡的关键。

5.3.4 物理层密钥技术

物理层密钥技术是一种利用无线信道的不对称性和随机性（如信道状态信息、接收信号强度或相位信息）来生成安全密钥的方法，它允许通信双方在不交换任何密钥信息的情况下生成共享密钥，即使在公开信道上，窃听者也难以获得相同的密钥，能有效抵抗窃听和重放攻击。同时密钥生成基于信道的即时特性，可适用于动态和非稳定的无线通信环境，密钥可以根据信道条件的变化动态更新，提供持续的安全保护，其不依赖于复杂的密钥分发和管理架构，可有效降低系统实施成本。

如图5-7所示，物理层密钥生成的关键步骤主要包括信道探测、量化、信息协商及密钥提炼。具体而言，① 信道测量：通信双方各自测量信道特征，如信道冲激响应、信道增益等，以获取信道状态信息，这一步是利用信道的互易性，确保双方可以从各自的角度观察到相同或相似的信道特性；② 信道特征量化：该步骤将连续的信道测量值转换为离散的比特序列，由于信道测量存在噪声和设备间的微小差异，量化过程需要既能最大化保留信道随机

性，又能最小化双方量化结果的不一致性；③ 密钥一致性协商：通过信息交换和一致性协议（如信息协调和错误校正编码），双方对量化后的密钥进行协商，以确保最终生成的密钥对双方完全一致，这可能包括差错控制和校正机制来对抗信道噪声和设备差异；④ 隐私放大：通过隐私放大技术可从预共享的信息中提炼出最终的密钥，该步骤旨在减少甚至消除窃听者可能获得的任何信息，增加密钥的随机性和安全性。

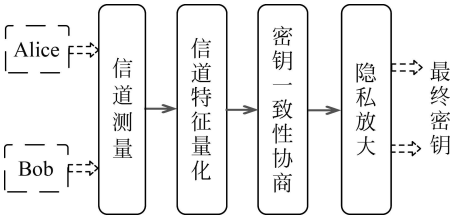


图 5-7　物理层密钥生成流程图

当完成密钥生成后，需要对生成的密钥进行随机性测试、一致性检验和性能评估，确保密钥的质量满足安全要求，评估这种技术的有效性主要依赖于几个关键指标：密钥熵、密钥生成速率、密钥误码率。具体而言，① 密钥熵是衡量密钥随机性的一个重要指标，高熵值意味着密钥的不可预测性强、难以被攻击者猜测，密钥随机性通常通过例如NIST测试套件对其进行标准的统计测试、评估；② 密钥生成速率描述了单位时间内系统能够生成的密钥位数，高密钥生成速率意味着系统能够更快地产生密钥，适应于动态变化的环境和应用；③ 密钥误码率则表示密钥一致性的准确度，即生成的密钥在通信双方之间存在不一致的概率，低密钥误码率对于保证密钥的可靠性和通信的安全性至关重要。

根据不同的随机特性，物理层密钥生成技术可以分为基于信道状态信息、基于接收信号强度、基于相位和基于窃听编码的四种主要类型的密钥生成技术。

- 基于信道状态信息的密钥生成：由于无线信道的互易性，双方经历的信道状态信息在理论上是相同的，可以用作生成共享密钥的基础。在时分双工系统中，通信双方通过测量来自对方的导频信号，获取信道状态信息。通过测量分析信道状态信息，能够精准捕捉信道的时间变化和空间特性，并生成具有高随机性的密钥。但是获取准确的信道状态信息需要复杂的信道估计技术，会增加系统的计算负担和实现成本。
- 基于接收信号强度的密钥生成：这种方法使用接收信号强度作为密钥生成的依据，接收信号强度是描述信号到达接收器时强度的指标，其易于获取且对环境的变化敏感，使其成为生成密钥的一个有效参数。然而，相较于信道状态信息，接收信号强度提供的信息量较少，会影响密钥的生成速率和安全性，并且它易受多路径效应和环境干扰的影响，进而导致密钥生成的随机性和一致性下降。
- 基于相位的密钥生成：这种技术直接利用信号的相位信息生成密钥，由于相位变化对环境变化非常敏感，这提供了一种高度随机和敏感的密钥生成手段，尤其是在高度动态的无人系统环境中。由于相位测量受到频率偏移和时间同步误差的影响，该方法的有效实施依靠高精度的相位测量和同步机制，以确保通信双方能够准确地获取相位信息。
- 基于窃听编码的密钥生成：这种方法基于窃听信道模型，通过设计特定的编码策略，即使在存在窃听者的情况下，也能在通信双方之间安全地共享密钥信息。该方法的

基本思想是，即使合法接收者的信道噪声很大，信道衰落也提供了传输少量机密比特的保密容量的机会，进而这些比特能被累积构建成一串更长的密钥序列，用于后续的安全通信。

5.3.5 物理层身份认证

认证过程的任务是验证用户和数据身份，以防恶意用户（例如，入侵者）访问网络或被授予访问机密信息的权限。物理层认证（Physical Layer Authentication, PLA）被认为是一种低计算开销的同时确保无线网络中节点和消息认证的可行手段。与传统的基于密码、数字证书或生物特征的认证方法不同，物理层身份认证依赖于无线信道本身的独特性，如信道冲激响应、信号强度、信道增益、环境噪声等，这些特性难以被模仿或伪造，为无人系统通信网络提供了一条坚固的安全防线。

物理层身份认证具备隐蔽性、实时性、低成本和抗欺骗性四个主要特点。具体来说，① 由于物理层身份认证依赖于无线信道的物理特性，这些特性通常对于攻击者是隐蔽的，难以被感知和捕获；② 物理层身份认证可以实时地根据当前的信道状态进行认证，适应动态变化的无线环境；③ 物理层身份认证不需要额外的硬件支持，可以直接利用现有的无线通信设备进行认证；④ 抗欺骗性：由于信道特性和设备特征难以被伪造，物理层身份认证具有较高的抗欺骗能力。

依据具体实现技术，物理层身份认证的方案可以分为无密钥和有密钥两类。

- 无密钥物理层身份认证：直接利用无线信道的物理特性或接收信号的物理层特征作为身份标识，如信号到达时间、信号到达角度、无线电频率指纹等，通过测量并分析这些特征，可以区分不同的设备或用户。
- 有密钥的物理层身份认证：依赖于无线信道的双向互易性（即在一定时间内两个方向的信道特性是相似的），通信双方可以独立地从各自观察到的信道特性中提取出相同的密钥，用于后续的认证过程。

无密钥物理层身份认证也可称为基于特征的身份认证，其本质依赖于持续监控的无线信道参数或所估计的硬件缺陷。它的核心思想是，每个无线信道特性和每个硬件设备的物理属性都是独一无二的，天然可作为身份认证的依据。根据认证所需的特征，可进一步将物理层身份认证分为三大类：基于信道特征、基于射频指纹特征及混合认证方案。

- 基于信道特征的认证方案：该方案基于多样且唯一的无线信道特征，信道特性是由无线信道的物理环境决定的，包括接收信号强度、相位响应、冲激响应和频率响应等。这些参数反映了信号传播的路径损耗、多径效应和信号衰落等空间上高度独特的信息，通常会随着环境的变化而变化，但在短时间内对于特定位置的通信双方来说是相对稳定的。这种方案的优点在于能够动态适应环境变化，同时信道特征不易仿冒且难修改，但方案效果易受干扰、多径效应等环境因素和设备差异的影响，需要精确的信道估计和复杂的误差校正技术。
- 基于射频指纹特征的认证方案：基于射频指纹的认证方案识别和利用无线设备在硬件级别产生的独特射频特征，这些特性包括但不限于瞬态特性、稳态特性及物理不可克隆函数等。具体来说，① 如瞬态信号的频谱图和时域的高阶统计特性可以反映出硬件在启动或响应时的独特行为；② 载波频偏、正交不平衡等稳态特性是由硬件制

造缺陷或设计上的不完美导致的，可以作为识别每个设备的独特指纹；③ 物理不可克隆函数是在制造过程中自然形成的微小差异来生成不可克隆的唯一设备标识，当输入任何激励时都会输出唯一且不可预测的响应。该类方案通过分析从设备发射的信号中提取的射频特征进行身份验证，具有很高的安全性和抗伪造能力。然而，它的挑战在于需要高精度的测量设备和复杂的信号处理算法来提取射频指纹，可能会增加系统的成本和复杂性。

- 混合认证方案：混合方案结合了上述认证方式，通过同时考虑信道特征和设备特有的射频指纹，该方案能有效适应复杂多变的环境和攻击场景、显著提高身份认证的安全性和鲁棒性。

基于密钥的物理层身份认证通过结合传统的密钥管理技术和物理层的独特信道特性来实现身份验证，该方法利用无线信道的互易性（即在短时间内，两个通信设备之间的信道特性是相似的）来生成一个共享的密钥，然后使用这个密钥来进行身份认证，常见方案主要包括联合信道-密钥认证和标签嵌入式认证两类。

- 联合信道-密钥认证方案：该方案将物理层信道特性与密钥认证过程结合起来，提高了身份验证的安全性。这个过程通常包括以下部分。① 信道测量：通信双方各自测量当前信道的特性，如信道状态信息；② 密钥提取：基于测量的信道特性，双方使用预先定义的算法独立生成一个共享密钥；③ 密钥一致性验证：通过安全的信息交换协议，双方验证生成的密钥是否一致，以确认对方的身份。在这种方案中，物理层的信道特性不仅用于生成密钥，还直接参与认证过程。例如，可以根据信道特性动态生成密钥，并利用该密钥对认证信息进行加密，从而实现身份验证。该方案的优势在于其增强了安全性，因为攻击者需要同时获得信道特性和密钥信息才能成功伪装，奏效的关键在于确保密钥的隐私性和一致性，同时防止中间人攻击和重放攻击。
- 标签嵌入式认证方案：该方案通过向通信信号中嵌入一个基于预先共享密钥生成的标签（即认证标签）来验证通信双方的身份。在这种方案中，发射方 Alice 将认证标签与原始信息结合，并将这个组合信号发送给接收方 Bob，当 Bob 接收到组合信号后，通过特定的物理层技术检测和解析标签信号以验证发射方的身份。标签信号通常是通过对信息进行哈希处理并使用双方共享的密钥加密生成的，这个过程确保了标签的唯一性和安全性。与传统的应用层或传输层的认证机制不同，基于标签嵌入的物理层身份认证直接在物理层进行操作，使其更适合于如无人机网络或工业物联网之类需要延迟敏感的无人系统通信网络。该方案的劣势在于嵌入认证标签会潜在影响通信性能，例如，原始信息的准确解码取决于所叠加的标签信号所引起的干扰程度。

5.4 入侵检测

入侵检测旨在监控和识别无人系统及网络中潜在的恶意行为或未经授权的行为，下面将分别介绍无人系统中常见入侵检测方法、入侵检测系统及其分类。

5.4.1 入侵检测概述

早在20世纪80年代，Dorothy Denning在其论文[95]中指出入侵是“任何违反系统安全策略的尝试”。Fred Cohen在研究计算机病毒和防御策略时，将入侵定义为“通过非授权的方式实现系统控制的尝试”[96]，强调入侵是对控制权的篡夺。国际电气和电子工程师协会（IEEE）在其安全标准中描述入侵为“对信息系统的非授权使用或非授权访问”，强调了授权范围的重要性。美国国家标准与技术研究所（NIST）将网络入侵定义为“任何未授权的访问、使用、披露、修改或破坏信息系统的尝试”，突出了对信息系统完整性的威胁。在无人系统中，入侵通常指的是任何未经授权的、恶意的或非法的行为，这些行为可能威胁到无人系统的安全性、完整性、可用性或机密性。

无人系统由于其自主性、远程操作特性和多样化的应用场景，可能面临着多种入侵风险，根据不同的分类标准可以将入侵分为不同的类别。例如，按照入侵的目的，可分为旨在访问或窃取数据的数据入侵和旨在破坏或干扰服务的服务入侵。按照入侵的行为，可分为被动入侵和主动入侵，前者不直接影响系统资源，主要涉及窃听或数据捕获，而后者可能导致系统资源篡改或服务中断，包括病毒、蠕虫、拒绝服务攻击等。按照入侵者角色，可分为内部入侵和外部入侵，前者是由系统内部用户或过程所执行的未授权操作，内部人员由于拥有系统访问权限，其发起的攻击往往更难以检测，而后者通常由系统外部人员通过网络访问发起的，试图未经授权地访问或控制系统。

在这种背景下，入侵检测系统（Intrusion Detection System，IDS）成为确保无人系统安全的关键技术。该系统是一种监视网络或系统中是否存在恶意活动的硬件设备或软件程序，通过收集和分析流量数据、系统日志等信息，入侵检测系统可以自动监测无人系统及其网络的活动，从而来识别潜在的非法活动或入侵尝试。入侵检测系统的实施不仅能够及时发现并警告系统管理员采取措施应对潜在的安全威胁，还能够与其他安全机制集成，形成全面的安全防御体系，进而保护无人系统免受入侵，确保其安全可靠地执行关键任务。入侵检测系统与防火墙的区别在于，防火墙是基于一组定义好的安全规则，用于允许或拒绝数据包，其主要目的是建立一个屏障来阻止未经授权的访问和保护网络内部的资源。而入侵检测系统更侧重于实时监控网络和系统活动，发现可能的入侵和威胁，即使这些活动可能已经穿过了防火墙。形象来说，防火墙作为第一道防线，用于阻止非授权访问，而入侵检测系统则为网络安全提供了一个更深层次的监控和分析，有助于识别和响应已经进入网络的潜在威胁，是对防火墙弱点的修补，在实际网络安全防护中通常将这两种技术结合使用以提供更全面的防御机制。

当前，入侵行为呈现出了技术复杂性、种类多样化、范围扩大化、行为隐蔽化的趋势，入侵检测系统随之也从最初的基本概念逐渐发展成为当今复杂的、多层次的安全防御体系。20世纪80年代初期，网络安全刚开始受到关注，那时的安全措施主要集中在基本的安全策略和防火墙技术上。James Anderson在1980年为美国空军所做的报告《计算机安全威胁监控与监视》中首次提出了安全威胁监测的概念，奠定了后续入侵检测理论的基础。20世纪80年代中后期，Dorothy Denning提出了一个入侵检测系统抽象概念性模型，旨在为入侵检测技术提供一个与系统平台、应用环境、特定漏洞及入侵手段无关的通用框架，标志着入侵检测方法向全面的计算机安全策略演进的重要步骤。紧接着1988年的莫里斯蠕虫事件显著

提高了公众对网络安全的意识，学术界及军方开始展开对分布式入侵检测系统的研究。20世纪90年代，随着互联网的迅速发展，入侵检测系统逐渐商业化和标准化，市场上出现了多种基于主机和基于网络的不同类型入侵检测模型及商业入侵检测系统产品。进入21世纪，随着大数据和人工智能技术的崛起，入侵检测系统开始融合更多智能化元素，提高了对复杂攻击模式的识别能力。同时，入侵检测系统开始与其他安全系统如入侵防御系统（Intrusion Prevention System，IPS）、安全信息和事件管理系统集成，形成更为全面的网络安全解决方案。2007年，CIDF工作组发布的一系列IETF RFC标准草稿，包括IDMEF（入侵检测消息交换要求）、IDMEF（入侵检测消息交换格式）和IDXP（入侵检测交换协议），为入侵检测系统的标准化和协议制定提供了重要支持。如今，入侵检测系统正面临着云计算、物联网和无人系统普及带来的新挑战，未来，预计入侵检测系统将进一步融合人工智能技术，以更有效地应对日益增长和多变的网络威胁。

5.4.2　入侵检测方法

入侵检测是基于系统行为分析建立的，旨在识别和防御潜在的安全威胁，通过检测与系统正常操作模式相偏离的行为来推断其是否为恶意的窃取、破坏、篡改数据或服务的入侵行为。但是入侵活动和异常行为并非等同，而是会有四种情况：不入侵且不异常、入侵但不异常、不入侵但异常、入侵且异常。具体来说，① 不入侵且不异常是理想的系统状态，表示系统运行正常，没有遭受任何入侵，所有行为都符合预期的安全策略和操作规范，在这种状态下系统的安全性和性能都得到了保证；② 某些攻击者可能采用隐蔽手段或利用合法权限进行入侵而不会立即引起系统异常，这种类型的行为对入侵检测系统来说是个挑战，因为它要求系统能够识别出看似正常但实际上具有恶意目的的行为；③ 不入侵但异常通常涉及系统的误操作、配置错误或非恶意的系统故障，虽然这些异常行为不是恶意的，但它们仍然需要被检测和解决，以维护系统的正常运行和性能；④ 入侵且异常是最典型的安全威胁情况，入侵行为导致了系统的异常状态，如未授权访问、系统资源被篡改或服务被拒绝等，入侵检测系统需要能够快速准确地识别这些异常并触发警报，以便采取相应的安全措施。

1. 入侵检测系统基本流程

如图5-8所示，入侵检测系统的基本工作流程主要分为四个阶段：数据收集、威胁检测、响应与处理以及更新与维护，每个阶段都对保障网络安全至关重要。

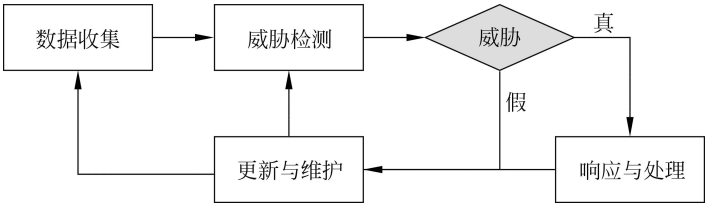


图 5-8　无人系统中入侵检测系统的工作流程图

- 数据收集：数据收集阶段是整个入侵检测过程的基础，在这一阶段，系统通过监控网络流量、分析系统和应用日志等手段收集关键数据。这不仅包括传统的网络数据包和连接日志，还可能涉及更高层次的用户行为和应用程序状态信息，为后续的威胁检测提供丰富的数据基础。

- 威胁检测：入侵检测系统拥有多种检测技术来识别潜在的安全威胁，例如，误用检测机制利用预先定义的攻击特征数据库进行模式匹配，有效地识别已知的攻击行为，而异常检测机制通过分析和比较当前行为与建立的基准行为之间的差异来识别未知或新型攻击。为了提高检测的准确性和覆盖面，混合检测机制结合了误用检测和异常检测的优势，通过综合分析来提高对潜在威胁的识别率。
- 响应与处理：一旦检测到潜在威胁，系统将进入响应与处理阶段，根据预定义的安全策略和响应规则，入侵检测系统可以采取多种措施，包括但不限于发出警告、自动隔离受影响的系统组件或直接阻断恶意流量。这些响应措施旨在最小化安全事件的潜在影响，同时为系统管理员提供足够的信息进行进一步分析和应对。
- 更新与维护：更新与维护阶段确保了入侵检测系统能够适应不断演化的安全威胁，包括定期更新攻击特征数据库、调整异常行为的检测阈值和算法，以及升级系统本身的软硬件资源。通过持续的更新和维护，入侵检测系统能够有效地应对新出现的攻击手段和策略，保持系统的安全性和稳定性。

高效的入侵检测系统应在准确识别入侵的同时尽量减少误报，为了应对入侵检测的复杂性，研究人员开发了包括基于主机、基于网络和分布式系统在内的多种范式及应用，将在下一节展开介绍。

威胁检测是入侵检测系统的核心任务，是通过对无人系统内发生的各种事件进行细致分析，以识别那些可能违反了安全策略的行为，通过各类入侵检测技术来及时发现并响应这些活动对维护系统的安全性至关重要。入侵检测技术也在不断发展，以适应新的安全挑战，本节将介绍三种主要的入侵检测方法：基于误用的检测策略、基于异常的检测策略和混合检测策略，图5-9列出了对典型入侵检测技术的对比及总结。

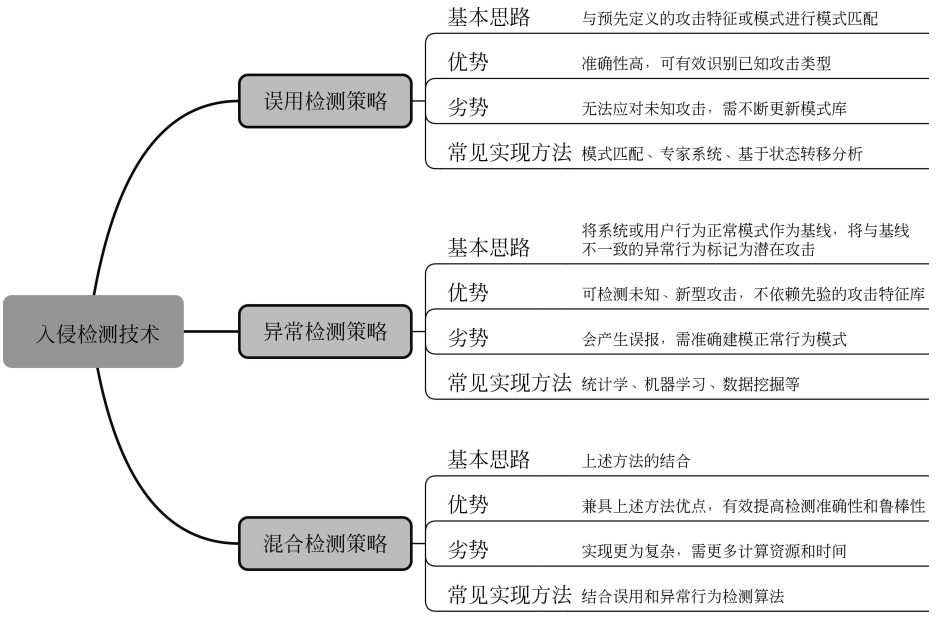


图 5-9　无人系统入侵检测技术分类

2. 入侵检测技术

- 基于误用的检测策略：又称为基于签名或知识的检测方法，该方法的实现思路是将网

络活动与预先定义的攻击模式或特征进行比对，当这些规则与当前事件相匹配时，将会触发警报。这种方法依赖于详尽的攻击特征数据库，其特征描述了已知攻击的典型行为，其优势在于对已知的攻击类型非常有效，识别率很高，误报率也相对较低，但其无法检测到新型或未知的攻击，并且需要不断地更新模式库以应对新出现的威胁。它常见的实现方法有模式匹配、专家系统和基于状态转移分析，具体来说，① 模式匹配：使用正则表达式或字符串匹配算法来识别攻击签名中的特定序列或模式，其直接在网络流量中搜索预定义的攻击模式；② 专家系统：利用基于规则的逻辑系统，其中包含了一系列的“if-else”规则，这些规则定义了已知攻击的特征和行为，当网络活动符合这些规则时，系统将触发警报；③ 基于状态转移分析：通过分析网络活动或系统状态的变化序列，识别符合已知攻击模式的状态转换，这种方法能够识别出需要多个步骤完成的复杂攻击。

- 基于异常的检测策略：这类方法将系统或用户行为的正常模式作为基线，当正常行为出现偏差时，检测器会将其视为潜在的攻击。异常检测器在防止未知、新型攻击方面很有效，并且不需要维护一个先验的攻击特征库，同时每个无人系统和每个网络的正常行为的配置文件都是定制化的，这使得攻击者很难确切地了解哪些活动可以不被检测到。然而，该方法倾向于产生高误报率（以前未知的合法活动也可能被归类为恶意活动），需要对正常行为模式进行准确的建模，常见实现方法有统计学方法、机器学习、数据挖掘等。具体地，① 统计学方法：利用统计模型来建立正常行为的基线，通过比较实时数据与基线的偏差来检测异常。这些方法可能包括均值、标准差、概率分布等统计指标；② 机器学习：使用机器学习算法（如聚类、神经网络、决策树等）自动学习正常行为的模式，并检测偏离这些模式的活动；③ 数据挖掘：应用数据挖掘技术来发现数据中的隐藏模式、关联或异常行为，这些技术能够处理大规模数据集，识别复杂的行为模式和关系。
- 混合检测策略：该类方法主要是通过结合误用和异常行为检测对入侵行为进行检测，大多数现有混合检测策略首先进行异常检测，通过检测网络行为的异常模式来识别出潜在安全威胁（包括未知攻击模式），一旦异常行为被识别，系统会尝试将其与已知的攻击签名或模式进行对比来确认异常行为是否为已知攻击。在某些情况下，混合检测系统可能同时运行两种检测方法，并在最后阶段进行结果的关联和综合决策。混合检测策略的优势在于兼具上述方法优点，检测的准确性和鲁棒性均得到提高，但是其实现更为复杂，需要更多计算资源和存储空间来进行两种检测方法。另外，通过结合机器学习算法的自适应能力和模式匹配的精确性，可以提高检测新型攻击和减少误报的能力。例如，可以使用机器学习算法预筛异常行为，然后通过模式匹配确认这些行为是否与已知攻击签名相符。

5.4.3　入侵检测系统分类及典型系统

依据系统分析数据的来源及其部署位置，入侵检测系统可被分为基于主机的入侵检测系统（Host-based Intrusion Detection Systems，HIDS）、基于网络的入侵检测系统（Network-based Intrusion Detection Systems，NIDS）及分布式入侵检测系统（Distributed Intrusion Detection Systems，DIDS）。表5-3提供了对无人系统中不同类型入侵检测系统的比较。其

中，HIDS是一种专门部署在主机上（例如智能体或服务器）的安全软件，旨在监测和分析主机自身的活动，以识别潜在的恶意行为或不合规操作，包括文件系统的变更、系统日志、关键系统调用甚至内存和网络活动。这种类型的入侵检测系统能够检测到例如恶意软件感染、未授权的数据访问或更改、权限提升攻击和其他对单个系统构成威胁的行为，它通常使用一套预定义的规则来分析主机的行为，当检测到规则中定义的可疑或不正常活动时，系统将发出警报。该类型系统的优势在于其对特定主机内部行为的深入洞察能力，能够提供对独立系统安全状态的详细视图。然而，HIDS也需要定期更新其规则集，以便能够识别新出现的威胁和攻击手段，另外可能需要较多的系统资源来运行，尤其是在需要实时分析大量数据时。

表 5-3　入侵检测系统类型比较

	基于主机的IDS	基于网络的IDS	分布式IDS
部署位置	单一主机	网络关键节点	多个网络节点与主机
数据来源	主机日志、进程等	网段中数据包	网络流量与主机数据
优势	检测精度高，不受网络流量影响	实时监控，快速响应攻击	综合HIDS与NIDS优点
劣势	需定期更新规则集，占用主机资源	高流量性能受限，易误报	部署、同步与管理复杂度高
适用场景	重要单一主机保护	核心网络段	复杂分布式系统

不同于HIDS，NIDS是专为监测和分析网络流量而设计的安全系统，其主要目的是在整个网络层面识别潜在的恶意活动或策略违规行为。NIDS部署在网络中的关键节点上，监控通过这些节点的所有进出流量，能够检测各种网络层面的威胁，如分布式拒绝服务攻击、网络扫描、钓鱼攻击及其他利用网络协议或应用漏洞的攻击。这些系统通常使用一组预定义的规则或启发式方法来分析网络数据包，寻找异常模式或已知攻击的特征，一旦检测到可疑行为或已知攻击签名，NIDS会发出警报并可能提供相关流量的详细信息，以便进一步分析。NIDS的一个关键优势是其能够提供网络覆盖范围的视角，监控跨越多个主机和设备的活动，从而增强了对复杂攻击链和大范围威胁的检测能力。然而，由于它们需处理大量流量数据，NIDS可能会存在性能挑战，并且可能在高流量条件下产生误报。为了提高准确性和效率，NIDS通常需要与其他安全系统（如防火墙、HIDS和安全信息与事件管理系统）协同工作，形成多层次的网络防御机制。

无人系统通常涉及全场景覆盖、多网络协议的操作环境，包括地面站、空中或水下无人系统及数据中心，DIDS通过其分布式和综合的检测能力，可为无人系统提供全面的安全监控。具体来说，DIDS兼顾NIDS和HIDS的特点，其分布式架构使得在多个网络节点和主机上部署检测组件成为可能，从而实现对整个网络的全面安全监控，包括子网间和边界的流量监控。在DIDS架构下，各检测节点负责搜集关于网络流量、系统日志、应用程序活动和智能体行为的各类数据，这些数据随后被送往中心分析系统，由该系统进行集中式的威胁分析和行为关联处理。得益于其协作性，DIDS能够可靠地识别那些单一IDS无法发现的复杂和多阶段攻击模式，例如分布式攻击、横向移动和多步骤攻击。此外，DIDS将检测任务分配到多节点之上，即使某一节点失效或被攻击，其他节点仍然可以正常运行。另外，DIDS的

全局视角和综合分析能力使其能够通过关联来自网络各部分的信息，更准确地识别真实的安全威胁，并减少误报的发生。然而，实施DIDS也伴随着一系列挑战，管理和维护一个分布式系统相比单一系统无疑是更为复杂的任务，它要求对网络的架构和无人系统的安全需求有深刻理解，并能有效协调各个检测节点。此外，鉴于中心分析系统需汇总和分析来自各节点的大量数据，DIDS在响应检测到的威胁时可能表现出滞后性，并且，一旦中心分析系统受到攻击或失效，整个系统的运作可能面临严重影响，甚至瘫痪。

为了更主动、更有效地防御这些威胁，入侵防御系统被提出，其结合了入侵检测系统的监测和分析功能，并通过主动干预来阻止已识别的威胁，从而提供了比传统入侵检测系统更高级的保护。与入侵检测系统相比，入侵防御系统具有更加主动的防御机制，不仅能够检测网络和系统中的安全威胁，还能够主动防止这些威胁对网络或系统造成伤害。在无人系统中，入侵防御系统可以保护如无人机、无人车等智能体和控制网络免受黑客攻击和恶意软件的侵害，通过监控设备通信、分析数据流量和执行安全策略，可以大大提高系统对外部威胁的防御能力，保障无人系统的稳定运行和数据安全。

经过几十年的发展，IDS领域已经涌现出了许多典型和高效的系统。这些系统各有其特色和应用领域，下面是对这些典型系统的介绍。

- Snort：该系统是由Sourcefire公司于1998年发布的一款开源入侵检测系统，能够实时进行流量分析和数据包记录，它可支持包括基于误用、基于异常、基于协议的多种检测方式，可提供丰富的自定义规则集来检测不同网络攻击和威胁，适应于从小型局域网到大型公用网络的各种规模网络环境。在实际工作阶段，Snort首先捕获网络流经的数据包，通过对每个数据包进行分析，来匹配预定义的规则集，当数据包与某个规则匹配时，Snort会生成警报或记录日志。
- Bro-IDS：现在通常称为Zeek，最初由Vern Paxson在20世纪90年代末开发。它并非传统意义上的入侵检测系统，更侧重于为用户提供详细的网络监控和实时数据分析。Zeek采用事件驱动的方式来分析网络活动，它首先通过将网络流量转换为一系列事件（例如新的HTTP请求或TCP连接），接着利用用户根据特定需求所定制的策略脚本来监控、分析及处理这些事件。
- Kismet：它是一个开源无线网络侦测系统、网络嗅探器及入侵检测系统。其主要适用于802.11 Wi-Fi网络，但也支持其他形式的无线网络。与其他侦测器不同，Kismet作为一个被动嗅探器，不会主动发送数据包来影响网络性能，而是通过监听空中的无线流量来检测无线网络的存在（包括不广播SSID的隐藏网络）。Kismet首先使用无线网卡的监听模式来捕获流经空气的所有无线流量，接着对捕获的数据包进行解析和分类，以提供有关网络和设备的详细信息，当检测到恶意流量或潜在网络攻击（如无线网卡的欺骗攻击）时，Kismet的警报系统会发出警报。
- Security Onion：它是一个强大且多功能的开源网络安全平台，由Doug Burks开发并首次发布于2008年，其集成了包括Snort、Suricata、Zeek等在内的多种工具，可提供全面的网络安全监控、日志管理和入侵检测功能。该平台使用网络探针捕获网络流量，并对数据进行深度分析，以识别异常模式和潜在的安全威胁，由于采用分布式架构，Security Onion允许在多个节点上部署，有效提高了数据处理的效率和系统的可扩展性。

- Suricata：Suricata是一个高性能的网络入侵检测、入侵防御和安全监控系统，它由开放信息安全基金会（OISF）支持并维护，并且拥有活跃的社区支持，能得到不断更新的技术支持。该系统支持多线程处理，能够高效地处理大量网络流量，适用于高速网络环境，拥有包括基于规则的攻击检测、自动协议识别、文件类型识别和流量行为分析在内的先进威胁检测技术。其首先使用高效的数据包捕获技术来监控网络流量，接着利用丰富的规则库来识别各种已知的恶意活动和攻击行为，最后对网络流量进行深入分析，包括应用层协议分析，以识别潜在的恶意行为或策略违规。
- OpenWIPS-ng：它作为一个专门针对无线网络的安全解决方案，提供了安全监控和威胁防御能力。该系统采用模块化设计，包括服务器、传感器和接口组件，以适应不同的部署需求。在实际工作中，OpenWIPS-ng首先利用无线传感器来捕获网络中的无线流量，接着通过分析捕获的流量来识别潜在安全威胁，服务器组件随后处理来自传感器的数据并执行入侵检测算法，在检测到威胁时，系统可以配置自动或手动响应措施。该系统的特点是能够实时监控无线网络来快速识别和响应安全威胁，并且支持在多个传感器节点上部署以适合不同规模和复杂度的无线网络环境。
- Sagan：Sagan是一个实时日志分析和关联引擎，旨在分析系统和应用程序日志并与其他网络监控工具协同工作，以识别潜在的安全威胁或异常行为。它能够解析多种格式的日志文件，并且与现有的日志管理和安全信息和事件管理（SIEM）解决方案兼容，例如与Snort或Suricata的规则兼容。其首先从包括主机、服务器和网络设备的不同日志来源收集数据，然后使用预定义的规则来检测、关联、分析、识别复杂的多步骤攻击或策略违规行为，在检测到可疑活动或符合特定条件的事件时，Sagan会生成警报。

这些系统各自以独特的方式满足了不同的网络安全需求，随着网络环境的日益复杂，这些系统不断发展和升级，以更有效地应对无人系统多样的安全威胁。

5.5 本章小结

本章首先从网络类型、安全威胁和安全挑战三方面概述了无人系统通信网络及其安全的现状，随后，全面探讨了通信网络安全的多维防御策略，构建了一个涵盖安全认证与访问控制、物理层安全及入侵检测技术的多层次防护体系，旨在有效应对持续演变的安全风险。具体内容如下。

（1）安全认证：此过程确认智能体的身份，确保无人系统及其资源不受未授权访问、数据泄露和恶意攻击的影响。安全认证可以基于知识、所持物、生物特征、位置、行为及多因素认证等多种验证因素实施。

（2）访问控制：在完成认证后，根据其身份和权限管理其访问资源，以维护数据和无人系统的安全。根据访问控制决策的依据和实施机制，访问控制策略可以分为强制访问控制、自主访问控制、基于角色的访问控制和基于属性的访问控制等类型。

（3）物理层安全技术：作为通信与安全一体化的关键手段，这些技术利用信道的随机性和不对称性为无人系统提供保密性和可验证的数据传输，主要技术包括安全预编码、物理

层密钥技术和物理层身份认证等。

（4）入侵检测：为了监控和识别无人系统网络中的潜在入侵风险，可采用基于误用、异常和混合策略等入侵检测技术对数据进行分析，根据数据来源及部署位置，入侵检测系统可被分为基于主机、网络、分布式的入侵检测系统。

接下来的章节将聚焦无人系统中的隐私问题和面临的挑战，并深入介绍各类隐私推理攻击和隐私计算技术。

5.6 习题

1. 无人系统的通信网络有哪些？请列举至少三种网络类型，并简要描述其独特优势和应用场景。

2. 请简要描述当前无人系统中通信网络的安全现状，分析可能遭受的三种安全威胁，并针对每种威胁提出相应的防御措施。解释这些措施如何减轻或消除相应的安全风险。

3. 解释为什么在无人系统的通信网络中，多因素认证比单一密码认证提供了更高的安全性。请列举至少两种多因素认证的实现方法，并讨论它们各自的优缺点。

4. 物理层安全技术利用无线信道的特性来增强通信的安全性。请解释以下两种物理层安全技术的基本原理，并比较它们的适用场景和效果：① 线性预编码技术；② 非线性预编码技术。

5. 描述一个入侵检测系统在无人系统通信网络中的工作原理，并讨论它如何与其他安全防御措施（如防火墙和安全认证）协同工作以提高系统的整体安全性。