**第1章 概述**

无线网络凭借无需物理线路即可实现以太网互连的特性，具备无线传输开放化、频率复用高效化、网络结构异构化、用户设备密集化等特点，在人们的生活与工作中得到了广泛应用，改变了信息传播和交互的方式。然而，其空口传输的特性使其面临窃听、信息篡改、中间人攻击等诸多安全威胁，严重阻碍了无线网络的进一步发展，因此，深入研究构建多层次、多维度的无线网络安全防护体系意义重大。本章围绕蜂窝网络的安全需求，重点介绍无线网络技术的分类、蜂窝网络的发展历程、蜂窝网络面临的问题与安全挑战、安全技术的发展现状及前景等方面内容，为后续的研究和应用提供坚实的理论基础。

**1.1 无线网络技术概述**

无线网络是无线通信技术和网络技术结合的产物，是对一类使用无线电技术传输数据网络的总称。无线网络通信因其无需物理线路就可实现以太网互连，具备安装简易、扩展性强、灵活性高等特点，所以发展十分迅速。

在无线通信技术的发展过程中，新的技术标准一直层出不穷，但相较于技术层面的不断发展，安全问题并没有获得与之相当的关注度。无线网络空口传输这一特性导致其易受到各种安全威胁，例如窃听、信息篡改、中间人攻击、重放攻击、未经授权的访问等。如果这些安全威胁得不到安全技术的有效防护，无线网络的发展必然会受到阻碍。未来，安全技术将是一个可持续发展的领域，对于保障个人隐私、企业数据安全甚至是国家信息安全都发挥着至关重要的作用。

无线网络技术可以分为以下几个方面：

1.蜂窝网络技术：该技术是一种依据地理区域划分的无线通信技术，会将覆盖范围划分为多个小区，并在每个小区中部署一个基站进行管理。移动设备可以通过基站接入网络，并在移动的过程中与相邻小区中的基站完成越区切换。

2.无线局域网技术：该技术通常应用于有限范围内，利用无线信号进行数据传输。我们经常使用的Wi-Fi技术就是一种无线局域网技术，通常用于家庭、企业、学校以及公共场所等环境中。

3. 无线自组网技术：该技术中设备能够在没有固定基础设施的情况下相互连接和通信，具有灵活性和自组织能力，适用于应急通信、军事行动和个人区域网络等场景，能够快速建立可靠的通信链路，特别在缺乏基础设施的环境中提供有效的解决方案。

4. 卫星通信技术：该技术是一种通过卫星进行数据传输的通信方式，具有覆盖范围广、高带宽和低延迟的特点，广泛应用于远程通信、广播服务、军事和应急通信以及科学研究等领域，能够在没有地面基础设施的地区提供可靠的通信手段。

5.蓝牙技术：该技术是一种短距离无线通信技术，通常用于个人设备之间的通信，例如手机、耳机、键盘、鼠标、电脑等。

6.ZigBee技术：该技术专用于物联网应用中的传感器和控制设备之间的通信，具有低功耗、低速率、短距离通信的特点，现已广泛应用于智能家居、医疗保健、工业控制、建筑自动化和农业等领域。

7.近场通讯技术：通常也称为NFC（Near Field Communication）。该技术同样是一种短距离的无线通信技术，距离一般不超过4厘米，可以实现两个设备之间的数据交换，通常应用于移动支付、门禁卡、数据传输、智能标签等方面。

可见，无线网络技术不仅极大地便捷了人们的通信方式，还推动了信息技术的快速发展。在下文中，我们主要对使用较为广泛的蜂窝网络进行介绍。

**1.2 蜂窝网络的发展历程**

移动通信技术旨在实现通信实体在移动过程中的信息收发，其移动性的特点决定了移动通信的实现离不开无线通信。移动通信的实现过程通常为无线通信或是无线通信和有线通信的结合，因此无线通信技术是移动通信技术实现的一种重要手段。在本节中我们就以移动通信中使用最广泛的蜂窝电话网为例进行重点介绍。

从技术角度而言，早期的蜂窝移动通信系统采用的是中央控制模式，采用中央控制器（例如基站控制器）来管理和控制多个基站的通信，可能导致单点故障、传输瓶颈等一系列的问题。随着技术的不断发展，分布式控制模式逐渐成为了蜂窝移动通信的主流控制方式，该方式允许节点之间直接进行通信，每个节点都能够独立进行管理和控制，消除了早期蜂窝网络的集中式故障问题，能够实现自组织、自优化等功能。除此之外，早期的蜂窝网络为半双工通信，即基站和移动设备在同一时刻只能实现数据的发送或接收。这种通信方式导致早期蜂窝网络存在效率低、延迟高、信道利用率低等问题，不适用于高速移动的设备。因此，为了提高通信效率、降低延迟、增加信道利用率，蜂窝网络后来采用了全双工通信方式，在该方式下，基站和终端设备之间可以同时发送和接收数据，无需等待对方的确认信号。

蜂窝理论最早于20世纪50年代末由贝尔实验室提出，为移动通信系统在全球的广泛应用开辟了道路。蜂窝技术之所以能够成为移动通信的基础，是因为以下两个重要概念：一是频率复用，二是小区分裂。现有的蜂窝网络都是将覆盖范围划分为多个正六边形的小区。具体地，频率复用是指每个小区使用同一组频率，并且同一工作频率可以在经过一定距离之后的另一组小区使用，从而解决了公用移动网络要求容量大和频率资源有限的矛盾。将小区划分为正六边形是因为信号的覆盖面是以基站为中心的有范围的圆形，而在可以无缝隙覆盖地面的多边形中，它是面积最大的一个，因此使用的节点数就最少，能够最大程度地减少小区间的干扰问题。小区分裂是指当信道容量不够时，可进一步将小区的范围缩小，划分出更多的蜂窝以提高频率的利用率。但实际上小区不可能无限进行分裂，因此蜂窝的概念也是存在局限性的。

蜂窝网络的主要组成包括基站（Base Station，BS）、移动台（Mobile Station，MS）和移动交换中心（Mobile Switching Center，MSC）。通常在蜂窝网络系统中，基站分布在小区中心，移动设备会通过基站接入移动交换中心，与公共电话网（Public Switched Telephone Network，PSTN）相连接。同一小区内的不同移动设备之间的通信需要通过该小区内基站的转接，不同小区之间的移动设备的通信需要通过不同小区的基站之间的转接，而两个基站之间的转接需要通过MSC来完成。基站和移动台之间存在无线链路，而和移动交换中心之间则存在固定链路。移动台向相邻小区移动时需要与相邻小区基站建立连接，这一过程称为越区切换。当移动台在不同移动交换中心之间切换时称为漫游。如图1.1所示，MS、BS、MSC、PSTN共同构成了传统的宏蜂窝网络。



图1.1 蜂窝网络布局

对于传统蜂窝网络而言，所使用的宏基站覆盖范围广，所产生的路径损耗会弱化小区边缘的通信质量，并且部署在用户非常密集的地区仍然会出现频率资源不足的问题，因此后来基于小区分裂的概念又提出了小蜂窝网络。小蜂窝网络实际上就是相对于传统宏蜂窝网络的一个概念，它可以在原有小区基础上再次进行划分，能够在原来的小区范围内重复使用频率，不仅增大了用户容量，而且可以解决宏基站在覆盖范围内未能充分覆盖边缘区域的问题。通过部署更小半径覆盖范围的小蜂窝基站，能够大大减轻宏基站负担，如图1.2为小蜂窝网络的部署示意图。通过表1.1中小蜂窝网络与传统宏蜂窝网络的比较可以发现，小蜂窝网络具有更小型、更便携、更低功耗的特点。但由于小蜂窝网络的部署更加密集，因此在实际的应用中会导致小区间的干扰增强，同时也会相应降低通信的服务质量。



图1.2小蜂窝网络部署

表1.1小蜂窝网络与宏蜂窝网络的比较

 第一个蜂窝网络系统于20世纪70年代初由美国AT$T公司提出，该系统名为IMTS（Improved Mobile Telephone Service），在美国进行测试后推广至其他国家。随后的几十年里，蜂窝网络获得了更加深入的发展和研究，现已从第一代蜂窝网络（1G）技术发展至第六代蜂窝网络（6G）技术。每一代蜂窝网络的改进和提升均以提高数据传输速率、增加信道容量、扩大网络覆盖范围、增强网络安全性、支持更广泛的应用场景为目标。

第一代蜂窝网络于20世纪80年代初诞生，采用频分多址接入（Frequency Division Multiple Access，FDMA）技术，实现了频谱资源的频分复用，有效地提高了系统容量。采用模拟信号传输数据，支持话音业务，具有稳定、易于实现、低成本等特点。主要标准包括美国的高级移动电话系统（Advanced Mobile Phone System，AMPS）、英国的总访问系统（Total Access Communications System，TACS）和日本总访问系统（Japan Total Access Communication System，JTAGS）。第二代蜂窝网络（2G）于1991年提出，采用时分多址接入（Time Division Multiple Access，TDMA）技术及窄带码分多址接入（Code Division Multiple Access，CDMA）技术，这两种技术均采用数字信号进行数据传输。数字信号由一系列断续变化的电压脉冲构成，与由连续的信号波构成的模拟信号相比，在长距离的信号传输中不易造成衰减和失真，具有更强的抗干扰能力；并且，数字信号能够通过各种编码方式实现信息加密，具有更高的保密性；此外，数字信号针对信号传输过程中的误码情况也有对应的解决措施，具有更强的稳定性。因此，第二代蜂窝网络系统相较于第一代在容量、保密性以及话音质量方面均得到了大幅提升。第二代蜂窝网络系统的主要标准为基于TDMA技术的全球移动通信系统（Global System for Mobile communications，GSM），使跨越国界的漫游首次成为了可能。GSM最早于1982年提出，并在1992年开始铺设，并且由于其优越的性能迅速在全球范围内推广，成为2G移动通信重要标准。第三代蜂窝网络（3G）于2000年被正式提出，采用更先进的宽带CDMA技术，能够在更高频段使用更大的系统带宽发送数据；支持高速率的业务，包括语音、数据以及多媒体业务；能够实现全球覆盖及全球无缝漫游。主要标准包括北美的CDMA2000（Code Division Multiple Access 2000）、欧洲和日本提出的宽带码分多址接入（Wide band Code Division Multiple Access，W-CDMA）技术以及中国提出的时分同步码分多址接入（Time Division-Synchronous Code Division Multiple Access，TD-SCDMA）技术。自2013年开始，第四代蜂窝网络（4G）开始盛行，采用正交频分多路复用（Orthogonal Frequency Division Multiplexing，OFDM）技术，该技术同样为数字调制技术，在数据传输的过程中将高速数据流分为多个低速载波信号，且低速载波信号之间两两正交，因此载波信号之间不会存在相互干扰的情况，相比于CDMA具有更强的抗干扰和抗衰落能力，以及更高的信道利用率。此外，OFDM能够与多输入多输出（Multiple Input Multiple Output，MIMO）技术相结合，为第四代蜂窝网络提供更高的数据传输率和信道容量。并且，4G网络能够提供更高的带宽，支持更多样化的设备（例如智能手机、笔记本电脑等）以及更丰富的业务（例如可视电话、视频会议、虚拟现实、无线局域网等）。4G的主要标准包括由第三代合作伙伴计划（3rd Generation Partnership Project，3GPP）提出的通用移动通信技术的长期演进（Long Term Evolution，LTE）以及由电气和电子工程师协会（Institute of Electrical and Electronics Engineers，IEEE）提出的全球微波接入互操作性（World Interoperability for Microwave Access，WiMAX），在全球范围内，LTE相比WiMAX而言应用更加广泛。第五代蜂窝网络（5G）技术最早于2010年由国际电信联盟（International Telecommunication Union，ITU）提出，并于2018年进入商用化阶段。第五代蜂窝网络采用了大规模MIMO、空间频率复用（Spatial Frequency Multiplexing，SFC）、网络切片以及超高频（Millimeter Wave，mmWave）等众多技术。其中，大规模MIMO能够提升信道容量；SFC技术能够提高频谱利用率；网络切片技术能够为不同的应用需求提供定制化的网络服务；mmWave技术能够提高带宽，加快数据传输速率。此外还采用了网络功能虚拟化（Network Function Virtualization，NFV）和软件定义网络（Software Defined Networking，SDN）等新兴技术，提高了网络的灵活性和可编程性。5G的主要标准为5G NR（5G New Radio），与4G的LTE相比具有更快的数据传输速率和更高的可靠性和安全性。随着5G技术的不断发展和商业应用，第六代蜂窝网络（6G）技术的研究和探讨正在持续深入，其采用智能天线、异构网络、人工智能（Artificial Intelligence，AI）等技术，致力于构建更加智能、自适应的网络。其中，智能天线技术能够对信号实现更精细化的控制，提高网络的数据传输速率；异构网络技术能够提高网络的覆盖范围和性能；全球通信技术能够实现全球范围的通信；AI技术实现了人工智能技术和蜂窝网络技术的结合，能够实现智能化的网络资源管理和调度。值得一提的是，6G 技术还力求实现空天地海一体化的通信格局。传统的通信网络主要集中于地面，存在诸多局限性，而 6G 通过构建包括高中低轨卫星网络、高空平台（例如无人机、平流层气球等）以及海洋基站等在内的全方位网络体系，将通信覆盖范围拓展至天空、海洋及偏远地区，不仅能为用户提供随时随地的网络接入，还将推动智能交通（包括高空高速飞行设备、海上船舶导航与通信等）、全域应急通信抢险、海洋资源开发等众多领域的创新发展。虽然目前6G标准尚未制定，但全球已经对6G技术展开了深入的探索和研究，并且在未来几年里，6G技术的研究和发展也将获得进一步的加速。

**1.3 蜂窝网络安全技术概述**

本节将对蜂窝网络安全技术进行介绍，包括蜂窝网络面临的问题、安全问题、安全发展现状以及发展前景。其中，蜂窝网络面临的问题涵盖系统容量瓶颈、小区间干扰，以及不同代技术的局限、建设维护成本和能耗等方面。安全问题包括无线窃听、假冒攻击、信息篡改、重放攻击和服务后抵赖等攻击。安全发展现状从学术界理论研究与技术创新、工业界实际应用解决方案两个角度进行阐述。发展前景则基于安全技术提升、政府和行业组织举措、用户安全意识增强等因素展开分析，为理解蜂窝网络安全技术提供全面视角。

**1.3.1 蜂窝网络面临的问题**

在1.2节提到过蜂窝网络的两个特点：一是频率复用，解决了以往移动通信频率资源无法满足需求的问题；二是小区分裂，由于小区不可能进行无限制的分裂，所以当系统容量到达瓶颈时，该特点会阻碍蜂窝移动通信网络的进一步发展，可能导致数据传输速率变慢、通信质量下降等问题，甚至是导致网络拥塞。

除此之外，对于小蜂窝网络而言，其面临的主要问题还有小区间干扰问题，小蜂窝网络的发展也是受限于此。随着移动用户数量的爆炸式增长，密集部署的小蜂窝会导致小区间干扰增强。由于在一定范围外的不同小区可以复用相同的频率，因此在上行链路和下行链路上均会产生小区间干扰情况。例如在上行链路上可能会产生不同移动终端在发送信号时复用相同频率的情况，如图1.3所示，可能导致基站同时收到使用相同频率的两个移动终端所发送的消息，此时相对于BS2来说，MS1所发送的这种无用信号就是干扰信号。同理，下行链路同样会产生与上行链路类似的干扰问题。当小区间干扰问题严重时，就会影响到系统的覆盖范围以及系统容量，尤其是对边缘用户，很可能会出现频繁掉网甚至是无法接入网络的情况。上行链路和下行链路均存在干扰，且小蜂窝网络进一步减少了用户到基站之间的距离，这将会产生更多的干扰信号。



图1.3小区间干扰示例

1G到5G是蜂窝网络技术发展的几个重要阶段，从演进历程的角度来看不同时期的蜂窝网络技术所面临的问题各有不同。其中，1G时期的蜂窝网络技术采用模拟信号进行数据传输，具有频谱利用率低、保密性差等弊端，无法支持数据传输功能，且通信设备体积庞大、续航能力差，无法满足现代移动通信的需求。2G时期的蜂窝网络技术带宽有限，只能提供中低速的数据传输功能，且无法满足多媒体数据传输的需求。3G时期的蜂窝网络覆盖范围有限、能耗较高且通话质量不够稳定。4G时期的蜂窝网络在传输速率和延迟等方面仍然受到限制，无法提供足够的带宽和响应速度来支持高度自动化的应用场景。5G时期网络覆盖范围存在盲区（例如海洋、沙漠等没有基站覆盖的地区）或信号质量不佳（例如偏远或设备量激增的地区）等问题。

再有，建设和维护蜂窝网络也需要大量的财力、人力资源。随着蜂窝网络技术的不断改进优化，网络设备和基础设施的成本也必然增加，如何有效降低蜂窝网络技术发展和更新过程中的成本也是需要考虑的重点问题。

除此之外，蜂窝网络基站需要保持持续稳定运行，以为用户提供连续不间断的无线通信服务。在5G网络盛行的当下，用户设备数量显著增多，相关数据呈爆炸式增长态势，这种变化使得基站的负荷量和通信网络能耗也随之不断地增加。然而，当前的能源资源和网络建设资源存在一定限制，无法无限制地满足能耗增长需求。在此背景下，如何有效降低蜂窝网络能耗、提高能源利用效率，成为通信行业亟待解决的关键问题。开发更高效节能的网络技术，不仅关系到蜂窝网络的可持续发展，更是整个通信领域实现绿色低碳转型、突破发展瓶颈的重要方向。

**1.3.2 蜂窝网络面临的安全问题**

在信息化社会的背景下，科技迅猛发展的同时，伴随着层出不穷的网络威胁，信息安全已经成为当今社会的重中之重。以下是针对蜂窝网络中可能存在的安全风险以及相应的安全需求的简单介绍。

（1）无线窃听

在蜂窝网络中，存在最严重的安全问题就是信息泄露。相比于传统的有线网络依赖于物理线路传播信息，蜂窝网络采用的是无线信号进行消息传输。在传统的有线网络上窃听信息必须要进行搭线操作，这种行为极易被探查到。而无线网络采用开放式的空口技术，窃听者无需复杂操作就能轻松截获消息，导致传送的消息很容易被窃听。攻击者从空中接口切入系统，可以实现不为通信双方所知的窃听，从而利用截获信息来跟踪用户窃取用户隐私，使其造成不必要的损失。

（2）假冒攻击

在蜂窝网络中，发送方移动台需要通过基站将其身份信息传送至接收方移动台或移动交换中心，用来验证是否为合法身份。在无线网络的开放性通道上，任何消息都有可能被窃听。进而，攻击者可以通过窃听轻松截获合法用户的身份信息，并利用该信息模仿合法用户访问网络资源，欺骗基站或其他合法用户进行交互。

（3）信息篡改

信息篡改是指攻击者对截获到的信息未经授权地进行删除、增添、修改等操作，再将篡改后的信息发送给接收方，使其按照自己的意愿进行网络操作或是阻止合法用户建立连接。例如在蜂窝网络的信息传递过程中，通常需要通过基站或移动交换中心进行转发，在这些“中转站”中就可能会发生篡改信息的行为。在移动设备与基站信息交互的过程中，攻击者可以通过无线窃听对数据进行篡改，或者通过在网络中插入恶意软件或病毒也能够实现对数据的篡改。这种攻击可能会导致信息泄露、身份欺骗、拒绝服务等严重后果。

（4）重放攻击

重放攻击是指攻击者将窃听到的信息间隔一段时间后原封不动的发送给接收方，重传曾经的有效信息，达到欺骗接收方的目的。例如，攻击者可以利用重放合法口令来获取对网络资源的访问权限。虽然蜂窝网络是通过无线信道来传输信息，但会与有线信道一样面临拒绝服务攻击、病毒攻击，这些攻击的目的不在于窃取信息或是非法访问网络资源，而是为了阻止网络的正常工作。

（5）服务后抵赖

服务后抵赖是指在通信的过程中，发送方发送了数据包但却否认发送过该数据包的行为。这种攻击通常是由于蜂窝网络中缺乏有效的身份认证和对数据完整性验证机制而导致的。例如攻击者通过窃取或假冒发送方的身份，向接收方发送虚假数据包并否认发送过虚假数据包的事实。一旦攻击成功，将导致接收方难以确定发送方的真实身份以及该数据包的真实来源。服务后抵赖攻击常发生在电子交易和移动支付等领域，例如交易双方的其中之一在交易完成后否认参与此次交易，这种攻击方式容易造成商家或是用户的经济损失。

蜂窝网络中存在的这些安全风险会对网络用户以及网络运营商造成不可小觑的风险，因此蜂窝网络需要提供相应的安全业务及维护工作，以应对这些不安全因素。主要的安全业务包括：

（1）机密性

机密性是无线网络通信中最重要的安全需求，是防止信息窃取的主要方法。在无线通信系统中将机密性分为四个级别：无机密性、等价于有线网络的机密性、商业级机密性、军队和政府级机密性。一般而言，无机密性和等价于有线网络的机密性就能够满足其所需。在蜂窝网络中，机密性主要包括对数据、语音的保密，对用户位置和隐私信息的保密，对用户和网络之间信令的保密等，目的是保障有用信息只为授权对象使用，杜绝泄露给未经授权的个人和实体。

（2）完整性

完整性保护主要是针对于信息篡改的安全技术，重点在于对数据篡改的检测。通过特定手段，确保接收方获取的信息自发送起，在整个传输过程中都没有经历未授权地新建、删除或修改。一旦数据遭到上述任何形式的篡改，完整性保护机制便能及时察觉，从而保障数据的原始性与可靠性。

（3）不可否认性

不可否认性是针对服务后抵赖的安全技术，通常依赖于某种机制，使得交易的双方无法否认参与过此次交易。在蜂窝网络通信中，不可否认性通常用于数据传输的过程中，其目的是使人们无法否认自己曾经发送过的信息和内容。在互联网的环境中，可以利用数字证书中的私钥进行数字签名等方式来保证数据的不可否认性。

（4）身份认证

身份认证是应对假冒攻击的主要安全技术，其目的是为了确认当前用户所声称的身份，确实是该用户的真实身份。在蜂窝网络通信中，主要针对于移动台和网络端的身份进行认证。对于移动台的用户而言，需要验证网络端身份的真实性，以防攻击者假冒网络端攻击用户或者获取用户的隐私信息；对于网络端而言，需要验证移动用户身份的真实性，以防非法用户冒充合法用户使用网络的资源和服务。

**1.3.3 蜂窝网络安全发展现状**

到目前为止，蜂窝网络安全问题方面已有不少的研究成果，学术界与工业界基于不同视角开展探索，共同推动技术演进。学术界侧重理论创新与技术突破，工业界则更关注实际应用与解决方案落地，二者相辅相成，为应对蜂窝网络安全挑战提供多元思路。

学术界围绕蜂窝网络安全开展了大量理论研究与技术创新。在移动通信中，实体的认证和机密性能够由认证密钥交换（Authentication Key Exchange，AKE）协议来保障。但若在小蜂窝网络中采用匿名AKE来隐藏用户的踪迹，就会因为小蜂窝网络频率增多的特点导致通信的延迟显著增加。因此，在文献[1]中，提出了一种基于安全区域保障用户匿名性和SCN快速撤销的切换方案，能够显著降低用户设备在宏基站区域内的小蜂窝网络之间重新连接的通信时延。

蜂窝网络设计的主要目标是为了在为用户提供高数据速率服务的同时保持节能传输。正如前文所提到的，蜂窝网络需要进行小区分裂以应对越来越多的用户设备，所以需要部署更高密度的网络拓扑结构。这些网络拓扑结构的出现也带来了研究物理层特性提高安全性的研究需求。文献[2]考虑了窃听者的信道状态信息的不确定性，提出了一种最小化网络功耗的优化模型，该模型既能满足一定的服务质量又能保证物理层的安全性。文献[3]同样针对窃听风险，提出了一种混合缓存传输策略，能够提高安全内容的交付概率，以应对窃听者不确定性分布的情况，保障了小蜂窝网络的物理层安全性。

移动通信的快速发展大大增加了蜂窝网络的传输负荷，频谱资源短缺的问题不能仅依靠小区分裂来缓解，因此出现了异构蜂窝网络。但这一网络同样存在安全风险，例如，当D2D（Device-to-Device）用户可与蜂窝用户共享频率资源时，蜂窝用户可能会接收到来自蜂窝链路上的D2D用户信息。针对这一问题，文献[4]提出了一种自适应功率控制和接入控制的方案，以提高异构蜂窝网络中D2D用户的保密能力。

在蜂窝网络中，将在网络边缘部署且具备高级服务能力的技术称为移动边缘计算（Mobile Edge Computing，MEC），文献[5]基于MEC辅助，针对虚拟化小蜂窝无线网络中快速移动用户的体验质量增强进行了安全建模，通过面向5G中代表性场景的演示，证明了该安全模型不仅能够识别关键资源进行保护，还能够识别安全威胁，确定出适当的安全约束和安全机制以应对5G网络中潜在的安全威胁。针对蜂窝网络移动性所带来的安全和隐私威胁，文献[6]提出了一种分散信任的网络体系结构所适用的密钥管理方案。虽然移动性管理安全方案在不断的更新，但在如何保证安全性的同时实现无缝连接、能效最大化、低信令开销等方面仍然缺少较理想的方案。

工业界在蜂窝网络安全领域更注重将技术成果转化为实际应用解决方案。第一代蜂窝网络（1G）受限于模拟通信技术，其安全设计存在明显不足。由于缺乏有效的加密和认证机制，通信数据在传输过程中易被窃听，用户身份和通信内容难以得到可靠保护。​第二代蜂窝网络（2G）实现从模拟到数字通信的转变，引入用户身份认证与数据加密机制。然而，2G 安全体系存在一定局限性，其认证过程仅实现网络对用户的单向认证，缺乏用户对网络合法性的验证；数据保护侧重于机密性，在数据完整性保护方面存在改进空间。​第三代（3G）和第四代（4G）蜂窝网络在安全机制上有显著改进，通过增强认证协议和加密算法提升通信安全性。但在用户隐私保护层面，仍存在可优化之处。​第五代蜂窝网络（5G）因海量设备连接、多样化应用场景以及边缘计算等新技术的引入，网络安全环境更为复杂，用户身份标识、位置信息等隐私数据存在被追踪的风险，同时网络切片隔离失效、边缘计算节点安全防护薄弱等问题也亟待解决。

尽管学术界与工业界在蜂窝网络安全领域取得诸多成果，但随着通信技术不断发展，新型安全威胁持续涌现。未来仍需学术界与工业界加强协同创新，持续优化和开发更安全高效的安全机制与算法，以适应蜂窝网络发展需求，筑牢网络安全防线。

**1.3.4 蜂窝网络安全发展前景**

蜂窝网络在现代通信中扮演着重要的角色，为人们提供了通信的灵活性和便利性。如今，5G已逐渐融入各行各业，在其不断发展的过程中，需要有更高的性能指标、更多的新型技术来支撑其发展。蜂窝网络所具备的众多优势使其成为了连接物联网设备的重要基础设施。未来，随着物联网的发展，更会有不尽其数的用户设备接入移动网络，为了满足无线通信快速增长的用户需求，蜂窝网络需要更加全面高效的发展，同时也面临着诸多安全方面的挑战，因此蜂窝网络安全发展前景仍需进一步的探讨。

一方面，在通信技术快速发展的同时，蜂窝网络安全技术也将得到进一步提升，不断会有新的安全技术被研发出来并应用于蜂窝网络中。例如，基于人工智能和深度学习等安全技术可以帮助实现自动检测和响应网络攻击，保护网络安全和数据隐私。

另一方面，政府和行业组织也在不断地采取措施，加强对蜂窝网络的安全保护。具体地，一些国家已经出台了网络安全法规和标准，例如，中国颁布的《网络安全法》、美国颁布的《网络安全信息共享发》、欧盟通过的《一般数据保护条例》（General Data Protection Regulation，GDPR）等，在很大程度上规范了蜂窝网络的安全管理。3GPP、ETSI、GSMA等行业组织也在不断探讨和指定安全标准和认证机制，促进蜂窝网络的安全发展。

最后，用户也越来越注重蜂窝网络的安全问题。他们更加关注数据隐私和网络安全，会倾向于使用安全性更高的通信方式和设备，保障自身在使用蜂窝网络过程中的隐私安全。

基于以上因素，我们对蜂窝网络的安全发展前景感到乐观，但仍需要持续关注和探讨如何应对安全挑战，不断提高蜂窝网络的安全性。

## 参考文献：

1. Fan C I, Huang J J, Zhong M Z, et al. ReHand: Secure region-based fast handover with user anonymity for small cell networks in mobile communications[J]. IEEE Transactions on Information Forensics and Security, 2019, 15: 927-942.
2. Bernardo N I, De Leon F. On the trade-off between physical layer security and energy efficiency of massive MIMO with small cells[C]//2016 International Conference on Advanced Technologies for Communications (ATC). IEEE, 2016: 135-140.

Zheng T X, Wang H M, Yuan J. Physical-layer security in cache-enabled cooperative small cell networks against randomly distributed eavesdroppers[J]. IEEE Transactions on Wireless Communications, 2018, 17(9): 5945-5958.

Zhang X, Shang Y, Yan S, et al. Adaptive power and access control for physical security of heterogeneous cellular network[C]//MILCOM 2016-2016 IEEE Military Communications Conference. IEEE, 2016: 1202-1206.

Vassilakis V G, Mouratidis H, Panaousis E, et al. Security requirements modelling for virtualized 5G small cell networks[C]//2017 24th International Conference on Telecommunications (ICT). IEEE, 2017: 1-5.

De Ree M, Mantas G, Radwan A, et al. Key management for beyond 5G mobile small cells: A survey[J]. IEEE Access, 2019, 7: 59200-59236.

缩略语

|  |  |  |
| --- | --- | --- |
| 缩写名词 | 英文全称 | 中文译名 |
| BS | Base Station | 基站 |
| MS | Mobile Station | 移动台 |
| MSC | Mobile Switching Center | 移动交换中心 |
| PSTN | Public Switched Telephone Network | 公共电话网 |
| NFC | Near Field Communication | 近场通讯技术 |
| FDMA | Frequency Division Multiple Access | 频分多址接入 |
| AMPS | Advanced Mobile Phone System | 高级移动电话系统 |
| TACS | Total Access Communications System | 总访问系统 |
| JTAGS | Japan Total Access Communication System | 日本总访问系统 |
| TDMA | Time Division Multiple Access | 时分多址接入 |
| CDMA | Code Division Multiple Access | 窄带码分多址接入 |
| GSM | Global System for Mobile communications | 全球移动通信系统 |
| W-CDMA | Wide band Code Division Multiple Access | 宽带码分多址接入 |
| TD-SCDMA | Time Division-Synchronous Code Division Multiple Access | 时分同步码分多址接入 |
| OFDM | Orthogonal Frequency Division Multiplexing | 正交频分多路复用 |
| MIMO | Multiple Input Multiple Output | 多输入多输出 |
| 3GPP | 3rd Generation Partnership Project | 第三代合作伙伴计划 |
| LTE | Long Term Evolution | 长期演进 |
| IEEE | Institute of Electrical and Electronics Engineers | 电气和电子工程师协会 |
| WiMAX | World Interoperability for Microwave Access | 全球微波接入互操作性 |
| ITU | International Telecommunication Union | 国际电信联盟 |
| SFC | Spatial Frequency Multiplexing | 空间频率复用 |
| mmWave | Millimeter Wave | 超高频 |
| NFV | Network Function Virtualization | 网络功能虚拟化 |
| SDN | Software Defined Networking | 软件定义网络 |
| AI | Artificial Intelligence | 人工智能 |
| AKE | Authentication Key Exchange | 认证密钥交换 |
| MEC | Mobile Edge Computing | 移动边缘计算 |
| GDPR | General Data Protection Regulation | 一般数据保护条例 |