Hans Journal of Wireless Communications 无线通信, 2023, 13(5), 65-74
Published Online October 2023 in Hans. https://www.hanspub.org/journal/hjwc
https://doi.org/10.12677/hjwc.2023.135007

Hans汉斯

5G技术在公安领域的应用现状、问题及对策建议

吴亚楠，许　杰

南京警察学院侦查学院，江苏 南京

收稿日期：2023年11月20日；录用日期：2023年12月19日；发布日期：2023年12月26日

摘　要

随着第5代移动通信技术(5G)的快速发展，公安部门也开始将其引入到自己的业务中。首先，梳理了5G技术在公安领域应用的发展现状，探讨其在公安工作中的潜力和优势；其次，分析了目前公安部门在应用5G技术过程中所面临的问题，如资源配置、数据安全、运营成本等方面的问题；最后，研究提出了包括统筹警用无线资源配置、加强数据安全保护、加快5G网络建设规划等对策与展望，具有指导5G技术在公安领域顺利应用的价值。

关键词

5G技术，公安领域，应用现状，对策建议

The Application Status, Problems and Countermeasures of 5G Technology in the Public Security Field

Yanan Wu, Jie Xu

Detective Academy, Nanjing Police University, Nanjing Jiangsu

Received: Nov. 20th, 2023; accepted: Dec. 19th, 2023; published: Dec. 26th, 2023

Abstract

With the rapid development of 5th generation mobile communication technology (5G), public security departments have also begun to introduce it into their own business. First, it sorted out the development status of 5G technology in the public security field and discussed its potential and advantages in public security work; secondly, it analyzed the problems currently faced by public

文章引用: 吴亚楠, 许杰. 5G 技术在公安领域的应用现状、问题及对策建议[J]. 无线通信, 2023, 13(5): 65-74.
DOI: 10.12677/hjwc.2023.135007

security departments in the application of 5G technology, such as resource allocation, data security, operating costs and other issues; finally, the study proposes countermeasures and prospects including coordinating the allocation of police wireless resources, strengthening data security protection, accelerating 5G network construction planning, etc., which has the value of guiding the smooth application of 5G technology in the public security field.

Keywords

5G Technology, Public Security Field, Application Status, Countermeasures and Suggestions

1. 5G 在公安工作中的应用现状

1.1. 基于 5G 的警用无人机

随着 5G 商用网络在全国大范围铺开，警用无人机与 5G 的结合应用也在蓬勃发展。2020 随着 5G 商用网络在全国范围内的大面积铺开，警用无人机与 5G 技术的结合应用也在蓬勃开展。在 2020 年，浙江杭州就成为较早使用 5G 网络进行无人机执法的典型案例，通过 5G 超高速传输实现无人机拍摄和传回 4K 超清视频。2021 年，山东青岛也与移动公司合作，使用 5G 网络让无人机进行高效巡逻。近年来，在重庆、深圳等城市，利用 5G 无人机进行春节和边境巡逻，并实现无人机实时传输高清画面和远程控制。北京等地更是推陈出新，使用 5G 打通天地数据链，将警用车辆、警用无人机无缝连接，建立天地一体的智能综合信息系统[1]-[8]。

5G 为警用无人机提供了 Gbps 级的高峰值数据率、1 ms 以下的超低时延以及海量连接的支持，使其获得了实时传输高清视讯和稳定控制指令所必须的通信保障，从而实现了跨区域、高动态的执法监控，极大提升了警务工作效率。与此同时，5G 通信的低延迟和海量连接，可以支持警用无人机之间进行灵活的组队协作。通过 5G 共享数据，无人机群可以建立起完整的任务区域画面，进行精确的目标识别和跟踪，实现协同决策。

1.2. 基于 5G 的公安物联网

5G 作为新一代信息技术，为物联网发展提供了强有力的支撑。5G 具备高速率、海量连接、低延时等技术特征，使物联网终端和应用可与云端进行实时、高效交互，从而推动新兴物联网应用蓬勃发展。同时，海量物联网设备对网络提出更高需求，5G 凭借技术优势满足物联网的接入和传输需求。在公安领域，5G 可为大量物联网设备提供高速低延迟连接，公安利用 5G 支撑的物联网技术，可以部署各类传感器设备，构建精细化的安防预警和监控系统，全面提升公共安全领域的作战效能。例如，在重要场所布置人脸识别摄像头，在公共区域收集声音、图像、温度等多维数据，并通过 5G 网络实时传输到云端分析，实现对突发事件的预警和响应，大幅提升公共安全治理效率。5G 还可支持公安系统实现更多智慧化应用，如人脸识别、VR 虚拟模拟等，可以进行虚拟的案发场景模拟和侦破演练，有助提升警务工作效率和案件侦破率。此外，警用机器人也可以通过 5G 进行远程控制，例如远程驾驶警用机器人进入化学品泄露区域进行侦查，避免人员近距离接触危险[9]-[14]。

1.3. 基于 5G 的 110 接处警

5G 技术的应用为 110 报警接处警工作带来了革命性的进步。在报警环节，民众可以通过 5G 网络实时上传现场视频，提供清晰、详细的情况告知。110 指挥中心利用 5G 定位快速派遣就近警力响应，还可远程连接现场监控进行风险评估。抵达后，警力通过佩戴单兵设备，配合 5G 实时传输让指挥中心全程掌握处警过程，并利用大数据分析提供关键情报支撑。此外，5G 车载终端可为警车智能导航以优化路线，大大提高了警力反应速度。返回填写电子笔录时，系统自动提取 5G 设备内容生成文本，免除了重复操作。可以说，5G 技术实现了 110 报警全链路的信息化、智能化和可视化，使公众报警更安全便捷，警力出警更高效精准。

1.4. 基于 5G 的新一代警用通信体系

2021 年，工业和信息化部印发《“5G + 公网安”工程建设行动计划(2021~2023 年)》，提出 2025 年要基本建成新一代宽窄融合的公网安通信基础设施体系。该计划的背景是，我国正处于经济社会数字化转型的关键时期，各行业对深度融合 5G 等新一代信息技术的需求日益增加。在公安领域，对利用信息化手段提高工作效率和能力的要求也越来越高。但是，传统以窄带为主的警用数字集群通信系统，已难以满足海量视频、图像等数据的传输需求，及对高移动性警务的支持。因此，采用 5G 等宽带移动通信网络与公安专网系统实现融合，发挥各自的技术优势，是公网安通信建设发展的必然趋势。

举例来说，应急通信是当前宽窄带融合通信系统在警务工作中的一个重要应用形式。当执行任务进入无法通信网络覆盖的区域时，可以利用装载 5G 基站和 PDT 基站的移动应急指挥车，在现场快速建立起无线通信网络。可同时使用支持 5G 和 PDT 的智能对讲机，通过 5G 网络传输高清图像视频，通过 PDT 网络进行实时可靠的语音指令通信。指挥车利用卫星和微波链路，与后方指挥中心保持通信联系。这样，就可以在无通信网络覆盖的偏远地区，利用 5G 和 PDT 的宽窄带融合应急通信系统，保证警务工作的顺利开展。这充分体现了宽窄带融合通信系统在扩展警务工作范围和确保任务完成方面的重要作用。

2. 5G 应用于公安工作出现的问题

2.1. 资源配置问题

2.1.1. 5G 网络覆盖范围有限

5G 网络商用布局与公安通信覆盖需求存在明显差异。为满足用户流量密集的需求，5G 商用网络重点布局在人口稠密的城市热点区域，然后从内向外逐步推进至城市周边、县区、乡镇和人口聚集的行政村。因此，偏远地区和边境地区的 5G 基站架设相对较少。而公安通信信号需要覆盖市县主城区、党政机关、商业网点、人员密集区域，以及边境地区、城市卡口、国省干道和高速公路沿线，还要兼顾重点乡镇和重要场所，这需要实现全区县乃至村级的连续覆盖，与 5G 商网覆盖侧重城市和热点区域的特点不符，无法满足公安业务对广泛区域覆盖的要求。此外，5G 基站建设成本高，运营商面临建设资金量大、建设周期长等问题，短时间内无法实现全面连续覆盖。现阶段公安部门无法放弃公安无线专网，需要继续依靠警用数字集群通信网(PDT)、340 M 公安无线图传网、350 M 移动通信网、LTE 专网、Mesh 自组网和卫星专网等，以免严重影响日常警务工作。

因此，5G 信号在当前只能作为公安通信网络的一个有限补充。为深入拓展 5G 在公安业务中的应用，必须跳出商用网络的覆盖思路，根据公安通信的应用场景和覆盖需求，进行差异化的 5G 网络规划和建设。

2.1.2. 室内分布覆盖不足

公安工作中的许多重要场景发生在室内，如办公区、审讯室、地下停车场等，这就需要 5G 提供可

靠的室内无线覆盖。但是 5G 使用 3~6 GHz 等毫米波高频段，容易受建筑遮挡衰落，导致室内覆盖效果较差。另外，5G 基站密度不足，室内小基站覆盖有限，室分小基站覆盖不足，无法提供均衡的室内信号。而且 5G 终端天线性能有待提升，而运营商更关注室外热点覆盖，室内覆盖部署不足。公安对网络安全管控的要求，也增加了在商用网络环境下建立独立的 5G 警用室内子网的难度。因此现有的 5G 室内小基站无法满足警用对关键室内区域的专项覆盖需求。

2.1.3. 警用无人机通信受限

商用 5G 信号服务的建设之初，主要是以地面用户为服务对象，基站天线波束朝下辐射，一般仅覆盖地面以上 120 米空域。但根据《公安机关使用警用无人机的规定(试行)》(公安部令第 140 号)第十七条，警用无人机任务飞行高度不设限制。实际作业高度常在 100~300 米左右，可能超出现有商用 5G 基站覆盖高度。这导致警用无人机不能在任何空间都能使用稳定且良好的 5G 信号。现有的商用 5G 基站无法满足警用无人机在更高海拔作业的需求。

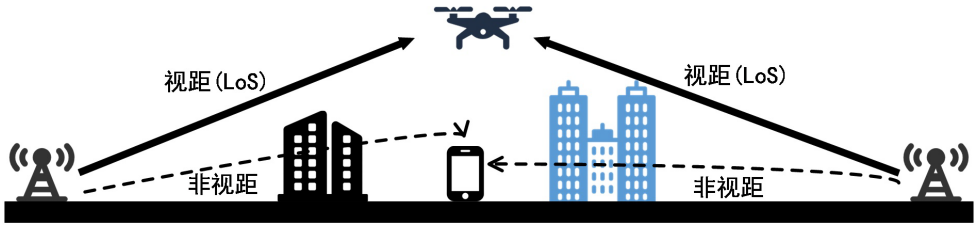

Figure 1. Communication signal connection diagram
图 1. 通信信号连接示意图

与此同时，如果大量投入使用 5G 警用无人机，随着无人机飞行高度的增加，高空环境更加开阔，高楼大厦对信号传播的屏蔽和衰减影响也越小，无人机与 5G 基站之间更容易建立直通视距(LoS)连接，无人机也更容易获得良好的直射信号质量(如图 1)。但这可能会对地面用户(非视距连接)产生一定程度的干扰，与 5G 商用网络建设初衷不符，也是限制 5G 网络服务警用无人机的问题之一。

此外，无人机在大气中的运动极为复杂，难以精确控制。例如，无人机的高机动性和任意变加速会引起接收信号频率的突然和瞬态变化。信号快速变化也增加了切换次数，高切换率可能导致更多切换失败，进而造成严重的乒乓效应(Ping-Pong Effect)等移动性相关问题。因此，当前 5G 的切换技术在处理无人机通信时，仍存在一定局限性。

2.2. 安全性问题

2.2.1. 数据传输安全隐患

5G 网络大幅提升了公安通信的数据传输速率与能力，但也带来了数据传输安全的潜在隐患。首先，5G 网络采用基于 IP 的开放架构，其安全性和稳定性还有待长期运行检验，而公安对通信保密性和抗攻击性要求极高。黑客可以通过攻击 5G 网络结构中的新漏洞获取敏感数据。其次，5G 条件下视频、音频、图像等多媒体数据流量大幅增加，对加密算法的性能提出了更高要求，需要更强大的计算能力来支持实时加密。再者，5G 网络切片技术和物联网的应用极大地扩展了连接的智能终端数量，这导致了网络的入侵面增大，也增加了被网络攻击的概率。最后，新型网络攻击手段层出不穷，5G 网络的防护体系也面临被未知攻击手段突破的风险[15]。

这些因素都可能导致公安敏感数据在 5G 网络传输过程中被非法获取，使用 5G 网络进行数据传输存在一定的安全隐患。

2.2.2. 系统及设备安全漏洞

尽管 5G 网络可以通过加密技术保护信息安全，但系统和设备层面依然存在安全风险。一方面，5G 的开放性较强，公安系统与各类终端和数据库对接，存在被非法访问和数据泄密的隐患。大量互联的智能终端也可能因软硬件漏洞而被远程控制或植入木马。另一方面，存储重要数据的 5G 存储设备以及分布广泛的基站等关键基础设施，包含成百上千个供应商的组件，这些组件在制造和运输过程中很容易被植入后门程序或恶意代码，同时也面临物理破坏的威胁。

相较于 5G 民用网络，专网能够提供更加可靠的安全防护，以保障数据和通信的机密性和完整性。由于 5G 技术的开放性和灵活性，它存在许多潜在的安全风险，因此公安系统在选择采用 5G 技术时必须保持高度警惕，确保网络的安全性。

2.2.3. 实际应用中的可控问题

公安专网，如同一台精密的机器，可根据实际需求灵活地调配系统资源，实现单呼、组呼、优先级通信等多种功能。它还可以遥控站点与信道，一旦遇到干扰立即关闭。作为公安系统的神经中枢，公安专网就像我们手指可及的每一处脉动，掌控着整个系统的运行，为公安工作提供强有力的支持。

相比之下，民用 5G 网络虽然开放，但其控制力及控制粒度远不及专网。对于公安系统而言，需要的不是一张大而繁杂的网络，而是一张可调可控、精密可靠的专网。因此，公安系统必须具备自主管理能力，这是确保公安无线网络安全性和稳定性的必然选择。

2.3. 运营成本问题

考虑到资源配置和安全性问题，公安系统在利用 5G 公网的同时，也需要在关键区域和重点部门自建 5G 专网。单个 5G 基站建设就需要大量资金，要实现公安重点区域的全面 5G 覆盖，基础设施投入将是一大笔支出。与此同时，5G 终端和专用设备价格也高于 4G，短期内不太适合大规模配置使用。另外，5G 的运维成本也高于 4G，这部分经费在可预见的未来也需要持续投入。更关键的是，要实现 5G 应用，还需统筹升级各警用信息系统和通信系统。总之，从基建投入到运维支出，再到系统改造，要实现 5G 网络在公安系统的规模化应用，必须稳扎稳打、循序渐进。

3. 解决方案

3.1. 统筹警用无线资源配置

3.1.1. 扩大 5G 网络覆盖范围

为充分发挥 5G 技术在公安工作中的优势，采取以下措施扩大 5G 网络覆盖范围：一是可以考虑与电信运营商开展合作，选择在城市重点区域、公共场所和交通要道等优先建设 5G 基站，使关键区域和设施实现 5G 网络的全面无缝覆盖。二是利用 5G 网络切片技术，构建独立的 5G 警用专网，保证警务工作尤其是突发事件响应和重要活动安保中的网络需求。三是向移动警力如警用车辆、警用无人机等配置 5G 移动基站，解决偏远及边境地区 5G 网络覆盖不足的问题。通过持续改善 5G 网络基础设施建设，可以为公安无线网络工作提供有益保障。

3.1.2. 针对公安工作优化 5G 室内覆盖建设方案

可通过设计有针对性的 5G 室内覆盖方案，提高室内 5G 信号质量。

首先重点确保政府机关、车站地铁、博物馆、图书馆、机场、医院、学校、体育场馆等关键室内区域能够实现 5G 室内全覆盖。其次使用多种室内配网技术，实现关键区域 5G 信号的无间断衔接和全方位覆盖。主要采用小基站、分布式天线、WiFi 热点等技术进行组合配网，对室内无线信号盲区有效补充。

针对案件多发的大型建筑群和地下区域等难以覆盖的场所，可以采用室内光纤分布、中继器等技术有效地增强室内无线信号发射强度，提高深室覆盖效果，确保信号能够到达每一个角落。另外，利用多频段及高低频段组合进行室内网络规划，可以充分利用不同频段的传输特性，有效改善室内无线信号的穿墙覆盖能力。

面对日新月异的高科技犯罪和复杂多变的环境，公安部门可以考虑与电信运营商和室内覆盖设备供应商展开深入合作，根据公安工作的特点和需求，共同研究设计定制化的 5G 室内覆盖方案。通过技术与应用的深度融合，解决 5G 室内覆盖将有助于公安部门革新通信手段和提高通信速率，从而提升工作效率。

3.1.3. 适配于警用无人机的 5G 网络

1) 为警用无人机建设专用网络或划分单独的频段

构建警用无人机专用网络无疑可以提供专属的信号覆盖和质量保障，确保通信速率。但是考虑到目前警用无人机数量有限，加之严格的飞行管理制约，投入建设整张独立网络不大可行。另外，仅为警用无人机划分单独频段资源也存在一定浪费，尚不实际。但随着无人机技术日趋成熟，无人机应用场景扩大，警用无人机数量增加，建设专用网络或分配专用频段将成为可行的网络规划选择之一。届时可评估无人机通信需求及频谱资源状况，以更经济高效的方式支撑警用无人机通信。

2) 警用无人机网络切片

目前，可以考虑采用网络切片技术，基于公共网络动态划分出逻辑子网，针对不同使用场景，按需为警用无人机提供网络资源隔离和优先调度，提供差异化的专网服务质量保证。例如，在实际飞行测试中，发现无人机在低空飞行路线上出现主服务小区频繁切换的情况，可以针对这些邻区关系，通过调整切换参数进行专门的网络优化，如采用切换迟滞、针对关键小区设置切换偏置等措施，规避频繁切换的影响。具体可以通过切片的方式，对警用无人机切片采用不同的切换机制和参数进行个性化优化和调整，以提高切换性能。总之，可利用 5G 网络切片技术为警用无人机通信提供重要支撑，实现场景化的网络调优，充分发挥 5G 网络的灵活性，动态满足警用无人机的通信需求。

3) 减轻对地面用户的干扰

首先，可以采用大规模 MIMO 天线，适当调高上方的天线旁瓣增益，实现对地面用户和低空无人机的一体化覆盖，解决目前 5G 基站覆盖高度不足的问题。

其次，可以通过智能的无线资源管理，实现地面用户和空中无人机的动态频谱和时隙分配，甚至可以基于机器学习和深度学习算法，创建切换模型，持续优化切换策略，使地面和空中业务实现良好的协同与优化。在无人机侧，可以使用固定波束天线网格系统，发挥其精确指向性的优势，将辐射能量集中投射到预定方向，从而大大降低对地面用户的旁瓣干扰。另外，通过与地面基站的混合接入，无人机可以快速切换到地面小区信号较强的位置，降低其对地面基站覆盖范围边缘的干扰。这种空地混合接入系统的设计，既满足了无人机的覆盖与速率需求，也尽可能减轻了其对地面用户的干扰影响，实现了空地用户的协调共存。

3.2. 警用 5G 网络安全性措施

3.2.1. 数据传输安全

为保障警用 5G 网络的数据传输安全，可以综合采取网络隔离、访问控制、数据加密、统一安全管理等技术手段进行保障。

1) 网络隔离和切片技术

可以利用 5G 网络切片技术，按照警用组织、业务类型、安全级别等要求划分出多个逻辑子网。每

个子网均作为独立的封闭网络单元，实现用户、数据和管理的隔离。子网间通过受控的接口进行有限的互联和交互。这种方式既可以根据警用业务需求提供定制化网络，也可以有效阻止来自公共网络的攻击。

尽管切片技术有其优势，但鉴于切片技术标准仍不完善，在采用时还需注意以下几个方面：首先，警用部门需要制定完善的网络切片安全策略，建立系统的风险防范和应急响应措施，在发生安全事件时能够快速有效地采取应对；其次，通过强大的安全边界和严格的访问控制机制，包括使用虚拟隔离、安全网关和防火墙等来限制切片间的通信和访问，防止未经授权的实体进入敏感切片，确保切片间的隔离；再次，引入安全的切片认证和授权机制，确保只有通过身份验证和授权的用户和设备才能访问特定的网络切片；最后，建立切片流量监测和入侵检测系统，对切片流量进行实时监控和分析，以便及时发现异常活动和潜在的安全威胁，并采取相应的安全应对措施。

2) 细粒度的访问控制

针对警用 5G 网络的访问控制，可对每个警用用户建立数字身份，进行多因素身份认证，绑定用户级安全策略，提高身份验证强度。对警用终端也可实施硬件检测、数字指纹等识别方法，授予最小权限的临时访问凭证。通过建立精细的身份认证和授权体系，以及严密的终端安全管理，可以有效实现警用 5G 网络的零信任访问控制，防止非法入侵。

3) 加强加密保护

为保障警用 5G 网络数据的保密性，应全面提高加密机制的强度。具体来说，需利用 5G 本身的加密算法，对用户身份、终端信令及业务数据流进行加密传输，防止信息泄露。同时，还需定期优化改进加密算法，增加被破解的难度；并建立严密的密钥管理体系，防止加密密钥被盗用或泄露。只有持续强化加密手段，并做好密钥管理，才能始终保证警用无线网络业务数据的保密性及传输安全性。

4) 自动化安全运维

可以通过建立人工智能 AI 驱动的统一安全管理平台，实现警用 5G 网络安全管理的智能化和自动化。该平台应具备全网范围的安全风险评估、资产监测、用户行为分析、威胁情报共享及漏洞扫描等安全防护功能。通过运用机器学习和大数据分析技术，平台可以持续主动发现网络的风险隐患和安全威胁，实现对网络安全态势的智能感知。在检测到网络异常或存在攻击行为时，平台将根据情况主动做出隔离审计、网络接管等对应措施，实现智能化的网络自我防护和快速应急响应。构建这样的自动化安全管理平台，将大幅提高警用 5G 网络的安全防护能力，使得对各类网络威胁能进行快速精确的监测和处理。

3.2.2. 重视设备和基础设施安全

为全面提升警用 5G 网络的安全性，公安部门必须高度重视设备和基础设施的安全防护，从供应链、运维、物理防护等方面采取有力措施，以消除系统安全隐患。一要加强供应链安全管理，对 5G 设备和软件的生产商进行严格安全审核，杜绝使用安全可靠性无法保证的供应商。同时应对关键组件实施全生命周期安全跟踪，防止组件在制造和运输环节被植入后门。二要建立规范的 5G 基础设施运维体系，实施严格的版本控制、漏洞修补和日志审计，对网络设备管理员进行多因子认证。只有全方位提升 5G 基础设施的供应链安全、运维安全及物理安全，公安部门才能有效降低警用 5G 网络面临的安全风险。

3.2.3. 智能呼叫处理与控制能力

为实现 5G 网络具有专网般的强大呼叫控制能力，可以在保障数据传输安全的前提下，通过在 5G 核心网内引入专网功能组件并与 5G 核心技术进行有机融合来实现。具体做法是：利用网络切片技术在公共 5G 核心网上创建安全的专网逻辑子网，实现呼叫控制、业务调度、资源优先级管理等功能；依托 5G 的服务质量保证机制为关键用户提供优质通信服务；采用 IP 多媒体子系统和多接入边缘计算等技术实现按需呼叫策略控制和低延时呼叫响应；开发安全的呼叫处理应用服务器并集成到 5G 网络中；利用 5G 的

数据分析能力提供安全的环境监听等功能。

通过在 5G 核心网内嵌入专网功能模块，并实现与 5G 核心技术的深度融合，5G 网络不仅可以获得与专网类似的呼叫处理与强大控制能力，还可以做到更加智能化。

3.3. 降低成本，共建警用 5G 网络

考虑到 5G 网络建设的高投入和公安系统的安全需求，推进 5G 网络在公安领域的规模化应用，需要采取循序渐进的策略。可以分类规划重点区域、重要单位及普通需要区，分批分期建设 5G 专网，既满足关键区域需求，又节省投资；与运营商和相关部门探索基础设施共建共享，减少基站和传输网络建设投入；因地制宜保留适量 4G 网络，与 5G 网统筹部署，实现混合网络；终端、专用设备及系统改造可按需求和步骤逐步推进，分期分批实现 5G 融合，避免一次性大规模投入。通过分区域分期建设、探索共建共享、4G/5G 混合部署、费用平滑化等策略，不仅能满足公安 5G 网络应用需求的逐步提升，也兼顾了警用无线网络建设的经济效益与安全性。

4. 总结与展望

本文通过分析 5G 技术在公安领域的应用现状和问题，提出了深入推进 5G 技术在公安工作中应用的对策建议(参考文献分类梳理见表 1)。为推进 5G 在公安领域的应用，需要统筹警用网络资源配置，重视警用无线网络数据安全，并关注设备和基础设施安全，提升网络的可控能力，最后要降低 5G 网络建设和运维成本。总之，5G 在推进公安信息化建设中将发挥重要作用，为公安工作的信息化建设打开了新的思路和提供了关键的技术基础，为公安工作的多场景、多业务提供了升级和革新的可能性，有助于侦查打击、现场执法、临时布控以及融合指挥等公安实战工作。例如警用无人机通过搭载 5G 网络，可以实现实时传输高清视频和稳定控制指令。公安利用 5G 支持的物联网技术，部署各类传感器设备，构建精细化的安防预警和监控系统。同时，可以利用 5G 宽带移动通信网络与公安专网系统融合，实现宽窄融合，满足公安工作中海量视频、图像等数据的传输需求。通过 5G 网络切片，可以在公网上实现超高速专网通道，确保公安关键业务的安全和无干扰传输，并实现按需定制的端到端网络服务。此外，5G 与边缘计算的结合将成为公安安防工作的关键技术应用。

Table 1. Reference list
表 1. 参考文献梳理

序号	内容	文献编号	分类
1	优化 5G 室内覆盖建设方案	[16]-[25]	统筹警用无线资源配置
2	适配于警用无人机的 5G 网络	[9]-[14] [26] [27] [28] [29]	
3	网络隔离和切片技术	[30]-[37]	
4	细粒度的访问控制	[38]-[43]	警用 5G 网络安全性措施
5	加强加密保护&自动化安全运维	[44]-[49]	

5G 技术在公安领域的应用前景和成效备受期待，以下几个方面尤其值得业界的关注和深入研究：

1) 为警用 5G 网络建设专用网络或划分单独的频段。虽然切片技术与网络隔离为专用网络带来了可能性，但是由于极大地扩展了接入终端，专网遭受攻击的风险也相应增大。因此专用网络可以提供更高的安全性和可靠性，确保警务通信不受外界干扰和攻击。

2) 运营商的 5G 警用专网切片技术还需要有针对性的成熟和优化，特别是在加密方面，需要采用先进的加密算法，确保数据传输过程中的机密性和完整性。其安全性需要由具备资质的第三方权威认证机

构进行测评认证，以符合公安警务行业的网络安全规范。

3) 充分利用 5G 技术的高峰值数据率、超低时延以及海量连接的优点和现有公安通信系统资源，采用标准化消息传输协议、灵活可靠的组网方式、安全保密的通信传输信道，搭建全新的警用通信技术，满足不同环境下执行多种任务的各级公安机关共享现场态势和实时指挥控制的需求，将上述所有应用串连起来互通有无，可以称之为警用数据链[3]。

4) 依托 5G 技术研发具有小型化、芯片集成化和软件化的警用综合化通信终端。将其设计成集成 5G、4G、WiFi、蓝牙等多种通信技术的小型手持设备，具备软件更新功能以满足不同执法需要，还可以与其他警用设备和系统进行无缝集成，如警用无人机、警用车载终端等，在降低执法人员的负重的同时实现信息共享和协同作战。

基金项目

江苏省教育厅高等学校哲学社会科学基金项目(2019SJA0534)。

参考文献

[1] 武龙, 邱祥平. 5G 技术在公安 110 应急反应机制中的应用[J]. 电信快报, 2022(8): 26-28.

[2] 张春慧, 周昕. 5G 技术下的公安行业应用探索[J]. 数字技术与应用, 2021, 39(10): 94-96+236.

[3] 高晓旭, 王海涛, 卢风云, 等. 5G 技术在公安机关警务合成行动领域的应用[J]. 电子元器件与信息技术, 2021, 5(12): 63-65+68.

[4] 柏维权, 左涛. 5G 时代的公安无线专网通信[J]. 物联网技术, 2021, 11(10): 36-37.

[5] 洪伟权, 陈久雨, 张海涛. 5G 移动警务创新应用及落地实践[J]. 通信企业管理, 2022(4): 66-68.

[6] 胡彬, 徐胜, 余爱民, 等. 公安 340 MHz 频谱基于 5G 技术的应用研究[J]. 数字通信世界, 2021(1): 24-28.

[7] 黄伟国, 李荣, 马鑫. 借力 5G 网络提升公安网络信息化能力[J]. 通信与信息技术, 2021(2): 93-95.

[8] 周德山, 唐俊胜, 王向龙, 等. 面向公安系统的 5G 专网分类及部署研究[J]. 邮电设计技术, 2021(9): 931-935.

[9] 吴文博, 唐艳. “5G + 无人机”的应用与发展问题研究[J]. 中国无线电, 2021(4): 71-72.

[10] 赵建先, 阮肖宾. 5G 通信面向无人机物联网低空覆盖组网探讨[J]. 广西通信技术, 2022(4): 1-8.

[11] 高骏峤, 周磊, 曹越, 等. 5G 无人机安全研究综述[J]. 移动通信, 2023, 47(1): 59-64.

[12] 付道繁. 兼顾民用无人机通信的 5G 网络部署方案探讨[J]. 电信快报, 2020(3): 6-11.

[13] 董春利, 王莉. 未来无人机网络及其切换挑战[J]. 软件, 2023, 44(7): 175-178.

[14] 万旖, 张法进, 王良慧. 无人驾驶飞行器在 5G 网络中的应用[J]. 信息通信, 2020(1): 29-30.

[15] 胡雪. 5G 网络安全问题的分析[J]. 数字通信世界, 2023(9): 47-49.

[16] 班亚明. 5G 与 4G 室内分布系统建设对比分析[J]. 江苏通信, 2023, 39(4): 31-34.

[17] 杨勇, 孙舒淼, 王国华, 等. 南京地铁 5G 公专网智能应用探索及实践[J]. 铁路通信信号工程技术, 2023, 20(8): 59-65.

[18] 王玺, 杨峥, 张鹏, 等. 地铁场景下 5G 网络立体覆盖方案的探究[J]. 物联网学报, 2023, 7(3): 103-112.

[19] 陶春花. 5G 网络建设发展历程解析[J]. 数字通信世界, 2023(10): 1.

[20] 谭亮, 石磊, 刘盛强, 等. 5G 室内通信网络规划与设计经验介绍[J]. 通信与信息技术, 2023(4): 73-76.

[21] 杨洁. 5G 时代室内分布系统的规划与设计研究[J]. 电子元器件与信息技术, 2023, 7(7): 147-150+154. https://doi.org/10.19772/j.cnki.2096-4455.2023.7.036

[22] 陈璐. 5G 室内分布系统规划与设计[J]. 科技与创新, 2021(24): 94-95+99.

[23] 梁力维, 魏广宁. 5G 室内分布系统解决方案[J]. 移动通信, 2019, 43(12): 67-73.

[24] 黎亚洲, 周文渊. 5G 室内分布性能与建设策略[J]. 电信技术, 2019(8): 9-11.

[25] 于建辉. 5G 网络室内覆盖解决方案的分析[J]. 中国新通信, 2019, 21(1): 32.

[26] 陈彦芳, 张雄, 李建辉, 等. 基于 5G 网络无人机的设计与实现[J]. 电子制作, 2023, 31(19): 47-51.
[27] 陈振龙. 基于 5G 的无人机智能组网的应急通信技术开发及应用[J]. 数字技术与应用, 2023, 41(1): 34-36.
[28] 贾维敏, 杨龑, 赵建伟, 等. 无人机蜂群通信感知一体化关键技术[J]. 国防科技, 2023, 44(3): 88-95.
[29] 车辉. 基于 5G 的立体化智慧安防建设方案设计[J]. 广播电视网络, 2022, 29(1): 52-55.
[30] 冯登国, 徐静, 兰晓. 5G 移动通信网络安全研究[J]. 软件学报, 2018, 29(6): 1813-1825.
[31] 王睿, 张克落. 5G 网络切片综述[J]. 南京邮电大学学报(自然科学版), 2018, 38(5): 19-27.
[32] 胡颖. 5G 网络切片关键技术综述与应用展望[J]. 数字通信世界, 2023(9): 111-113+116.
[33] 牛犇, 游伟, 汤红波. 基于安全信任的网络切片部署策略研究[J]. 计算机应用研究, 2019, 36(2): 574-579.
[34] 马洪源, 肖子玉, 卜忠贵, 等. 5G 边缘计算技术及应用展望[J]. 电信科学, 2019, 35(6): 114-123.
[35] 王淼. 面向隔离需求的网络切片部署方法研究[D]: [硕士学位论文]. 郑州: 战略支援部队信息工程大学, 2023.
[36] 卜绪萌. 5G 网络切片安全认证机制研究[D]: [硕士学位论文]. 西安: 西安电子科技大学, 2023.
[37] 刘建伟, 韩祎然, 刘斌, 等. 5G 网络切片安全模型研究[J]. 信息网络安全, 2020, 20(4): 1-11.
[38] 刘津羽. 5G 北向接口安全访问策略研究[J]. 广东通信技术, 2022, 42(11): 34-37.
[39] 李立平, 李振东, 方琰崴. 5G 专网技术解决方案和建设策略[J]. 移动通信, 2020, 44(3): 8-13.
[40] 徐相杰. 面向 5G 网络的数据安全访问控制算法研究[D]: [硕士学位论文]. 南京: 东南大学, 2022.
[41] 刘田. 边缘计算下的两种访问控制方案研究[D]: [硕士学位论文]. 湘潭: 湖南科技大学, 2023.
[42] 李直斌. 5G 网络安全技术发展展望[J]. 知识文库, 2020(3): 52.
[43] 张雷, 杨杰. 5G 网络安全问题探析[J]. 金融电子化, 2020(1): 87.
[44] 张佳乐, 赵彦超, 陈兵, 等. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报, 2018, 39(3): 1-21.
[45] 黄开枝, 金梁, 赵华. 5G 安全威胁及防护技术研究[J]. 邮电设计技术, 2015(6): 8-12.
[46] 强奇, 武刚, 黄开枝, 等. 5G 安全技术研究与标准进展[J]. 中国科学: 信息科学, 2021, 51(3): 347-366.
[47] 冯国聪, 王健, 付志博. 5G 网络信息安全的威胁及防护技术探讨[J]. 工程技术研究, 2023, 8(1): 226-228.
[48] 方东旭, 周徐, 薛晓宇, 等. 4G/5G 极简网络智能运维体系研究和应用[J]. 电信工程技术与标准化, 2023, 36(4): 30-34.
[49] 詹勇, 吴枫. 5G 网络自动化: 从人工运维到全自治[J]. 电信科学, 2022, 38(8): 140-150.