5G 技术支撑下物联网自动化远程控制安全保障研究

王侠

杭州精鼎玻璃制品有限公司，浙江省杭州市，310000；

摘要：随着 5G 网络的规模化部署与物联网设备的普及，远程控制系统在工业制造、交通调度、医疗服务等领域快速发展，实现了生产效率与响应速度的双重提升。然而，远程控制系统的智能化和网络化同时带来了巨大的安全挑战。尤其是在 5G 超高速率、超低延迟、海量连接的特性支撑下，远程控制的数据传输、身份认证、系统防护机制面临更高复杂度的安全风险。本文围绕 5G 技术下物联网自动化远程控制系统的结构特性，深入分析其面临的主要安全威胁，并从网络协议、边缘防护、数据加密、访问控制等多个维度提出系统性的安全保障策略，为构建高可靠性、低风险的远程控制体系提供理论基础与技术路径。

关键词：5G 通信；物联网；远程控制；网络安全；自动化系统；安全防护机制

DOI：10.64216/3080-1508.25.03.044

引言

在工业4.0与“万物互联”愿景加速落地的背景下，物联网（IoT）与自动化控制的融合日趋紧密，远程控制作为其核心应用形式，在电力、交通、制造、医疗、农业等多个领域迅速扩展。传统远程控制系统多依赖于4G 或有线网络进行信号传输，存在传输时延高、网络带宽不足、设备连接容量有限等技术瓶颈，难以满足高实时性与高可靠性并存的业务需求。5G 网络的兴起，特别是其“eMBB（增强型移动宽带）”、“uRLLC（超高可靠低时延通信）”和“mMTC（大规模物联）”三大特性，为远程控制系统带来了前所未有的发展机遇。

然而，在大幅提升通信性能的同时，远程控制系统也暴露于更为复杂和动态的网络安全环境之中。攻击者可以通过 5G 网络劫持控制指令、干扰设备执行逻辑、甚至控制关键基础设施的运行，造成重大经济损失乃至公共安全事故。因此，如何在享受 5G 带来的便利与效率的同时，构建起一个安全可控的远程控制系统，已成为物联网时代安全技术发展的核心议题。本文将围绕 5G 下的远程控制体系架构、安全威胁分析与防护机制设计三方面展开研究，系统梳理问题根源与解决思路，力求为安全可信的物联网应用提供理论与实践支持。

1 5G 赋能下远程控制系统的新架构演化

1.1 网络性能变革对远程控制的推动作用

5G 网络的三大核心能力，即更高带宽、更低延迟和更广连接，为远程控制系统带来了革命性的变化。相比于 4G 网络，5G 在理论上可实现低至 1ms 的时延传输，峰值速率可达 10Gbps 以上，使得原本依赖本地控制器完成的任务可以通过远程服务器或云平台实时调度。在实际应用中，这种性能突破使得诸如工业机器人、自动驾驶车辆、远程医疗手术等对实时性极高的应用场景成为现实。例如，在某大型机械厂中，通过 5G 网络将边缘控制单元与中央指挥平台实时联通，可实现毫秒级的响应与反馈，从而在远程对重型设备进行精密控制时保障操作流畅与无误。

此外，5G 的高连接密度能力使得一个控制单元可同时管理上万台终端设备，显著提升了控制系统的并行处理能力，也使得系统设计从“局部控制”向“协同控制”转型。值得注意的是，远程控制的物理空间从传统的“点对点”跃迁为“面对面”甚至“网对网”，这在极大提升系统弹性与管理能力的同时，也对其安全架构提出了更复杂的要求。

1.2 控制系统向“云-边-端”协同体系转型

随着控制场景的复杂化与任务处理的多样化，远程控制系统的架构正在从传统的集中式控制模型向“云-边-端”协同架构转变。在这一架构中，云平台主要承担指令下发、数据聚合与模型推理等高算力任务；边缘节点则作为本地控制中枢，实现数据初处理与快速反馈；终端设备负责最前线的任务执行与状态采集。5G 网络作为连接这三层之间的高效通道，在带宽与延迟性能方面提供了重要保障。

这一协同架构的优势在于能够根据任务紧急程度灵活分配控制资源，并在通信中断或延迟发生时保持本地控制能力，从而提升系统的鲁棒性与稳定性。例如，在智能电网场景下，终端传感器可实时将数据传输至边缘网关完成初步分析，若检测出异常，再上传云端进行高级决策，进而通过反馈机制优化整体调度策略。整体来看，这种协同机制增强了远程控制系统的分布式处理

能力，但同时也拓展了攻击面与潜在的安全薄弱环节，对系统的安全策略提出更高要求。

1.3 新通信协议与数据流模型的构建需求

传统远程控制系统多依赖 TCP/IP 或 UDP 协议进行数据传输，而在 5G 环境下，这些协议在高频高速、大规模并发连接环境中易出现拥堵、丢包等现象，不利于保障关键控制指令的时效与完整性。因此，面向 5G 远程控制的新通信协议亟需构建。部分新兴的轻量级协议，如 QUIC、CoAP、DDS 等，因其低延迟、高可靠性特性而被广泛关注。

同时，在数据流设计上，系统不再以“集中传送+定时汇总”的方式处理信息，而是倾向于“事件触发+状态流动”的连续交互模型。每一控制事件都伴随着动态数据包的生成、路径选择与反馈验证，构建一种更符合 5G 场景下低延迟特征的数据流通机制。这种变化虽然增强了控制系统的敏捷性，但也加大了对数据链路完整性、数据源验证与流程加密等安全需求的依赖。

2 远程控制系统在 5G 环境下的安全挑战分析

2.1 控制信道劫持与指令篡改风险

远程控制系统最重要的组成部分是各种“指令”——也就是控制端利用网络给被控设备发操作命令，如果这些指令被篡改或者造假了，就可能让整个系统出大问题。在 5G 的网络结构里，控制信道的传输路线从物理层一直到应用层变得更长更麻烦，虽然这样传输速度更快连接设备更多了，但攻击者能找到漏洞的地方也更多了。要是有坏人用假基站、中间人攻击或者信号重放这些方法截获或者偷偷塞指令进去，他们就有机会远程控制重要设备或者让它们乱操作。比如说在智能工厂里，要是机器人的控制系统被黑了，坏人就能改参数，让机器撞东西、焊歪了，或者干脆停机不干活。

5G 的虚拟化功能比如切片技术虽然让资源利用得更好了，不过也带来了隔离方面的新问题。要是某个切片被攻击的话，可能就会波及整个物联网控制网络，让指令发送和反馈都出故障。所以在搞 5G 远程控制的时候，需要重点加强几个环节的设计，比如信号的完整性检查、指令来源的身份确认，还有动态加密通道的设计啥的，这样才能让指令在传输过程中既安全又可靠。

2.2 边缘节点成为攻击重点目标

边缘计算属于 5G 远程控制架构里的重要组成，它是终端和云平台中间的连接东西，负责数据初步处理，做一些简单分析，然后快速做出决定这些工作。不过这些边缘节点很多都放在工厂现场、交通要道、基础设施最边边的地方，本身安全性就不太好，装的设备的计算能力也不太行，这就让它们变成黑客最先想攻击的地方。如果边缘节点被黑客搞到手的话，他们不光能拿到一大堆现场的数据，还能通过这个去改控制指令，让终端设备被控制，或者让整个控制流程出问题。

另外边缘节点之间有很多点对点的数据传输和一起协作，这种横向的连接方法太复杂了也让一个地方被攻破可能变成大范围感染问题。比如有个石油公司的边缘网关被攻击案例里，黑客利用漏洞进入了一台没有加固过的边缘节点，然后拿到了远程控制的密钥，导致了上百台设备乱掉、数据都泄漏了。所以边缘计算安全应该被当作 5G 远程控制系统建设里最要紧的事，需要做好本地身份验证、设置防火墙、行为监控和软件加固这些多层次的保护手段，避免攻击在边缘这边发生，同时阻止它们扩散。

2.3 数据传输与隐私泄露的双重隐患

远控系统在做任务时会生成好多设备状态的数据、操作记录和反馈信息这些机密的东西，5G 这种高速网络虽然让数据传得特别快让控制更方便了，但这些数据在传输过程中可能被别人中途拿走或者乱改。尤其是医疗啊金融啊电力这些领域，那些控制设备的数据经常直接连着用户的身份信息、商业机密还有国家运行的基础数据，要是这些数据被泄漏出去的话事情就会变得特别糟糕。

在现有 5G 系统里，虽然有 IPSec、TLS、SSL 等多种加密通讯方式，但实际使用时经常因为考虑到性能或者设备兼容性问题，导致存在数据明文传输的情况。而且 5G 边缘节点和终端设备的资源都比较有限，很难运行复杂加密算法或者经常交换密钥，这让数据传输的安全性变得不够稳定。另外现在很多物联网终端用嵌入式芯片和开源系统，如果缺少系统层面的管控策略的话，攻击者很容易利用漏洞窃取数据甚至上传病毒程序，破坏控制系统。所以必须针对 5G 远程控制系统的整个数据传输路径进行全程安全监测，从底层通讯到上层应用，每一层都要做数据加密、权限管理、数据完整性验证这些隐私保护措施。

3 5G 环境下远程控制系统的安全保障机制构建

3.1 构建以身份为核心的分层认证体系

现在 5G 物联网远程控制用到很多设备，这些设备经常连进来，以前那种用固定密码的单一验证方法不够

安全。为了确认通信的设备和操作都是可靠的，必须建立以身份验证为主的多层认证系统。第一步连设备的时候要用 SIM 卡或者 TPM 芯片这些东西，给每个设备单独编号，这样能查到哪里来的。同时用零信任的方法，每次设备要和平台打交道都得重新检查。第二步在边缘层和云平台中间，需要弄双向 TLS 认证，用证书来保证传数据的时候不被偷看或者篡改。特别重要的地方还要多因素认证，比如用密码锁、手机定位或者指纹这些方式，这样安全性更高。

另外，应该要建立一个统一平台来管理身份，能够支持设备身份进行实时注册、取消、更新和授权的处理，做到不同领域不同系统的认证方式统一管理。管理策略不仅确定谁能访问，还要说清楚可以访问哪些东西，什么时候能访问，能做哪些操作。这样就能从识别身份开始到限制行为进行整体管理，让远程控制整个过程的审查都包括进去形成完整的流程。

3.2 引入可信计算与边缘防御能力协同机制

关于边缘节点可能被攻击或者篡改的问题，可信计算变成了保护远程控制系统中边缘安全的重要方法。通过在硬件里加入信任根比如 TPM/TEE 这种东西，能让系统启动时候保持完整并且控制逻辑不会被修改。再加上边缘网关那边做的行为模式分析和实时监控功能，就可以建立那种'只能运行安全代码、只听靠谱指令'的安全防护，这样就能有效减少被入侵或者被操控的可能了。

同时，我们需要增强边缘节点的防护能力，并在这些节点上布置有自我学习和反应能力的安全代理。这些模块可以通过智能算法对过去的数据和操作记录开展分析，找出不正常的模式，当检测到可能有攻击时，能够马上切断数据连接、恢复成默认设置、触发警报系统。特别是在设备操作频繁、信息特别重要的区域，就可以做到在边缘侧自动发布安全规则并及时更新，让系统拥有‘本地防护、即时应对’的自我处理能力。另外，建立云端和边缘协同保护的模式，当发现有问题操作或者攻击时，就能通过云端的统一管理来调整边缘节点的工作方式，达到安全规则快速统一调整和远程控制的目标，进而形成能够灵活变化、自主调节的多层防护架构。

3.3 完善数据安全保障与隐私保护策略

数据作为远程控制系统里关键的东西，传输、保存和用的时候的安全性问题密切影响系统稳定和大家相信程度。首先，在数据传输方面，应该全面使用端到端加密的技术手段，用 AES-256 这种很强级别的算法把指令、情况和操作记录都加密了，这样就算在传输路上被别人拿到，也解读不出来有用内容。然后还要做完整性检查比如SHA-3算法和时间戳功能，加上签名哈希方法，避免数据被别人随便改动或者造假。

在数据存储和处理时候，应该根据数据分类分级的政策，把敏感数据和普通数据分开处理，严格不让高敏数据随便跨域访问和外部调取的权限。比方说对关键设施运行日志、用户控制命令这些数据，需要安装专门加密存储的模块，搞好多层访问授权和审计追踪的功能；至于各个业务系统之间共享的数据，就要用 API 网关加上沙箱的办法，让信息只能在规定的范围里被控制着使用。

最后一个方面，隐私保护在远程控制系统的长期运行中是最基本的伦理要求。在 5G 物联网的场景下，像远程医疗、智能家居这些应用里边会用到很多用户的私人信息，必须要按照《数据安全法》和《个人信息保护法》这些规定来做，比如收集数据要合法、有明确目的而且不能多收。现在有一些新技术比如说差分隐私和联邦学习，可以在不直接拿到原始数据的情况下做数据分析，这样既能发挥数据的用处，又不会让用户的隐私被泄露或者乱用，这样才能让企业和用户之间保持长期的信任关系。

4 结语

未来，随着工业互联网、车联网、医疗物联网等关键领域的深入应用，远程控制的需求将更加普遍、复杂、关键。构建一个以“身份可信、通信安全、数据保护、边缘自防”为核心的全链路安全保障体系，将成为实现 5G 时代物联网远程控制“敢用、能用、好用”的基础保障。只有在安全与创新同步推进的前提下，远程控制才能真正成为数字化时代高质量发展的中坚力量

参考文献

[1]于海燕.物联网形势下的5G通信技术应用探讨[J].产业与科技论坛，2022，21（1）：30-31.

[2]许振华，王广宇.物联网发展中的5G通信技术应用[J].电子技术与软件工程，2019，8（22）：29-30.

[3]业皓然，杨世舟，张书铭.5G通信技术下的物联网技术应用阐述[J].数字技术与应用，2021，39（10）：3335.

[4]杨万辉.5G通信技术背景下物联网应用发展[J].通信世界,2019,26(12):121-122.

[5]张宁,杨经纬,陈启鑫,等.面向泛在电力物联网的5G通信:技术原理与典型应用[J].我国电机工程学报,2019,39(14):4015-4025.