

公网对讲机在应急响应中的安全通信保障机制

冷雨晨

杭州红蓝黄通讯科技有限公司 浙江 杭州 310000

摘要：应急响应场景如自然灾害、公共安全事件发生时，通信的高效与可靠是救援行动顺利推进的核心要素。公网对讲机以广阔覆盖范围、灵活部署方式等特点，于应急通信领域获得大量实践应用。但由于该设备对公众通信网络存在依赖性，不可避免遭遇数据泄露、信号干扰、恶意攻击等安全隐患。文章剖析公网对讲机在应急响应中的应用实况，探究安全通信所受主要威胁，深入钻研加密技术、网络优化、身份认证等保障手段，从管理策略、技术方案、人员培训等多个层面构建完备的安全通信保障体系，期望能为应急响应中公网对讲机安全稳定运行提供理论支撑与实践指引。

关键词：公网对讲机；应急响应；安全通信；保障机制；加密技术

引言

突发事件降临，应急响应关乎生命财产安全，是减少损失的重中之重，而通信恰似应急救援的“生命线”，左右着救援效率与最终成效。公网对讲机借助运营商移动网络，突破传统对讲机距离局限，实现跨区域、多群组通信，于应急救援中占据关键地位。应急响应场景的独特性，对应急通信的安全性、稳定性提出严苛标准。公网对讲机置身复杂网络环境，面临诸多潜在安全威胁，如何搭建行之有效的安全通信保障体系，保障应急响应时信息精准、迅速传递，已然成为当下亟需破解的重要难题。

1 公网对讲机在应急响应中的应用现状

1.1 应用场景

自然灾害侵袭，地震撼动大地、洪水肆虐城乡，传统通信设施常受冲击损毁。公网对讲机凭借无需自建基站的特性，迅速搭建临时通信网络，助力救援人员跨越区域协同，及时上报灾情，调配救援物资与人力。公共安全事件突发，火灾现场烈焰灼空、交通事故现场混乱不堪，公网对讲机为多部门联合指挥架起桥梁，消防、医疗、公安人员借此实时交流，提升救援协同效能。大型活动安保严密部署、城市应急管理有序开展，公网对讲机于各场景不可或缺，确保信息在各环节畅通无阻、高效传递。

1.2 应用优势

依托运营商规模庞大的移动网络架构，公网对讲机通信范围极为广阔，可达成全国乃至全球通信连接，地理距离与地形地貌均无法对其形成阻碍，相较于传统对讲机，显著延伸通信覆盖范畴。在部署层面，公网对讲机呈现出高度灵活性与便捷性，无需烦琐的基站建设与

维护流程，仅需完成账号开通及设备配置，便能即刻投入运行，可在短时间内迅速构建应急通信网络，契合应急响应对于通信时效性的严苛需求。

1.3 存在的问题

公网对讲机于应急响应中优势显著，却也伴随诸多隐忧。该设备对公众通信网络依存度极高，一旦网络遭遇拥塞、故障或恶意攻击，通信品质将遭受重创，极端情况下甚至致使通信链路中断^[1]。鉴于公网对讲机运行于开放性公众网络环境，数据泄露、窃听及篡改风险始终存在，尤其在传输敏感救援信息过程中，安全隐患更为凸显。各品牌、型号公网对讲机在兼容性与互操作性方面参差不齐，于多部门协同应急响应场景下，设备间通信不畅现象时有发生，掣肘救援行动高效协同推进。

2 公网对讲机在应急响应中安全通信面临的主要威胁

2.1 网络安全威胁

网络漏洞为黑客入侵公网对讲机系统提供可乘之机，他们发动拒绝服务攻击（DoS），阻碍设备接入网络、接收信息，直接造成通信瘫痪。中间人攻击同样频发，攻击者截取、篡改对讲机传输数据，扰乱应急救援指令的准确传达。恶意软件的传播亦构成威胁，像木马程序能盗取设备内救援计划、人员位置等敏感信息，严重危及应急响应安全。此类攻击者还会伪装成合法通信节点，恶意篡改物资调配指令，致使救援资源错配，错过黄金救援时机，给应急工作带来巨大风险。

2.2 数据安全威胁

应急响应所涉数据涵盖受灾状况、救援动态、人员伤亡等敏感内容，传输环节若未实施有力加密举措，极易遭窃取与破解。数据存储层面，若存储设备防护存在缺陷，同样会引发泄漏风险。数据于不同设备及系统间

流转时,由于缺失可靠的数据完整性验证机制,易出现被篡改情形,干扰应急决策的精准度。救援人员的医疗记录若存于防护薄弱的服务器,一旦外泄,既侵犯个人隐私,又会给救援人员带来心理压力,掣肘救援工作的有序推进。

2.3 设备安全威胁

不少设备存在设计瑕疵与安全隐患,易为攻击者所利用。身份认证机制不完备,非法设备便有机可乘,得以接入通信网络、窃取敏感信息或干扰正常通信流程^[2]。应急响应环境往往恶劣,高温炙烤、潮气侵蚀、震动冲击等状况下,设备硬件易出故障,通信功能难以正常运行。设备一旦遗失或被盗,若缺乏有效的远程管控及数据擦除手段,应急通信数据便有泄露之虞。现实中,地震救援时就曾出现对讲机因剧烈震动致使内部元件移位,频繁中断信号。若丢失的对讲机未配备远程锁定与数据清除功能,拾获者不仅能获取灾区地图、救援路线等关键信息,更可能冒用救援人员身份,破坏应急响应的正常秩序。

3 公网对讲机在应急响应中安全通信保障技术手段

3.1 加密技术

将对称加密算法与非对称加密算法融合运用,能够切实增强数据传输的安全性。在数据发送之前,运用对称加密算法迅速对数据加密,以此提升加密效率;借助非对称加密算法交换对称加密的密钥,保障密钥的安全性。于应急救援指令传输过程中,对指令内容实施加密操作,唯有持有正确密钥的接收者方可解密获取信息,从而防范数据被窃取与篡改。同态加密技术也可加以采用,实现在密文状态下处理数据,进一步守护数据隐私与安全。以AES(高级加密标准)作为对称加密算法、RSA作为非对称加密算法的组合,AES凭借高效加密特性契合应急数据快速处理要求,RSA通过安全的密钥交换确保加密体系稳固。伴随量子计算技术发展,抗量子密码算法逐步应用于公网对讲机加密,像基于格的密码算法,能够抵御未来量子计算机可能带来的破解风险,为应急通信数据安全提供更持久保障。

3.2 网络优化技术

软件定义网络(SDN)赋能网络资源弹性调度管理,依应急响应实际需求动态分配带宽,有效缓解网络拥塞困境。网络局部故障发生时,SDN控制器迅速重构数据传输路径,维系通信链路稳定运行^[3]。融合5G、卫星通信等多元通信技术,打造异构网络协同体系,公众网络正常期间5G承载高速数据传输重任,网络受损时卫星通信无缝接管保障应急通信不断线。洪涝灾害场景下

SDN优先保障公网对讲机网络资源供给,实现救援信息实时交互;5G与卫星通信互补架构,确保偏远地区及基站损毁区域公网对讲机通信畅通无阻。边缘计算技术将数据处理存储前置至网络边缘节点,大幅削减数据回传时延,全方位提升公网对讲机应急通信效能与可靠性。

3.3 身份认证与访问控制技术

运用多因素身份认证体系,将用户名、密码与指纹识别、人脸识别等生物特征认证要素深度融合,全方位强化设备身份认证的精准性与安全性。唯有通过完整认证流程的合法设备,方能获取公网对讲机通信网络的接入资格,从源头上有效抵御非法设备的恶意侵入。在访问控制架构搭建中,严格依据不同用户的职能属性与权限等级,构建严密的访问策略体系,对用户接触敏感信息的范围及操作权限实施精细化管控。例如救援指挥人员被赋予高级权限,得以全面查看各类救援数据并下达指挥指令;普通救援人员仅可接收和反馈与其任务紧密相关的信息,以此大幅降低数据泄漏风险。当下,基于区块链技术的去中心化身份认证系统在实际应用中渐成趋势,其依托分布式账本的独特特性,能够有效杜绝身份信息被恶意篡改与伪造,显著提升身份认证的可信度与权威性。与此同时,动态访问控制策略持续迭代升级,可根据用户的实时地理位置变动、任务执行状态转换等多元动态因素,自动触发访问权限的灵活调整机制。如当救援人员深入核心灾区执行关键任务时,系统将依据预设规则自动提升其获取重要信息的权限等级,通过这种方式进一步增强应急通信系统的安全性与响应灵活性,为应急救援工作的高效开展筑牢坚实的信息安全防线。

4 公网对讲机在应急响应中安全通信保障机制的构建

4.1 管理保障机制

多因素身份认证融合用户名密码、指纹人脸生物特征与动态口令卡,随机生成的时间敏感性数字组合强化认证精度与安全性,只有认证完备的设备才能接入公网对讲机通信网络,从根本上杜绝非法设备入侵。访问控制依用户职能权限构建严密策略,实现敏感信息操作权限的分级管控,赋予救援指挥人员全面查看下达指令权限,限制普通救援人员仅能处理任务相关信息,有效降低数据泄漏风险。设备全生命周期管理制度覆盖采购、登记、使用、维护、报废各环节,明确责任归属与操作标准^[4]。设备统一编号标识,定期开展安全检测维护,及时发现修复隐患。采购环节专业测评筛选合格产品,登记时详尽记录设备参数、使用人员与部门信息,形成完备档案体系。应急通信指挥管理体系界定部门职责与

通信流程,保障信息传递精准及时。设立专职指挥中心统筹公网对讲机资源调度,协调多部门通信协作,在森林火灾救援中通过对讲机实时掌握消防、林业、医疗等部门行动,实现资源精准配置。人员安全意识教育与技能培训提升安全通信认知,掌握基础操作与应急处理方法。安全知识讲座结合典型事故案例剖析,强化风险防范意识,将每位使用者塑造为通信安全的前沿防线。

4.2 技术保障机制

推进前沿安全通信技术的持续研发与实践应用,着重完善加密算法、网络优化及身份认证等核心技术。构建安全监测预警系统,实时追踪公网对讲机通信动态与网络安全态势,敏锐捕捉潜在安全隐患并及时发出预警。系统具备智能响应能力,一旦检测到异常,即刻启动防护机制,诸如拦截非法访问、隔离感染设备等。监测到设备遭受频繁网络攻击时,系统迅速切断其网络连接,有效遏制攻击蔓延。深化与通信设备制造商、网络运营商的合作,共同攻克公网对讲机安全通信技术难题,驱动技术创新迭代。携手设备制造商开展新型加密芯片联合研发,提升数据加密效率与强度;与网络运营商协同优化网络架构,于应急响应关键区域布设专用基站,确保通信质量稳定可靠。凭借技术创新与多方协同合作,筑牢公网对讲机安全通信的技术根基。

4.3 培训与演练保障机制

周期性开展公网对讲机操作与安全通信专题培训,聘请领域专家进行授课指导,助力救援人员熟练掌握设备操作、安全配置及常见故障处理方法。培训模式融合理论阐释与实操训练,创设模拟故障情境,推动学员在实践中提升问题应对能力^[5]。策划实施应急通信演练活动,模拟多元应急场景,检验公网对讲机实际通信效能与安全性能,及时发现并整改潜在问题。模拟地震引发

通信网络崩溃情形,考察多部门运用公网对讲机开展应急通信的协同水平。借助演练实践,强化部门间协同配合与应急处置能力,保障公网对讲机在真实应急响应中稳定可靠运行。演练结束后组织复盘研讨,梳理经验教训,将优化后的通信流程与操作规范融入后续培训,构建培训、演练、优化相互促进的良性循环体系。

结语

公网对讲机于应急响应领域展现显著应用价值,然而安全通信难题成为其拓展应用的瓶颈。深入剖析公网对讲机在应急场景下的应用实况、面临的各类安全威胁,探索并运用加密技术、网络优化方案、身份认证体系等保障手段,同时搭建集管理策略、技术措施、培训教育与实战演练于一体的综合性安全通信保障体系,可切实增强公网对讲机在应急响应中的安全可靠性能。展望未来,伴随通信技术持续革新演进,需时刻聚焦公网对讲机安全通信领域涌现的新状况、新挑战,持续优化完善保障机制,为应急响应筑牢通信根基,推动应急救援工作高效有序实施。

参考文献

- [1]牟佳.公网对讲在专业移动通信领域警务工作中的应用探讨[J].警察技术,2018,(05):36-38.
- [2]舒舜.公网对讲业务的发展及其行业应用[J].信息通信,2017,(07):185-186.DOI:10.20153/j.issn.2096-9759.2017.07.086.
- [3]柴长杰.构建防止车辆伤害安全保障体系的思考[J].上海铁道科技,2018,(01):131-132.
- [4]丁思丝,冯铁男,姜成华.我国渔民海上急救通信方式研究进展[J].中华卫生应急电子杂志,2017,3(01):57-61.
- [5]监狱专用对讲机报警定位系统——禁区内的安全防范专家[J].中国司法,2013,(05):106.