

基于5G的智慧机场网络安全方案设计与安全性分析

邢馨心¹, 左青雅², 刘建伟¹

(1. 北京航空航天大学网络空间安全学院, 北京 100083; 2. 北京邮电大学国际学院, 北京 100876)

摘要: 面向智慧机场网络安全方案的实际应用需求, 提出了一种基于5G的智慧机场网络安全方案。该方案分析了智慧机场5G场景的安全特点及安全需求, 从统一安全管控、网络切片安全、安全监测预警、边缘计算安全、物联网感知节点安全5方面总结了当前场景下存在的安全需求痛点, 并设计了基于5G的智慧机场网络安全方案, 其功能组成包括面向泛在网络的5G网络统一安全管控功能、轻量化的5G网络身份认证鉴权功能、面向多业务需求的5G网络切片安全防护、基于大数据分析的5G网络安全监测预警、基于边缘计算的一体化安全防护功能、基于设备行为分析的感知节点安全防护功能, 构建了集业务加密、网络安全、终端可信、身份可信、安全管控于一体的安全平台。此外, 分析了现有5G认证与密钥协商(AKA, authentication and key agreement)协议中潜在的伪造基站攻击。由于缺少对SN转发的消息的真实性验证, 攻击者可以冒充真实的服务网络与用户设备和归属网络进行通信, 从而进行基站伪装攻击。这种攻击可能会导致智慧机场网络数据泄露, 并遭遇敌手的篡改、欺骗等问题。针对智慧机场网络安全需求和5G认证与密钥协商协议的安全问题, 设计了抗攻击的改进5G认证与密钥协商协议, 并通过形式化安全模型、安全目标定义与形式化的安全性分析证明了所提方案的抗攻击能力。

关键词: 5G; 系统设计; 安全协议; 安全性分析

中图分类号: TP393

文献标志码: A

DOI: 10.11959/j.issn.2096-109x.2023075

5G-based smart airport network security scheme design and security analysis

XING Xinxin¹, ZUO Qingya², LIU Jianwei¹

1. School of Cyber Science and Technology, Beihang University, Beijing 100083, China

2. International School, Beijing University of Posts and Telecommunications, Beijing 100876, China

Abstract: To meet the security requirements of smart airports, a 5G-based smart airport network security solution

收稿日期: 2023-05-08; 修回日期: 2023-08-18

通信作者: 左青雅, 3495128112@qq.com

基金项目: 国家自然科学基金(U21B2021, 61972018, 61932014); 国家重点研发计划(2021YFB2700200)

Foundation Items: The National Natural Science Foundation of China (U21B2021, 61972018, 61932014), The National Key R&D Program of China (2021YFB2700200)

引用格式: 邢馨心, 左青雅, 刘建伟. 基于5G的智慧机场网络安全方案设计与安全性分析[J]. 网络与信息安全学报, 2023, 9(5): 116-126.

Citation Format: XING X X, ZUO Q Y, LIU J W. 5G-based smart airport network security scheme design and security analysis[J]. Chinese Journal of Network and Information Security, 2023, 9(5): 116-126.

was proposed. The security characteristics and security requirements of the 5G scenario in smart airport were analyzed, and the pain points of security requirements in the current scenario were summarized in five aspects: unified security management and control, network slicing security, security monitoring and early warning, edge computing security, and IoT-aware node security. And then a 5G network security system was designed for smart airports. The functional components of this system included 5G network unified security management and control functions for ubiquitous networks, lightweight 5G network identity authentication and authentication functions, 5G network slice security protection for multi-service requirements, 5G network security monitoring and early warning based on big data analysis, integrated security protection function based on edge computing, and sensory node security protection function based on device behavior analysis. This comprehensive approach built an all-in-one security platform covering business encryption, network security, terminal trustworthiness, identity trustworthiness, and security management and control. Additionally, the potential counterfeit base station attacks in the existing 5G authentication and key agreement (AKA) were analyzed. Due to the lack of authenticity verification of the messages forwarded by the SN, the attacker can pretend to be the real SN to communicate with the UE and the HN, thus carrying out the base station masquerading attack. This kind of attack may lead to the leakage of smart airport network data, and encounter problems such as tampering and deception by opponents. Aiming at the network security requirements of smart airports and the security issues of 5G authentication and key agreement protocol, an improved 5G authentication and key agreement protocol was designed. Formal security models, security goal definitions, and analysis were performed to ensure the robustness and effectiveness of the protocol against attacks.

Keywords: 5G, system design, security protocol, security analysis

0 引言

5G 作为新一代的通信技术与智能产业创新的重要底层基础设施, 5G 技术主要面向“增强型移动宽带 (eMBB, enhanced mobile broadband)”“高可靠低时延连接 (uRLLC, ultra reliable and low latency communication)”“海量物联 (mMTC, massive machine type communications)”三大应用场景, 突破了传统通信环境的底层制约, 解除了传统移动业务发展的限制, 充分拓展了移动业务系统的应用能力。通过运用网络功能虚拟化^[1] (NFV, network functions virtualization)、软件定义网络^[2] (SDN, software defined network)、网络切片^[3]、移动边缘计算^[4] (MEC, mobile edge computing) 等技术, 5G 能够为业务资源按需获取、业务运行快速响应等提供重要的技术支撑^[5-6], 催生社会经济向数字化的转型升级。5G 技术的发展带动了技术生态系统的全面繁荣, 包括物联网、自动驾驶、智能制造、智慧医疗、航空、云边端协同计算等领域, 使得“万物互联”时代的到来不再遥远。

近年来, 中国民用航空经历了快速发展的阶

段, 中国民用航空的客运量和货运量呈现持续增长的态势, 年均增长率高于全球平均水平。此外, 中国民用航空产业的技术水平不断提高。目前, 5G 通信技术已经在我国民用航空领域得到应用, 主要包含大规模设备与传感器的联网管理、乘客与货物的智能管理、大规模指挥调度、地面应急事件处理等。

5G 移动通信技术在为智慧机场提供新服务的同时, 也给其网络安全防护设计带来了新的挑战。传统的安全设计主要是识别并建立信息系统的安全边界, 并在安全边界处实施安全隔离与信息流管控, 允许合法的信息进入系统, 拒绝非法的信息进入系统。然而, 在 5G 移动通信网络中, NFV 与 SDN 等技术的使用, 使得控制面与数据面分离, 导致网络安全边界更加模糊, 信息交互更加复杂, 网络安全防护难度增大^[6]。此外, 在智慧机场场景下, 大规模异构设备的管理为网络认证与安全管控提出了新的挑战。因此, 传统的安全防护设计难以有效应对新型的 5G 网络安全威胁, 需要采取更加先进的安全防护措施, 如秘密信息安全流转、网络流量监测、行为分析等技术, 以确保 5G 移动通信网络的安全。

1 基于 5G 的智慧机场网络安全特点及安全需求

随着 5G 技术的迅速发展,其高速率、高可靠、低时延、大容量等优势,使其成为建设智慧机场网络的重要支撑。基于 5G 的智慧机场网络的风险挑战与安全需求^[7-8]体现在以下 5 个方面。

(1) 统一安全管控

智慧机场 5G 核心网后台中存在大量安全敏感网元(如策略控制功能、鉴权服务器功能等)。核心网的安全性直接保证了系统中资源、数据的保密性和完整性,保护了系统设备不受未授权用户的侵犯。但其易遭到分布式拒绝服务(DDoS, distributed denial of service)、女巫攻击等敌手攻击,使终端节点暴露于未授权使用者^[9],影响系统的可用性。因此,需要将智慧机场 5G 网络中各系统、设备、虚拟网元等纳入统一的安全监控,并提供实时、稳定、高效的安全管控手段。

(2) 网络切片安全

网络切片技术作为智慧机场 5G 网络的重要组成部分,通过应用软件定义网络、网络功能虚拟化等技术,将单个物理网络划分为多个逻辑子网,服务于智慧机场中具有不同网络性能需求的垂直业务,提高了网络的灵活性和可扩展性。但同时多业务切片的虚拟化和服务化技术使得设备的控制面和数据面解耦,导致网络边界模糊。

智慧机场 5G 安全需求异构化程度高,在网络切片技术方面提出了更高的安全要求。结合 NGMN(next generation mobile network)联盟列举的 5G 网络切片安全问题^[10]进行分析,智慧机场 5G 网络要求在切片的跨片安全通信、切片隔离、切片资源安全配置^[11]、切片虚拟化安全等方面实现更加完善的保障^[12],以满足智慧机场中具有不同网络性能需求的垂直业务的安全需求。

(3) 安全监测预警

智慧机场 5G 核心网大量引入了 NFV、SDN、网络切片等技术,随着各业务系统的深度融合,智慧机场场景下产生海量的信息数据、服务数据、指挥数据等,使得 5G 网络流量、数据类型、数据关联度大幅增加。随着数据与信息的不断产生和流动,攻击者更加容易利用各种手段发起攻击,

导致系统功能失效、数据泄露、隐私泄露等风险。因此,需要在 5G 网络安全体系架构中引入新技术,以实时、全面地监测、预警和评估系统的安全状态,并根据监测结果及时做出响应。

(4) 边缘计算安全

在智慧机场数字化塔台、地勤应急处置业务应用中,由于 5G 基站数量多、分布广,传统依赖中心化的安全防护方案面临时延高、响应慢、服务阻塞、单点故障等问题。为解决上述问题,需实现基于边缘计算的一体化安全防护,将 5G 网络安全防护能力下沉到网络边缘节点,强化边缘服务器的本地数据分析处理和网络威胁感知能力,分担核心网的安全防护负载。

(5) 物联网感知节点安全

在 5G 智慧机场应用场景中,存在大量规模庞大、异构程度高的摄像头、传感器、安检闸机等感知节点,用于部署智能化的运营管理系统。这些感知节点的网络接入技术差异较大,且部署在安全风险较大的开放环境中,容易被攻击者捕获、替换和篡改,进而对物联网生态或智能机场系统发起攻击。为了提高感知节点的安全性,需要在感知节点上实施安全防护措施,如加密通信、身份验证、数据完整性检查和实时监测。同时,需要持续采集设备状态与行为信息,分析感知节点的安全状态,动态调整感知节点的安全防护策略,实现对物联网及其感知节点的有效接入控制和安全防护,以提高感知节点的安全性和稳定性。

2 相关工作

传统的机场网络安全系统建设主要集中在保护传统的局域网和广域网设施,主要依赖防火墙和入侵检测系统^[13]来保护网络免受外部攻击。随着信息技术的快速发展,机场网络的规模和复杂性逐渐增加,带来了更多的网络安全挑战。

随着机场网络安全系统对于功能性与安全性的要求逐渐提高,采用加密与隧道技术的虚拟专用网络^[14]、病毒和恶意软件防护系统^[13]、安全认证与访问控制系统^[15]、安全审计与合规性审查等被引入。为了防止安全漏洞扩散和限制潜在攻击者的行动范围,机场网络开始采用网络分段和隔

离策略^[16]。随着机场网络的规模不断扩大, 网络安全事件的数量和复杂性增加。安全信息与事件管理(SIEM)系统^[17]被引入, 其被用于集中管理和分析来自各个安全设备的事件日志, 从而更好地监测和响应安全事件。

传统机场网络安全系统的局限性主要体现在: 传统机场网络安全系统的管理和维护通常较为复杂。由于机场网络的规模和复杂性不断增加, 作为重要基础设施的机场网络安全系统可能面临各种安全挑战, 对于传统机场网络安全的需求提高。新的智慧机场网络安全架构方案采用更先进、更完整的技术和策略来应对新形势下的安全挑战。

3 基于5G的智慧机场网络安全方案设计

3.1 总体架构设计

基于上述网络安全新需求, 本文选取典型的智慧机场应用场景, 提出了智慧机场5G移动通信网络安全架构, 主要针对5G用户终端、5G无线接入网、5G核心网等区域, 构建集业务加密、网络安全、终端可信、身份可信、安全管控于一体的安全平台。

基于5G的智慧机场网络安全架构由5G用户终端域、5G无线接入网域和5G核心网域部署的各类网络安全防护系统组成。① 5G用户终端域主要部署生物认证客户端, 主机综合防护代理和防病毒代理等系统, 用于各类用户5G智能终端、

5G移动终端和5G数字化塔台的安全认证和保护, 实现用户终端安全可靠接入5G核心网后台业务; 同时还部署了感知节点安全接入模块, 用于5G智能安检、5G视频监控等物联网终端的安全认证和保护, 实现物联网终端安全可靠接入5G核心网后台物联网业务。② 5G无线接入网域主要部署边缘计算安全防护设备, 以实现5G基站边缘计算网络的防火墙、入侵防御、网络防病毒、移动安全管理等一体化纵深安全防护。③ 5G核心网域主要部署防火墙、Web应用防火墙、数据库行为分析仪、入侵检测系统、漏洞扫描系统、终端防病毒系统、网络接入控制设备、安全审计系统等传统安防系统, 以及5G安全统一管控系统、5G安全态势监测预警系统、5G轻量化身份认证系统、5G网络切片防护系统和5G感知节点安全防护系统等专用安防系统, 实现针对5G核心网的安全防护能力。

3.2 功能组成

通过各类网络安全系统的集成运用, 能够为智慧机场网络提供统一安全管控、网络身份认证鉴权、网络切片安全防护、网络安全监测预警、边缘计算安全防护与感知节点安全防护功能。

(1) 面向泛在网络的5G网络统一安全管控功能

面向泛在网络的5G网络统一安全管控功能主要针对5G网络的泛在化特点, 从安全状态管

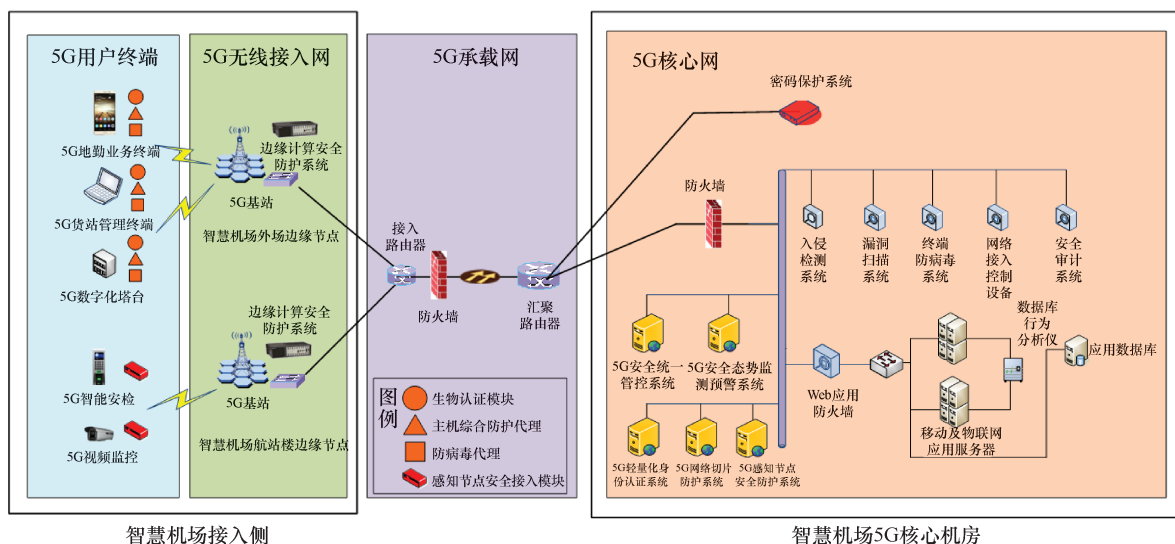


图1 基于5G的智慧机场网络安全方案架构
Figure 1 Architecture of 5G network security system for smart airports

理实现入手,实现全网设备系统的可控可管。具体来说,该安全方案包括以下3个方面。①安全状态管理:该功能针对5G网络中的各种软硬设备,实现全面的安全状态管理。通过实时监测5G终端、传感器、5G切片、核心网元在内的软硬设备的安全状态,可以对各类设备的异常行为及时发现和处置,保障5G网络的安全稳定运行。②安全事件管理和安全策略管理:在安全状态管理实现的基础上,实现各安全日志及事件的集中管理,各类服务、设备、系统的安全策略集中管理。通过对各类安全事件的集中管理和安全策略的集中管理,可以更好地发现和应对各种安全威胁。③安全联动分析:该功能主要实现在特定安全威胁场景下,各安全系统的快速联动响应。通过不同安全系统之间的联动分析,可以更加准确地判断安全威胁的严重性和影响程度,并做出快速响应,从而最大程度地保障5G网络的安全稳定运行。

(2) 轻量化的5G网络身份认证鉴权功能

轻量化的5G网络身份认证鉴权功能是为了确保可信实体能够安全可控地访问各类业务网络资源,解决5G网络的统一身份管控、统一接入认证、统一鉴权管理等问题^[18]。该功能基于3GPP 5G认证协议标准,实现二次身份认证级轻量化的权限鉴别,并在广域跨域身份认证场景研究的基础上,实现统一身份管控、统一接入认证、统一鉴权管理。具体来说,统一身份管控主要解决5G终端身份管理及用户身份管理问题。通过对终端设备及用户进行身份识别和管理,可以确保网络访问的可信性和可控性。统一接入认证在5G核心网接入认证的基础上,统一考虑二次身份认证及业务层认证的关联性。该功能可以对接入设备进行身份认证,并对接入的业务进行认证。统一鉴权管理主要解决轻量级快速鉴权及跨域权限同步的问题。该功能可以实现轻量级快速的鉴权流程,并保障跨域权限同步的一致性。

(3) 面向多业务需求的5G网络切片安全防护

面向多业务需求的5G网络切片安全防护功能主要是针对新型5G切片应用场景中的各种虚拟化安全问题而设计的。该功能主要包括3个部分:网络切片虚拟资源管理、网络切片端到端安全隔离和切片安全功能动态实现。网络切片虚拟

资源管理是指在5G核心网中建立各种切片类型的虚拟资源池,实现对切片资源的统一管控和保护,包括对切片资源的配置、分配、调度和监控等。在这个基础上,网络切片端到端安全隔离实现了对切片间、切片内部和切片与非切片网络之间的安全隔离,避免了攻击者跨越切片访问其他网络资源的风险。同时,为了进一步保护用户隐私和数据安全,切片安全功能动态实现了二次认证和访问控制、用户身份掩护以及网络接入安全增强等安全功能。这些功能可以有效地防范恶意攻击和数据泄露等安全风险,保障5G网络切片的安全和稳定运行。

(4) 基于大数据分析的5G网络安全监测预警

基于大数据分析的5G网络安全监测预警功能主要解决5G网络大数据传输场景下的实时安全态势监测预警与快速响应问题,主要包含5G网络安全数据采集提取、态势数据计算关联分析、5G网络安全智能分析和5G网络安全态势智能评估。①5G网络安全数据采集提取:该部分的主要作用是在5G网络的接入网和核心网的各个网络设备中设置安全监测点,实时采集网络信令、流量等数据,将采集到的数据进行加工和处理,形成统一的数据格式和标准,方便后续的数据分析和建模。②态势数据计算关联分析:该部分的主要作用是通过运用大数据分析和机器学习等方法,对采集到的数据进行处理和计算,并对数据之间的关系和规律进行分析和挖掘,以便更好地了解网络中存在的潜在威胁和安全风险^[19-20]。③5G网络安全智能分析:该部分的主要作用是将经过关联分析后的数据,应用到安全分析模型中,进行更加深入的安全分析和评估,如对网络中异常流量、异常设备等进行自动化分析,生成分析报告,以便安全管理人员及时进行安全决策。④5G网络安全态势智能评估:该部分的主要作用是对5G网络的安全态势进行全面的评估和预警,及时发现和处理网络中的潜在威胁和风险。对于异常的网络行为,可以及时触发告警,并且可以快速响应,采取相应的措施,以保障5G网络的安全稳定运行。

(5) 基于边缘计算的一体化安全防护功能

基于边缘计算的一体化安全防护功能主要解

决5G边缘网络中可定制编排的综合安全防护问题。该功能基于高性能硬件平台,采用虚拟化技术构建内置基础虚拟安全网元和第三方扩展虚拟安全网元,并以服务链方式来编排调度各安全网元的排列组合,为5G边缘计算网络提供虚拟化防火墙、虚拟化入侵防御、虚拟化网络防病毒、移动设备安全管理系统等一体化的纵深安全防护。

(6) 基于设备行为分析的感知节点安全防护功能

基于设备行为分析的感知节点安全防护功能主要解决物联网及其感知节点的有效接入控制和安全防护问题。该功能由感知节点安全接入探针和感知节点安全防护分析两部分组成。感知节点安全接入探针主要负责对感知节点进行流量采集和信息探测,探测感知节点的流量、属性、协议、服务等信息,并将采集的日志发送到后台的感知节点安全防护分析系统^[21-23]。感知节点安全防护分析系统则负责对采集到的感知节点日志数据进行清洗、归一、富化等处理,分析感知节点的属性、协议、服务、攻击等行为,并产生相应的安全告警和数据展示。该系统通过策略的形式将数据传输给感知节点安全接入探针,从而实现对相应物联网感知节点的策略响应,保护物联网感知节点的安全,避免被恶意攻击者攻击。

4 基于5G的智慧机场网络安全协议分析与设计

4.1 5G AKA协议的架构

5G认证与密钥协商(AKA, authentication and key agreement)^[24]协议的执行主体包含用户设备(UE, user equipment)、服务网络(SN, serving network)和归属网络(HN, home network)。

在基于5G的智慧机场网络方案中,UE是包括管理终端、业务终端、感知节点等在内的需要使用5G网络通信服务的设备。UE的异构程度较高,包含固定设备与移动设备等。SN通常由基站构成,SN主要负责为完成双向认证流程的UE提供无线通信服务。HN由智慧机场5G核心机房中的服务器构成,主要负责UE的认证。

4.2 相关工作

3GPP组织提出的第三代与第四代移动通信

技术为用户带来了更好的移动通信体验与更高的移动通信安全。3G、4G网络中的用户与基站之间需要借助归属网络完成信任关系与密钥的建立,这个过程通过认证与密钥协商协议完成。尽管4G在3G的基础上提供了层次化密钥传输与秘密传输密钥的安全功能,但是通信过程中IMSI(international mobile subscriber identity)泄露^[18,25]与骨干网传输未加密的问题仍然没有得到很好的解决。

随着5G移动网络的广泛应用,安全问题成为5G技术的重中之重^[26]。5G AKA协议中针对IMSI泄露和明文传输的问题做出了重大的安全改进,但是由于5G采用了许多新技术和新架构,同时黑客的攻击技术在不断提高,传统3G和4G中使用的许多安全机制^[27-30]无法直接适用于5G系统。因此,对5G AKA协议进行形式化分析与安全性改进^[31-35]成为当下研究的热点。

4.3 5G AKA协议安全问题分析

在5G AKA协议中,由于缺少对SN转发的消息的真实性验证,攻击者可以冒充真实的SN与UE和HN进行通信,并将自己伪装成通信的另一方,从而进行基站伪装攻击,这种攻击可能会导致数据泄露、篡改、欺骗等问题。

5G AKA协议是5G移动通信中用户和基站之间进行安全认证的协议,用于保护通信的机密性、完整性和可用性。在该协议中,UE通过向HN发送认证请求来请求连接网络。如果HN能够验证UE的身份,则HN将向UE发送挑战。UE会使用其预共享密钥和随机数来计算响应,以证明自己的身份,并通过SN将响应发送给HN。最终在UE与SN之间建立相同的密钥。

然而,由于5G AKA协议中没有验证消息是否由真实的SN转发,攻击者可以轻易地冒充SN与UE进行通信,并在后续的认证过程中伪装自己是真正的基站。攻击者可以伪装成真正的基站,以此获得UE的SUCI()和其他信息,并将其转发给HN。攻击者此后就能够代替真正的SN与UE和HN进行通信,并且在最后完成认证过程时与UE建立相同的锚密钥。

通过这种方式,攻击者伪造的SN可以与UE建立相同的锚密钥,并进一步窃取通信内容、篡

改通信内容、欺骗通信双方等。因此,对于 5G AKA 协议中的这种漏洞,需要采取相应的安全措施进行防范和修补。

4.4 改进的 5G AKA 协议

本文为了解决上述问题,为 SN 引入了公钥与私钥,并额外为 HN 引入了提供数字证书颁发的能力。方案中的合法基站均拥有 HN 提供的公钥合法性证书。

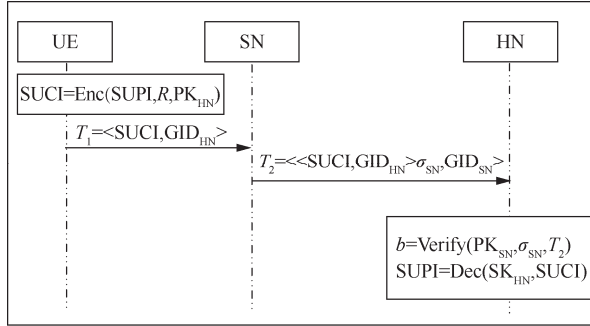


图2 改进的 5G AKA 协议 (初始化阶段)

Figure 2 Improved 5G AKA protocol (initialization phase)

(1) 永久身份标识注册阶段

当 UE 身份认证流程被触发, UE 首先向 HN 秘密注册永久身份标识 (SUPI, subscription permanent identifier), 该过程如下。① UE 选择随机数 R , 使用随机加密算法加密 SUPI 获得 SUCI; 使用 SUCI 与 HN 的全局唯一身份标识 GID_{HN} 构造消息元组 T_1 ; UE 向 SN 发送 T_1 。② SN 在 T_1 中加入本基站的全局唯一身份标识 GID_{SN} , 使用本基站的私钥对其哈希值签名后, 转发至 HN。

$$\begin{aligned} SUCI &= \text{Enc}(\text{SUPI}, R, \text{PK}_{HN}) \\ T_1 &= \langle SUCI, GID_{HN} \rangle \\ T_2 &= \langle \langle SUCI, GID_{HN} \rangle_{\sigma_{SN}}, GID_{SN} \rangle \end{aligned}$$

当 HN 接收到 T_2 后, 首先使用对应 SN 的公钥验证签名的正确性, 接着使用私钥解密 SUCI, 以获得用户的 SUPI 与随机数 R 。

$$\begin{aligned} b &= \text{Verify}(\text{PK}_{SN}, \sigma_{SN}, T_2) \\ \text{SUPI} &= \text{Dec}(\text{SK}_{HN}, \text{SUCI}) \end{aligned}$$

(2) 双向认证与密钥协商阶段

HN 使用随机数 R , 连同密钥 CK、IK 与 SN 的全局身份标识 GID_{SN} 计算预期回复值 $XRES^*$ 及预期回复哈希 $HXRES^*$ 。

$$\begin{aligned} XRES^* &= \text{Challenge}(\text{CK} \parallel \text{IK}, R, GID_{SN}) \\ HXRES^* &= \text{SHA256}(R \parallel XRES^*) \end{aligned}$$

接着, HN 使用密钥 CK、IK 与随机数 R 导出匿名密钥 AK。HN 计算新的序列号 SQN_{HN} , 输入 f_1 函数中, 以获得鉴权码 MAC。HN 使用 AK 与 MAC 计算认证令牌 AUTN。

$$\begin{aligned} AK &= f_5(\text{CK} \parallel \text{IK}, R) \\ MAC &= f_1(\text{CK} \parallel \text{IK}, \langle SQN_{HN}, R \rangle) \\ \text{CONC} &= SQN_{HN} \oplus AK \\ \text{AUTN} &= \langle \text{CONC}, \text{MAC} \rangle \end{aligned}$$

HN 构造元组 T_3 , 使用私钥签名后发送至 SN。

$$T_3 = \langle \text{AUTN}, R, HXRES^* \rangle_{\sigma_{HN}}$$

SN 通过数字签名验证 T_3 来源的真实性, 并对 AUTN 与 R 使用私钥签名, 连同公钥的数字证书 CERT_{SN} 一同转发给用户设备 UE。

$$T_4 = \langle \langle \text{AUTN}, R \rangle_{\sigma_{SN}}, \text{CERT}_{SN} \rangle$$

UE 获得 T_4 后, 首先使用 HN 的公钥验证数字证书的合法性, 保证 SN 公钥的真实性。UE 使用 SN 的公钥验证 T_4 中签名的合法性, 保证信息来源真实。UE 使用密钥与随机数计算 AK, 结合从 AUTN 中提取的 $x\text{Conc}$ 计算 $xSQN$, 进一步计算 MAC, 验证该值与 $x\text{MAC}$ 是否相等, 验证本地序列号是否不大于 $xSQN$, 验证无误则说明 HN 对于挑战值的响应无误, 完成 UE 对 HN 的验证过程。

$$\begin{aligned} (x\text{MAC}, x\text{Conc}) &\leftarrow \text{AUTN} \\ AK &= f_5(\text{CK} \parallel \text{IK}, R) \\ xSQN &= AK \oplus x\text{Conc} \\ \text{MAC} &= f_1(\text{CK} \parallel \text{IK}, \langle xSQN, R \rangle) \end{aligned}$$

UE 使用密钥 CK、IK、随机数 R 、SN 的身份标识 GID_{SN} 一同计算响应值 RES^* 。UE 将响应值 RES^* 转发给 SN。

$$RES^* = \text{Challenge}(\text{CK} \parallel \text{IK}, R, GID_{SN})$$

SN 使用接收到的 RES^* 计算响应哈希 $HRES^*$ 。将 $HRES^*$ 与 $HXRES^*$ 比较, 若相等, 则构造元组 T_5 后, 对其哈希值签名并转发给 HN。

$$\begin{aligned} HRES^* &= \text{SHA256}(R \parallel RES^*) \\ T_6 &= \langle RES^*, \text{SUCI} \rangle_{\sigma_{SN}} \end{aligned}$$

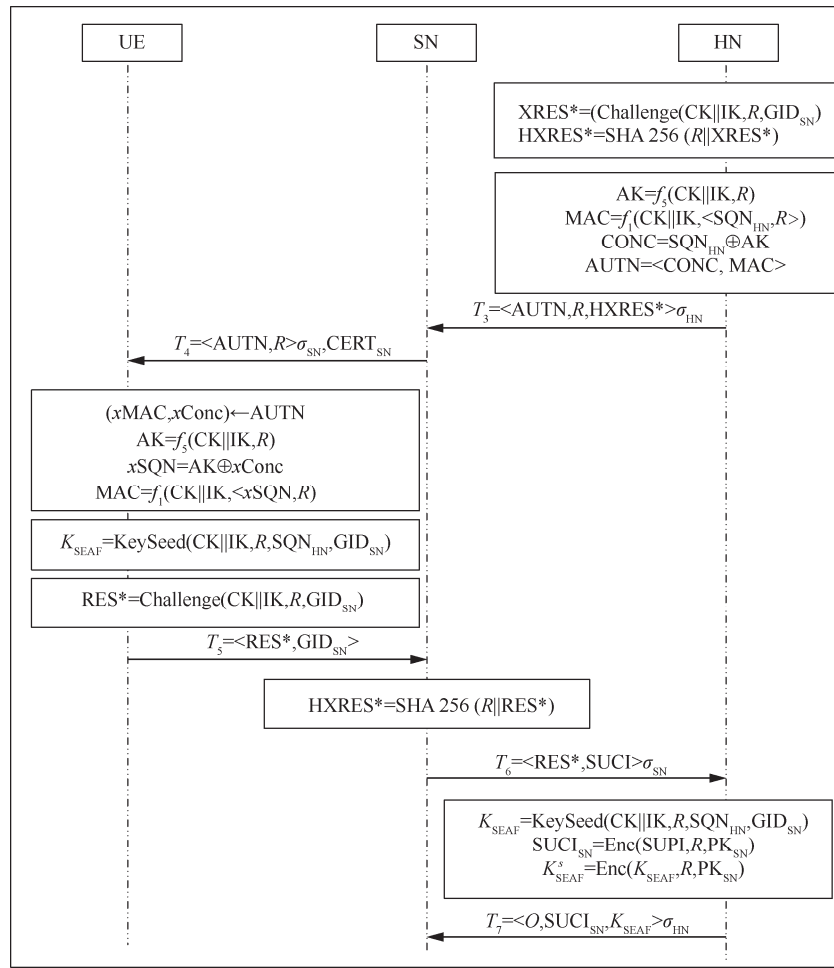


图 3 改进的 5G AKA 协议（认证与密钥协商阶段）

Figure 3 Improved 5G AKA protocol (mutual authentication and key agreement phase)

HN 验证 RES^* 与 $XRES^*$ 是否相等，若相等，说明用户的响应值无误，SN 对 UE 的验证完成。HN 计算会话密钥 K_{SEAF} 。HN 使用 SN 的公钥加密永久身份标识 $SUPI$ 获得 $SUCI_{SN}$ ，并加密锚密钥 K_{SEAF} ，将二者与验证结果 O 一同构造为元组，对其哈希值签名后转发给 SN。

$$K_{SEAF} = \text{KeySeed}(CK || IK, R, SQN_{HN}, \text{GID}_{SN})$$

$$SUCI_{SN} = \text{Enc}(SUPI, R, PK_{SN})$$

$$K_{SEAF}^s = \text{Enc}(K_{SEAF}, R, PK_{SN})$$

$$T_7 = \langle O, SUCI_{SN}, K_{SEAF}^s \rangle_{\sigma_{HN}}$$

SN 验证元组的哈希值及签名，解密获得 UE 的永久身份标识 $SUPI$ 与锚密钥 K_{SEAF} 。

(3) 认证失败情况处理

在初始化阶段中，HN 使用本地保存的 SN 公钥验证元组 T_2 ，若失败，HN 返回签名错误信息。

$$P_{SG} = \langle \text{'SIGN_Failure'} \rangle$$

若验证成功，说明基站为合法基站，则 HN 使用本地私钥解密 $SUCI$ 。若解密所得的数据格式错误，或 $SUPI$ 不在 HN 本地的设备列表中，则 HN 构造错误应答元组 P_1 ，签名后转发给 SN。

$$P_{SP} = \langle \text{'SUPI_Failure'}, SUCI, \text{GID}_{SN} \rangle_{\sigma_{HN}}$$

在双向认证与密钥协商阶段中，SN 首先验证 T_3 签名的合法性，若不合法，则关闭会话并返回错误信息 P 。此后，UE 使用本地保存的 HN 公钥，验证 SN 公钥数字证书的合法性，若不合法，则关闭会话并返回 P_{CT} 。

$$P_{CT} = \langle \text{'CERT_Failure'} \rangle$$

UE 验证 T_4 中签名的合法性，若不合法，则关闭当前会话，并返回错误信息 P_{SG} 。

若验证成功, UE 进一步验证本地计算的 MAC 值与接收到的 XMAC 值是否相等, 若不等, UE 将错误信息转发至 SN, 由 SN 转发至 HN。

$$P_{MC} = \langle \text{'MAC_Failure'} \rangle$$

若验证成功, UE 验证序列号是否同步, 若同步失败, UE 使用本地序列号 SQN_{UE} 构造 $CONC_{UE}$ 与 MAC_{UE} , 进而构造 AUTS 与同步失败信息元组 P_{SN} 。

$$\begin{aligned} CONC_{UE} &= SQN_{UE} \oplus AK \\ MAC_{UE} &= f_1(CK \parallel IK, \langle SQN_{UE}, R \rangle) \\ AUTS &= \langle CONC_{UE}, MAC_{UE} \rangle \\ P_{SN} &= \langle \text{'SYNC_Failure'}, AUTS \rangle \end{aligned}$$

在认证成功后, 还有 HN 对 SN 签名的验证及 SN 对 HN 签名的验证步骤, 若验证失败, 则对应的实体发送签名错误信息 P_{SG} 。

4.5 安全性分析

在本文协议中, UE 与 SN、SN 与 HN 之间的认证通过数字签名来实现。SN 使用自己的私钥对消息进行签名, 将附加签名的消息发送给 UE 或 SN。接收方使用 SN 的公钥验证签名, 如果验证成功, 则可以确认该请求来自合法的 SN, 从而进行相应的操作。下面对该协议的抗中间基站攻击安全性进行形式化的描述。

定义 (安全模型) 假设存在一个概率多项式时间的攻击者 A , 其目标是伪造有效的请求, 使得 UE 或服务器接受并执行该请求。

敌手已知: SN 与 HN 的公钥。

敌手能力: ① 窃听 UE、SN 和 HN 之间的通信内容; ② 篡改消息 T_1 、 T_2 、 T_3 、 T_4 、 T_5 、 T_6 、 T_7 ; ③ 使用窃听到的 T_1 、 T_2 、 T_3 、 T_4 、 T_5 、 T_6 、 T_7 , 执行消息篡改攻击或者消息伪造攻击。

敌手目标: ① 伪造合法的请求消息 T_4 , 使得 UE 接受并执行该请求; ② 伪造合法的请求消息 T_2 , T_6 , 使得 SN 接受并执行该请求。

定理 (安全目标) 若协议中使用的数字签名是不可伪造的, 且哈希函数是抗碰撞的, 则①对于任意的 SN 请求消息 m , 如果 m 由合法的 SN 中合法的基站发送, 则 HN 或 UE 会接受并执行该请求, 否则不会接受或执行该请求; ② 对于任意的伪造请求消息 m' , 如果该消息不是由合法的

SN 发送的, 则 UE 与 SN 不会接受或执行该请求。

证明 假设 A 尝试伪造一个请求消息 m' , m' 为伪造的 T'_2 , T'_4 或 T'_6 。

若 $m' = T'_2$ 或 $m' = T'_6$, A 将 m' 发送给 HN。

若 $m' = T'_4$, A 将 m' 发送给 UE。

若 m' 被 UE 或 SN 接收, 则说明 A 伪造的签名合法, 这与数字签名的不可伪造假设矛盾。因此, A 无法伪造一个带有正确数字签名的请求消息 m' , 满足安全性目标②。

假设 A 尝试截获一个合法的请求消息 m , 并将其篡改为 m' 后发送给 UE 或 SN。若 m' 被 UE 或 SN 接收, 则说明 A 伪造的签名合法, 且

$$\text{Hash}(m) = \text{Hash}(m')$$

这与数字签名的不可伪造假设以及哈希函数的抗碰撞假设矛盾。因此, A 无法篡改一个带有正确数字签名的请求消息 m' , HN 或 UE 能够正确接收并执行来自合法基站的请求, 满足了安全性目标①。

证毕。

5 结束语

随着 5G 技术的飞速发展, 其高速率、高可靠性、低时延和大容量等, 成为建设智慧机场网络不可或缺的支撑。本文对基于 5G 的智慧机场网络的安全特点和安全需求进行了梳理, 以及选取了典型的智慧机场应用场景, 提出了一种智慧机场 5G 移动通信网络安全系统的设计方案。此外, 本文对智慧机场场景下 5G 认证与密钥协商协议中存在的安全问题进行了分析, 提出了改进的 5G AKA 协议, 并进行了形式化的安全性分析。

然而, 本文方案的应用场景较为局限, 智慧机场之外的应用存在不同的网络安全挑战与需求, 因此可能不适用于其他场景或者行业。此外, 建议未来的实践者在应用时, 考虑不同机场的规模和网络架构等因素的差异, 根据具体情况进行必要的定制化和调整, 以满足不同机场的特定需求和挑战。在未来的应用中, 5G 技术能够为智慧机场提升安全性、鲁棒性, 强化物联网应用, 推动虚拟化与网络切片, 以及增强乘客体验, 为智慧机场带来更高水平的智能化、高效性和用户满意度。

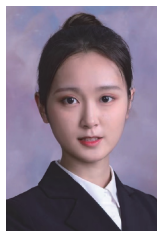
参考文献:

- [1] HERRERA J G, BOTERO J F. Resource allocation in NFV: a comprehensive survey[J]. *IEEE Transactions on Network and Service Management*, 2016, 13(3): 518-532.
- [2] YAN Q, YU F R, GONG Q, et al. Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: a survey, some research issues, and challenges[J]. *IEEE Communications Surveys & Tutorials*, 2015, 18(1): 602-622.
- [3] ZHANG S. An overview of network slicing for 5G[J]. *IEEE Wireless Communications*, 2019, 26(3): 111-117.
- [4] KEKKI S, FEATHERSTONE W, FANG Y, et al. MEC in 5G networks[J]. *ETSI White Paper*, 2018, 28(2018): 1-28.
- [5] IMT-2020(5G)推进组. 5G 网络架构设计白皮书[EB]. IMT-2020 (5G) Promotion Group. 5G Network architecture design white paper[EB].
- [6] IMT-2020(5G)推进组. 5G 网络安全需求与架构白皮书[EB]. IMT-2020 (5G) Promotion Group. 5G network security requirements and architecture white Paper[EB].
- [7] HUMAYUN M, HAMID B, JHANJHI N Z, et al. 5G network security issues, challenges, opportunities and future directions: a survey[J]. *Journal of Physics: Conference Series*. IOP Publishing, 2021, 1979(1): 12-37.
- [8] AHMAD I, KUMAR T, LIYANAGE M, et al. Overview of 5G security challenges and solutions[J]. *IEEE Communications Standards Magazine*, 2018, 2(1): 36-43.
- [9] BEHRAD S, BERTIN E, CRESPI N. A survey on authentication and access control for mobile networks: from 4G to 5G[J]. *Annals of Telecommunications*, 2019, 74: 593-603.
- [10] NGMN. 5G security-network slicing version 1. 0, 5G security recommendations package# 2: network slicing[S]. 2016.
- [11] OLIMID R F, NENCIONI G. 5G network slicing: a security overview[J]. *IEEE Access*, 2020, 8: 99999-100009.
- [12] JI X, HUANG K, JIN L, et al. Overview of 5G security technology[J]. *Science China Information Sciences*, 2018, 61(8): 081301.
- [13] FAN C, XIONG H, ZHANG H, et al. Analysis of network security and risks prevention strategies of hongqiao airport west terminal[J]. *Comput Inf Sci*, 2009, 2(3): 46-52.
- [14] PATEL K J. Successful implementation of emerging communication technologies in a mobile-intense organization: a case study of sydney airport[M]//*Handbook of Research in Mobile Business: Technical, Methodological, and Social Perspectives*. 2006: 728-739.
- [15] BARTOLI G, FANTACCI R, MARABISSI D. AeroMACS: a new perspective for mobile airport communications and services[J]. *IEEE Wireless Communications*, 2013, 20(6): 44-50.
- [16] CASADO-VARA R, MARTIN-DEL REY A, AFFES S, et al. IoT network slicing on virtual layers of homogeneous data for improved algorithm operation in smart buildings[J]. *Future Generation Computer Systems*, 2020, 102: 965-977.
- [17] BHATT P R, BHATT R R. Managing change at muhibbah engineering (M) Bhd[J]. *South Asian Journal of Business and Management Cases*, 2017, 6(1): 12-25.
- [18] STROBEL D. IMSI catcher[J]. *Chair for Communication Security, Ruhr-Universität Bochum*, 2007, 14.
- [19] MOROCHO-CAYAMCELA M E, LEE H, LIM W. Machine learning for 5G/B5G mobile and wireless communications: Potential, limitations, and future directions[J]. *IEEE Access*, 2019, 7: 137184-137206.
- [20] MOYSEN J, GIUPPONI L. From 4G to 5G: self-organized network management meets machine learning[J]. *Computer Communications*, 2018, 129: 248-268.
- [21] LI S, DA XU L, ZHAO S. 5G internet of things: a survey[J]. *Journal of Industrial Information Integration*, 2018, 10: 1-9.
- [22] SHAFIQUE K, KHAWAJA B A, SABIR F, et al. Internet of things (IoT) for next-generation smart systems: a review of current challenges, future trends and prospects for emerging 5G-IoT scenarios[J]. *IEEE Access*, 2020, 8: 23022-23040.
- [23] CHETTRI L, BERA R. A comprehensive survey on internet of things (IoT) toward 5G wireless systems[J]. *IEEE Internet of Things Journal*, 2019, 7(1): 16-32.
- [24] CREMERS C, DEHNEL-WILD M. Component-based formal analysis of 5G-AKA: channel assumptions and session confusion[R]. 2019.
- [25] BORGAONKAR R, HIRSHI L, PARK S, et al. New adventures in spying 3G & 4G users: locate, track, monitor[C]//*Blackhat*. 2017.
- [26] BORGAONKAR R, HIRSCHI L, PARK S, et al. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols[J]. *Cryptology ePrint Archive*, 2018.
- [27] HE D, ZHANG Y, WANG D, et al. Secure and efficient two-party signing protocol for the identity-based signature scheme in the IEEE P1363 standard for public key cryptography[J]. *IEEE Transactions on Dependable and Secure Computing*, 2018, 17(5): 1124-1132.
- [28] FERRAG M A, MAGLARAS L, ARGYRIOU A, et al. Security for 4G and 5G cellular networks: a survey of existing authentication and privacy-preserving schemes[J]. *Journal of Network and Computer Applications*, 2018, 101: 55-82.
- [29] HAN C K, CHOI H K. Security analysis of handover key management in 4G LTE/SAE networks[J]. *IEEE Transactions on Mobile Computing*, 2012, 13(2): 457-468.
- [30] CHEN K, NATARAJAN B B, SHATTIL S. Secret key generation rate with power allocation in relay-based LTE-A networks[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(11): 2424-2434.
- [31] BASIN D, DREIER J, HIRSCHI L, et al. A formal analysis of 5G authentication[C]//*Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 2018: 1383-1396.
- [32] REMERS C, DEHNEL-WILD M. Component-based formal analysis of 5G-AKA: Channel assumptions and session confusion[C]//*Network and Distributed System Security Symposium (NDSS)*. 2019.
- [33] WANG Y, ZHANG Z, XIE Y. Privacy-preserving and standard-compatible AKA protocol for 5G[C]//*USENIX Security Symposium*. 2021: 3595-3612.

[34] MUNILLA J, BURMESTER M, BARCO R. An enhanced symmetric-key based 5G-AKA protocol[J]. Computer Networks, 2021, 198: 108373.

[35] BRAEKEN A. Symmetric key based 5G AKA authentication protocol satisfying anonymity and unlinkability[J]. Computer Networks, 2020, 181: 107424.

[作者简介]



邢馨心（1999—），女，河北秦皇岛人，北京航空航天大学硕士生，主要研究方向为密码学、区块链与信息安全。



左青雅（2001—），女，河北遵化人，主要研究方向为信息安全与电子商务。



刘建伟（1964—），男，山东莱州人，博士，北京航空航天大学教授、博士生导师，主要研究方向为密码学与网络安全。