

Design of Encrypted Network Access Equipment Based on 5G Communication Technology

Yuhan Yang Renbiao Wang Wenguang Zhang

Shenzhen Wojia Communications Co., Ltd., Shenzhen, Guangdong, 518000, China

Abstract

Based to the current development of network security and the characteristics of 5G communication technology, this paper designs an encrypted network access device based on 5G communication technology. Firstly, the characteristics and security architecture of 5G communication technology are analyzed, and then the system architecture and hardware and software modules of encrypted network access equipment are designed, and experiments and tests are conducted. The device can effectively guarantee the security of network communication and has a broad application prospect.

Keywords

5G communication technology; encrypted network access equipment; security architecture; system architecture

基于 5G 通信技术的加密网络接入设备设计

杨钰涵 王仁彪 张文广

深圳市沃嘉通信有限公司, 中国 · 广东 深圳 518000

摘 要

论文针对当前网络安全领域的发展和 5G 通信技术的特点, 设计了一种基于 5G 通信技术的加密网络接入设备。首先对 5G 通信技术的特点和安全体系结构进行了分析, 然后设计了加密网络接入设备的系统架构和硬件、软件模块, 并进行了实验与测试。该设备能够有效保障网络通信安全, 具有广阔的应用前景。

关键词

5G 通信技术; 加密网络接入设备; 安全体系结构; 系统架构

1 引言

随着互联网技术的快速发展, 网络安全问题日益凸显。为了保障网络通信的安全性和稳定性, 加密技术逐渐成为网络安全领域的重要研究方向。而 5G 通信技术作为新一代移动通信技术, 其高速、低延迟、大容量、高可靠性等特点为网络安全提供了新的保障手段。论文结合 5G 通信技术的特点和安全体系结构, 设计了一种基于 5G 通信技术的加密网络接入设备, 旨在提高网络通信的安全性和稳定性。

2 5G 通信技术概述

2.1 5G 通信技术的发展历程

5G 通信技术的发展可以追溯到 2013 年, 当时欧洲联盟提出了“5G 公私合作伙伴关系”(5G PPP)计划, 旨在推动 5G 通信技术的研发和应用。随后, 各国和企业纷纷加入 5G 技术研究和标准制定的行列, 5G 技术的标准化工作

也逐渐展开。2018 年, 国际电信联盟发布了 5G 的三个标准, 即非独立组网(NSA)、独立组网(SA)和增强型移动宽带(eMBB), 标志着 5G 技术进入了商用阶段^[1]。

2.2 5G 通信技术的特点与优势

高速率: 5G 网络的理论传输速率可以达到 10Gbps 以上, 比 4G 网络提升了 10 倍以上。

低延迟: 5G 网络的延迟可以控制在 1ms 以下, 4G 网络比 5G 网络高了 10 倍以上, 更适合需要实时交互和响应的应用场景。

大容量: 5G 网络支持更多的用户和设备同时接入, 可以满足物联网等大规模设备接入的需求。

高可靠性: 5G 网络具有更好的容错能力和网络自愈能力, 可以提高网络的可靠性和稳定性。

广泛应用: 5G 技术适用于更多的应用场景, 如智能家居、智慧城市、智能制造、虚拟现实等。

2.3 5G 通信技术的架构与标准

5G 通信技术的架构采用了虚拟化、云化、软件化的设计理念, 将无线接入网、核心网和终端设备进行了功能分离, 实现了灵活、可编程的网络架构。无线接入网由基站和用户

【作者简介】杨钰涵(1987-), 女, 侗族, 中国湖南洪江人, 本科, 从事通信传输研究。

终端设备组成, 采用了新型的天线和波束赋形技术, 实现了更高的传输速率和更好的网络覆盖。同时, 无线接入网支持不同频段的频谱资源共享, 提高了网络的利用效率。核心网是 5G 网络的控制中心, 主要负责网络的管理、调度和安全保障。5G 核心网采用了分布式架构, 通过网络切片的方式, 为不同的应用场景提供不同的服务质量保障。终端设备是 5G 网络的用户接入终端, 包括手机、平板电脑、物联网设备等。5G 终端设备具有更高的传输速率、更低的延迟和更好的网络覆盖能力, 支持更多的应用场景和业务需求^[2]。

5G 通信技术的标准主要由国际电信联盟（ITU）和第三代合作伙伴计划（3GPP）制定。ITU 制定了 5G 的总体技术架构和网络性能要求，而 3GPP 则负责制定 5G 的具体技术标准和规范，包括无线接口技术、核心网技术、安全技术等方面。目前，5G 技术标准已经基本确定，5G 网络商用已经进入了快速发展的阶段。

图 1 显示了 5G 通信网络的架构图，可以看出其采用了非常灵活的网络架构，以满足不同的通信需求。5G 通信技术还通过网络功能虚拟化和软件定义网络等技术，实现了灵活可编程的网络切片，使不同业务之间的网络资源能够互相独立，并能够实现快速配置、部署和管理。这些特性为 5G 通信技术提供了高效、安全、可靠的通信服务，并为未来的智能化应用奠定了基础。

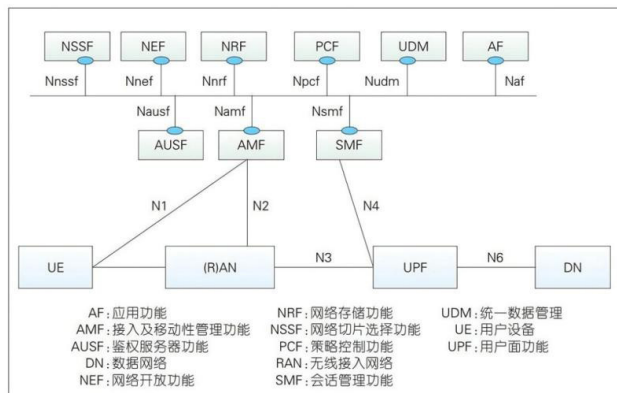


图 1 5G 的网络架构

3 5G 安全体系结构分析

3.1 5G 安全需求分析

5G 通信技术的特点和应用场景的变化，对网络的安全提出了更高的要求。5G 安全需求主要包括保密性、完整性、可用性、可信度、可审计性等方面。保密性要求网络数据传输过程中不被窃听、不被篡改；完整性要求网络数据在传输过程中不被篡改、不被破坏；可用性要求网络能够正常运行，不受攻击影响；可信度要求网络中的实体和操作可以被信任和验证；可审计性要求网络中的所有操作和事件都能够被记录和审计。

3.2 5G 安全体系结构框架

在 5G 网络中,安全是一个至关重要的问题。为了确保网络和用户的安全,5G 采用了一些安全功能和措施。图 2 中, (I) 是网络访问安全,表示一组安全功能,使 UE 能够安全地通过网络验证和访问服务,包括 3GPP 访问和非 3GPP 访问; (II) 是网络域安全,表示一组安全功能,使网络节点能够安全地交换信令数据和用户平面数据; (III) 是用户域安全,表示保护用户访问移动设备的一组安全功能; (VI) 是应用域安全,表示一组安全性功能,使用户和供应商中的应用程序能够安全地交换消息。5G 协议引入了用户永久标识符 (SUPI) 和用户隐藏标识符 (SUCI) 的概念。更重要的是,5G 规范中引入了基于公钥基础设施 (PKI) 的安全体系结构,允许验证和鉴别源自 5GC 的控制面消息 (CPM)。这是 3GPP 协议在 5G 体系架构上的安全考虑。具体地,针对 5G 基站设备及其接入,并根据图 2 所示的 4 个方面的安全威胁,我们分别采用了不同的安全解决方案^[3]。

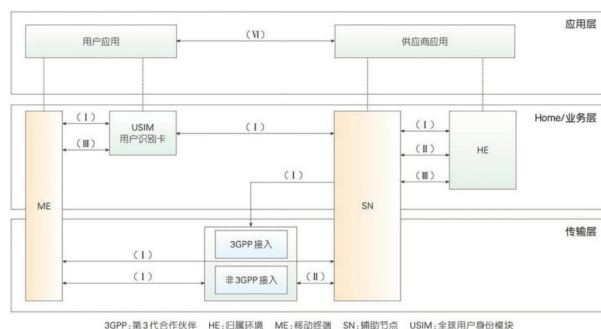


图 2 5G 安全体系结构

4 加密网络接入设备的设计

4.1 设计需求分析

加密网络接入设备是 5G 网络通信安全的重要组成部分，其设计需求分析主要包括五个方面：第一，高效可靠的数据加密传输是加密网络接入设备的主要需求之一，保障数据在传输过程中不被篡改和窃取，保证数据的安全性和完整性。第二，安全可靠的身份验证是保证加密网络接入设备能够正确识别接入设备身份的重要保障，确保只有授权设备才能接入网络。第三，强大的防攻击能力是保护加密网络接入设备不受黑客攻击、病毒和木马等恶意软件的入侵和破坏，保障设备的稳定性和安全性。第四，灵活的网络接入管理可以对设备接入进行有效的控制和管理，实现对设备的授权和限制，提高网络的安全性和管理效率。第五，高可用性和可扩展性是确保加密网络接入设备能够在面对大量用户和高负载情况下，保持稳定运行和保障网络安全的重要要求。

4.2 系统架构设计

加密网络接入设备基于 5G 安全体系结构框架，采用虚拟化技术，将虚拟化网关和虚拟化基础设施融合在一起，形成一个高效可靠的系统架构。该设备包含多个模块，包括数

据处理模块、安全管理模块、认证模块和网络接入控制模块等。数据处理模块负责对网络数据进行加密解密等数据处理,以确保数据传输过程的安全性和可靠性。安全管理模块则实现了加密、认证、访问控制和审计等安全管理功能,保障系统的安全性和可靠性。认证模块则实现了用户身份验证功能,以确保只有经过验证的用户才能访问网络资源。网络接入控制模块则负责管理网络接入流量,确保网络接入的合法性。采用虚拟化技术,能够灵活地管理网络资源,提高系统的可用性和可扩展性,同时还能够降低系统的成本和复杂度,提高系统的性能和效率^[4]。综合来看,本文提出的加密网络接入设备的系统架构设计满足了高效可靠的数据加密传输、安全可靠的身份验证、强大的防攻击能力、灵活的网络接入管理以及高可用性和可扩展性等设计需求。

4.3 硬件设计

加密网络接入设备采用高性能处理器,以保证设备的数据处理能力和运行效率。同时,该设备还采用了专用加密硬件加速器,实现了快速高效的加密处理,提高了系统的安全性和性能。硬件方面,该设备具有高速网络接口,支持千兆以太网接口、5G 无线接口等多种接入方式,能够满足不同场景下的网络接入需求。此外,该设备还具有可扩展性,可以通过添加硬件模块或扩展功能模块来满足不同场景下的需求。整体来看,该设备硬件设计优化了设备的数据处理能力和网络接入能力,增强了设备的可靠性和稳定性,同时也保障了设备的扩展性和适应性。这些优势在实际应用场景中将会有明显的效果,为加密网络接入设备的发展提供了强有力的支持。

4.4 软件设计

首先,系统软件方面,我们将采用基于 Linux 操作系统的设计。我们将使用 Linux 内核中提供的网络协议栈来实现网络连接和数据传输的功能,并基于此开发自定义的驱动程序,实现对硬件的控制和操作。此外,我们还将采用防火墙和 VPN 等技术,保证网络的安全性和稳定性。

其次,应用软件方面,我们将开发一套适用于加密网络接入设备的定制化软件。该软件将包括用户身份验证、加密解密、访问控制等多种安全功能,并且具备良好的用户友好性和易用性。我们将采用 C++、Python 等编程语言,结

合相关的开源库和算法,实现软件功能的开发和优化^[5]。

5 实验与测试

首先,为了保证测试的真实性和可靠性,我们将搭建一个真实的测试环境,包括测试服务器、客户端、网络设备等。测试环境应该与实际使用场景尽量一致,这有助于我们更好地了解设备在不同条件下的表现和性能。

其次,在这个过程中,我们将测试设备的基本功能,如连接网络、数据传输、用户身份验证等。我们将通过模拟实际使用场景,对设备的功能进行全面的测试和评估,确保设备能够稳定、高效地工作。

最后,在这个过程中,我们将模拟各种攻击场景,如黑客攻击、DDoS 攻击等,对设备的安全性能进行测试。通过这一步骤,我们可以检测和排除设备中存在的安全漏洞,提高设备的安全性和稳定性。

6 结语

论文中,我们研究了基于 5G 通信技术的加密网络接入设备设计。我们分析了 5G 通信技术的发展历程、特点和优势,以及其架构和标准。我们还分析了 5G 安全需求、体系结构和机制。在此基础上,我们提出了加密网络接入设备的设计方案,并详细介绍了系统架构、硬件设计和软件设计。最后,我们进行了实验和测试,通过论文的研究,我们认为基于 5G 通信技术的加密网络接入设备具有很高的应用价值。它可以保护网络通信的安全和隐私,对于保护用户的利益和维护网络安全具有重要意义。

参考文献

- [1] 李明华.5G无线通信技术及其应用[M].北京:电子工业出版社,2019.
- [2] 方琰崑,陈亚权.基于虚拟化的电信云网络安全解决方案[J].移动通信,2018,42(12):8.
- [3] 陈晓东,徐丽萍,肖珊珊.基于5G的安全接入网络设计[J].通信技术,2020(9):127-132.
- [4] 陈志勇,刘岳峰,丁锋.5G网络安全关键技术综述[J].计算机研究与发展,2019,56(5):973-986.
- [5] 曾志杰,王菲.5G加密技术研究进展[J].电信科学,2020(7):62-68.