学　　号：23120208013
论 文 密 级：公开
中图分类号：TP393
学科分类号：520.6099
学 校 代 码：91037

硕士学位论文

移动边缘计算接入安全防护技术研究

论 文 作 者：常敬超
指 导 教 师：汤红波
申 请 学 位：工学硕士
学 科 名 称：网络空间安全
研 究 方 向：移动互联数据安全
论文提交日期：2023 年 4 月 10 日
论文答辩日期：2023 年 6 月 9 日

战略支援部队信息工程大学

2023 年 6 月

A Dissertation Submitted to
PLA Strategic Support Force Information Engineering University
for the Degree of Master of Engineering

Research on Mobile Edge Computing Access Security Protection Technology

Candidate: Chang Jingchao

Supervisor: Prof. Tang Hongbo

Jun. 2023

摘　要

随着5G时代万物互联的发展，网络中产生了各式各样的连接，智能终端、物联网设备的数量和相应服务产生的数据呈爆炸式增长，传统集中式的云计算不再能满足用户侧的高带宽、低时延极致体验。移动边缘计算（Mobile Edge Computing, MEC）将云计算的计算和存储能力拓展到靠近用户的网络边缘，成为5G业务场景实现的关键技术之一，为服务商提供先进开放的应用计算平台。移动边缘计算存在广泛的应用场景，如车联网、工业物联网、智慧城市、虚拟现实技术等，带来全新服务的同时，也面临着安全挑战。攻击者劫持控制大量低安全能力终端向边缘网络服务发起资源耗尽和拒绝服务攻击，边缘设备易被攻击者入侵控制窃取用户敏感信息，未授权用户非法接入边缘网络，导致用户隐私泄露，用户数据传输流程存在恶意行为降低网络整体效率等。移动边缘计算环境中存在海量资源受限的多类型终端设备，计算能力和架构存在较大差异，难以适用统一的认证协议。随着边缘服务在国防、政府等高安全等级行业广阔的应用，现有的接入认证方案，难以满足边缘网络终端设备的安全接入，移动边缘计算的接入安全防护技术至关重要。

本文对移动边缘计算接入安全防护技术进行了研究，分析了现有安全防护机制的不足，为实现MEC场景下终端设备的安全防护，聚焦于终端获取网络服务的流程展开研究，分为用户接入边缘服务的流程和数据传输流程。针对用户接入边缘网络身份认证、终端与边缘网络交互的数据传输监管和终端之间的交互的信任评估三个方面展开研究，分别提出了可信身份认证的边缘计算防护方法、边缘网关的恶意流量检测防御策略和边缘终端设备信任评估的方法，增强移动边缘计算整个服务过程的安全性，具体工作如下：

（1）针对边缘计算的高安全等级边缘计算专网安全接入问题，提出一种于基于可信身份认证的边缘计算服务防护方法，该方法面向边缘计算高安全等级专网场景的可信身份认证需求，给出5G核心网的移动边缘计算高安全等级专网身份认证解决方案。首先通过基于5G核心网的用户身份信息嵌入和接口标识替换，实现了接入核心网用户身份真实可信。然后，在核心网侧用户身份真实可信的基础上，增设了边缘防护网关和边缘防护网关控制器，通过DN和边缘防护网关的双重认证及基于通行令牌的身份认证机制实现对于访问DN用户身份真实可信的认证和准入。最后，以5G车联网场景为例，在保护边缘计算节点安全和阻止用户隐私的泄露的前提下设计了车辆运动轨迹预测算法，实现了车辆在高速运动过程中边缘服务节点的高效切换，对基于可信身份认证的边缘计算服务防护方案进行了系统的验证和测试，证明了方案的安全性。

（2）针对移动边缘计算中终端和边缘间的数据传输安全问题，提出基于遗传算法的恶意流量检测防御策略，实现边缘计算防护网关安全与性能平衡。首先，采用零信任的思想在边缘防护网关设置网关控制器，对业务数据流量进行抽样检测。其次，考虑网关控制器的恶意流量检测效率，在保证网关数据正常传输的前提下实施合理的恶意流量检测策

略，以低成本的拦截对业务流数据包的篡改与恶意伪造。分析恶意流量的攻击收益和边缘防护网关的防御收益，设计基于遗传算法的抽样检测概率优化目标，并进行求解，确定边缘网关恶意流量检测的最佳防御策略。

（3）针对现有边缘计算环境中终端设备信任评估的准确度不高，无法有效处理恶意终端对边缘网络服务带来的安全威胁问题，提出一种基于信誉反馈的边缘设备信任评估方法。首先，以节点服务交互信息评估其信任度，筛选恶意节点，降低边缘网络受到攻击风险。其次，通过设备反馈评价的模糊贴近度分析出节点的可靠程度，降低恶意节点在间接信任中的权重占比，减轻节点恶意行为对诚实节点信任评估的影响。最后对直接信任与间接信任采用一种动态加权的方法得出设备全局信任，能够适应边缘环境，使全局信任度值更加客观。仿真实验证明信任评估方案的准确性，有效提高边缘服务交互成功率。

关键词：移动边缘计算，5G 核心网，身份认证，数据包检测，信任评估

Abstract

With the development of Internet of Everything in the 5G era, various kinds of connections are generated in the network, the number of smart terminals and IoT devices and the data generated by corresponding services are exploding, and the traditional centralized cloud computing can no longer meet the high bandwidth and low latency extreme experience on the user side. Mobile Edge Computing (MEC) extends the computing and storage capabilities of cloud computing to the edge of the network close to the user, becoming one of the key technologies for the realization of 5G service scenarios and providing an advanced and open application computing platform for service providers. MEC exists in a wide range of application scenarios, such as automotive networking, industrial IoT, smart cities, virtual reality technologies, etc., bringing new services and facing security challenges at the same time. Attackers hijack and control a large number of low-security-capable terminals to launch resource exhaustion and denial-of-service attacks on edge network services, edge devices are vulnerable to intrusion and control by attackers to steal sensitive user information, unauthorized users illegally access the edge network, resulting in user privacy leakage, and malicious behavior of user data transmission processes reduce the overall efficiency of the network. The mobile edge computing environment has a large number of resource-constrained multi-type terminal devices with widely varying computing capabilities and architectures, making it difficult to apply a unified authentication protocol. With the broad application of edge services in defense, government and other high security level industries, the existing access authentication scheme, it is difficult to meet the security access of edge network terminal devices, mobile edge computing access security protection technology is critical.

In this paper, the mobile edge computing access security protection technology is studied, the shortcomings of the existing security protection mechanism are analyzed, and in order to realize the security protection of terminal devices in the MEC scenario, the research is focused on the process of terminal access to network services, which is divided into the process of user access to edge services and the data transmission process. Research is conducted on three aspects of user access to edge network identity authentication, data transmission supervision of terminal-edge network interaction and trust assessment of interaction between terminals, and proposed edge computing protection methods for trusted identity authentication, malicious traffic detection and defense strategies for edge gateways and methods for trust assessment of edge terminal devices, respectively, to enhance the security of the entire service process of mobile edge computing, with the following work:

(1) In order to address the security access problem of high security level edge computing private network of edge computing, a method of edge computing service protection based on trusted identity authentication is proposed, which is oriented to the trusted identity authentication requirement of edge computing high security level private network scenario, and a mobile edge computing high security level private network identity authentication solution for 5G core network is given. Firstly, through the embedding of user identity information and interface identification replacement based on the 5G core network, the real and trustworthy user identity of the access core network is realized. Then, on the basis of authenticated and trusted user identity on the core network side, edge protection gateway and edge protection gateway controller are added to achieve authentication and access for authenticated and trusted user identity of accessing DN through dual authentication of DN and edge protection gateway and identity authentication mechanism based on pass token. Finally, taking the 5G Telematics scenario as an example, the vehicle motion trajectory prediction algorithm is designed under the premise of protecting the security of edge computing nodes and stopping the leakage of user privacy, which realizes the efficient switching of edge service nodes during the high-speed motion of vehicles, and the edge computing service protection scheme based on trusted identity authentication is systematically verified and tested to prove the security of the scheme.

(2) For data transmission security between terminals and edges in mobile edge computing, a genetic algorithm-based malicious traffic detection and defense strategy is proposed to achieve a balance between security and performance of edge computing guard gateways. First, a gateway controller is set up at the edge protection gateway using the idea of zero trust to perform security inspection of service data traffic. Second, consider the gateway controller's malicious traffic detection efficiency, and implement a reasonable malicious traffic detection strategy under the premise of ensuring normal gateway data transmission to intercept tampering and malicious forgery of business flow packets at low cost. Analyze the attack gain of malicious traffic and the defense gain of the edge protection gateway, design a genetic algorithm-based probability optimization objective for sampling detection, and solve it to determine the best defense strategy for malicious traffic detection at the edge gateway.

(3) Aiming at the problem that the accuracy of end-device trust assessment in the existing edge computing environment is not high and cannot effectively deal with the security threats posed by evil terminals to edge network services, a trust assessment method for edge devices based on reputation feedback is proposed. First, the node service interaction information is used to assess its trustworthiness, screen malicious nodes, and reduce the risk of attack on the edge network. Secondly, the reliability degree of nodes is analyzed by the fuzzy closeness of device feedback evaluation, and the weight share of malicious nodes in indirect trust is reduced to

mitigate the influence of nodes' malicious behavior on the trust assessment of honest nodes. Finally a dynamic weighting method for direct and indirect trust is used to derive the device global trust, which can adapt to the edge environment and make the global trust degree value more objective. Simulation experiments demonstrate the accuracy of the trust assessment scheme and effectively improve the success rate of edge service interactions.

Key Words：Mobile Edge Computing, 5G Core Network，Identity Authentication, Packet Inspection, Trust Assessment

目 录

图 录

表 录

第一章　绪论

移动边缘计算[1]作为5G移动通信的一大关键实现技术，将云计算的能力扩展到网络边缘，为用户提供就近的计算和存储，极大减小了数据的传输时延和通信网带宽压力，为多样的业务需求提供平台和技术支撑，但同时也带来了全新的安全挑战。本章首先介绍了课题的研究背景和意义；随后介绍了边缘计算的相关概念，总结移动边缘计算面临的安全风险，分析移动边缘计算接入安全防护技术研究的不足，引出了本文研究的具体问题与其研究意义。最后对本文的主要研究内容和组织结构关系进行了总结。

1.1　研究背景及意义

5G移动通信技术和伴随其新兴的网络服务应用（例如移动社交媒体、物联网、工业互联网和车联网等），带来网络流量的指数级增长，对服务器和通信网络的数据传输和处理能力提出了更高的要求。5G目标的应用场景支持增强型移动宽带、超可靠低延迟通信和大规模机器类型通信，这些场景下的应用对通信带宽和计算存储资源的需求大幅增加。在移动边缘计算出现之前，互联网已经产生发展了如移动云计算、云计算和雾计算等技术。移动云计算[2]（Mobile Cloud Computing，MCC）技术实现了用户计算需求与终端设备的解耦，将移动用户的计算密集型任务卸载到网络的云数据中心，并使用拥有海量计算资源的云服务器加速任务的处理。移动设备在面对复杂计算和存储密集型应用时，会将任务传输至云数据中心进行处理。然而尽管移动云计算具有在协助终端设备进行数据处理方面的优势，但由于网络带宽限制，计算任务的远程卸载过程会产生较大的传输延迟，多跳传输和回程通信拥塞而导致的不良延迟波动会降低用户的服务体验质量（Quality of Experience，QoE），无法满足短时间内的大量计算密集型任务需求。此外，用户数据从终端到云服务器的远程传输还可能导致隐私的泄露。

为解决网络边缘流量激增，保障用户高可靠、低时延业务需求服务质量，降低网络负载，移动边缘计算应运而生[3]。移动边缘计算技术由欧洲电信标准协会[4]（European Telecommunications Standards Institute，ETSI）行业规范组织于2014年率先提出定义。移动边缘计算的基本思想是把核心网内部的云计算功能扩展到接入终端的网络边缘[5]，在网络边缘部署服务器，提供在网络逻辑边缘更靠近用户的计算和存储能力，并通过接入网络连接到移动设备。应用程序可以直接在边缘计算平台执行，并允许移动设备将其密集的计算任务通过无线卸载[6]到附近更强大的边缘服务器，从而使移动终端更快地执行任务。ETSI在2017年将移动边缘计算的概念扩展为多接入边缘计算（Multi-access Edge Computing），支持4G、5G、WiFi和固定连接等不同的接入方式，网络服务商能够将边缘计算服务器部署在网络接入过程中的不同位置。移动边缘计算部署在本地边缘，临近用户，具有超低时延，以及感知位置和网络上下文信息的能力。

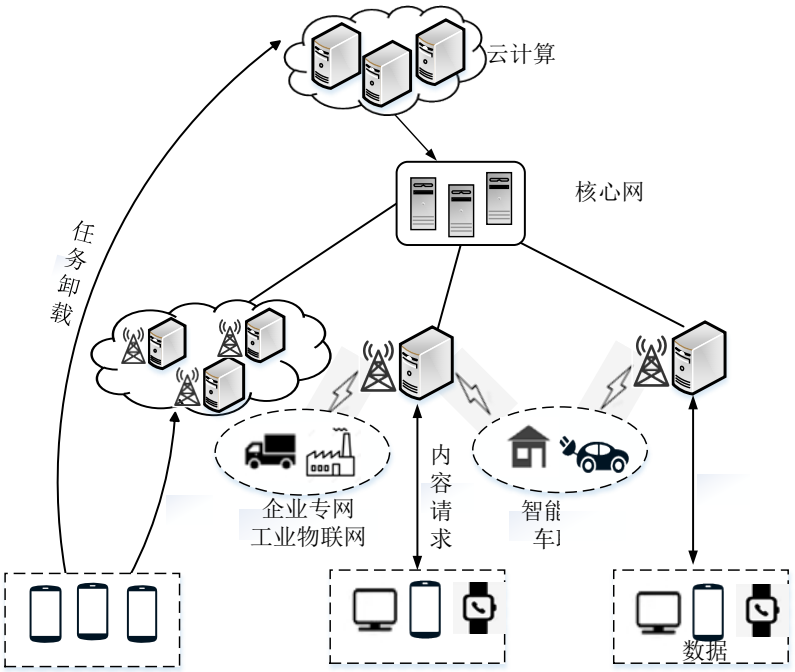

图 1.0.1 移动边缘计算场景架构

移动边缘计算[7]由如图1.1所示的三层架构组成。MEC网络由位于基站旁边的多个边缘服务器组成，每台边缘服务器都可以看作是一个运营商为满足相应的服务请求而部署的小型数据中心，处理用户诸如数据预处理、内容请求处理和任务卸载等业务需求。边缘服务器通过基站连接到核心网络的网关与中心云协作进行任务卸载。通过先进的无线通信和网络技术，边缘服务器可以建立可靠的无线链路来与移动设备进行数据传输。移动边缘计算存在的典型应用场景包括诸如车联网[8]、工业物联网[9]、智慧城市[10]等垂直行业[11]。然而，MEC将IT应用引入到电信领域将带来更为严峻的安全威胁[12]，例如：拒绝服务攻击、隐私泄露、仿冒攻击、中间人攻击等。MEC环境中有着移动用户、云服务、物联网设备等多种多样的网络连接，网络空间环境风险激增，基于IP地址和防火墙的传统安全边界正在逐步瓦解，无法满足终端用户的动态接入和高安全等级的业务需求。一是由于移动边缘计算网络采用分布式架构，MEC环境中存在着多实体间信息交互协作，可能发生用户的非授权访问[13]，非法接入边缘计算网络的未授权的用户及其可能做出的恶意行为对边缘网络的整体安全性造成了威胁。攻击者一旦突破移动边缘计算的网络边界便在可能在网络内部中进行无阻碍的横向攻击，对边缘计算高安全等级服务发起攻击。二是考虑用户发生越权访问，又或是边缘服务的账号被盗取，攻击者使用合法的身份窃取敏感信息，用户向边缘网络传输恶意流量，接入边缘服务的实体不能被一直信任，采用零信任思想对用户的行为进行实时监管，包括对数据传输流量的检测，对用户行为的异常检测，应对数据层面的安全风险。三是接入边缘网络的终端设备由于资源受限处在网络边缘安全能力不足且自身可能存在漏洞，容易被攻击者入侵和控制，边缘设备节点也可能存在用户发起恶意行为，影响边缘网络的资源利用效率。移动边缘计算面临着海量资源受限的异构终端设备接入，传统云计

算场景下的安全防护手段难以应对边缘计算应用带来的新安全风险，对移动边缘计算的安全防护至关重要。

移动边缘计算的接入安全防护[14]是指保障用户合法的接入服务，贯穿用户获取网络服务的整个服务。分为终端接入流程的安全防护和数据传输的安全防护，终端设备接入边缘计算服务需要身份认证的访问控制机制阻止非法用户的接入，同时管理服务过程中正常设备的行为，防止其发生恶意高于自身安全等级的越权访问行为，及时发现其异常。一是边缘计算作为终端网络数据的第一道收集和处理入口，包含着大量的实时用户信息，身份认证机制的安全有效能确保边缘服务的用户数据不被窃取，在用户接入边缘服务器时，通过可信身份的认证与识别能够阻断终端非法接入窃取敏感信息。二是终端和边缘网络间的数据传输，可能存在恶意流量，攻击者越权访问窃取敏感信息，接入网络后的实体行为不是一直可被信任。采用零信任思想对用户的流量传输行为进行实时监管，包括对数据传输流量的检测，对用户行为的异常检测，避免恶意流量因素对边缘网络服务的影响。三是边缘网络的终端设备计算存储能力不足安全性较低，容易被入侵和控制，攻击者伪装成合法的用户设备发起恶意行为，影响终端设备间正常的服务交互，采用信任评估的方法对设备服务交互能力进行评价，规范其如中断服务或传播虚假信息的恶意行为，能够提高边缘网络的整体安全性和服务效率。

本课题依托国家重点研发计划课题《6G移动通信安全内生及隐私保护技术》项目，围绕MEC场景下的接入安全防护展开研究，聚焦于终端实体获取网络服务的流程展开研究，分为用户接入流程和数据传输流程。一是针对用户接入边缘网络存在的安全隐患与不足，采用可信身份认证和边缘防护网关的方案阻止非法接入。二是考虑到用户在边缘网络数据传输过程中的安全问题：1）针对终端和边缘节点间的交互，采用边缘防护网关对流量进行监测，2）针对终端设备之间的交互，通过对终端设备进行信任关系的评估保障其服务能力，增强移动边缘计算整个服务流程的安全性。

1.2　移动边缘计算概述

1.2.1　移动边缘计算概念及安全威胁

MEC的参考架构[15]分为两层边缘实体，包括MEC系统层和MEC主机层，如图1.2所示。边缘计算系统层由移动边缘编排器（Mobile Edge Orchestrator，MEO）负责管理。MEO由移动边缘平台管理器和虚拟基础设施管理器组成，主要负责管理使用虚拟化基础设施资源的应用程序和服务配置，维护资源信息。业务运营支撑系统（Operations Support System，OSS）负责用户应用程序的生命周期管理，对用户的服务请求进行授权和管理。MEC主机层包括移动边缘主机（Mobile Edge Hosts，MEH）和移动边缘平台管理器（Mobile Edge Platform Manager，MEPM）。移动边缘主机包括移动边缘平台，移动边缘应用程序和虚拟化基础设施。虚拟设施管理（Virtualization Infrastructure Manager，VIM）提供计算、网络

和存储的设施用来托管应用程序和服务。移动边缘平台（Mobile Edge Platform，MEP），MEP负责分配给应用程序和服务的主机提供资源与网络。

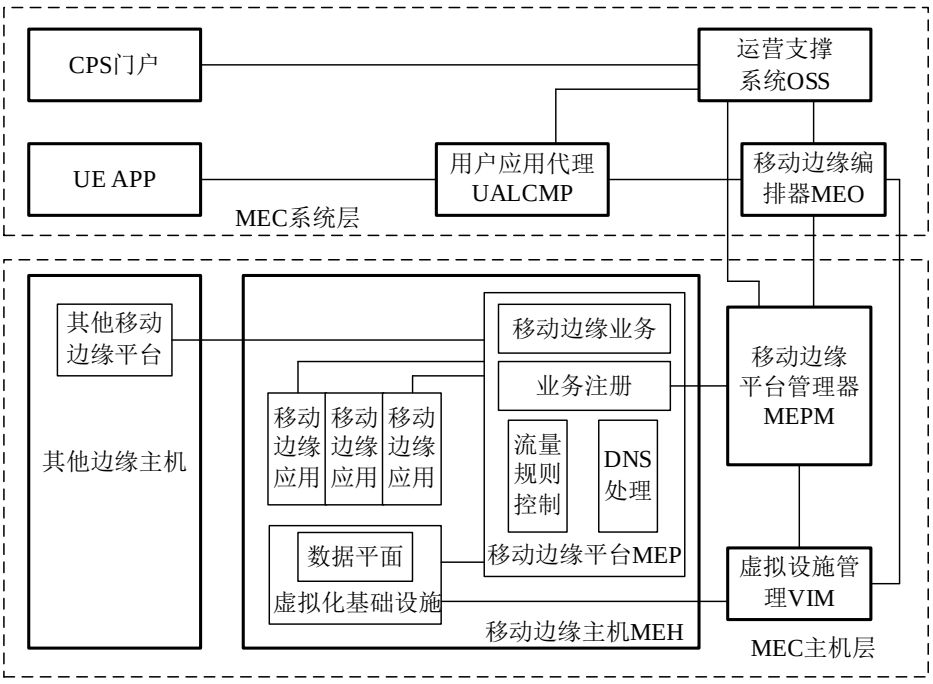

图 1.0.2　边缘计算平台架构

在移动边缘计算的实际部署中，MEC的数据平面和5G系统的数据平面之间需要协调，以便将流量转发和引导到应用程序。在边缘计算平台可以部署一个与5G控制平面功能交互的应用程序功能，以增强流量路由和转向，收集有关5G网络功能的信息并实现移动性。移动边缘计算在5G核心网下的部署，需要以下的功能来保障其需求。5G核心网络支持用户功能面（User Plane Function，UPF）选择和重选，用于选择性地将流量分流路由到数据网络，支持业务数据的路由转发、业务识别和策略执行等。UPF为5G网络中的边缘计算应用适配各种流量路由方案，应用程序会影响UPF的选择，并为用户制定不同的流量路由规则。移动边缘计算支持面向局域网的UPF灵活部署，可以将MEC主机部署在UPF和数据网络之间，MEC服务的用户可能会根据注册过程的局域网信息中发现其是否可用。5G允许授权的边缘计算直接访问网络功能，也可以通过网络开放功能（Network Exposure Function，NEF）间接访问，核心网中的策略控制功能（Policy Control function，PCF）为路由到局域网的用户流量定义服务质量（Quality of Service，QoS）和计费规则。

移动边缘计算环境中存在用户和应用程序的移动[15]，5G核心网通过会话管理功能（Session Management Function，SSC）或数据网络分配的历史记录保证服务连续性。MEC应用可以在三种SSC模式中选择一种，SSC模式1为用户提供稳定的网络连接，SSC模式2在建立新连接之前向用户释放当前连接，SSC模式3在断开现有UPF之前更改新UPF来确保用户的服务连续性。

移动边缘计算能够做到实时和上下 文感知，为用户提供个性化、实时化、多样化的计算服务，有效克服移动设备计算和存储能力不足的缺点。边缘计算为服务提供商和开发

人员提供灵活的技术平台，为信息和通信技术领域带来了新的活力。MEC提供的本地计算和数据处理功能能够减少5G网络的网络延迟和回程带宽压力，然而由于涉及的实体数量众多且具有开放性，MEC存在多方面的安全威胁[17]，包括边缘设备安全威胁、接入网络安全威胁、边缘网络威胁、核心基础设施安全威胁：

（1）边缘设备安全威胁

边缘网络根据用户设备（如智能手机、标签、计算机等）的内容敏感程度确定其安全和隐私要求。MEC环境中存在广泛的设备协作，用户不仅可以充当服务消费者，还可以生成数据并参与作为信息分发的服务提供者。边缘计算中复杂多样的接入设备中，容易存在恶意终端中断服务并影响边缘设备的安全运行。攻击者可以将恶意数据注入受感染的设备，发起信息注入攻击，传播虚假信息。攻击者发起窃听攻击，侧信道攻击获取用户敏感数据。

（2）接入网络安全威胁

接入网络安全是边缘计算节点高效运行的关键，同时能够影响用户和云基础设施的安全。边缘环境中的终端设备缺乏执行认证加密的存储和计算资源，需要严格的访问控制。攻击者攻击接入网络基础设施、连接的设备或通信信道，对网络基础设施发起中间人攻击。当边缘应用程序或服务受到损害，消耗MEC资源（例如网络带宽，计算能力或内存）时，易发生拒绝服务攻击，造成应用程序或服务响应延迟，或破坏MEC节点的功能，导致应用程序或服务中断。在分布式的边缘计算架构中，恶意攻击者可以通过未授权的网关接入边缘网络执行非法活动，访问网络设备、应用程序和边缘服务。

（3）边缘网络安全威胁

边缘网络承载计算能力、数据存储、虚拟化基础设备和管理服务，共享基础架构、平台和管理平面来支持应用程序和服务的配置。未经授权访问MEC节点可能导致信息隐私泄露，边缘网络可能会泄露敏感信息和网络上下文信息。恶意攻击者获取高于该用户的安全等级资源的访问权限，窃取机密数据，运行管理命令或部署恶意软件。攻击者还可能发起服务操纵攻击，插入虚假信息，操纵信息流，提供虚假的管理信息和历史数据。恶意行为者利用MEC资源来攻击用户，扫描本地网络中易受攻击的物联网设备并托管僵尸网络服务器。

（4）核心基础设施安全威胁

核心基础设施用于支持和管理边缘和接入网络运营，存储在边缘基础设施上的信息可能受到攻击并导致隐私泄露。攻击者入侵设备或系统以故意操纵数据并控制其驻留的硬件，可以发起包括诸如数据篡改，窃听和身份攻击等。移动边源计算的底层依托网络功能虚拟化（Network Function Virtualization，NFV）实现，NFV的安全性影响系统弹性以及服务的整体质量，虚拟化技术在应用于MEC时面临包括虚拟机操纵、虚拟机逃逸等攻击。虚拟安全功能可以应用于网络边界，以检测潜在威胁，隔离不安全的网络设备。

移动边缘计算还面临隐私泄露[17]的安全风险。移动边缘计算处理终端设备传输的数据不再由用户直接传输给云中心，而是由终端将数据传输到边缘节点，经边缘节点或云中心协同处理后返回至数据终端。虽然减少了数据远距离传输诱发的隐私泄露风险，但新引入了终端上传边缘节点的数据隐私、边缘节点存储转发和处理终端的数据隐私。边缘节点在网络中分散排布，对于数据的收集和分析缺乏有效的集中控制，边缘节点相比云中心缺乏对应的隐私保护措施，边缘节点面临多种形势的用户隐私泄露风险。

边缘计算存在海量资源受限的异构接入设备，多种不同类型的传输协议存在通信安全问题；边缘节点实体众多，靠近用户，防护能力弱，可能存在恶意的边缘节点；安全性不足的终端设备可能被恶意劫持，边缘网络容易受到分布式拒绝服务攻击[19]（Distributed Denial-of-Service，DDoS）；部署在网络边缘的基础设施存储的数据缺少有效的备份与审计，存在篡改和丢失的可能。

1.2.2 移动边缘计算安全防护技术

移动边缘计算场景下的安全防护涉及边缘用户和设备的安全防护、边缘网络的接入安全防护、边缘网络节点协同的安全防护和边缘核心网基础设施的防护。欧洲电信标准协会ETSI，边缘计算产业联盟[20]，国内外研究学者[7][12]对边缘计算安全防护机制和对应的安全措施展开了广泛的研究。边缘计算的安全防护机制包括：身份认证[21]、访问控制授权[22]、入侵检测[23]、隐私保护和数据安全[17]等。零信任作为一种网络安全防护手段，能够有效增强网络实体的安全性，其架构的实施包含用户身份、访问凭证、设备接入管理、服务生命周期管理、主机环境和互联网的基础设施等多个方面。边缘网络环境中包含海量异构且安全能力不足的终端设备接入，移动用户和终端还会在边缘网络节点间移动和切换，针对安全等级较高的边缘计算网络，传统的基于IP地址的访问安全边界难以应对边缘计算复杂多变的海量用户接入，可以考虑使用零信任思想改进边缘计算网络的安全防护。

零信任[24]是一种端到端的网络安全防护方法。零信任安全的实施包含身份、访问凭证、接入管理、终端设备、生命周期管理、主机环境和互联网的基础设施等多个方面。零信任安全架构的核心思想是：认为攻击者可能出现在内部网络，打破传统物理安全边界，不再默认信任传统边界内外的任何用户、设备、应用，以身份认证为基础，通过持续认证评估，细粒度最小授权，构建以身份为基础的网络安全边界，对内部关键资产实施持续风险评估和动态访问控制，处理身份滥用、越权访问、数据窃取等安全风险，保障客体关键资产的安全可信访问。零信任有着先进性及广泛的应用前景，其思想和架构是对传统安全模式的一种变革。

2010年Forrester分析师JohnKindervag正式提出零信任[25]概念，认为所有网络流量都不可信，需要对访问资源的所有请求进行安全认证。2011年Google公司开始BeyondCorp[26]项目零信任实践，并于2017年成功完成，旨在让员工不使用VPN的情况下实现对企业网络的安全访问。国际云安全联盟在2013年提出了零信任理念下的软件定义边界[27]（Software

Defined Perimeter, SDP）安全模型，其思想是将企业网络隐藏在网关之后，成为广泛应用的一种零信任实践方式。2020年，美国国家标准技术研究院NIST发表《零信任架构》草案[28]，给出企业零信任架构的实践指南。2021年，Forrester提出零信任边缘概念（Zero Trust Edge，ZTE），将零信任思想应用到云化架构下的边缘计算节点安全。

本文考虑零信任思想在移动边缘计算接入安全防护中进行应用。零信任安全架构[29]如图1.3所示，包含访问主体、资源客体、访问控制、网络安全基础设施等。零信任架构实现了数据平面与控制平面的分离，访问主体通过控制平面发起请求，信任评估引擎对主体的安全等级进行评估生并成权限策略，访问控制中心实施策略，请求获得许可，代理网关建立起加密的安全访问数据连接。数据连接的过程中，信任评估引擎会收集访问上下文日志信息，主体的行为、环境的变化等，结合访问主体的身份属性，使用基于大数据人工智能的终端可信环境感知、态势感知等技术对主体信任等级持续进行多维度的评估，一旦访问主体的信任等级不满足要求，连接便会中断，实现对资源的保护。

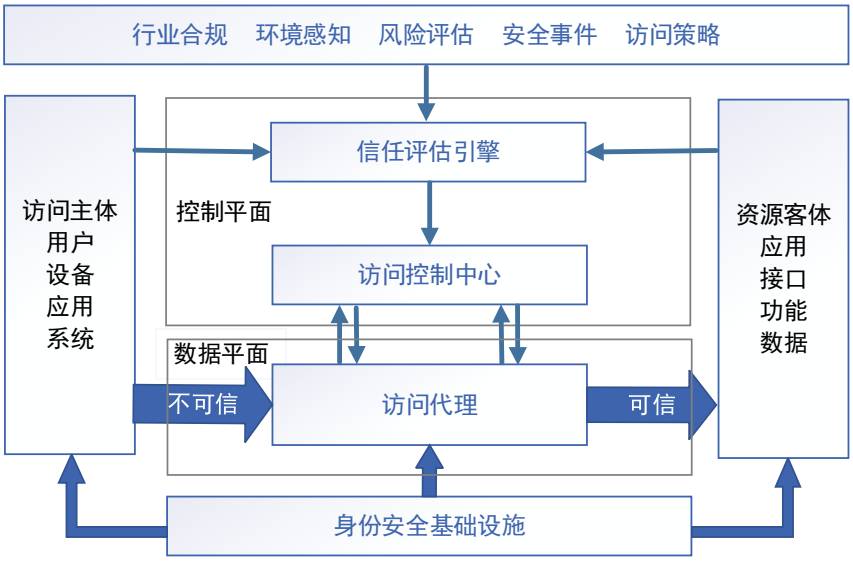

图 1.3　零信任安全架构

访问的主体包含用户、设备、应用、系统等多个维度，资源客体包含应用、接口、功能、数据等是需要保护的关键资产。访问代理是策略的执行点，负责建立、监控访问主体与资源的连接；访问控制中心依托信任评估引擎，负责生成客体访问资源的许可或凭证，建立连接；信任评估引擎能够依靠外部环境安全事件，风险评估计算出用户的安全等级，生成对应的访问策略。身份安全基础设施包括身份管理系统、认证管理、公钥基础设施、客体资源管理等。

零信任安全架构的实践可总结为三个技术发展方向[30]，以身份为基础构建的身份识别与访问控制体系（Identity and Access Management，IAM），实现细粒度动态授权；软件定义边界SDP以软件方式建立起虚拟的网络边界，使用代理网关隐藏资源网络，限制其在互联网的连接和暴露；以微分段MSG技术实现对网络资源的细粒度分隔访问；以微隔离技术

（Micro-segmentation，MSG），实现不同业务、人员、资源等横向访问的隔离，处理越权访问、内部攻击者问题。三者集成在一起实现端到端的零信任安全体系。

1）身份识别与访问控制：增强的身份与访问控制，包括身份鉴权、授权、管理、分析和审计，是数据及业务的重要基础。IAM的构建可分为三类，身份的定义和在线体验即生命周期管理；身份认证；权限授予。IAM使用身份作为策略创建的关键，基于身份和属性（设备、资产、环境、行为等关键属性）的多因子认证来决定信任程度和授权策略，统一管理控制接入实体，使用不同的访问控制模型，实现细粒度的授权管理。访问控制策略包含基于角色的访问控制（Role Based Access Control，RBAC）、基于属性的访问控制（Attribute Based Access control，ABAC）、基于策略的访问控制（Policy Based Access Control，PBAC）等。PBAC可简化访问控制和智能化权限设置，使用自然语言设置策略，支持环境控制策略的快速调整。

2）软件定义边界：SDP是国际云安全联盟提出的零信任的网络安全方案，并成为最佳的零信任实践方式。SDP强调网络的隐身而不是防御，控制面数据面分离，从架构设计上改变攻防不平等，解决TCP（Transport Control Protocol）协议的先连接后验证问题。SDP的核心是网络隐藏，使用单包授权认证[31](Single Packet Authorization，SPA)和数据平面实现可信连接，建立起基于身份和上下文的虚拟访问边界，结合身份与动态访问控制，对网络访问连接进行持续监控，对访问主体的信任等级做实时评估，动态调整访问权限策略。

3）微隔离：VMware在应对虚拟化隔离时提出了微隔离技术[31]，传统防火墙缺乏对内部流量访问的控制手段，随着内部间访问流量逐渐增大，产生了微隔离技术，目的在于阻止攻击者进入数据中心后的横向攻击，应对虚拟化、云化复杂环境下的安全。微隔离是细粒度的网络隔离技术，使用策略驱动的防火墙技术或是网络加密技术，将数据中心在逻辑上分段、分层，隔离不同的工作负载。微隔离通过授权的用户和应用程序关联访问程序，存在两种模式：虚拟化技术微隔离、如使用软件定义网络（Software-defined Networking，SDN）策略的隔离技术、VMware的虚拟化分层；基于主机防火墙和网络过滤的微隔离。

1.3 研究现状

1.3.1 移动边缘计算安全防护研究现状

移动边缘计算场景下的安全防护涉及边缘用户和设备的安全防护、边缘网络的接入安全防护、边缘网络节点协同的安全防护和边缘核心网基础设施的防护。欧洲电信标准协会ETSI，边缘计算产业联盟，移动通信运营商和国内外研究学者对边缘计算安全防护机制和对应的安全措施展开了广泛的研究。边缘计算的安全防护机制包括：身份认证、访问控制授权、入侵检测、隐私保护和数据安全等。零信任安全思想的实施包含对用户身份、访问凭证、设备接入管理、服务生命周期管理、主机环境和互联网的基础设施等多个方面。边缘计算作为一个网络实体，可以考虑使用零信任思想的设计一种边缘计算的网络安全防护方法。本文重点关注边缘计算场景终端接入安全防护。

零信任是在当前网络边界日益模糊场景下新的网络安全防护模式，何国锋提出基于零信任的5G云网防护方案[33]，包含客户自建模式、运营商虚拟专网VPDN改造模式、公共零信任架构模式。文献[34]提出一种5G零信任智能医疗平台，从主体、对象、环境及行为建立动态访问模型，实现了实时的网络安全态势感知、持续身份认证、访问行为分析和细粒度授权。文献[35]提出一种基于上下文和数据包标记的零信任微服务框架，使用eBPF（Extended Berkeley Packet Filter）跟踪微服务负载上下文并执行包的标签与认证，将安全边界从网络端点转移到细粒度的上下文微服务身份核验。文献[36]提出一种在零信任架构下基于区块链的连续身份认证协议，通过拜占庭共识机制选取节点实体生成密钥进行身份认证，无需权威的信任机构。文献[37]分析物联网安全问题，使用基于区块链技术的身份标识、区块链节点与零信任分段网关共享访问控制信息并存储设备的配置与更新建立的安全框架，提高物联网网络可靠性。

身份认证机制是指终端设备首次向边缘节点发起服务请求，边缘节点需要完成对终端合法身份的初始化验证确保只有合法设备的接入。移动边缘计算环境中存在海量的异构设备接入边缘网络，边缘网络中存在节点间频繁的数据交互，边缘计算中的身份认证安全至关重要。边缘环境中的身份认证技术包含；终端通过授权中心的获取资源访问权限的单一身份认证；终端用户在不同边缘服务商间跨域访问所有相互信任的边缘服务的联合身份信任；边缘计算中终端用户高速移动过程中服务切换重认证的切换身份认证。边缘计算网络中的通信主体边缘节点和终端设备部署在靠近用户的边缘，用户终端设备相较于云中心更容易受到例如数据窃取、身份假冒和中间人攻击等。文献[38]指出通过身份鉴权认证将攻击者的连接阻拦，是保护边缘用户敏感数据的重要安全手段，传统的集中式数字签名安全认证等方法需要较高的计算能力与资源消耗，无法满足海量终端的同时接入，不同实体间的信任问题复杂。移动边缘计算是分布式架构，终端的数量众多且会频繁地移动切换，群组认证、跨域认证等分布式认证研究是边缘计算身份认证的关键，实现轻量级的边缘计算安全防护方法。文献[39]提出一种匿名身份的移动边缘计算轻量级身份认证架构。文献[40]基于身份的密码学，给出一种在移动边缘计算基础设施间无缝切换的匿名身份认证协议。文献[41]在使用区块链的零信任分布式物联网场景下，提出基于零知识证明和中继跨链交易的跨链隐私保护协议，能够有效保护零信任物联网环境中的用户隐私信息。文献[21]在云边端场景下使用安全协议解决设备边缘的数据传输和存储面临的安全挑战，已有的边缘计算认证协议解决非固定移动边缘节点、手机等移动设备节点和跨域认证等场景下的安全问题，但大多仍采用云中心分发的安全凭证，没有非常完善的分布式边缘计算跨域认证协议。

文献[42]提出一种敏感数据访问保护的零信任模型，使用访问控制代理，通过分析访问请求、用户、设备、应用及数据类型来控制敏感数据的访问。文献[43]描述了一种基于首个数据包认证实现零信任网络的方法，并展示了该方法在保护SDN控制器免受网络攻击中的使用，在TCP连接请求中嵌入网络认证令牌，并阻止未经授权的流量完成请求，有效

地隐藏了攻击者的侦察尝试。文献[43]使用SDP保障云服务的安全，并在本地环境验证了SDP抵抗拒绝服务攻击的性能。文献[45]分析了SDP架构SPA协议，开发了一种建立初始用户身份验证的双向TLS加密算法，提升了SDP的安全与扩展性能。文献[45]通过抽象策略配置、网络设备和应用服务器实现网络访问和行为管理控制过程，建立了基于策略的访问控制和行为管理控制的框架。郭仲勇，刘扬等人[47]提出基于零信任思想，结合区块链、设备指纹、人工智能、轻量化安全协议和算法等技术作为基础设施确保用户的身份安全，并设计优化了身份认证方案。文献[48]提出一种基于用户画像信任的零信任访问控制动态细粒度授权系统，对用户行为生成画像，以当前行为与历史行为的偏差判断其异常行为，根据安全环境的变化调整权限信任阈值，根据用户行为的信任和信任阈值调整用户的访问权限，实现动态的细粒度访问控制授权。

1.3.2 移动边缘计算信任管理研究现状

移动边缘计算环境中存在海量动态和异构的终端设备参与数据传输和资源共享，传统的认证和鉴权普遍采用数字证书、公钥基础设施等方法需要耗费大量的计算和存储资源，难以管理海量计算和存储能力存在差异的边缘终端设备。边缘网络中的通信连接包含多种通信协议的共存使用，终端设备的任务交互过程中仍可能存在安全风险[49]。信任评估作为一种恶意节点的筛选机制，具备对恶意攻击的动态威胁感知能力，有助于边缘计算对节点行为的防范[50]，增强边缘网络的安全性。

移动边缘终端设备节点的信任度根据节点间的经验和交互历史得出评价，在节点交互之后周期性地评估和更新其信任度。在移动边缘节点之间的交互过程中，终端设备应协同监视相邻节点以检测恶意行为，收集信任信息并计算信任值。终端设备的信任度代表其未来的服务交互可信度，信任机制将边缘网络上信任度较低的节点划分为不可信或恶意节点，并与边缘网络隔离；具有较高信任值的节点被认为是可信的，并被选择用于存储和处理潜在的重要任务。信任评估的建立包括确定设备间的信任关系，评估、表示、维护和分配边缘计算节点间的信任值。

信任评估机制被广泛应用在分布式场景中，例如云计算[51]、无线传感器网络[52]、社交网络[53]等。信任是服务请求者对目标节点能否安全可靠地进行服务交互的一种综合判断。信任评估机制对历史服务交互信息做出评价，识别恶意终端节点，提供一种动态的恶意行为感知能力。目前对边缘计算信任机制的研究分为信任模型的构建和信任管理机制的设计，其中信任模型的构建工作主要集中于信任度计算。信任度计算的方法有：基于评分的简单总和或平均值、模糊逻辑[54]、贝叶斯概率模型[55]、beta概率密度[56]和主观逻辑方法[57]等。边缘环境中的终端设备节点容易受到各种攻击，信任机制同样会受到恶意攻击的危害，影响节点的信誉。恶意节点传播虚假信息反馈导致用户做出错误决策，例如节点传播诚实节点虚假的负面信息，降低其信任度。

文献[58]面向B5G场景下移动网络实体间的相互信任，总结现有的信任模型进行关键指标与需求，提出基于信誉的信任模型与标准化方法。文献[59]对边缘用户服务体验质量进行全面考量，结合计算资源、移动性、时延、带宽、能耗等多重约束因素，给出一种综合身份、行为、能力的边缘计算信任评估体系模型，优化边缘计算资源管理使用，提升边缘计算服务质量。文献[60]提出一种边缘计算信誉评估管理模型，基于设备身份、运算存储配置、交互行为信息确保节点的安全可靠，同时考虑了评估节点是否可信，通过直接信任、间接信任计算设备信任值。文献[60]通过移动边缘节点收集物联网节点信任信息，使用改进的最短路径算法访问主题和评估对象间的相关节点来推断信息关系的可靠与否，但需要评估节点移动的信息采集。文献[62]提出一种信任评估、过滤和选择的边缘计算任务卸载框架，引入包含隐私保护信任和行为的信任评估方法，分等级约束服务提供者敏感行为，筛选出低时延、低能耗且可信的资源提供者，研究更偏向于边缘计算节点的信任。文献[63]针对智能交通系统设备与边缘服务器的数据存储安全问题，联合边缘服务器和数据用户的直接信任与间接信任，建立一种基于流行度和信任度的强化学习边缘数据存储模型，但没有涉及带有攻击的场景设计。文献[64]对雾计算社交传感器网络节点的多种信任反馈数据进行分层采集和加权聚合，提出一种可靠快速的多源数据反馈聚合的信任计算机制，用于社交传感器节点的信任值评估。文献[65]采用多标准决策分析的方法对延迟、丢包率、抖动、吞吐量和任务失败率五种服务质量参数计算信任值，使用奇异值分解的协同过滤推荐算法计算设备整体信任度，进而给出一种轻量级服务信任管理模型。

1.4　问题提出

移动边缘计算技术在保障用户超可靠、低时延业务需求服务质量等方面具有显著优势，但也由于边缘计算环境节点多样、设备异构等特点，导致接入侧安全威胁突出。现有研究中虽然采用零信任架构、基于信任评估的节点交互等技术提升了边缘接入安全性。但面对日益严峻的网络攻击还存在单纯依赖应用层认证方案强度低、零信任防护架构效率低、授权节点恶意行为难以准确评估等问题。具体总结如下：

（1）现有MEC应用层和核心网独立式安全接入认证方案，难以满足高安全等级行业应用需求

MEC和核心网络的设备之间的消息流攻击者可以瞄准接入网络基础设施、连接的设备或通信信道。对MEC应用程序和服务的威胁包括设备、应用程序或服务劫持和DDoS攻击。当前，终端安全接入边缘服务，一方面通过运营商对终端进行授权保证终端从边缘侧接入网络，另一方面边缘服务也会在应用层采用授权认证方式来授权终端访问应用。然而由于终端类型众多，计算能力和架构存在较大差异，难以适用复杂的认证协议。因此，授权终端可能会被恶意劫持，加之轻量化的认证协议，边缘服务的安全性难以保证。此外，随着边缘服务在国防、政府等高安全等级行业的广阔应用需求。现有的认证接入方案，将难以满足上述边缘网络的接入，并可对内部网络稳定性产生威胁。

（2）在基于零信任边缘防护网关的用户面流量负载方案中，安全与效率均衡问题有待研究

边缘计算的用户数据平面应支持以下网络安全要求：不同安全区域的隔离、内置接口安全功能和信令数据的流量控制。UPF应支持以下业务安全要求：防御移动终端发起的DoS攻击、协议控制、虚假移动终端地址检测和流量控制。基于零信任软件定义边界的边缘防护网关将为用户数据面安全提供有效解决手段，采用将所有流量身份都标注为不可信状态的策略，逐一对用户数据身份进行检测和认证，最大程度保证用户面流量安全性。但是采用逐包验证的方式，将带来吞吐量的显著下降，这与引入MEC的低时延优势天然相悖。因此，如何在保证通信效率的情况下，选择最佳的边缘网关恶意流量检测防御策略，实现最大程度的安全，有待深入研究。

（3）现有边缘服务网络的信任评估机制无法有效抵抗节点恶意行为

边缘计算服务器靠近终端设备，更容易受到恶意用户和病毒的攻击。信任评估作为一种恶意节点的筛选机制，可以有助于边缘计算对恶意节点的防范，增强边缘环境的安全性。因而，信任评估机制被部署应用于边缘服务接入认证。然而，边缘计算环境中存在海量动态和异构的终端设备参与数据传输和资源共享，现有的信任评估算法面对复杂动态边缘计算环境还存在若干挑战。一方面，已授权的节点可能会存在恶意行为，比如进行恶意的虚假反馈攻击，另一方面，现有评估算法在对终端设备直接信任和间接信任采用固定的权重，会导致信任评估准确度降低。因此，有必要在评估算法中综合考虑节点交互行为等信息，从而确保信任评估准确度。

1.5 研究内容

为实现移动边缘计算场景下终端设备的安全防护，在对当前移动边缘计算主要安全威胁和安全防护方案现状分析的基础上，从终端实体接入网络流程和终端服务流程两个方面展开研究，针对用户接入边缘、终端和边缘交互、终端间的数据交互，分别设计了可信身份认证与边缘防护网关、边缘防护网关的流量监测和边缘终端设备信任关系评估的方案，增强边缘计算整个服务过程中的安全性。

（1）提出了一种基于可信身份认证的边缘计算服务防护方法

针对边缘计算的高安全等级边缘计算专网安全接入问题，提出一种于基于可信身份认证的边缘计算服务防护方法，该方法面向边缘计算高安全等级专网场景的可信身份认证需求，给出5G核心网的移动边缘计算高安全等级专网身份认证解决方案。首先通过基于5G核心网的用户身份信息嵌入和接口标识替换，实现了接入核心网用户身份真实可信。然后，在核心网侧用户身份真实可信的基础上，增设了边缘防护网关和边缘防护网关控制器，通过数据网络（Data Network，DN）和边缘防护网关的双重认证及基于通行令牌的身份认证机制实现对于访问DN用户身份真实可信的认证和准入。最后，以5G车联网场景为例，在保护边缘计算节点安全和阻止用户隐私的泄露的前提下设计了一种车辆运动轨迹预测算

法，实现了车辆在高速运动过程中边缘服务节点的高效切换，降低了通信开销和切换时延，对所提出的基于可信身份认证的边缘计算服务防护方案进行了系统的验证和测试。

（2）提出了一种基于遗传算法的恶意流量检测防御策略

针对终端到边缘网络数据传输安全，提出了一种基于遗传算法的恶意流量检测防御策略，实现边缘计算防护网关的安全与性能平衡。首先，设置边缘网关控制器对业务数据流量进行安全检测。考虑SDP控制器的恶意流量检测效率，在保证网关数据正常传输的前提下实施合理的恶意流量检测策略，以低成本的有效拦截对业务流数据包的篡改与恶意伪造。然后，分析恶意流量的攻击收益和边缘防护网关的防御收益模型，设计基于遗传算法的抽样检测概率优化目标，并进行求解，确定最佳的恶意流量检测防御策略。

（3）提出了一种基于信誉反馈的边缘设备信任评估方法

针对现有边缘计算环境中终端设备信任评估的准确度不高，无法有效处理恶意终端对边缘网络服务带来的安全威胁问题，提出一种基于信誉反馈的边缘设备信任评估方法，以节点服务交互信息评估其信任度，筛选恶意节点，降低边缘网络受到攻击风险；通过设备反馈评价的模糊贴近度分析出节点的可靠程度，降低恶意节点在间接信任中的权重占比，减轻节点恶意行为对诚实节点信任评估的影响；对直接信任与间接信任采用一种动态加权的方法得出设备全局信任，能够适应边缘环境，使全局信任度值更加客观，对所提出的信任评估方法进行了模拟实验，证明信任评估方案的准确性，有效提高边缘服务交互成功率。

1.6　本文组织结构

本文对移动边缘计算环境下的接入安全防护关键技术开展研究，全文共分为五个章节，其具体研究内容和各章节之间的结构关系如图1.4所示。

第一章为绪论，主要阐明本文研究课题的意义及背景，介绍移动边缘计算的特性，垂直行业应用场景、面临的安全威胁和边缘计算接入安全防护技术与边缘设备的信任管理机制，指出现有研究内容存在的不足，并针对性提出本文的研究内容。

第二章为针对边缘计算网络在接入层面可能存在的未授权用户对网络造成危害，提出一种于基于可信身份认证的边缘计算服务防护方法，实现了接入核心网用户的身份真实可信和接入边缘网络的用户身份真实可信。

第三章针对边缘计算防护网关的安全与性能平衡问题，考虑网关控制器安全防御机制的数据包检测认证效率，提出一种基于遗传算法的边缘计算网关的恶意流量检测防御策略，确定最优的授权检测机制。

第四章面向边缘计算场景下终端交互的信任关系，针对现有信任评估的准确度不高，无法有效处理恶意节点对边缘网络服务威胁的问题，提出一种基于信誉反馈的边缘设备节点信任评估方法，提高边缘网络中终端设备间交互的成功率。

第五章为总结与展望，对本文研究内容进行总结，并提出需进一步研究和完善的问题。

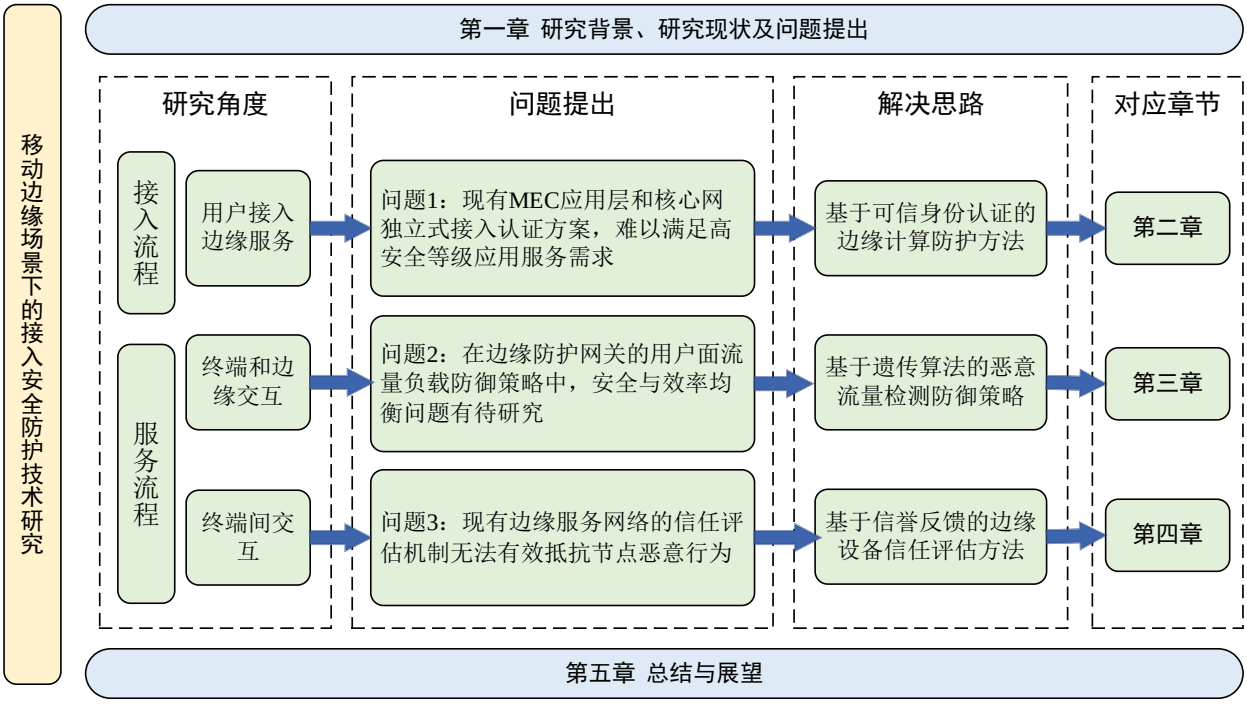

图 1.4　论文组织结构图

第二章　基于可信身份认证的边缘计算服务防护方法

边缘计算连接大量异构设备，承载多种垂直行业的应用，大量异构设备的接入，难以适用复杂的认证协议和集中认证管理，增加了边缘网络的安全风险。随着边缘服务在国防、政府等高安全等级行业的广阔应用需求，现有的认证接入方案，将难以满足边缘网络的安全接入需求。本章设计了一种基于身份可信的边缘计算服务防护方法，该方法在5G核心网侧通过身份信息的嵌入实现用户身份真实可信，增设了边缘防护网关和边缘防护网关控制器，通过DN和边缘防护网关的双重认证及基于通行令牌的身份认证机制实现对于访问DN用户身份真实可信的认证和准入。以车联网场景为例，在保护边缘计算节点安全和阻止用户隐私的泄露的前提下设计了一种车辆运动轨迹预测算法，实现了车辆在高速运动过程中边缘服务节点的高效切换，对基于可信身份认证的边缘计算服务防护方法进行了系统模拟实现验证了本方案的安全能力。

2.1　引言

移动边缘计算场景下，移动用户终端将计算密集型和时延敏感型的任务卸载到MEC服务器上，可以显著提高延迟性能并减少移动设备的能耗，并将为5G用户带来极致体验。然而，由于MEC部署位置靠近用户，以及其分布式特性，MEC节点相交于云节点更易被攻击者攻破，如用户侧容易发生非授权访问，如用户侧容易发生非授权访问，用户侧实体未经合法授权接入边缘网络后能够窃取保存在边缘侧的敏感信息，同时由于MEC实体间存在信息交互，攻击者可通过非法接入边缘网络的实体向其它区域内的MEC发起攻击。身份认证作为安全防护的第一道防线能够第一时间阻断非法实体的接入，有效预防攻击者窃取用户隐私信息的恶意行为发生[66]。

现有的认证方案主要是边缘服务在应用层通过授权认证方式来实现终端可信接入。文献[67]给出一种基于位置的轻量级身份认证机制，实现智慧医院场景下终端在不同区域边缘计算服务器之间的快速切换认证，采用椭圆曲线密码加密用户的敏感隐私数据，并证明了身份认证和密钥分发在BAN（Burrows-Abadi-Needham logic, BAN）逻辑下的安全性。文献[68]提出一种多因素身份认证方案，用户首先在网关节点注册，注册通过后的用户可以在传感器节点直接获取服务，该方案仅使用开销较小的哈希函数和异或运算能够应用于资源受限的设备。

然而，由于终端类型众多，计算能力和架构存在较大差异，且终端通常位于公共的开放空间，基于应用层的身份认证方案容易遭受身份信息泄露、用户假冒等攻击，缺乏网络层对于终端身份信息的感知，一定程度限制了移动边缘计算在政府、国防等安全等级要求较高的网络场景中的应用。近年来，有部分研究提出将终端的设备指纹、生物特征等信息嵌入到嵌入到数据包中，从而在网络层进一步对身份进行认证。清华大学吴建平等利用IP地址的逻辑、拓扑、所有者等多重属性，面向互联网提出一种地址驱动的网络体系结构，

来解决当前互联网面临的安全可信、服务质量等问题[69]。清华大学毕军等[70]通过将用户身份嵌入到IPv6地址，然后扩展改进DHCPv6协议，设计实现了面向互联网接入域的真实可信身份通信系统，从而阻止用户身份被假冒。解冲锋等人[71]提出了一种5G物联网终端的身份认证方法，利用终端的IMSI信息以及设备的物理特征来生成IP地址，进而实现网络层对终端唯一性的标识验证，从而确保物联网终端接入的安全性。文献[72]给出一种基于软件定义边界SDP的边缘计算多层安全架构模型，保障边缘网络服务的安全。然而，面向边缘计算环境中各类异构设备，如何提供通用的网络层认证方案，并进而实现网络层与应用层的双重认证，尚有待研究。

基于此，本章设计了基于可信身份认证的边缘计算服务防护方法。首先提出一种5G核心网的可信身份认证方案，充分利用64bit接口标识嵌入用户特征信息，给出通用的基于需求驱动的5G网络接口标识生成方案，实现边缘计算用户在5G核心网接入的身份真实可信，而后结合零信任中的软件定义边界SDP模型，设计了一种针对高安全等级边缘计算专网的基于DN和边缘防护SDP网关的双重认证机制，分别从网络层和应用层对用户实现身份认证增强。

2.2 系统架构

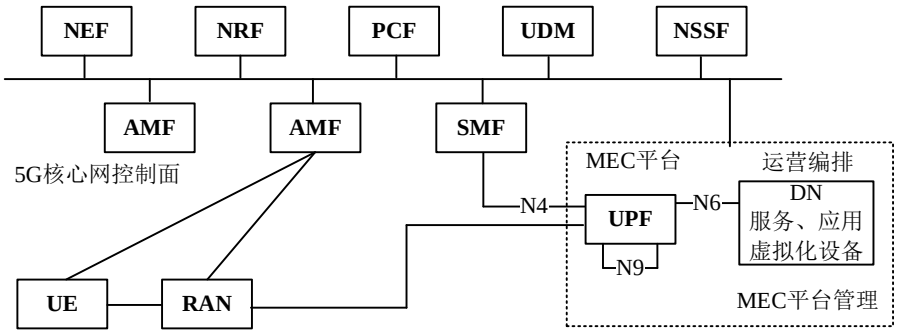

图 2.1 5G 核心网-边缘计算

MEC在5G生态系统中的部署示例如图2.1所示，其中MEC的数据平面映射到5G的数据面功能网元UPF和应用功能网元（Application Function，AF）。在依托5G部署的边缘计算系统中，左侧为基于服务化架构的5G核心网，右侧是MEC系统架构。在5G环境中集成部署的MEC系统，其功能需要和5G核心网元进行交互。边缘计算程序产生的服务在MEC平台进行注册，需要鉴权服务功能网元（Authentication Server Function，AUSF）授权才能与生成服务的网元进行交互。MEC可以部署本地用户数据面功能UPF作为分布式可配置的数据平面。

本章针对5G核心网-边缘计算的部署架构下用户接入高安全等级边缘计算专网服务，设计了一种基于可信身份认证的边缘计算服务防护方法。其整体架构如图2.2所示。基于可信身份认证的边缘计算服务防护方法可分为两部分，可信身份嵌入的5G核心网实现和SDP边缘安全防护网关。可信身份嵌入的5G核心网包含身份信息的嵌入和用户IP接口标识的替

换，将用户身份信息加密嵌入其IP地址当中，实现了用户IP与身份的唯一对应关系，保证用户在核心网中的身份可信。身份可信的用户接入核心网后用户向边缘计算高安全等级专网发起服务订阅，SDP网关只对密钥令牌正确的终端用户开放接口，并监管用户到边缘网络的数据传输。

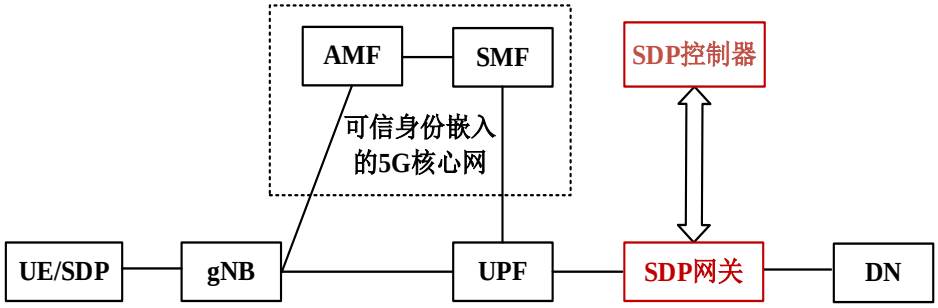

图 2.2　基于可信身份认证的边缘计算服务防护方法总体架构图

2.2.1　身份可信的 5G 核心网

（1）身份信息嵌入

针对多样用户信息类型、复杂身份认证需求，设计5G核心网IPv6场景下身份特征嵌入。该嵌入方案采用自定义信息嵌入方式，根据不同使用需求实现IPv6地址接口标识的自定义用户信息嵌入。

图 2.3　自定义用户信息格式

自定义输入信息格式包括两部分：4bit标志位和60bit自定义用户信息，如图2.3所示：

标志位占用4bit长度（不得大于4bit，不足4bit则高位补零），取值范围为0000-1111，标志位用于指示60bit自定义用户信息的类型，如用户手机号码（0000）、用户归属域（0010）时间信息（0011）自定义信息，具体格式要求如表所示：

表 2.1　标志位定义规则

标志位	自定义用户信息类型
0000	用户手机号码
0001	SUCI
0010	用户归属域
0011	时间信息
0100	用户手机号码+时间信息
……	其他自定义类型

自定义用户信息部分占用 60bit 长度（不得大于 60bit，不足 60bit 则高位补零），用于表示需要嵌入 IPv6 地址标识的自定义用户信息，其中依据标志位定义，自定义用户信息支

持单一类型用户信息嵌入和多种类型用户信息嵌入模式，只需要满足 X+Y+Z=64，如图 2.4 所示：

图 2.4　自定义用户信息格式

用户接入核心网后，SMF 网元的认证模块为其生成嵌入身份信息的 64bit 接口标识，随后将替换策略下发至用户侧 UPF 网元。

（2）接口标识替换

在核心网侧，当用户接入时，网元SMF会与UE建立pdu会话，并为UE分配IPv6入网前缀，将认证模块生成的嵌入用户身份信息的64bit接口标识和入网前缀合成该用户的IPv6地址，并将接口标识替换策略下发至用户侧网元UPF。在UPF侧，会根据接收到的来自SMF的策略，对用户上行的业务数据包进行IPv6地址接口标识的替换，实现用户入网流量的身份真实可信，同时，对于来自DN流向用户的流量，在UPF处也会根据本地存储的地址池匹配到该用户原本的IPv6地址，对数据包的IP头进行替换，将下行数据发回给用户。

接口标识替换模块的具体流程如图2.5所示：

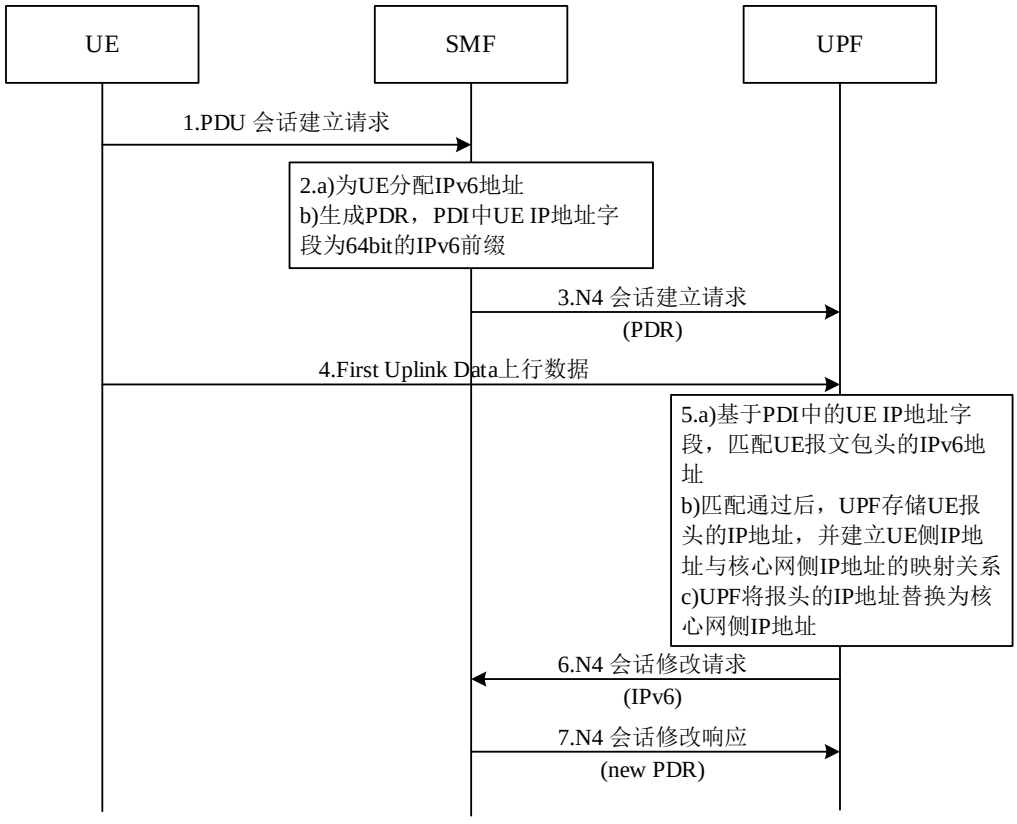

图 2.5　接口标识替换工作流程示意图

UE 向核心网请求建立 PDU 会话时，SMF 生成源地址匹配规则并向 UPF 下发匹配规则的流程如下：

1. UE 向核心网发送 PDU 会话建立的请求。

2. SMF 收到 UE 的 PDU 会话建立请求，SMF 为 UE 分配 IP 地址前缀，SMF 生成流处理策略（PDR），其中并在流规则报文检测信息（PDI）的 UE IP 字段中填入为 UE 分配的 64bit IPv6 前缀。
3. SMF 向 UPF 发送 N4 会话建立请求，SMF 在请求消息中将 PDR 和核心网侧 IPv6 地址发送给 UPF。
4. UE 首次向 UPF 发送上行数据。
5. UPF 收到 UE 的报文后，找到 UE 对应的 PDR 策略和流规则 PDI，将 PDI 中的 UE IP 字段与报头中的 IP 地址字段进行匹配；匹配通过后，UPF 存储 UE 报头的 IP 地址，并建立 UE 侧 IP 地址与核心网侧 IP 地址的映射关系；UPF 将 UE 报头的 IP 地址替换为核心网侧 IP 地址。
6. UPF 向 SMF 发送 N4 会话修改请求，请求消息中携带 SMF 分配的核心网侧 IPv6 地址和 UE 生成的 UE 侧 IPv6 地址。
7. SMF 根据 UPF 请求消息的内容，重新生成新的 PDR，新生成的 PDR 策略 PDI 中的 UE IP 地址字段是 UE 侧的 IPv6 地址。

接口标识替换将生成的用户身份信息的接口标识和用户上行接入核心网的业务流量的接口标识进行替换，实现了用户 IP 与身份信息的绑定，使接入核心网终端用户的不可仿冒。

2.2.2　边缘防护网关

本节主要是边缘防护网关的设计，基于SDP的边缘防护网关包含SDP网关和SDP网关控制器。网关基于通行令牌的身份认证，实现对于DN的非法访问流量的防护和合法用户访问的准入，确保通过核心网接入边缘计算用户身份的真实可信。SDP边缘防护网关的部署位置参照整体架构，部署在在边缘服务节点DN之前，对高安全等级服务边缘网络的数据传输进行准入和监管。

在传统的互联网通信模型C/S中，用户之间的端到端通信经常采用UDP、TCP或者ICMP协议，单个数据包被送到指定端口，服务器检测数据包，验证负载中包含的数据，通常采用将IP报头的首部进行校验得到校验值确定数据报包头是否被篡改。但这种方法无法确定目标来源的真实性与可靠性，攻击者也可通过重新构造校验和通过校验。本节基于已有工作，在核心网侧实现用户身份真实可信的基础上，参考软件定义边界SDP的零信任架构增加设计了SDP边缘防护网关和SDP边缘防护网关控制器。

SDP软件定义边界使用单包授权认证(Single Packet Authorization，SPA)和数据平面实现可信连接，建立起基于身份的虚拟访问边界，SDP安全模型由SDP客户端、SDP控制器、SDP网关三部分组成，其工作流程如图2.6所示，SDP控制器上线与SDP网关建立双向TLS连接，SDP客户端向网关发起SPA认证请求，经SDP控制器的认证控制获取安全策略，建立双向TLS连接到SDP网关，SDP网关。

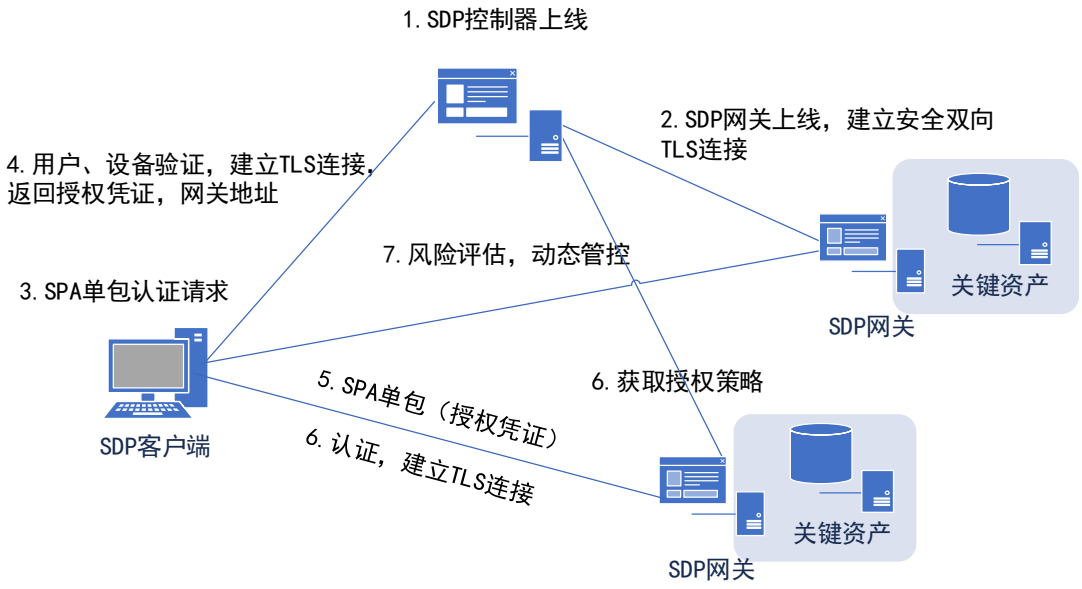

图 2.6 SDP 工作流程

2.2.3 DN 和边缘防护网关的双重认证

本节在核心网侧用户身份真实可信方案的基础上利用网络层IP与用户信息的绑定关系设计了一种基于DN和边缘防护网关的双重认证机制，分别从网络层和应用层对用户实现身份认证增强。

用户的上行数据经基站进入核心网后，核心网网元SMF中的认证模块根据用户的隧道信息、SIM信息等为其生成64bit接口标识，随后下发策略给UPF。在UPF处将用户数据包的包头IP地址的接口标识进行替换，随后发往DN。DN侧则会根据已有白名单对访问的用户进行筛选和准入，增设的边缘防护网关会将所有流网DN的数据包进行拦截和处理，根据历史数据对第一次收到的IP源的数据包，会进行解析并根据自身数据库中用户白名单对数据包中用户信息进行匹配，准许白名单内的用户访问，并将准许的数据包IP地址与终端用户信息进行处理，转发给核心网SMF网元进行双重认证。SMF基于其存储的地址池进行匹配，成功则向DN确认用户合法，同时生成该用户的许可令牌，向UPF下发许可策略的同时也将令牌加密后发给DN，UPF根据许可策略为来自该用户的数据包颁发令牌，当用户数据包到达边缘防护网关时，边缘防护网关根据边缘防护网关控制器配置的策略匹配数据包携带的令牌，成功则转发给DN，不成功则直接丢弃。

当用户经核心网接入互联网的上行业务数据到达DN时，由边缘防护SDP网关对其进行拦截和处理，首先基于边缘防护网关存储的历史数据对数据包IP进行解析，将获得的有关用户id和password的信息发送到DN发起询问请求，由DN对该用户合法性进行检测，若该用户不在DN的用户白名单中则直接丢弃；若该用户在DN的用户白名单中，则判断该用户为合法用户，DN发送应用层认证通过响应消息给边缘防护网关，边缘防护网关将其IP地址与数据包中有关用户的身份信息转发到核心网SMF网元。SMF根据存储的有关该用户的身份信息和IPv6地址的对应关系判断该用户是否合法，若不合法，则SMF将不合法的结果作为

响应消息发还给DN，DN随后将来自该用户的数据包丢弃；若合法则将网络层认证通过响应消息回传给边缘防护网关，随后准备进行基于通行令牌的身份认证。通过双重身份认证，验证了数据包的可靠性，校验了用户信息的正确性，并从网络层和应用层的双重认证中实现了对用户身份的增强认证，且开销较小、效率较高。

2.3　融合应用场景的设计与分析

在军事化应用方面的典型场景可划分为四大场景分别为：作战指挥、作训演习、后勤保障和特装保障。后勤保障以及特装保障场景中涉及到物资供应管理应用，基于5G移动通信技术构建边缘专网，实现特定场景下的快速机动性组网，可保障军事应用数据的绝对安全。

2.3.1　车联网防护描述

当前车载设备有限的计算和存储能力难以满足大量计算需求和低时延的限制，车联网方案选择在路面上广泛部署的路侧单元承担的计算任务，为汽车提供车联网快速接入和边缘计算等服务。车辆的通过订阅计算服务将任务卸载到边缘节点，缓解自身计算和存储能力的不足，却也带来新的安全问题。边缘计算节点位置相对静止且分布较散，节点各自负责其所属区域车辆的计算任务。在边缘计算服务器工作过程中，考虑到终端车辆的灵活性，可能存在由于终端车辆的高速移动，导致为其服务的边缘计算服务器频繁切换，任务在服务器之间跳跃和迁移，从而导致更大的开销和更高的延时，为车联网场景下边缘计算服务的切换效率、连续性和可靠性带来了巨大的挑战。通过对终端车辆的运动轨迹进行预测得出将要切换的边缘服务节点，提前分配资源和任务，能够解决由于终端车辆的高速移动性引起的边缘计算服务器频繁切换的问题。但车辆行进轨迹的预测势必会涉及到用户的行车位置、目的地等关键隐私信息，如何在保护用户隐私数据不泄露给边缘计算节点的前提下，进行用户行进轨迹预测和计算节点预分配，完成边缘计算服务器的切换和任务的迁移，为车辆提供安全可靠、高效快速的计算服务，越来越成为业界关注的焦点问题。

本章在已有的基于可信身份认证的边缘计算服务防护方法的基础上，设计了一种车辆运动轨迹预测算法，通过对用户位置数据进行处理，在确保边缘计算节点安全和用户隐私不被泄露的前提下，得到其未来的模糊运动轨迹，使边缘计算节点预测出用户车辆的相对运动方向和距离，筛选出距离终端车辆运动轨迹最接近的边缘计算服务器，及时建立连接并切换任务载体，实现边缘计算节点资源的预分配，进而解决由于终端车辆的高速移动性引起的边缘计算服务器频繁切换的问题，降低切换边缘计算节点和任务迁移带来的时延。

2.3.2　模型及求解

车联网位置预测将保护终端车辆和用户隐私作为前提，边缘服务器不可获取终端车辆和用户的具体位置、用户喜好及出行兴趣等信息，基于此建立用户位置移动模型，预测用户的运行轨迹，选择下一步将要切换的边缘计算服务器节点，实现边缘计算服务的高效切换及任务的快速迁移。

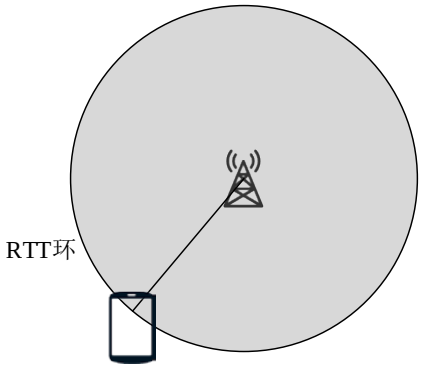

图 2.7　终端车辆定位技术原理示意图

采用 5G NR 新空口定位技术，在核心网接入侧估测终端车辆的具体位置，其原理如图 2.7 所示：基站发射定位参考（PRS）信号，终端发射信道探测参考（SRS）信号测量时差。首先通过多小区往返时间（RTT）来获得基站和终端之间的距离信息，然后通过基站的大规模 MIMO 多输入多输出来测量终端 SRS 信号的上行到达角 UL-AOA，以得到角度信息，最后通过距离信息和上行到达角来计算出终端的具体位置。随后，对该终端目标进行短时间内的持续跟踪，并将记录各个时间点终端位置，确定用户的下一步运动方向，形成终端用户的运动轨迹。5G 定位网络架构下的终端定位，基于核心网定位管理功能、认证管理功能、统一数据管理功能等多个网元执行位置服务操作。核心网将终端车辆在短期内的移动趋势发送至 MEC 服务器。将在核心网侧测量出的终端用户移动轨迹模糊化处理，去除用户关键敏感信息，提取终端用户的运动趋势信息发送给原承载服务连接的边缘计算服务器，使得该边缘计算服务器节点能够预判在当前终端用户的下一步运动轨迹，计算出将要切换的下一个边缘计算服务器，进行节点的提前配置，从而顺利完成任务迁移。

2.4　实验仿真

本节首先模拟融合场景下车联网的快速切换，然后对基于可信身份认证的边缘计算服务防护方法进行了系统的实现与验证。

2.4.1　仿真实验

（1）仿真设置

为验证本章提出的位置预测算法的准确性，现通过 Argorverse 车辆行进数据集来测试算法。该数据集收集了实际场景中在美国迈阿密和匹兹堡一段时间内车辆的位置信息和行进轨迹。实验在测试时，将数据集划分为两部分，一部分作为预测车辆行进轨迹的样本，另一部分则作为对照评价算法性能。首先在划定的目标区域内随机布设边缘计算服务器，根据样本数据计算得到用户的下一步行进轨迹，并将结果与原数据集中的车辆轨迹进行比较，根据相应指标分析算法性能，并将基于预测轨迹所确定的切换目标与真实轨迹应当切换的边缘计算服务器目标重合率进行比对，得到算法准确率。

现利用最小平均位移误差（aveADE）、最小最终位移误差（aveFDE）和漏失率（MR）评估标准来评价所提出算法预测车辆行进轨迹的准确率，各项误差指标越小反应算法的准确率好：

1.aveADE：预测轨迹与地面实况之间的平均欧几里得距离均值。

2.aveFDE：预测轨迹终点与地面实况之间的欧几里得距离均值。

3.MR：根据端点误差，预测的轨迹都不在地面实况 2.0m 以内的场景数量。

表 2.2　算法测试效果

指标	指标性能
aveADE	0.972
aveFDE	1.711
MR	0.213
准确率	90.46%

随后，本章将提出的边缘计算服务切换算法下面两种算法进行比较：文献[73]算法：对迁移目标的边缘计算服务器的资源进行考量，挑选资源剩余量较多、处理当前用户待迁移任务时延最小的边缘计算服务器完成服务迁移；随机算法，在多个边缘计算服务器中，随机挑选一些边缘计算服务器完成服务迁移。

仿真实验过程中设定的相关参数如任务的大小、服务器覆盖范围、服务器计算能力、传输功率和传输带宽，如下表 2.3 所示。

表 2.3　仿真实验具体参数设置

实验参数	数值
任务大小	100kb-500kb
服务器覆盖范围	500m
服务器计算能力	3GHz
传输功率	1.5w
传输带宽	10MHZ

（2）结果分析

实验结果分别从通信开销和切换时延两方面讨论算法的性能。图中三种算法分别为：本章提出的算法（Ours）、文献[73]中算法（TG）和随机算法（RA）。图 2.8 为算法的切换时延随着边缘计算服务器切换次数增加的变化情况，可以看出，随着边缘计算服务器切换次数的增多，切换总时延也在增大，其中，随机算法和文献中的方案的切换总时延相较于本方案更偏向于线性增长，即随着切换次数的增加，每次切换的效率不会明显变化，而本章提出的方案中，随着切换次数的增加，由于已经基于终端用户的预测移动轨迹进行了下一切换目标服务器进行了预分配，因此会减少切换的时延。

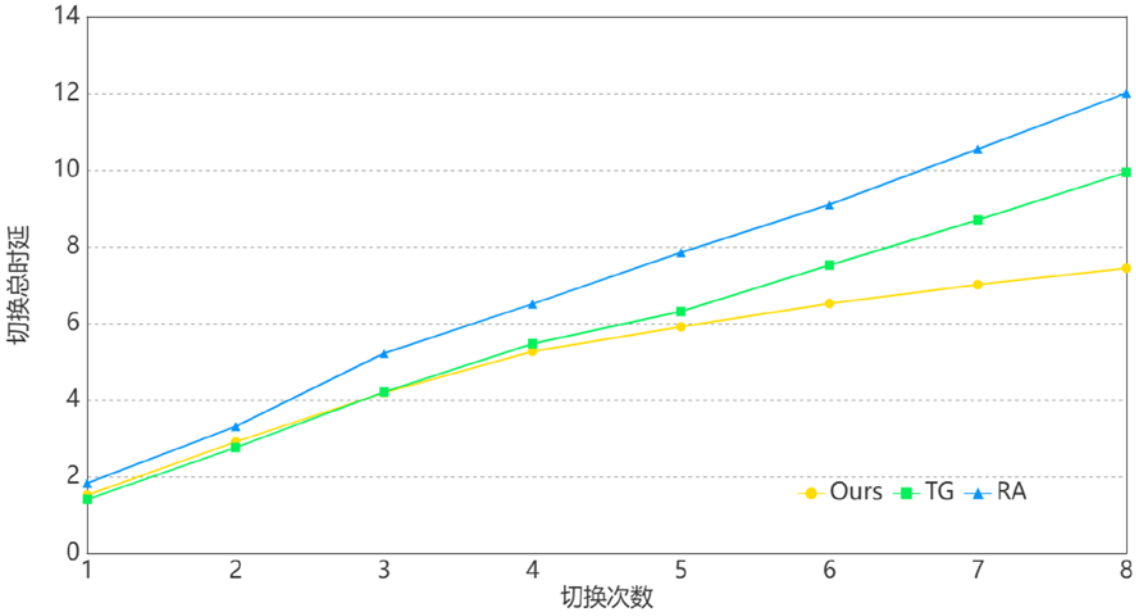

图 2.8　边缘服务器切换时延变化图

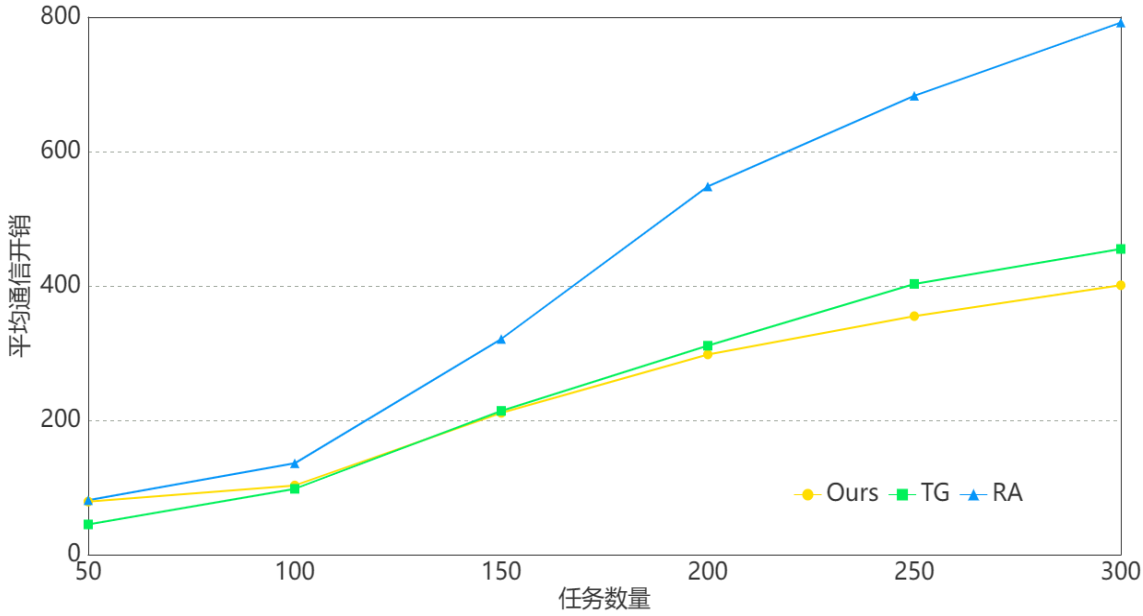

图 2.9　平均通信开销变化图

图 2.9 为算法的平均通信开销随着任务量增加的变化情况，可以看出，由于通信资源有限，随着任务数量的增加，剩余可用的通信资源将越来越少，平均通信开销均会随着需要迁移任务数量的增加而增加。当迁移任务的数量比较少时，三种算法的通信开销几乎相等，随着任务数量的增加，随机算法与另外两种算法的通信开销的差距加大。通过用户位置移动算法来预测终端用户的行动轨迹，找到即将切换的目标服务器，可以避免不必要的任务迁移跳数，让服务更快速的完成迁移。

2.4.2　系统实现与验证

本节将所提出的基于可信身份认证的边缘计算服务防护方法在模拟的5G移动边缘计算网络中进行了系统的验证，测试针对用户接口标识恶意欺骗的防护验证。记录测试设备、测试数据并分析实验结果，验证了系统方案的功能。基于可信身份认证的边缘计算服务防护方法通过自定义用户信息嵌入IPv6地址实现用户的可信身份认证，结合5G高安全等级专网的边缘计算场景，提出了一种可信身份特征嵌入测试方案，通过展示基于可信身份认证的边缘计算服务防护效果。

（1）测试环境

系统测试环境模拟 5G 移动边缘计算环境，包括基站、5G 核心网、边缘计算服务端、5G IPv6 终端。系统测试环境如下图 2.10 所示：

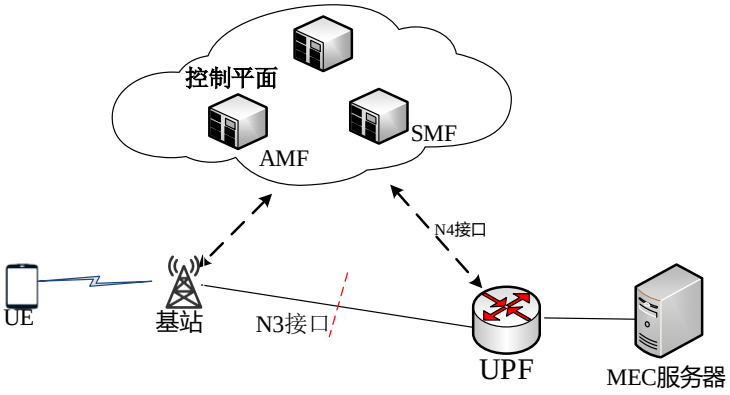

图 2.10　系统环境示意图

相关的测试工具，设备型号及参数具体如下表：

表 2.4　边缘计算防护方案系统测试设备

测试设备名称	设备型号
5G IPv6 终端	模拟发包工具 Insomnia
	华为 Mate30pro *2
5G 核心网	浪潮服务器 M620
边缘计算服务端 DN	浪潮服务器 M620
基站	电信科学技术第四研究所 FRI-NR01
测试工具	Wireshark、5G 仪表

测试过程中使用到的终端及设备实物图如下：

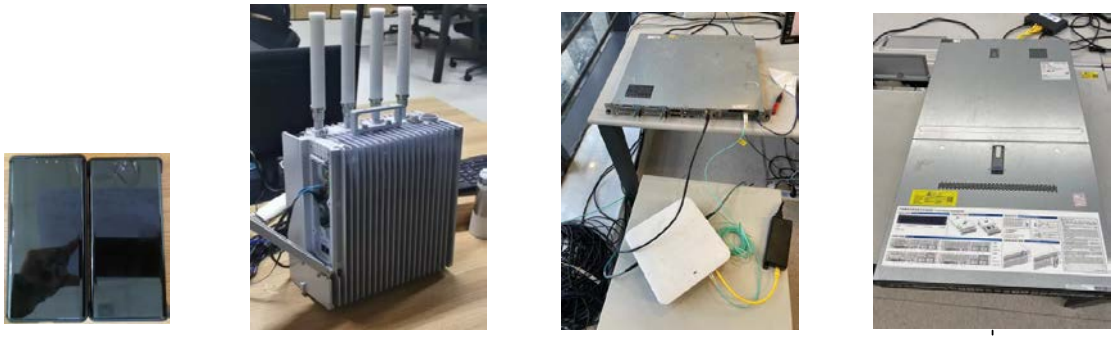

图 2.11 终端及设备实物图

（2）接口标识测试

手机终端访问服务端，在核心网修改来自于 UE 数据包的 IPv6 接口标识，观察 IPv6 接口标识修改对终端访问服务端的影响。

测试流程如下：

1. 终端建立会话阶段，终端获得核心网 SMF 分配的 IPv6 前缀为 E，UE 生成的接口标识为 F，则终端的 IPv6 地址为(E, F)；
2. IPv6 地址为(E, F)终端 ping 边缘计算服务端 IPv6 地址；
3. 边缘计算服务端用 wireshark 抓包，观察接收报文情况；
4. 在 gNB-UPF 接口上行 gNB 侧，根据为终端分配的隧道号，解析出终端的数据报文，并修改报文中终端的 IPv6 地址接口标识，修改后的 IPv6 地址为(E, H)，然后转发报文至服务端；
5. 终端观察 ping 情况；服务端观察 wireshark 抓包情况；
6. 服务端 pingIPv6 地址为(E, H)的终端，观察 ping 情况，终端使用 wireshark 抓包。

A）实验网 Free 5GC 中 IP 地址接口标识欺骗测试结果

实验网 IPv6 地址接口标识欺骗测试，手机终端访问服务端，在 N3 口修改来自于 UE 数据包的 IPv6 接口标识，观察 IPv6 接口标识修改对终端访问服务端的影响，如下图所示：

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2022:0:0:1::1	2018::40	GTP <ICMPv6>		164 Echo (ping) request id=0xd8e5, seq=1, hop limit=64 (reply in 6)
2	0.000019	2022:0:0:1::1	2018::40	ICMPv6		120 Echo (ping) request id=0xd8e5, seq=1, hop limit=64 (no response found!)
3	0.000026	2022:0:0:1::1	2018::40	ICMPv6		120 Echo (ping) request id=0xd8e5, seq=1, hop limit=63 (reply in 4)
4	0.000145	2018::40	2022:0:0:1::1	ICMPv6		120 Echo (ping) reply id=0xd8e5, seq=1, hop limit=64 (request in 3)
5	0.000148	2018::40	2022:0:0:1::1	ICMPv6		120 Echo (ping) reply id=0xd8e5, seq=1, hop limit=63
6	0.000212	2018::40	2022:0:0:1::1	GTP <ICMPv6>		156 Echo (ping) reply id=0xd8e5, seq=1, hop limit=63 (request in 1)
7	7.348432	2022:0:0:1::1	2018::40	GTP <ICMPv6>		164 Echo (ping) request id=0xd8e5, seq=1, hop limit=64 (reply in 12)

图 2.12 UE 数据包可达通服务端

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2022::1:0:0:abbc:ef01	2018::40	GTP <ICMPv6>		164 Echo (ping) request id=0xd8e5, seq=1, hop limit=64 (reply in 6)
2	0.000014	2022::1:0:0:abbc:ef01	2018::40	ICMPv6		120 Echo (ping) request id=0xd8e5, seq=1, hop limit=64 (no response found!)
3	0.000274	2022::1:0:0:abbc:ef01	2018::40	ICMPv6		120 Echo (ping) request id=0xd8e5, seq=1, hop limit=63 (reply in 4)
4	0.000438	2018::40	2022::1:0:0:abbc:ef…	ICMPv6		120 Echo (ping) reply id=0xd8e5, seq=1, hop limit=64 (request in 3)
5	0.000445	2018::40	2022::1:0:0:abbc:ef…	ICMPv6		120 Echo (ping) reply id=0xd8e5, seq=1, hop limit=63
6	0.000476	2018::40	2022::1:0:0:abbc:ef…	GTP <ICMPv6>		156 Echo (ping) reply id=0xd8e5, seq=1, hop limit=63 (request in 1)
7	5.916141	2022::1:0:0:abbc:ef01	2018::40	GTP <ICMPv6>		164 Echo (ping) request id=0xd8e5, seq=1, hop limit=64 (reply in 12)

图 2.13 IPv6 接口修改标识后，UE 仍可达通服务端

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2022::1:0:0:abbc:ef01	2018::40	ICMPv6	120	Echo (ping) request id=0xd8e5, seq=1, hop limit=63 (reply in 2)
2	0.000020	2018::40	2022::1:0:0:abbc:ef01	ICMPv6	120	Echo (ping) reply id=0xd8e5, seq=1, hop limit=64 (request in 1)
3	5.915666	2022::1:0:0:abbc:ef01	2018::40	ICMPv6	120	Echo (ping) request id=0xd8e5, seq=1, hop limit=63 (reply in 4)
4	5.915683	2018::40	2022::1:0:0:abbc:ef01	ICMPv6	120	Echo (ping) reply id=0xd8e5, seq=1, hop limit=64 (request in 3)
5	11.815561	2022::1:0:0:abbc:ef01	2018::40	ICMPv6	120	Echo (ping) request id=0xd8e5, seq=1, hop limit=63 (reply in 6)
6	11.815579	2018::40	2022::1:0:0:abbc:ef01	ICMPv6	120	Echo (ping) reply id=0xd8e5, seq=1, hop limit=64 (request in 5)
7	18.097901	2022::1:0:0:abbc:ef01	2018::40	ICMPv6	120	Echo (ping) request id=0xd8e5, seq=1, hop limit=63 (reply in 8)
8	18.097921	2018::40	2022::1:0:0:abbc:ef01	ICMPv6	120	Echo (ping) reply id=0xd8e5, seq=1, hop limit=64 (request in 7)
9	24.294689	2022::1:0:0:abbc:ef01	2018::40	ICMPv6	120	Echo (ping) request id=0xd8e5, seq=1, hop limit=63 (reply in 10)
10	24.294711	2018::40	2022::1:0:0:abbc:ef01	ICMPv6	120	Echo (ping) reply id=0xd8e5, seq=1, hop limit=64 (request in 9)

图 2.14　IPv6 接口标识修改后，服务侧抓取 ping 报文

```
root@5GCTE-eb1d63b274:/home/ixia# ping  2022::1:0:0:abbc:ef01
PING 2022::1:0:0:abbc:ef01(2022::1:0:0:abbc:ef01) 56 data bytes
^C
--- 2022::1:0:0:abbc:ef01 ping statistics ---
8 packets transmitted, 0 received, 100% packet loss, time 7160ms

root@5GCTE-eb1d63b274:/home/ixia#
```

图 2.15　接口标识修改后服务端无法连通地址为(E, H)的终端

可以看出在使用 IPv6 的 5G 核心网网络中存在接口标识仿冒的风险，数据包(E, F)更改终端接口标识的 IP 数据包(E, H)同样到达了边缘计算服务端，然而实际中接口标识修改后服务端无法连通地址为(E, H)的终端，地址并不存在，网络中存在接口标识的仿冒风险。

B）现网 IP LOOK 环境下 IP 地址接口标识欺骗测试

在现网环境下，手机终端访问服务端，在 N3 口修改来自于 UE 数据包的 IPv6 前缀，观察 IPv6 地址前缀修改对终端访问服务端的影响，如下图所示：

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2022:1108:0:80:c137:4176:2bae:cdab	2018::45	GTP <ICM…	164	Echo (ping) request id=0x000d, seq=1, hop limit=100 (reply in 2)
2	0.001796	2018::45	2022:1108:…	GTP <ICM…	164	Echo (ping) reply id=0x000d, seq=1, hop limit=128 (request in 1)
3	1.040000	2022:1108:0:80:c137:4176:2bae:cdab	2018::45	GTP <ICM…	164	Echo (ping) request id=0x000d, seq=2, hop limit=100 (reply in 4)
4	1.041981	2018::45	2022:1108:…	GTP <ICM…	164	Echo (ping) reply id=0x000d, seq=2, hop limit=128 (request in 3)

图 2.16　现网 UE 数据可达通服务端

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2022:1108:0:80::2bae:cdab	2018::45	GTP <ICM…	164	Echo (ping) request id=0x0011, seq=1, hop limit=99 (no response found!)
2	7.694996	2022:1108:0:80::2bae:cdab	2018::45	GTP <ICM…	164	Echo (ping) request id=0x0011, seq=1, hop limit=99 (no response found!)
3	14.650789	2022:1108:0:80::2bae:cdab	2018::45	GTP <ICM…	164	Echo (ping) request id=0x0011, seq=1, hop limit=99 (no response found!)
4	22.587785	2022:1108:0:80::2bae:cdab	2018::45	GTP <ICM…	164	Echo (ping) request id=0x0011, seq=1, hop limit=99 (no response found!)
5	29.551888	2022:1108:0:80::2bae:cdab	2018::45	GTP <ICM…	164	Echo (ping) request id=0x0011, seq=1, hop limit=99 (no response found!)

图 2.17　现网 IPv6 接口修改标识后，UE 仍可达通服务端

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	2022:1108:0:80::2bae:cdab	2018::45	ICMPv6	118	Echo (ping) request id=0x0011, seq=1, hop limit=98 (no response found!)
2	7.694948	2022:1108:0:80::2bae:cdab	2018::45	ICMPv6	118	Echo (ping) request id=0x0011, seq=1, hop limit=98 (no response found!)
3	14.650891	2022:1108:0:80::2bae:cdab	2018::45	ICMPv6	118	Echo (ping) request id=0x0011, seq=1, hop limit=98 (no response found!)
4	22.587942	2022:1108:0:80::2bae:cdab	2018::45	ICMPv6	118	Echo (ping) request id=0x0011, seq=1, hop limit=98 (no response found!)
5	29.552565	2022:1108:0:80::2bae:cdab	2018::45	ICMPv6	118	Echo (ping) request id=0x0011, seq=1, hop limit=98 (no response found!)

图 2.18　现网 IPv6 接口标识修改后，服务侧抓取 ping 报文

No.	Time	Source	Destination	Dport	Protocol	Length	Info
1	0.000000	2018::45	2022:1108:0:80::2bae:cdab	2152	GTP <I…	164	Echo (ping) reply id=0x000d, seq=1, hop limit=128
2	0.000001	2018::45	2022:1108:0:80::2bae:cdab	2152	GTP <I…	164	Echo (ping) reply id=0x000d, seq=2, hop limit=128
3	0.000002	2018::45	2022:1108:0:80::2bae:cdab	2152	GTP <I…	164	Echo (ping) reply id=0x000d, seq=3, hop limit=128
4	0.000003	2018::45	2022:1108:0:80::2bae:cdab	2152	GTP <I…	164	Echo (ping) reply id=0x000d, seq=4, hop limit=128
5	0.000004	2018::45	2022:1108:0:80::2bae:cdab	2152	GTP <I…	164	Echo (ping) reply id=0x000d, seq=5, hop limit=128

图 2.19　服务端抓取到 IPv6 地址为（E,H）终端的报文

可以看出在使用IPv6的IP LOOK 5G核心网现网中同样存在接口标识仿冒的风险，IP地址(E, F)下数据包更改终端接口标识后的IP数据包(E, H)同样到达了边缘计算服务端，网络中存在接口标识的仿冒风险。

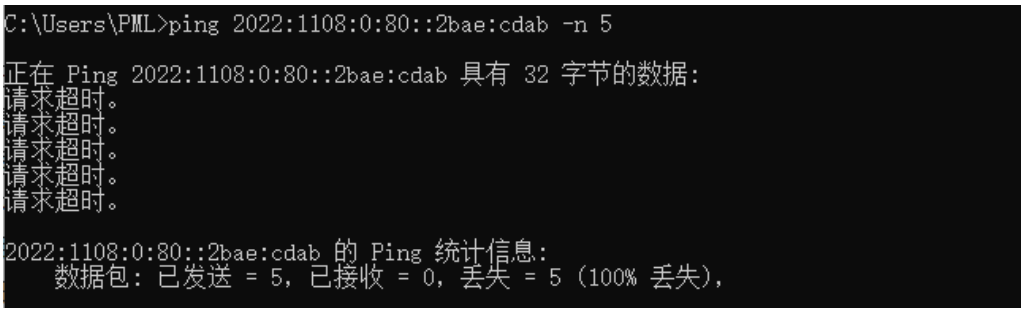

图 2.20　接口标识修改后服务端无法 ping 通地址为(E,H)的终端

（3）可信身份认证的防护能力验证

基于可信身份认证的边缘计算防护方案能够抵制接口标识仿冒的数据包对边缘计算服务的访问。测试流程如下

1. UE 从核心网获得 SMF 分配的 IPv6 前缀为 E，UE 生成的接口标识为 F，则 UE 获得的 IPv6 地址为(E,F)；
2. UE 用该地址向服务端发送服务请求；
3. 十个被劫持的 UE 视作恶意 UE，每个 UE 有一个正常分配的 IPv6 前缀 Mi，生成接口标识 Ni，恶意 UE 向服务端发起 DDoS 攻击。
4. DDoS 的具体实现方案为，单位时间内每个恶意 UE 基于正常分配的 IPv6 前缀，伪造 99 个接口标识，每个恶意 UE 分别使用正常的 IPv6 地址和 99 个伪造的 IPv6 地址向服务端发送服务请求。
5. 服务端观察当前流量和 wireshark 抓包情况；
6. UE 再次用该地址向服务端发送服务请求；
7. UE 观察服务端的响应情况，同时用 wireshark 抓取服务端响应的报文；
8. UPF 增加接口标识过滤；
9. 恶意 UE 向服务端发起 DDoS 攻击；
10. 同时合法 UE 再次用该地址向服务端发送服务请求；
11. UE 观察服务端的响应情况，同时用 wireshark 抓取服务端响应的报文，服务端观察当前流量和 wireshark 抓包情况

系统测试实验结果如下图所示的描述，充分证明了基于可信身份认证的边缘计算防护方案对恶意用户仿冒虚假 IP 接口标识地址攻击的防御能力，方案是可行有效的。

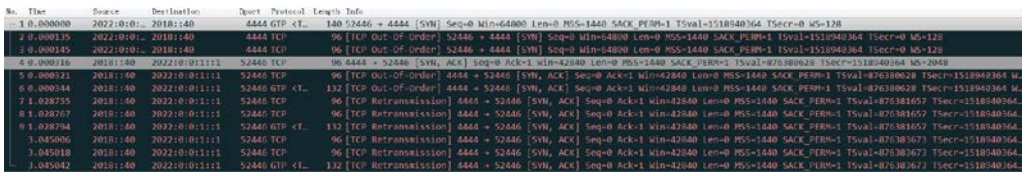

图 2.21　正常情况下，UE 使用 wireshark 可以抓取服务端的响应报文

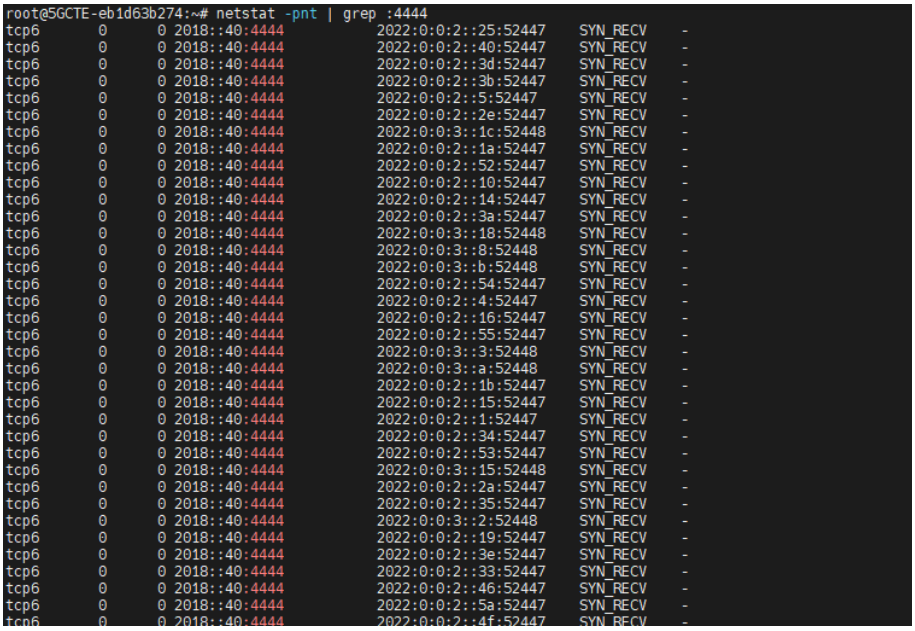

图 2.22　未启用可信身份认证功能，服务端观察到新增大量 TCP 连接

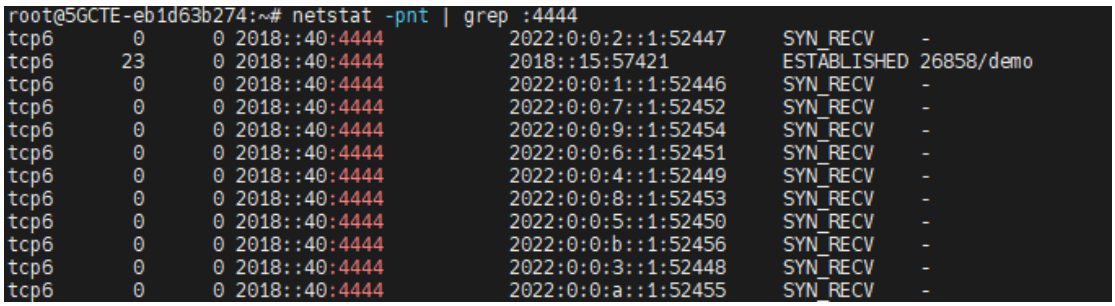

图 2.23　启用可信身份认证防护后，TCP 连接量下降，只有合法 UE 的 TCP 连接

（4）服务时延分析

在基于可信身份认证的边缘计算服务防护方案基础上，观察增加接口标识过滤功能对 UPF 服务质量影响程度，测试过程如下：

1.UE 从核心网获得 SMF 分配的 IPv6 前缀为 E，UE 生成的接口标识为 F，则 UE 获得的 IPv6 地址为(E,F)；

2.未增加接口标识过滤功能前，UE 向服务端发送请求 TCP SYN 请求，观察时间开销。

3.增加接口标识过滤功能后，UE 向服务端发送请求 TCP SYN 请求，观察时间开销。

测试结果如下图描述，UE 请求响应时间增加了 666 微秒，从终端访问服务端整个业务流程来看，本防护方案处理时延相较于数据传输时间可以忽略不计，对性能影响较小。

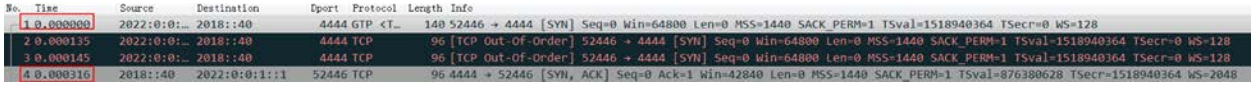

图 2.24　UE 请求响应时延 316 微秒

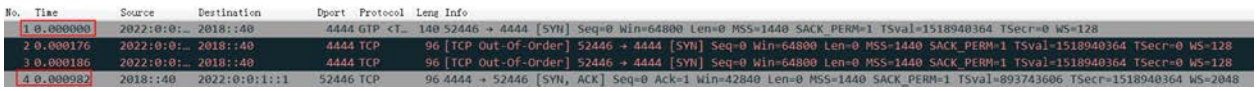

图 2.25　启用可信身份认证防护，UE 请求响应时延 982 微秒

2.5 本章小结

本章在现有5G核心网的基础上，提出基于可信身份认证的边缘计算服务防护方法，通过用户身份信息嵌入和接口标识替换实现了接入核心网用户身份的真实可信。在核心网侧实现用户身份真实可信的基础上，增设了边缘防护网关和边缘防护网关控制器，通过DN和边缘防护网关的双重认证及基于通行令牌的身份认证机制，实现对于访问DN用户身份真实可信的认证和准入。最后，把视线聚焦到5G车联网场景中，在保护边缘计算节点安全和阻止用户隐私的泄露的前提下设计了一种车辆运动轨迹预测算法，实现了车辆在高速运动过程中边缘服务节点的高效切换，降低通信开销和切换时延。在模拟的5G边缘计算网络中对基于可信身份认证的边缘计算节点防护方法进行了整体的系统实现和验证测试，证明了防护方案的有效，能够为高安全等级专网的边缘计算服务提供对应的可信身份接入安全访问。

第三章　基于遗传算法的恶意流量检测防御策略

传统的边缘计算网络安全防护架构，一旦攻击者合法地接入网络之后，便可在网络中横行，缺乏对终端在网络内的行为监管。本章结合第二章的基于可信身份认证的边缘计算服务防护方法在边缘计算侧部署的SDP边缘防护网关，网关控制器对业务恶意流量传输进行抽样的安全检测防御策略，分析攻击者恶意流量攻击和边缘防护网关的攻击和防御收益，使用遗传算法对恶意流量检测防御策略进行优化，平衡边缘网关的安全和性能，保障用户面流量的安全性。

3.1　引言

边缘计算将服务下沉到距离终端用户更近的位置，在服务时延、服务质量等方面具有优异性能。然而，边缘计算实现服务下沉的同时一定程度上带来安全威胁与安全风险。边缘计算环境中存在多种异构的连接设备，使用的传输通信协议不同。移动终端会发生较多的网络切换，边缘终端设备的资源有限，其安全防护能力不足，容易被入侵和控制，边缘网络可能存在数据传输的安全风险。边缘计算应具有以下安全能力：不同安全区域的隔离、内置接口安全功能和信令数据的流量控制，同时UPF应支持以下业务安全要求：防御移动终端发起的DDoS攻击、协议控制、虚假移动终端地址检测和流量控制。

文献[74]结合5G网络安全现状，给出了单包授权、网络功能信任评分等5G核心网安全设计的零信任增强方案，通过把安全能力沉浸到5G网络每个节点,将有助于提高5G核心网的安全性。文献[75]设计了一种基于零信任安全框架的5G网络切片方案，通过身份认证、权限判定等过程实现访问主体合法性验证，验证通过后进行业务请求，同时通过对资源访问信息进行按需加密，提升了业务访问过程的安全性。文献[76]提出一种基于用户实体行为分析的移动互联网安全态势感知模型，对用户的访问控制行为进行评估，并使用差分隐私机制保护终端数据隐私。范伟等人[77]对基于博弈论的入侵检测方法进行研究，寻找能够应对多种入侵行为的通用防御策略，提出基于博弈论的入侵响应决策模型，分析边缘节点的网络行为，考虑攻防双方的节点资源、代价损失、防御成本、攻击类型等多种因素，针对不同安全目标采取不同防御策略，实现了边缘网络损失和防御成本的平衡。

为解决边缘计算用户在数据层面上的安全威胁，本章在上一章节提出的基于可信身份认证的边缘计算服务安全防护方案的基础之上展开研究，使用SDP边缘网关[78]对终端传输的流量进行数据包检测以检测其用户身份合法性。为此边缘防护网关需要设计一种更有效、更安全的防御策略防止报文数据被篡改。基于零信任思想的安全架构将为数据平面安全提供有效解决手段，采用将所有用户身份都标注为不可信状态的策略，逐一对用户身份进行认证与鉴权，最大程度保证用户面流量安全性。但是基于零信任的架构采用逐包认证方式为安全性提供可靠保障，将影响吞吐量、服务时延等性能指标，这与边缘计算低时延

优势天然相悖。因此，本章节考虑在保证通信效率的情况下，分析如何实现最大程度的安全。

鉴于上述零信任安全在安全性能和服务质量的矛盾问题，针对边缘计算传输数据安全，为SDP网关设计了一种基于数据包检测的安全防护方案，对于网络内部的数据进行数据包检测与授权。同时为平衡安全性能和服务质量的关系，本章考虑采用流量数据包抽样检测机制应对此问题，同时设计了一种基于遗传算法的SDP控制器防御策略选择方法，保证SDP控制器安全机制的认证效率，以确保服务器不会过载或通信延迟不会显著增加。

3.2 系统架构

边缘网关的设计考虑终端与边缘服务器节点的数据传输安全，本章设计基于SDP边缘防护网关的数据恶意流量检测防御系统方案，网关的恶意流量检测系统架构如下图所示：本方案基于数据包的数据机密性、完整性、真实性，设计基于SDP架构的恶意数据包流量传输检测方法。

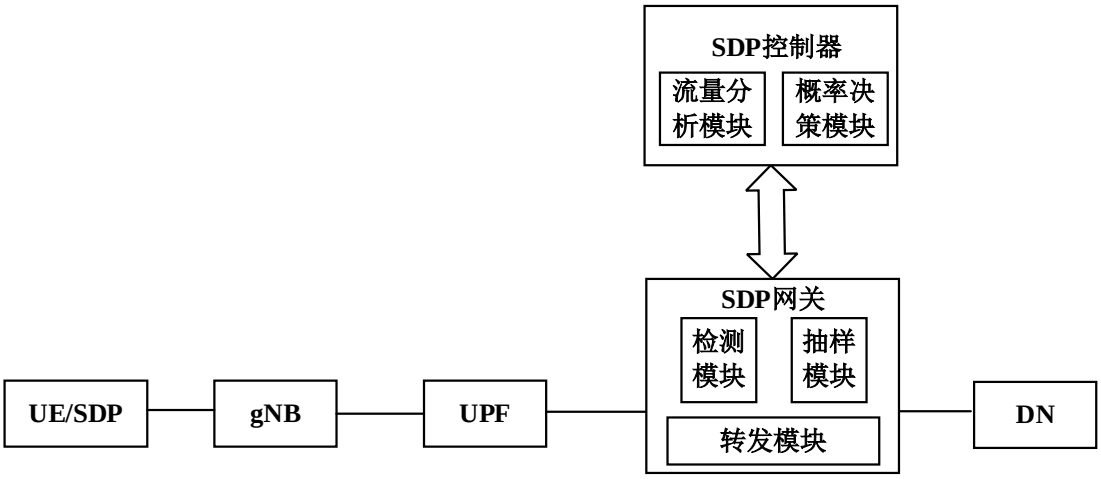

图 3.1 系统架构图

SDP控制器主要由流量分析模块和概率决策模块组成，通过收集流量状态信息并进行安全性分析，将分析结果发送至概率决策模块，概率决策模块根据流量分析结果选择最优抽样概率实现最佳防御策略；SDP网关由抽样模块、检测模块、转发模块组成，实现抽样包的恶意性检测。其中，各部分功能具体如下：

（1）SDP控制器

恶意流量分析模块：收集5G核心网数据面流量信息，通过对流量进行分析得到流量安全性信息。

概率决策模块：作为恶意流量检测方案的控制器关键模块，接收流量分析模块的安全性分析结果，结合流量负载、SDP防御能力、安全性分析结果得到最佳抽样概率，并下发至SDP网关抽样模块，实现流量包抽样。

（2）SDP网关

抽样模块：接收控制器下发的抽样策略，并根据抽样策略实现数据包的抽样，将抽样数据包转发至检测模块进行恶意检测，除抽样数据以外的其他数据进入转发模块参与数据包的正常转发。

转发模块：对数据包进行转发处理，包括未抽样数据包和经过检测模块检测的正常抽样数据包；

检测模块：作为SDP网关的关键模块，通过恶意检测方案实现抽样数据包的恶意性检测，其中检测结果为恶意的数据包被丢弃，检测结果为正常的数据包发送至转发模块进行数据包的正常转发。

3.3　恶意流量检测防御

恶意数据包检测基于验证签名技术，首先用户与服务器经协商得出一个随机的参数salt，用户发送的数据中利用该参数salt对于数据进行哈希签名，服务端获取请求需要重新计算一次签名进行对比，只有签名一致验证才会通过。同时为了考虑数据的时效性、完整性以及来源的真实性，本方案对于数据报文中的相应字段结合salt参数同时进行签名并进行校验，具体的设计方案如下：

（1）时效性设计，利用检测延迟技术协议提供时效性，考虑将数据包中的时间戳加入哈希签名的选择范围。

（2）数据完整性设计，对于数据包进行完整性检测时，需要将数据负载部分加入哈希签名的选择范围字段防止内容被篡改。

（3）来源真实性设计，对于用户数据包的源IP地址、源端口号、目的IP地址、目的端口号、协议版本类型五元组加入哈希签名的选择范围。

（4）哈希算法选择，选取SHA256散列算法，对于任意长度的信息，利用SHA256进行散列值函数计算都会产生256位哈希值，称之为消息摘要，其长度为32字节的数组表现形式为长度为64的十六进制字符串。

SHA256目前是一种较强的加密函数之一，由于其突出的安全性，被用于比特币的加密。SHA256是一个确定的单向哈希函数，具备确定性、不可逆性、无冲突性等重要特性。确定性是指对于单一的输入x确定唯一的输出y。不可逆性是指其属于单向函数，无法通过输出y求解出输入x，无冲突性指的是任何消息输入不同的x不会输出相同的y。

SHA256算法生成数据包签名的结构如下图所示：

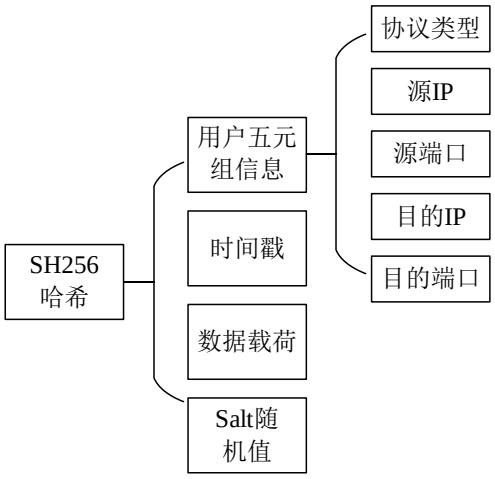

图 3.2　哈希签名流程

3.4　基于遗传算法的恶意流量检测防御策略

3.4.1　模型建立

考虑到海量的用户业务流数据，将所有的用户业务流数据包进行检测不具有可行性，为此本节提出了一种抽样检测模型，将用户发往SDP控制器的业务流数据进行抽样建模，综合考虑攻击者伪造篡改合法用户数据包所付出的攻击代价，依据攻击者攻击的概率设定合适的防御策略，即设定合适的抽样概率使得攻击者的攻击收益尽可能小达到防御的目的，具体的建模如下：

表 3.1　模型符号及含义

符号	含义	符号	含义
N	恶意包识别数量	P_{sample}	防御者抽样概率
L	流量负载	P_{attack}	攻击者攻击概率
A	最大攻击成本	$C_{packageAttack}$	单包攻击成本
D	最大防御成本	$C_{packageDefense}$	单包防御成本
B	最大流量负载	C_{attack}	攻击总成本
Per_{gain}	单位防御成本的收益	$C_{defense}$	防御总成本

单位防御成本的防御收益可以通过防御总成本和包抽样检测所识别到的恶意包数量得到，即：

$$Per_{gain} = N / C_{deffence} \tag{3-1}$$

Per_{gain} 表示单位防御成本的收益，N 表示通过包检测方案识别到的恶意包数量。防御总成本 $C_{defense}$ 可以通过抽样概率、单包防御成本和流量负载得到，考虑到量产思想检测包数量越多单包检测的成本开销越小，通过指数函数刻画这一特点，因此防御总成本 $C_{defense}$ 可以表示为

$$C_{defense} = C_{packageDefense} \cdot L \cdot P_{sample} \cdot e^{-P_{sample}} \tag{3-2}$$

其中，P_{sample} 表示网关实现包检测的抽样概率，且 $P \in [0,1]$，$C_{packageDefense}$ 表示网关对任一数据包实现检测所需要的成本，L 表示当前流量负载情况。攻击总成本 C_{attack} 可以通过攻击概率、单包攻击成本和流量负载得到，即：

$$C_{attack} = P_{attack} \cdot C_{packageAttack} \cdot L \tag{3-3}$$

P_{attack} 表示攻击者发起恶意包攻击的攻击概率，且 $P \in [0,1]$，$C_{packageAttack}$ 表示攻击者对任一数据包发起恶意包攻击所需要的成本。

通过上述分析，网关通过分析网络安全态势选择合适的抽样概率对经过网关的数据包进行恶意包检测，实现单位防御成本下的防御成本最大化，即：

$$\max Per_{gain} \tag{3-4}$$

对于防御者而言，其具有的防御能力防御成本都是有限的，尤其对于大流量场景下对所有数据包实现包检测难度极大，因此，应保证网关防御成本满足网关的防御能力约束，即：

$$0 \le P_{sample} \cdot C_{packageDefense} \cdot L \le \mathrm{D} \tag{3-5}$$

同样，攻击者自身的攻击能力攻击成本也是有限的，不可能实现对所有数据包的恶意攻击，因此攻击者发起攻击应满足攻击能力约束，即

$$0 \le P_{attack} \cdot C_{packageAttack} \cdot L \le \mathrm{A} \tag{3-6}$$

因此，抽样概率选择问题可以建模为一个单目标优化问题，具体优化问题可以表示为：

$$\arg\max Per_{gain} \tag{3-7}$$

$$s.t. 0 \le P_{attack} \cdot C_{packageAttack} \cdot L \le \mathrm{A} \tag{3-8}$$

$$0 \le P_{sample} \cdot C_{packageDefense} \cdot L \le \mathrm{D} \tag{3-9}$$

$$0 \le L \le B \tag{3-10}$$

$$P \in [0,1] \tag{3-11}$$

3.4.2　算法设计

遗传算法属于进化算法，通过模拟自然界“物竞天择，适者生存”的遗传变异规律来寻求问题的最优解。作为解决最优化问题的一种搜索式算法，遗传算法有三个基本的算子：选择、交叉和变异，本节将要求解的最优化目标也即网关实现包检测的抽样概率（初始时设成多个随机值）进行14bit的二进制编码，构建初始群体，利用遗传算法选择、交叉、变异等操作进行最优化求解，而使用遗传算法具备以下优点：

（1）与问题领域无关且随机快速的搜索能力；

（2）搜索从群体出发，可以多个体间同时比较，具备一定的并行性；

（3）搜索使用具有启发性质的评价函数，过程较为简单；

（4）具有可扩展性，易与其他算法结合；

本文采用遗传算法解决该最优化问题最主要是因为遗传算法能够以随机搜索的技术从概率意义上找出目标函数的全体解空间，不会陷入局部最优解，并且能够借助它的内在并行性，分布式进行计算进而提高求解效率。遗传算法可以定义为一个8元组，其具体公式为：

$$SGA = (C, E, P_0, M, \Phi, \Gamma, \Psi, T) \tag{3-12}$$

其中，C 代表个体编码方法，E 代表个体适应度评价函数，P_0 代表初始群体，M 代表群体大小，Φ 代表选择算子，Γ 代表交叉算子，Ψ 代表变异算子，T 代表遗传运算终止条件。遗传算法的计算流程如图3.3所示：

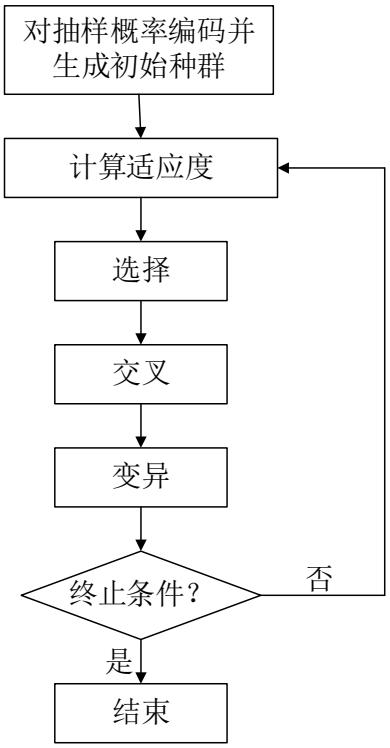

图 3.3　遗传算法流程图

本文采用交叉方式为采用单点交叉，根据交叉概率选择两个染色体并选择交叉点进行染色体间的交叉，变异方式为根据变异概率选择变异染色体并选择某一基因进行变异，适应度函数即优化目标，具体的符号及含义如表3.2所示：

表 3.2　符号及含义

符号	含义
T	遗传迭代次数
K	群体中个体的基因数
M	群体所含数量大小，一般取 20~100
x	交叉概率
y	变异概率

3.5　仿真结果与分析

3.5.1　仿真设置

本章通过数值仿真对所提基于遗传算法的SDP控制器策略选择算法实现仿真与评估。首先对所提算法的收敛性有效性进行分析，然后对不同实验环境下，不同的网络流量情况、攻击场景、防御者防御成本和单包防御成本等因素对SDP控制器防御策略进行分析。数值仿真实验使用Matlab进行模拟，使用的计算机配置为：CPU 3.4GHz，内存大小16GB，硬盘1T。

3.5.2　结果分析

（1）收敛性

针对SDP控制器恶意流量检测问题，提出一种基于遗传算法的SDP控制器策略选择算法，本算法基于遗传算法进行设计，参数选择对于算法的收敛性具有关键影响。其中，染色体个数设置为40，基因数量为14。

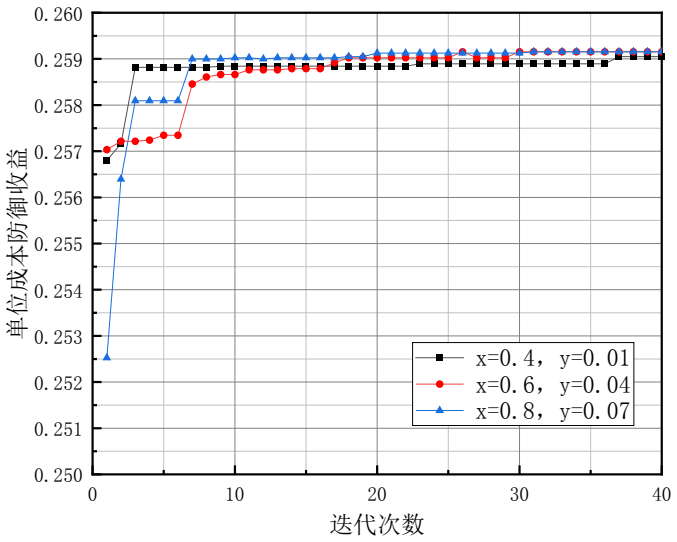

图 3.4　单位成本防御收益变化图

如图3.4、图3.5所示，分别为单位成本防御收益随迭代次数的变化趋势和抽样概率随迭代次数的变化趋势，共选取三种交叉概率和变异概率的组合。从图中可以发现，无论是哪种交叉概率和变异概率的组合，单位成本防御收益和抽样概率都随着迭代次数的增加不断优化，并且在迭代20次之后，单位成本防御收益和抽样概率均趋于收敛。可知，基于遗传算法的控制器防御策略选择算法具有优秀的收敛性，因此为保证实验性能，后续实验参数如不特殊说明，交叉概率取值0.6，变异概率取值0.04，迭代次数取值为40。

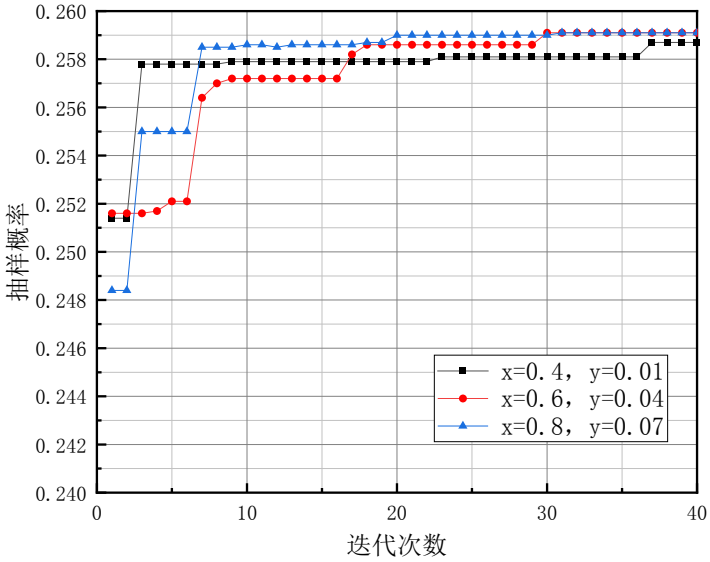

图 3.5　抽样概率变化图

（2）抽样概率

下面对不同SDP控制器场景下网络流量情况、攻击场景、防御者防御成本和单包防御成本等因素对SDP控制器抽样概率的影响进行分析。其中，如不特殊说明，流量负载取值为100000，单包检测成本取值为1，防御总成本取值为20000，攻击概率取值为20%，单包攻击成本取值为1。抽样概率采用遗传算法进行优化求解。

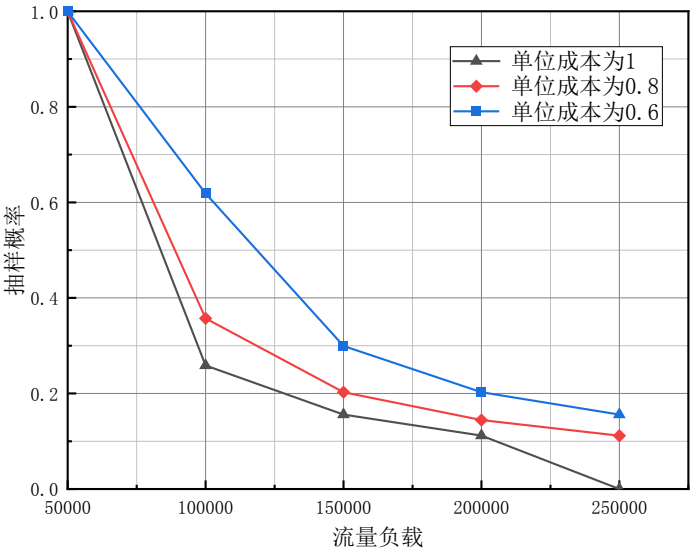

图 3.6　流量负载下抽样概率变化图

图 3.6 展示了在不同流量负载条件下最佳抽样概率策略选择的变化情况，可以看到，随着流量负载的增加，防御总成本固定的情况下为保证满足防御总成本约束，抽样概率取值越来越小；在同样的流量负载情况下，防御总成本固定的情况下抽样概率随单包检测成本的增大而减小，不难理解，单包成本越大，其可检测包的总数就越小，符合实验预期。

图 3.7 展示了在不同防御总成本下的最佳抽样概率策略选择的变化情况，可以看到，随着防御总成本的增加，流量负载固定的情况下为实现单位成本的防御收益最大化，抽样概率的选择越来越大，同时，当防御总成本相对于当前流量负载和单包检测成本足够充裕时，抽样概率稳定趋近于 1，进而实现最优的防御效果；在同样防御总成本情况下，流量负载固定的情况下抽样概率随单包检测成本的增大而减小，符合实验预期。

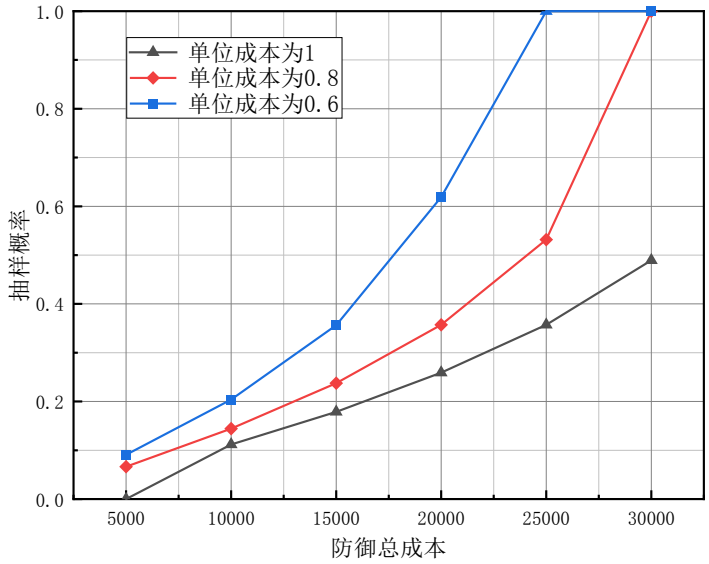

图 3.7　防御总成本下抽样概率变化图

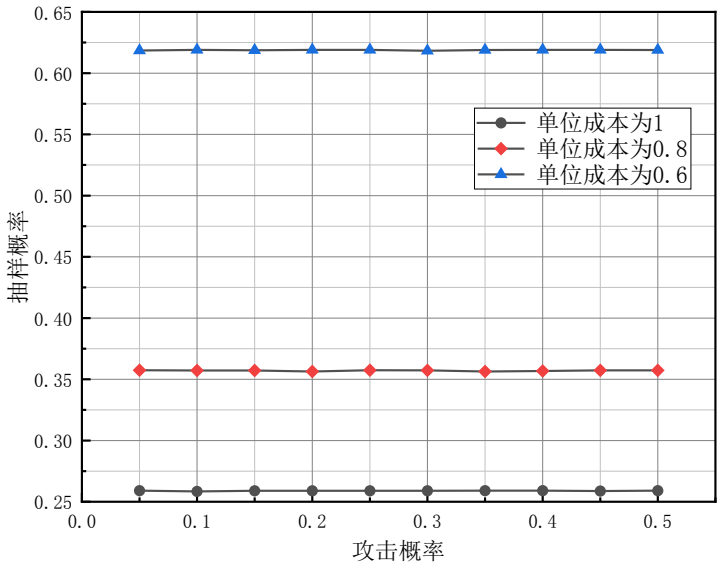

图 3.8　攻击概率下抽样概率变化图

图3.8展示了攻击者不同攻击概率攻击能力下的最佳抽样概率策略选择的变化情况，可以看到，随着攻击概率的变化，最佳抽样概率变化不大，这是因为基于抽样的恶意包检测存在随机性，不针对特定的用户传输流量，在一定成本下，边缘防护网关的安全防御能力稳定。因此无视攻击概率的变化，实现最优单位成本防御收益所对应的抽样概率是稳定的，

选择当前防御总成本下的最大抽样概率以实现最优的防御效果，能够为边缘网关SDP控制器提供良好的策略支撑，平衡边缘SDP安全网关的安全能力和资源开销。

3.6 本章小结

本章针对边缘计算的用户数据传输安全问题，采用SDP边缘防护网关对用户传输至高安全等级边缘网络的流量进行检测，网关控制器对用户数据传输流量使用抽样检测的安全策略，对边缘网关的安全性和资源性能进行平衡，分别分析攻击者的攻击收益和防御者的防御收益，SDP控制器应当选择最优的防御策略实现恶意包检测，达到最佳的防御收益。为此本章设计了一种基于遗传算法的控制器防御策略选择方法，通过实验证明了所提算法的稳定性和收敛性，在不同实验环境下测试，得到其最佳抽样概率，证明了该算法在不同场景下的优良性能，可以为边缘安全网关的SDP控制器数据包检测提供策略上的支撑。

第四章　基于信誉反馈的边缘设备信任评估方法

移动边缘计算应用在车联网、物联网、智慧城市等人们生活的诸多方面，大量的数据和服务在网络的边缘产生，终端设备因防护能力弱容易被入侵和控制，边缘环境中的终端设备间交互容易存在恶意行为，从而降低网络运行效率。本章提出了一种基于信誉反馈的边缘设备信任评估方法，建立终端设备间的信任关系，以减轻恶意行为对边缘网络造成的危害。首先，以节点服务交互的历史信息评估节点信任度，采用模糊贴近度分析节点信誉反馈的诚实度，降低节点恶意行为对信任度值的影响，而后对边缘网络中的直接信任评价和间接信任反馈采用动态的自适应权重进行聚合，使得信任评估更加客观。最后，仿真实验验证了基于信誉反馈的边缘设备信任评估方法的有效性，并与传统逻辑算法和贝叶斯信任模型对比了边缘网络中的服务交互成功率。

4.1　引言

MEC环境中存在海量动态和异构的终端设备参与数据传输和资源共享，边缘计算服务器靠近终端设备，更容易受到恶意用户和病毒的攻击[49]。边缘计算网络中的认证和鉴权普遍采用数字证书、公钥基础设施等方法，需要可信的权威中心，但由于网络中终端的多样复杂、计算存储能力存在的差异，边缘终端设备的任务交互过程中仍可能存在安全威胁[12]。以往的研究更多的考虑边缘网络受到攻击时如何保证完成任务，如文献[21]研究了边缘网络节点数据传输安全,文献[79]研究计算节点对恶意攻击的容忍能力，这些研究保障了任务的完成，却未考虑恶意节点会在边缘网络持续造成危害。信任评估作为一种恶意节点的筛选机制，可以有助于边缘计算对恶意节点的防范[50]，增强边缘环境的安全性。

信任是服务请求者对目标节点能否安全可靠地进行服务交互的一种综合判断。信任评估机制对历史服务交互信息做出评价，识别恶意终端节点，提供一种动态的恶意行为感知能力。目前对边缘计算信任机制的研究分为信任模型的构建和信任管理机制的设计，其中信任模型的构建工作主要集中于信任度计算。文献[60]提出一种边缘计算信誉评估管理模型，基于设备身份、运算存储配置、交互行为信息确保节点的安全可靠，同时考虑了评估节点是否可信，通过直接信任、间接信任计算设备信任值。针对物联网场景，文献[61]通过移动边缘节点收集物联网节点的信任信息，使用改进的最短路径算法访问主题和评估对象间的相关节点来推断信息关系的可靠与否，其信任关系的评估过度依赖移动节点的信息采集。文献[62]提出一种信任评估、过滤和选择的边缘计算任务卸载框架，引入隐私保护信任和行为的信任评估，分等级约束服务提供者敏感行为，筛选出低时延、低能耗且可信的资源提供者，研究倾向于卸载对象边缘服务器节点的选择，不考虑设备节点的信任。文献[64]对雾计算社交传感器网络节点的多种信任反馈数据进行分层采集和加权聚合，提出一种可靠快速的多源数据反馈聚合的信任计算机制，用于社交传感器节点的信任值评估，但应用场景中未考虑可能存在恶意节点的情况。文献[65]采用多标准决策分析的方法对延

迟、丢包率、抖动、吞吐量和任务失败率五种服务质量参数计算信任值，提出一种轻量级服务信任管理模型，使用奇异值分解的协同过滤推荐算法计算设备整体信任度，但其仅计算设备的静态信任值，未考虑随着时间变化设备的信任评估会发生变化。

一方面，上述研究未考虑边缘设备节点中可能存在恶意节点，另一方面，在对终端设备信任评估时仅依赖边缘服务器节点信息收集而未考虑设备间的直接交互，导致信任评估的准确度低。本章聚焦于常见的智慧家庭、传感器网络等场景下的信任评估，其中存在终端-边缘计算节点-终端的交互方式。本章研究边缘计算环境中的终端设备的信任评估，结合终端设备在边缘网络的服务交互评价反馈，提出一种基于信誉反馈的边缘设备节点信任评估算法（Edge Device Trust Evaluation Based on Reputation Feedback，EDTERF）。首先，为提升信任评估的可靠度，EDTERF使用模糊贴近度通过设备反馈评价的模糊贴近度分析出终端节点的可靠程度，优化终端设备的信任反馈，降低恶意节点虚假反馈对终端信任度的影响。然后，通过对边缘环境中终端信任反馈的聚合计算，提出一种动态的自适应加权方法，能够适应边缘环境，可以降低恶意节点行为的影响，使全局信任度值更加客观，有效提高边缘服务交互成功率。

4.2 系统模型

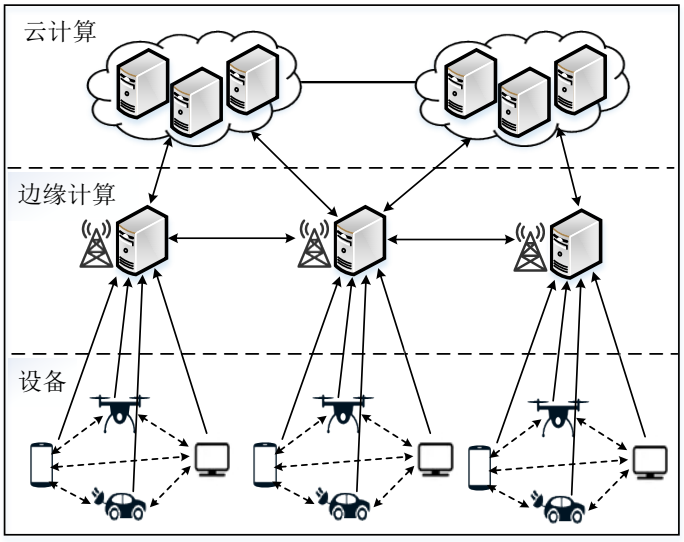

图 4.1 边缘计算网络架构

边缘计算网络架构如图4.1所示，由云计算层、边缘计算层和边缘设备层三部分组成。云计算层主要包括中心管理数据库服务器，提供强大的基础设施服务能力、平台软件服务和高安全等级的数据存储与访问。边缘计算层由边缘服务器组成，用于监控和汇总边缘设备的信息反馈和数据融合。边缘设备层由协作交互共同完成任务的终端设备组成。

边缘计算架构内在的信任关系可以在图4.2中得到体现，其信任主体为边缘服务器与边缘设备节点。信任的计算涉及两组实体，边缘终端设备集合（$D=\{d_1,d_2,\cdots d_n\}$，其中i为终端设备编号，n为在边缘计算中参与信任计算的设备总数），边缘计算服务器集合（$S=\{s_1,s_2,\ldots,s_m\}$，其中m为边缘计算网络服务器总数）。边缘设备之间的交互产生直接信

任，并将直接信任反馈到边缘服务器，边缘服务器汇总直接信任数据计算出间接信任并聚合得到全局信任，边缘设备可以向服务器请求某一设备节点的全局信任值。

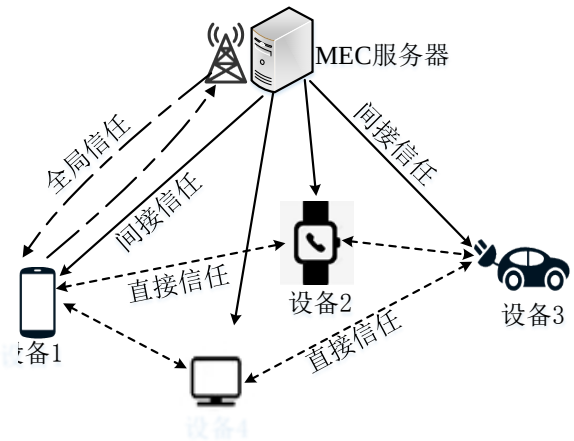

图 4.2　信任关系构成

定义 1 直接信任 $D_{d_i,d_j}(\Delta t)$，基于设备间的直接交互，将设备节点 d_i 与设备 d_j 的交互服务质量历史数据量化得出直接信任。

定义 2 间接信任 $I_{d_i,d_j}(\Delta t)$，基于所有与目标设备有过交互设备的服务评价，边缘计算服务器将与目标节点 d_j 交互的所有设备直接信任 $D_{d_i,d_j}(\Delta t)$ 聚合计算出对设备 d_j 的间接推荐信任。

定义 3 全局信任 $G_{d_i,d_j}(\Delta t)$，边缘计算网络对边缘设备的客观综合信任评价，融合计算来自设备主体的直接信任和间接信任。

4.3　信任评估算法

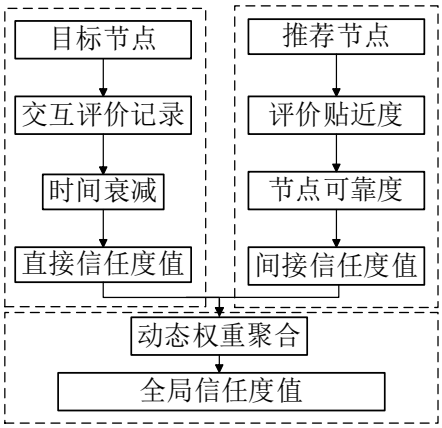

图 4.3　EDTERF 信任架构

基于信誉反馈的边缘设备节点信任评估算法如图4.3所示。首先，终端设备节点发生交互并记录服务交互评价，由节点服务交互记录得出直接信任，历史的评价记录在直接信任的影响随间隔时间的增大而衰减。之后，所有与目标节点发生过交互的节点作为间接信任的推荐节点，使用模糊贴近度理论对节点的评价进行考量，得出推荐节点的评价可靠程度，

确定节点推荐的信任占比重大小，对推荐节点的直接信任加权计算得出间接信任。最后，将直接信任和间接信任采用动态变化的权重进行聚合计算，得出节点的全局信任值。

4.3.1 直接信任度计算

直接信任 $D_{d_i,d_j}(\Delta t)$ 是边缘设备评估节点 d_i 对被评估节点 d_j 的历史通信交互服务满意度的评价。节点服务质量受多种因素的影响，应当根据不同的网络的特征而选择，诸如数据包大小、数据包准确率、网络转发延迟、任务成功率等因素。设备节点每次发生交互后都会生成直接信任，服务请求节点记录对服务的满意度，直接信任的获取不需要其他网络实体的参与。假设已知设备节点 d_i 与 d_j 在一次信任计算周期 Δt 内的 $\mathrm{t_k}$ 次交互服务质量评价 $H_{ij}=(h_1,h_2,\cdots,h_k)$，其中高质量交互成功 u 次，低质量交互失败 v 次，使用 Beta 分布对设备节点 d_i 和 d_j 的信任度进行拟合，可得设备直接信任度期望值 $D_{d_i,d_j}(t)$ 为：

$$D_{d_i,d_j}(t)=E(Beta(u+1,v+1))=\frac{u+1}{u+v+2} \tag{4-1}$$

设备节点的信任度随时间变化，其历史服务评价的影响应当随着时间间隔的增加而减小，临近发生的服务质量评价更能够代表设备节点当前的信任值，在此引入时间衰减[80]因子 φ 来反映信任：

$$\varphi_x=\frac{1}{1+(t-t_x)/\rho} \tag{4-2}$$

其中 t 为当前时间，t_x 是第 x 次交互发生的时间，其中 ρ 为速率调节因子，能够改变时间对直接信任的影响，此处设置 $\rho=1$，当 ρ 越小信任值随时间衰减越大，当 ρ 越大时间对信任度影响越小。在 Beta 函数下计算设备信任值，对 h_{ij} 中的交互成功正面评价取 $h=1$，交互失败的负面评价取 $h=0$，可得出：

$$\begin{cases}\mathrm{u_t}=\sum_{x=1}^{k}\varphi_x h_x\\ \mathrm{v_t}=\sum_{x=1}^{k}\varphi_x(1\text{-}\mathrm{h}_x)\end{cases} \tag{4-3}$$

u_t 和 v_t 分别是加入时间衰减因子后的成功和失败次数。

4.3.2 间接信任度计算

在边缘设备与设备之间发生直接交互时，能够根据直接交互的服务质量评价对目标设备节点进行直接信任评估。在评估设备与目标设备没有直接交互的情况下，缺乏有效的服务评价数据，无法采用直接信任评估对目标设备节点进行评价，需要引入间接信任来对设备进行评级，间接信任够汇总当前网络内所有设备对目标节点的直接信任，由区域内设备反馈给边缘服务器进行收集并处理。边缘设备的间接信任度矩阵表示为：

$$I_{d_i \to d_j} = \begin{bmatrix} D_{d_1,d_1}(\Delta t) & D_{d_1,d_2}(\Delta t) & \cdots & D_{d_1,d_n}(\Delta t) \\ D_{d_2,d_1}(\Delta t) & D_{d_2,d_2}(\Delta t) & \cdots & D_{d_2,d_n}(\Delta t) \\ \vdots & \vdots & \ddots & \vdots \\ D_{d_n,d_1}(\Delta t) & D_{d_n,d_2}(\Delta t) & \cdots & D_{d_n,d_n}(\Delta t) \end{bmatrix} \tag{4-4}$$

$D_{d_i,d_j}(\Delta t)$是直接信任值。如果$i=j$，则定义$D_{d_i,d_j}(\Delta t)=0$。间接信任由下面的公式计算得出：

$$I_{d_i,d_j}(t) = \sum_{i=1}^{n} w_i * D_{d_i,d_j}(\Delta t) \tag{4-5}$$

设备的间接信任来自不同的设备直接信任推荐的聚合，其间接信任推荐的权重记为$W=\{w_1,w_2,w_3,\cdots,w_n\}$，其中$\sum_{i=1}^{n} w_i = 1$，$w_i > 0$。边缘环境中的各节点行为不同，在间接信任的计算中占有不同的权重。w_i的取值大小表示设备的信任反馈是否可靠，对于诚实节点的反馈应当给与更高的权重。

在一段时间内，与同一目标节点发生交互的众多设备对该节点的直接信任应当具有较大的相似性，并趋向于中心值的客观稳定评价。在边缘环境中的恶意设备不诚实反馈，恶意设备对目标节点的信任值将会偏离正常值。在上述的场景下，使用模糊数学中最大和最小模糊贴近度的概念[81]，反应设备对目标节点信任值的可靠性。边缘设备节点i和l对目标节点j的贴近度计算公式如下：

$$\lambda_{i,l} = \frac{\min\left\{D_{d_i,d_j}(\Delta t), D_{d_l,d_j}(\Delta t)\right\}}{\max\left\{D_{d_i,d_j}(\Delta t), D_{d_l,d_j}(\Delta t)\right\}} \tag{4-6}$$

可得对目标节点j的直接信任值模糊贴近度矩阵α：

$$\alpha = \begin{bmatrix} \lambda_{1,1} & \lambda_{1,2} & \cdots & \lambda_{1,n} \\ \lambda_{2,1} & \lambda_{2,2} & \cdots & \lambda_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n,1} & \lambda_{n,2} & \cdots & \lambda_{n,n} \end{bmatrix} \tag{4-7}$$

对贴近度矩阵α中的第i行元素$\{\lambda_{i,1},\lambda_{i,2},\cdots\lambda_{i,n}\}$求和$\sum_{l=1}^{n}\lambda_{i,l}$，表示设备$i$直接信任评价的总贴近度，当$\sum_{l=1}^{n}\lambda_{i,l}$越大节点$i$对目标设备的信任评价越贴近总评价的中心值，其反馈诚实度越高；当$\sum_{l=1}^{n}\lambda_{i,l}$的值越小，节点$i$对目标设备的信任评价偏离程度越大，其反馈诚实度变低。根据上述内容，节点设备i间接信任推荐权重w_i：

$$w_i = \sum_{l=1}^{n}\lambda_{i,l} \Big/ \sum_{i=1}^{n}\sum_{l=1}^{n}\lambda_{i,l} \tag{4-8}$$

使用模糊贴近度来衡量设备信任反馈的诚实度，当恶意设备出现偏离正常值的信任评价，对公有节点的评价贴近度将会降低，恶意设备w_i下降，以此减轻边缘环境中恶意评价对设备信任度的影响。

4.3.3 全局信任度聚合

设备的全局信任度是融合直接信任与间接信任对设备的客观整体评价。设备 d_i 对目标设备 d_j 的全局信任度：

$$G_{d_i,d_j}(\Delta t) = w_D * D_{d_i,d_j}(\Delta t) + (1-w_D) * I_{d_i,d_j}(\Delta t) \tag{4-9}$$

w_D，$1-w_D$ 分别代表了直接信任、间接信任在全局信任中的权重占比。边缘计算环境下，全局信任计算的权重分配应当随着设备的行为发生变化。传统的固定值分配存在局限性，不能应对边缘设备交互中的突发情况和恶意行为。结合边缘设备的近期行为，采用动态的权重分配方法增强全局信任的可靠性：

$$w_D = \frac{1}{1+\sqrt{v_t}} \tag{4-10}$$

直接信任的权重 w_D 随着交互失败的次数增加逐渐减少，严格惩罚发生的交互失败，快速降低恶意设备信任值，能够有效防止恶意设备积累较高信任度后突然发起的攻击。

4.3.4 复杂度分析

本章所提的信任评估算法是轻量级算法，终端设备之间无需信息共享，由边缘服务器收集设备的反馈并聚合计算信任值，能够部署在计算资源有限的边缘终端设备上。

在空间复杂度上，假设边缘网络环境中有 m 个服务器，每个服务器域内设备总数为 n 给定的时间间隔 Δt 内，全局信任计算的最大数量为 γ，信任评估算法的最大通信开销为：

$$S = m*(2n+n)*\gamma = 3mn\gamma \tag{4-11}$$

空间复杂度计算：设备 d_i 将与节点 d_j 的直接信任反馈给服务器，通信开销为 $n\gamma$，边缘服务器接受来自设备 d_i 发起的请求，并反馈目标设备的全局信任值，通信开销 $2n\gamma$。边缘网络中共有 m 个服务器，全局信任计算所需的最大通信开销为 $3mn\gamma$。

基于服务反馈的边缘设备信任评估算法，全局信任计算的时间复杂度为：

$$T(\Delta t) = O(n^2) \tag{4-12}$$

时间复杂度计算：全局信任的计算由直接信任和间接信任两部分组成，总的时间复杂度由算法执行次数决定，n 个设备的信任计算周期最大为 n^2，因此全局信任的时间复杂度为 $O(n^2)$。

本文所提出的信任评估算法的通信开销跟随边缘服务器数量、设备总数的增加线性增长，相较于传统的使用广播机制的信任聚合，无需考虑设备间的反馈，算法轻量级传输开销少，能够降低在边缘网络侧的资源消耗。

4.4 仿真结果与分析

4.4.1 仿真设置

边缘设备节点间的通信交互使用NetLogo事件模拟器进行实验，该模拟器在AI社区中以Java实现，提供多代理的可编程建模环境，导出实验结 果数据。数据仿真实验使用Matlab

进行模拟，使用的计算机配置为：CPU 3.4GHz，内存大小16GB，硬盘1T。实验场　景设置两种身份：边缘设备和边缘计算服务器。边缘终端设备分为两种类型节点：善意设备和恶意设备节点，善意节点提供真实的服务对参与交互的其他设备进行诚实的评价，恶意节点提供虚假的反馈或恶意服务，两种节点的比例由实验要求确定。模拟实验的具体参数如表4.1所示。

表 4.1　实验参数设置

符号	描述	值
n	终端设备数量	1000
m	服务器数量	4
Δt	信任计算周期	20s
G	信任度取值	0-1
t	计算总步长	200
MD	恶意节点比例	10%，40%

将信任阈值设置为0.5，低于0.5即认为是不可信恶意节点。节点初始信任值均大于0.5，信任值随着正常交互次数的增多而提升。实验分别设置恶意节点比例为10%，40%的两种场景。

4.4.2　结果分析

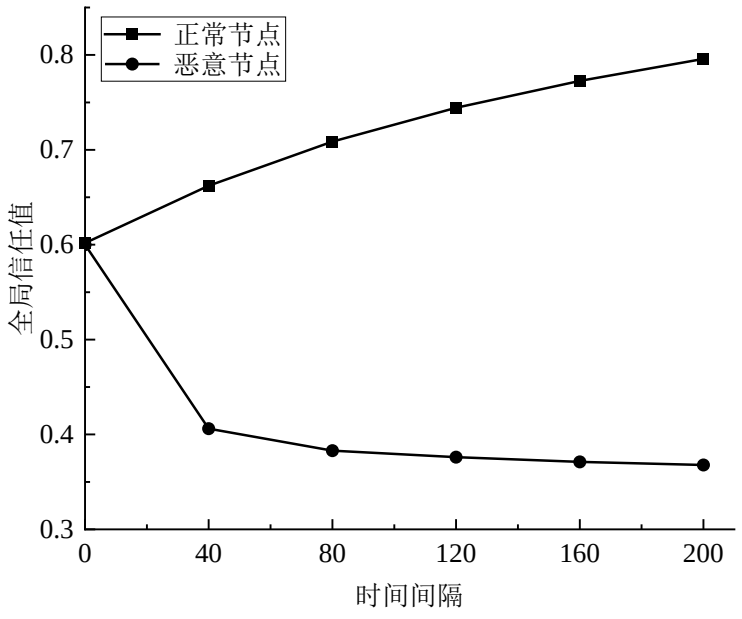

图 4.4　全局信任值变化

图 4.4 给出了恶意节点占比 10%场景下，正常节点和恶意节点平均全局信任值随时间的动态变化，信任评估开始时两类节点的全局信任值均为 0.6。正常节点之间发起成功的通信交互，节点直接信任值上升，成功交互记录提交给边缘服务器，计算间接信任值。恶意节点的交互失败，节点直接信任值下降，节点信任评价的模糊贴近度值降低，其节点的

信任推荐在间接信任中的权重占比将会下降，减轻恶意节点反馈的影响。失败的交互同样影响全局信任的聚合，直接信任占比权重降低，恶意节点全局信任值快速下降；若正常节点收到恶意评价的攻击，全局信任聚合中直接信任占比将会下降，节点的全局信任将更多的依赖间接信任评估值，也能够减轻恶意虚假反馈对正常节点全局信任评估的影响。

上述的仿真结果反映出本章提出的信任评估算法对恶意节点攻击行为的信任变化，DTERF 算法能够识别出恶意攻击节点，算法通过对节点评价的模糊贴近度分析，降低间接信任聚合中恶意节点评价的权重占比。

为验证算法DTERF可靠性，实验对比选择传统逻辑算法TSL（Traditional Subject Logic）和基于贝叶斯模型的信任评估 RFSN[82]（Reputation-based Framework for high integrity Sensor Network）机制。RFSN 算法使用贝叶斯公式表示信誉的更新和变化，但不共享节点信息，模型计算量大。边缘服务器会根据通信服务提供节点的信任评估值，优化资源的分配[83]，诚实的正常节点拥有更多的资源分配，高可靠的信任评估，能够提升设备节点在不同场景下的任务交互成功率。根据请求节点能否成功获得目标节点的通信服务作为判断服务交互成功与否的标准。计算节点在实验场景下随时间变化的任务成功率以此反应信任计算的可靠性。

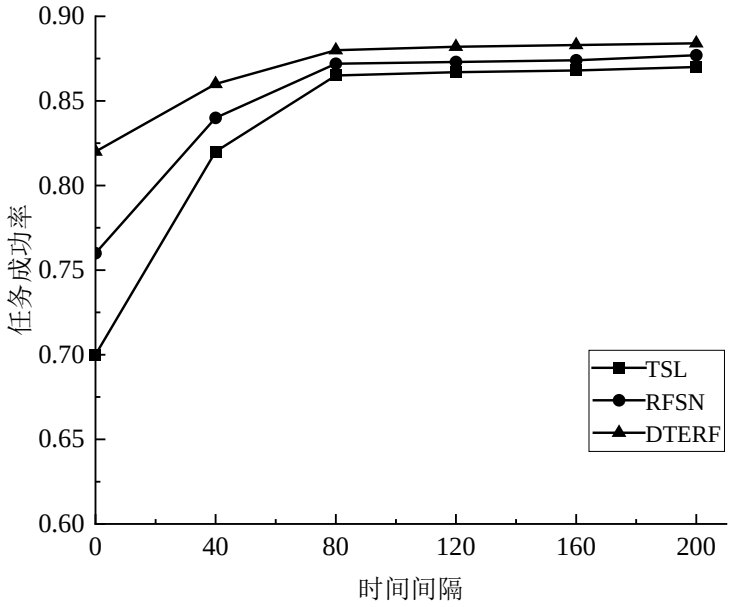

图 4.5　MD=0.1 任务成功率

图4.5和图4.6分别为恶意节点占比10%、40%场景下随时间变化的任务交互成功率。图4.5结果表明，在恶意节点比例较低的情况下，三种信任评估算法在初始时的任务成功率存在差异，本文算法DTERF任务成功率82%，优于TSL、RFSN。随着时间的增加，三种信任模型都能排除恶意节点，使任务成功率达到较高水平，信任的评估具有可靠性。图4.6为在恶意节点比例40%的环境下，任务交互成功率随时间的变化。结果表明，在恶意节点较多的场景下，会影响边缘设备间的通信任务交互，降低信任计算的效率。DTERF的初始任务

成功率为58%、RFSN初始成功率为46%、TSL为35%，随着时间的增加，三种算法的任务成功率缓慢增长，DTERF算法采用动态的全局信任聚合严格惩罚任务失败，加速恶意设备节点全局信任值的收敛，其信任评估可靠性优于其他两种算法，能够更加有效的降低恶意节点的攻击行为对节点服务交互的不良影响。

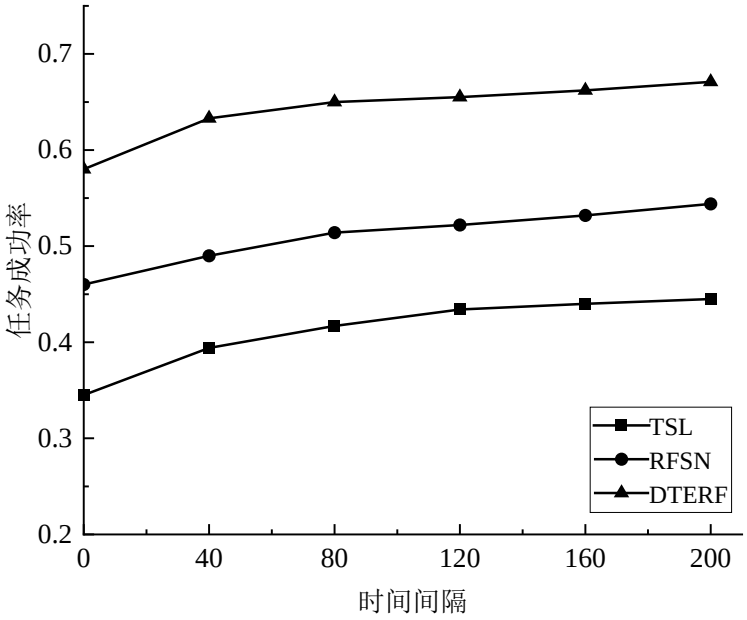

图 4.6　MD=0.4 任务成功率

4.5　本章小结

本章提出了一种在边缘环境中基于服务反馈的设备信任评估算法，该算法使用模糊贴近度理论量化设备信任反馈的可靠度，确定间接信任的推荐权重，能够有效降低设备恶意反馈的影响，使间接信任评估更加准确。在全局信任的聚合过程中，采用动态的权重克服传统信任计算主观加权机制的局限性，同时严格惩罚失败的交互，对恶意攻击进行快速反应。本文提出的信任评估算法评估准确度高，能够抵抗恶意的虚假反馈攻击，提高设备服务交互的任务成功率，在时间复杂度和空间复杂度方面优于传统算法。

第五章　总结与展望

本章对全文的主要研究内容及所做工作进行总结，并针对研究过程中存在不足给出下一步的研究方向。

5.1　论文工作总结

随着5G时代万物互联的发展，网络中产生了各式各样的连接，智能终端、物联网设备的数量和相应服务产生的数据呈爆炸式增长，传统集中式的云计算无法满足用户侧的低时延极致体验。移动边缘计算将云计算的计算和存储能力拓展到靠近用户的网络边缘，成为5G业务场景实现的一大关键技术，为服务商提供先进开放的应用计算平台。移动边缘计算存在广泛的应用场景，如车联网、工业物联网、智慧城市、虚拟现实技术等，带来全新服务的同时，也面临着新的安全挑战。边缘设备易被攻击者入侵控制窃取用户敏感信息；非法用户接入边缘网络，导致用户隐私泄露；合法接入的用户存在恶意行为向边缘计算内部发起攻击，降低网络整体效率；攻击者劫持控制大量安全能力较低终端向边缘网络发起资源耗尽和拒绝服务攻击；攻击者对网络发起窃听或侧信道攻击。移动边缘计算环境中存在海量的多种类型终端设备，计算能力和架构存在较大差异，难以适用复杂的认证协议，边缘计算用户接入侧的安全防护至关重要。身份认证是终端连接移动边缘计算服务的入口，对终端设备的合法接入起着决定性作用，随着边缘服务在国防、政府等高安全等级行业广阔的应用，现有的接入认证方案，难以满足边缘网络设备的统一接入。

基于此本文对移动边缘计算面临的安全威胁及安全防护机制进行了研究，从实体接入边缘计算网络服务前和接入服务后两个方面展开研究，分别设计了可信身份认证与边缘防护网关、边缘防护网关的流量检测防御策略和移动边缘计算终端设备的信任评估方案，实现边缘计算用户接入身份安全可信、用户接入后传输数据恶意流量检测、用户服务交互过程中的恶意行为防范三个层面的安全防护，增强边缘计算服务过程中整体的安全性。概括起来，本文的主要工作总结如下：

（1）针对现有MEC应用层和核心网独立式安全接入认证方案，难以满足高安全等级行业应用需求，提出一种于基于可信身份认证的边缘计算服务防护方法，该方法面向边缘计算高安全等级专网场景的可信身份认证需求，给出5G核心网的移动边缘计算高安全等级专网身份认证解决方案。通过基于5G核心网的用户身份信息嵌入和接口标识替换，实现了接入核心网用户身份真实可信。然后，在核心网侧用户身份真实可信的基础上，增设了边缘防护网关和边缘防护网关控制器，通过DN和边缘防护网关的双重认证及基于通行令牌的身份认证机制实现对于访问DN用户身份真实可信的认证和准入。最后，以5G车联网场景为例，在保护边缘计算节点安全和阻止用户隐私的泄露的前提下设计了一种车辆运动轨迹预测算法，实现了车辆在高速运动过程中边缘服务节点的高效切换，降低了通信开销和切

换时延，并对所提出的基于可信身份认证的边缘计算服务防护方案进行了系统的验证和测试。

（2）针对边缘计算传输数据安全，网关控制器对业务流量数据包进行抽样的安全检测，使用遗传算法对请求数据包检测的安全和性能进行优化。边缘计算安全数据网关，采用零信任的思想，设计 SDP 控制器，对于网络内部的数据使用进行数据包检测与授权。在资源受限的网络边缘，对每个设备发起的服务请求中的每个业务流数据包都进行验证，会产生大量的资源开销。设计合理的请求验证策略能够有效的提升系统的安全性和资源利用效率，以确保服务器不会过载或通信延迟不会显著增加。对此，提出基于遗传算法的边缘网关恶意流量检测防御策略，对用户数据传输进行抽样的数据包授权检测方案，利用 SDP 控制器进行流量抽样检测，并建立攻击者和防御者的攻击与防御收益模型，设计优化目标，建模求解获得最优的流量采样概率

（3）针对现有边缘计算环境中终端设备信任评估的准确度不高，无法有效处理恶意终端对边缘网络服务带来的安全威胁问题，提出一种基于信誉反馈的边缘设备信任评估方法，以节点服务交互信息评估其信任度，筛选恶意节点，降低边缘网络受到攻击风险；通过设备反馈评价的模糊贴近度分析出节点的可靠程度，降低恶意节点在间接信任中的权重占比，减轻节点恶意行为对诚实节点信任评估的影响；对直接信任与间接信任采用一种动态加权的方法得出设备全局信任，能够适应边缘环境，使全局信任度值更加客观，对所提出的信任评估方法进行了模拟实验，证明信任评估方案的准确性，有效提高边缘服务交互成功率。

5.2 后续工作展望

本文对移动边缘计算场景下的接入安全防护技术和移动边缘计算终端设备的信任管理机制进行了研究，对边缘计算环境中存在的安全威胁，从接入边缘计算网络服务的前后两方面开展安全措施，取得了一定进展，但由于时间有限，相关研究方向仍存在一些问题需要继续解决，主要有以下几点：

（1）移动边缘计算的接入认证防护，在考虑用户接入身份的真实可信同时，还需要考虑用户在边缘网络节点间的移动和切换。因此，考虑使用零信任建立统一的分布式的跨域认证方案是移动边缘计算未来用户接入认证的一种可能解决方案。参考SDP架构的边缘服务安全网关同样面临挑战，由于SDP架构与网络中部署的传统安全措施不同，现有解决方案可能会带来网络和基础设施服务质量的下降，需要和网络场景深度适配改进，并融合网络实体已有的安全措施。

（2）边缘安全网关的恶意流量检测考虑了用户安全和服务质量的平衡，选择在边缘网关部署最合适的防御策略。边缘安全网关对于数据包流量的身份安全检测机制，还能够进一步提升，总结不同业务场景下的恶意流量特征，适配到边缘网关进行应用，能够达到更好的恶意数据传输防御效果。

（3）信任评估应涉及对连接到网络的每个实体的持续监视和分析。信任模型可能会产生延迟，因为它涉及远程监视应用程序、收集数据并将其发送到核心信任管理应用程序。下一步工作将研究信任管理与激励机制的建立，并考虑将边缘节点在特定的业务场景下的对应能力添加到节点信任度的评估之中，提高边缘设备间的协作能力。

参考文献

[1] 李子姝, 谢人超, 孙礼, 等. 移动边缘计算综述[J]. 电信科学, 2018, 34(01): 87-101.

[2] 刘明月, 涂崎, 汪洋, 等. 移动云计算卸载技术研究现状及其在电网中的应用[J]. 电力信息与通信技术, 2021, 19(01): 49-56.

[3] 王哲. 边缘计算发展现状与趋势展望[J]. 自动化博览, 2021, 38(02): 22-29.

[4] HU Y C, PATEL M, SABELLA D, et al. Mobile edge computing—a key technology towards 5G[J]. ETSI White Paper, 2015, 11(11): 1-16.

[5] 赵明.边缘计算技术及应用综述[J].计算机科学,2020,47(S1):268-272+282.

[6] Islam A, Debnath A, Ghose M, et al. A survey on task offloading in multi-access edge computing[J]. Journal of Systems Architecture, 2021, 118: 102225.

[7] Filali A, Abouaomar A, Cherkaoui S, et al. Multi-access edge computing: A survey[J]. IEEE Access, 2020, 8: 197017-197046.

[8] Pang S, Wang N, Wang M, et al. A smart network resource management system for high mobility edge computing in 5G internet of vehicles[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(4): 3179-3191.

[9] Malik P K, Singh R, Gehlot A. Industrial Internet of Things and its Applications in Industry 4.0: State of The Art[J]. Computer Communications, 2021, 166: 125-139.

[10] Tufail A, Namoun A, Alrehaili A, et al. A Survey on 5G Enabled Multi-Access Edge Computing for Smart Cities: Issues and Future Prospects, 2021, 21(6): 107-118.

[11] Spinelli F, Mancuso V. Toward Enabled Industrial Verticals in 5G: A Survey on MEC-Based Approaches to Provisioning and Flexibility[J]. IEEE Communications Surveys&Tutorials, 2021, 23(1): 596-630.

[12] G. Zhao, F. Zhang, L. Yu, H. Zhang, Q. Qiu and S. Xu. Collaborative 5G Multiaccess Computing Security: Threats, Protection Requirements and Scenarios[C]. 2021 ITU Kaleidoscope: Connecting Physical and Virtual Worlds, 2021: 1-8.

[13] Ranaweera P, Jurcut A D, Liyanage M. Realizing multi-access edge computing feasibility: Security perspective[C]. 2019 IEEE Conference on Standards for Communications and Networking (CSCN), 2019, 1-7.

[14] B. Ali, M. A. Gregory and S. Li, Multi-Access Edge Computing Architecture, Data Security and Privacy: A Review[J]. IEEE Access, 2021, 9: 18706-18721.

[15] ETSI GS MEC 003. Multi-access edge computing (MEC); framework and reference architecture[S]. 2020.

[16] 王秋宁, 谢人超, 黄韬. 移动边缘计算的移动性管理研究[J]. 中兴通讯技术, 2018, 24(01): 37-41.

[17] Ranaweera P, Jurcut A, Liyanage M. MEC-enabled 5G use cases: a survey on security vulnerabilities and countermeasures[J]. ACM Computing Surveys(CSUR), 2021, 54(9): 1-37.

[18] 张佳乐，赵彦超，陈兵，胡峰，朱琨. 边缘计算数据安全与隐私保护研究综述[J]. 通信学报，2018, 39(03): 1-21.

[19] Li H, Yang C, Wang L, et al. A cooperative defense framework against application-level DDoS attacks on mobile edge computing services[J]. IEEE Transactions on Mobile Computing, 2021, 22(1): 1-18.

[20] 边缘计算产业联盟，工业互联网产业联盟. 边缘计算安全白皮书[R]. 2019.

[21] 李晓伟，陈本辉，杨邓奇，伍高飞. 边缘计算环境下安全协议综述[J]. 计算机研究与发展，2022, 59(04): 765-780.

[22] Khalid T, Abbasi M A K, Zuraiz M, et al. A survey on privacy and access control schemes in fog computing[J]. International Journal of Communication Systems, 2021, 34(2): 4181-4190.

[23] 张伟成，卫红权，刘树新，等. 面向 5G MEC 基于行为的用户异常检测方案[J]. 计算机工程，2022, 48(5): 27-34.

[24] Buck C, Olenberger C, Schweizer A, et al. Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust[J]. Computers&Security, 2021, 110: 102436.

[25] Kindervag J. Build security into your network’s dna: The zero trust network architecture[J]. Forrester Research Inc, 2010: 1-27.

[26] Escobedo V M, Zyzniewski F, Saltonstall M. BeyondCorp: the user experience[J]. 2017, 42(3): 1-6.

[27] 于欣越，孙刚，张亚伟. 基于零信任的软件定义边界网络隐身技术研究[J]. 通信技术，2021，54(5): 1229-1234.

[28] ROSE S, BORCHERT O, MITCHELL S, et al. Zero trust architecture[R]. National Institute of Standards and Tech nology, 2020.

[29] 张宇，张妍. 零信任研究综述[J]. 信息安全研究, 2020, 6(7): 608-614.

[30] 诸葛程晨，王群，刘家银，梁广俊. 零信任网络综述[J]. 计算机工程与应用, 2022, 58(22): 12-29.

[31] MICHAEL RASH. Single Packet Authorization: The fwknop Approach[EB/OL]. [2020-9-10]. http://www.cipherdyne.org/blog/2012/09/single-packet-authorization-the-fwknop-approach.

[32] Klein D. Micro-segmentation: securing complex cloud environments[J]. Network Security, 2019, 2019(3): 6-10.

[33] 何国锋. 零信任架构在 5G 云网中应用防护的研究[J]. 电信科学, 2020, 36(12): 127-136.

[34] Chen B, Qiao S, Zhao J, et al. A Security Awareness and Protection System for 5G Smart Healthcare Based on Zero-Trust Architecture[J]. IEEE Internet of Things Journal, 2020, 8(13): 10248-10263.

[35] Zaheer Z, Chang H, Mukherjee S, et al. eZTrust: Network-Independent Zero-Trust Perimeterization for Microservices[C]. the 2019 ACM Symposium, 2019: 49-61.

[36] Meng L, Huang D, An J, et al. A continuous authentication protocol without trust authority for zero trust architecture[J]. China Communications, 2022, 19(8): 198-213.

[37] Dhar S, Bose I. Securing IoT Devices Using Zero Trust and Blockchain[J]. Journal of Organizational Computing and Electronic Commerce, 2021, 31(1): 18-34.

[38] 沈传年. 边缘计算安全与隐私保护研究进展[J]. 网络安全与数据治理, 2022, 41(2): 41-48.

[39] Li Y, Cheng Q, Liu X, et al. A secure anonymous identity-based scheme in new authentication architecture for mobile edge computing[J]. IEEE Systems Journal, 2020, 15(1): 935-946.

[40] Mahmood K, Ayub M F, Hassan S Z, et al. A seamless anonymous authentication protocol for mobile edge computing infrastructure[J]. Computer Communications, 2022, 186: 12-21.

[41] Yang Y, Bai F, Yu Z, et al. An Anonymous and Supervisory Cross-Chain Privacy Protection Protocol for Zero-Trust IoT Application[J]. ACM Transactions on Sensor Networks, 2023.

[42] Ahmed I, Nahar T, Urmi S S, et al. Protection of Sensitive Data in Zero Trust Model[C]. Proceedings of the International Conference on Computing Advancements, 2020: 1-5.

[43] Decusatis C, Pinelli M. Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication[C]. IEEE International Conference on Smart Cloud, 2016: 5-10.

[44] Singh J, Refaey A, Koilpillai J. Adoption of the Software-Defined Perimeter (SDP) Architecture for Infrastructure as a Service[J]. Canadian Journal of Electrical and Computer Engineering, 2021, 43(4): 357-363.

[45] Lucion E, Nunes R C. Software Defined Perimeter: Improvements in the Security of Single Packet Authorization and user Authentication[C]. 2018 XLIV Latin American Computer Conference (CLEI), 2018, 708-717.

[46] Tang C, Fu X, Tang P. Policy-Based Network Access a nd Behavior Control Management[C]. 2020 IEEE 20th International Conference on Communication Technology (ICCT), 2020: 1102-1106.

[47] 郭仲勇, 刘扬, 张宏元, 刘帅洲. 基于零信任架构的IoT设备身份认证机制研究[J]. 信息技术与网络安全, 2020, 523(11): 27-34.

[48] Yao Qigui, Wang Qi, Zhang Xiaojian, et al. Dynamic Access Control and Authorization System based on Zero-trust architecture[C]. 2020 International Conference on Control, Robotics and Intelligent System (CCRIS 2020), 2020: 123-127.

[49] 陈璐, 汤红波, 游伟, 柏溢. 移动边缘计算安全防御研究[J]. 网络与信息安全报, 2021, 7(1): 130-142.

[50] Nikravan M, Kashani M H. A review on trust management in fog/edge computing: Techniques, trends, and challenges[J]. Journal of Network and Computer Applications, 2022: 103402.

[51] Zhang P Y, Kong Y, Zhou M C. A domain partition-based trust model for unreliable clouds[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(9): 2167-2178.

[52] 江金芳, 韩光洁. 无线传感器网络中信任管理机制研究综述[J]. 信息网络安全, 2020, 20(04): 12-20

[53] 闫峥, 吴宸梓, 冯伟等. 可信普适社交网络研究综述和展望[J]. 网络与信息安全学报, 2016, 2(02): 30-40.

[54] 马小信，曾国荪．一种基于模糊策略的自动信任协商方案[J]．计算机科学，2015，42(12): 220-223+239.

[55] 沈宏伟，邵堃，张阳洋等．基于朴素贝叶斯的信任决策模型[J]．小型微型计算机系统，2018，39(02): 275-279.

[56] 房卫东，石志东，单联海,等．一种基于 BETA 分布抗 On-off 攻击的信任机制[J]．系统仿真学报，2015(11): 2722-2728.

[57] 田俊峰，吴丽娟．基于多项式主观逻辑的扩展信任传播模型[J]．通信学报, 2013, 34(05): 12-19.

[58] Valero J, PMS Sánchez, MG Pérez, et al. Toward pre-standardization of reputation-based trust models beyond 5G[J]. Computer Standards & Interfaces, 2022, 81: 103596- 103603.

[59] 邓晓衡，关培源，万志文，刘恩陆，罗杰，赵智慧，刘亚军，张洪刚．基于综合信任的边缘计算资源协同研究[J]．计算机研究与发展, 2018, 55(03): 449-477.

[60] Deng, X., Liu, J., Wang, L. et al. A trust evaluation system based on reputation data in Mobile edge computing network[J]. Peer-to-Peer Networking and Applications, 2020, 13: 1744–1755.

[61] Tian Wang, Pan Wang, Shaobin Cai, et al. Mobile edge-enabled trust evaluation for the Internet of Things[J]. Information Fusion, 2021, 75: 90-100.

[62] Wu D, Shen G, Huang Z, et al. A trust-aware task offloading framework in mobile edge computing[J]. IEEE Access, 2019, 7: 150105-150119.

[63] Qiao F, Wu J, Li J, et al. Trustworthy Edge Storage Orchestration in Intelligent Transportation Systems Using Reinforcement Learning[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, (99): 1-14.

[64] J. Liang, M. Zhang and V. C. M. Leung. A Reliable Trust Computing Mechanism Based on Multisource Feedback and Fog Computing in Social Sensor Cloud[J]. IEEE Internet of Things Journal, 2020,7(6): 5481-5490.

[65] Latif, R., Ahmed, M.U., Tahir, S. et al. A novel trust management model for edge computing[J]. Complex&Intelligent Systems, 2022, 8(5): 3747–3763.

[66] 胡鑫鑫，刘彩霞，刘树新，等．移动通信网鉴权认证综述[J]．网络与信息安全学报，2018，4(12): 1-15.

[67] Chen C L, Chiang M L, Hsieh H C, et al. A lightweight mutual authentication with wearable device in location-based mobile edge computing[J]. Wireless Personal Communications, 2020, 113(1): 575-598.

[68] Dhillon P K, Kalra S. A lightweight biometrics based remote user authentication scheme for IoT services[J]. Journal of Information Security and Applications, 2017, 34: 255-270.

[69] 吴建平，李丹，毕军，等. ADN:地址驱动的网络体系结构[J]．计算机学报, 2016, 39(6): 1081-1091.

[70] 周端奇，毕军，姚广．基于 IPv6 源地址验证的一种可信身份系统[J]．通信学报, 2014, 35(z1): 20-26.

[71] 李聪，孙吉斌，解冲锋．基于 IPv6 的 5G 专网终端身份认证技术与应用[J]．移动通信，2022，46(8): 47-52.

[72] Singh J, Bello Y, Hussein A R, et al. Hierarchical security paradigm for iot multiaccess edge computing[J]. IEEE Internet of Things Journal, 2020, 7(7): 5794-5805.

[73] T G Rodrigues, K Suto, H Nishiysima, et al. Hubrid method for minimizing service delay in edge cloud computing through VMmigration and transmission power control[J]. IEEE Transactions on Computers, 2016, 66(5): 810-819.

[74] 刘建华. 基于零信任架构的 5G 核心网安全改进研究[J]. 邮电设计技术, 2020, 9: 75-78.

[75] 单英. 基于零信任的 5G 安全切片架构设计[J]. 通信管理与技术, 2022, 1: 47-49+59.

[76] Dai Z, Li N, Li Y, et al. Research on power mobile Internet security situation awareness model based on zero trust[C]. Artificial Intelligence and Security: 8th International Conference, ICAIS 2022: 507-519.

[77] 范伟, 彭诚, 朱大立, 王雨晴. 移动边缘计算网络下基于静态贝叶斯博弈的入侵响应策略研究[J]. 通信学报, 2023, 44(02): 70-81.

[78] SDP Specification v1.0[S]. https: //cloudsecurityalliance.org/download/sdp-specification-v1-0/.

[79] Qian Yu, Songze Li, Netanel Raviv, et al. Lagrange Coded Computing: Optimal Design for Resiliency, Security, and Privacy[C]. Proceedings of the Twenty-Second International Conference on Artificial Intelligence and Statistics, 2019: 1215-1225.

[80] 游静, 上官经伦, 徐守坤, 等. 考虑信任可靠度的分布式动态信任管理模型[J]. 软件学报, 2017, 28(9): 2354-2369.

[81] Shao N, Zhou Z, Sun Z. A lightweight and dependable trust model for clustered wireless sensor networks[C]. Cloud Computing and Security: First International Conference, ICCCS 2015: 157-168.

[82] Y. Sun, Z. Han and K. J. R. Liu. Defense of trust management vulnerabilities in distributed networks[J]. IEEE Co mmunications Magazine, 2008, 46(2): 112-119.

[83] Li X, Zhou F, Du J. LDTS: A lightweight and dependable trust system for clustered wireless sensor networks[J]. IEEE transactions on information forensics and security, 2013, 8(6): 924-935.