一种面向 5G 网络的动态安全边界防护机制

张 莹[1], 张 勖[2,3], 王东滨[2,5], 蔡昌俊[6], 陆月明[2,4]

[1]北京邮电大学网络教育学院 北京 中国 100876
[2]北京邮电大学网络空间安全学院 北京 中国 100876
[3]移动互联网安全国家工程研究中心 北京 中国 100876
[4]可信分布式计算与服务教育部重点实验室 北京 中国 100876
[5]链网融合技术教育部工程研究中心 北京 中国 100876
[6]广州地铁集团有限公司 广州 中国 510030

摘要 第五代移动通信网络 5G 以融合网络为目标, 其标准不仅覆盖公共通信网络, 也同时应用于下一代垂直行业网络。传统垂直行业网络是以工业自动化和控制系统为主的运营/操作技术(Operational Technology, OT)网络, OT 网络采取安全域划分方式, 将大规模复杂系统分为不同安全子区域, 在边界处部署专用安全设备/系统进行安全防护。目前实践中多采用网闸等设备以硬隔离方式阻断恶意流量, 带来的问题是严重影响正常业务的通过。依托 5G 的网络功能虚拟化(Network Function Virtualization, NFV)技术和软件定义网络(Software Defined Network, SDN), 本文提出了一种面向 5G 网络的动态安全边界防护机制。该机制构建虚拟化的边界网络安全功能资源池和边界安全服务规则库, 对到达边界的业务流量进行防护等级分析, 并根据规则库中的规则动态生成边界安全服务功能链。机制还具备对边界服务功能链进行优化部署的能力, 通过建模和启发式算法实现满足业务防护等级需求和最小化处理时延的多目标优化部署策略。基于本机制, 我们设计并提出轨交行业 5G 专网动态安全边界防护机制实例, 旨在为工程实践服务。最后, 我们搭建了基于 Mininet+Ryu 仿真平台, 模拟轨交行业 5G 示范网络中的安全域组成和边界安全能力, 并对机制进行实验验证, 结果表明, 该机制能够有效地动态生成边界服务功能链并且达到控制不同防护等级业务流量通过的目标。

关键词 5G; 动态安全边界防护机制; 软件定义网络; 网络功能虚拟化; 服务功能链; 时延
中图法分类号 TP309 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2025.09.03

A Dynamic Security Perimeter Protection Mechanism for 5G Network

ZHANG Ying[1], ZHANG Xu[2,3], WANG Dongbin[2,5], CAI Changjun[6], LU Yueming[2,4]

[1] School of Network Education, Beijing University of Posts and Telecommunications, Beijing 100876, China
[2] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3] National Engineering Research Center for Mobile Internet Security, Beijing 100876, China
[4] Key Laboratory of Trustworthy Distributed Computing and Service (BUPT), Ministry of Education, Beijing 100876, China,
[5] Engineering Research Center of Blockchain and Network Convergence Technology, Ministry of Education, Beijing 100876, China
[6] Guangzhou Metro, Guangzhou 510030, China

Abstract The fifth-generation mobile communication network 5G aims to integrate networks. Its standards not only cover public communication networks, but also are applied to next-generation vertical industry networks. Traditional vertical industry networks are Operational Technology (OT) networks that focus on industrial automation and control systems. OT networks adopt a security domain division method to divide large-scale complex systems into different security sub-domains and deploy dedicated security equipment/systems at the boundaries for security protection. In current practice, gatekeeper and other equipment are often used to block malicious traffic in a hard isolation manner, which causes problems that seriously affect the pass of normal traffics. Relying on 5G's network function virtualization (NFV) technology and software defined network (SDN), this paper proposes a dynamic security perimeter protection mechanism for 5G network. This mechanism builds a virtualized border network security function resource pool and a border security service rule base, analyzes the protection level of traffic arriving at the border, and generates dynamically a border security service function chain based on the rules. The mechanism also has the function of optimizing the deployment of perimeter service function chains, and uses modeling and heuristic algorithms to achieve multi-objective optimal deployment strategies that

通讯作者: 张勖, 博士, 副教授, Email: selina_zhangx@bupt.edu.cn。
本课题得到国家重点研发计划项目 (No. 2020YFB1808100); 中国高校产学研创新基金-未来网络创新研究与应用项目(No. 2021FNA02004)资助。
收稿日期: 2023-10-12; 修改日期: 2024-02-28; 定稿日期: 2025-08-14

meet services protection level requirements and minimize processing delays. Based on this mechanism, we design an example case of a dynamic security perimeter protection mechanism for 5G private networks in the subway industry, aiming to serve engineering practice. Finally, we built a simulation platform based on Mininet+Ryu to simulate the security domain composition and boundary security capabilities of the 5G demonstration network in the subway industry, and conducted experimental verification of the mechanism. The results show that the mechanism can generate effectively and dynamically perimeter service function chains and achieve the goal of controlling the passage of different protection level's traffic.

Key words 5G; dynamic security perimeter protection mechanism; software defined networking; network function virtualization; service function chain; latency

1 引言

以工业自动化和控制系统(Industrial Automation and Control Systems, IACS)为主的垂直行业运营/操作技术(Operational Technology, OT)网络, 具有如下特性[1]: (1) 满足行业特定处理和运营需求的专用通信基础设施; (2) 不同行业的底层技术组件具有相似性和标准化, 但网络结构和运营模式差异大; (3) 各个行业依据不同的安全目标和要求自行定义所面临的安全威胁。为解决 IACS 安全问题, IEC 62443 系列标准给出了功能和处理流程框架, 国际组织互联产业与自动化 5G 联盟(5G Alliance for Connected Industries and Automation, 5G-ACIA)提出了 5G 应用于工业网络的安全白皮书。其中, 安全域定义为: 一组共享共同安全要求的物理、信息和应用程序的逻辑分组资产。安全域具有明确定义的边界, 在域内部和外部资产之间创建出分离边界, 不同安全区域中的资产通常彼此隔离。

OT 网络的通用安全需求与公共陆地移动通信网络(Public Landing Mobile Network, PLMN)和传统 IT 网络有明显不同。OT 网络传统上采用物理隔离方式, 边界保护和访问控制被广泛用于保护流程、操作数据、用户和设备的机密性。外部访问受到严格控制, 操作数据流到外面也受到限制。网络安全边界的主要作用是把一个大规模复杂系统的安全问题细分为不同区域/等级的安全问题, 以实现大规模复杂网络系统的安全等级保护。当前, 典型场景下的工业 OT 网络中分期分批部署了各种提供边界安全服务的设备或系统, 如防火墙、网闸、入侵检测系统、入侵防御系统、负载均衡网关、防病毒软件等。

但是, 垂直行业业务的复杂性导致其内部业务系统在互联互通过程中, 兼顾业务连续性、边界隔离和安全服务配置部署成为系统建设难点。以轨道交通行业实践为例, 相较于传统信号系统, 现今的基于无线通信的列车控制技术(Communication-Based Train Control, CBTC)能更准确地追踪列车位置。依据美国电气电子工程师学会(IEEE)1474.1 号标准的定义, CBTC 系统是连续、不须依赖轨道电路、高分辨率之列车位置侦测的列车自动控制系统, 可利用车载及道旁之处理器传输行车监控信息, 让列车与信号间进行连续、大容量、双向的数据通信。目前地铁信号系统存在的网络安全问题是: (1) 信号系统与综合监控、站台门、通信系统等多个外部系统互联互通, 但在该网络边界处缺乏访问控制功能, 缺少为数据流提供明确的允许/拒绝访问的能力; (2) 不能对进出网络的信息内容进行过滤, 不能实现对应用层协议命令级的控制; (3) 缺少防止地址欺骗的技术手段, 容易遭受基本的网络攻击; (4) 缺乏对非授权设备私自连接到内部网络的行为进行检查、定位和阻断的能力, 无法有效地监测到网络攻击行为, 也无法对攻击源 IP、攻击类型等信息进行记录; (5) 无法在网络边界处对恶意代码进行监测。

根据《信息安全技术 网络安全等级保护基本要求》(GB/T 22239-2019)、《信息安全技术 网络安全等级保护实施指南》(GB/T 25058-2019)和《中华人民共和国计算机信息系统安全保护条例》(国务院 147 号令)等相关技术标准, 地铁信号系统信息安全目前暂按三级标准执行, 极大提高了信号系统信息安全的稳定性。但现有的等保系统主要依赖于在安全域边界处, 采用网闸设备实施物理隔离方式满足三级标准。这种边界防护措施缺乏完整性及主动性, 在遇到网络攻击时, 网闸的物理隔离方式严重影响了正常业务流通信。

5G 标准不仅针对下一代移动通信网络基础设施(公共通信网络), 第三代合作伙伴计划 3GPP 以融合网络为目标, 提出的 5G 标准也同时应用于下一代垂直行业网络。5G 网络通过统一的物理设备和网络功能虚拟化(Network Function Virtualization, NFV)实现业务多样化、处理能力按需配置。3GPP 33.501[2]定义的 5G 网络安全整体架构也体现了该特点。5G 安全以抽象后的能力形式进行组织, 逻辑安全功能独立于其他网络功能, 在网络中可以单独部署、配置或定制。同时从安全视角考虑风险级别, 应当进行安全边界防护设计[3]。

具体来说, NFV 旨在利用标准的 IT 虚拟化技术将网络功能模块拆分为不依赖于物理硬件的虚拟网络功能(Virtual Network Function, VNF), 可根据服务租户需求进行 VNF 实例的灵活部署和扩展, 从而降低运营成本、提高资源利用率和可控性。软件定义网络(Software Defined Network, SDN)将网络的数据平面和控制平面分离, 可以实现对网络功能的灵活控制和高效部署。NFV 基于虚拟化技术为网络提供软件形式的安全功能, SDN 集中式控制网络为虚拟化后的网络安全功能部署提供了高效快捷的方式。综合以上 NFV 和 SDN 技术, 服务功能链(Service Function Chain, SFC)技术应运而生。服务功能链即将多个 VNF 整合为一个链, 业务流依次通过链上的 VNF 进行处理, 具有灵活多变、快速响应等特点, 在网络安全边界防护上也可发挥出巨大作用。

为了尽可能地提高业务流在边界设备上的通过率, 本文提出了一种动态安全边界防护机制, 根据不同业务流量的防护等级需求, 配置不同的服务功能链, 以解决网闸过度隔离问题, 提高网络安全防护的效果。论文主要贡献如下:

(1) 基于 5G NFV/SDN 技术设计了动态安全边界防护模型。本模型由边界网络安全功能资源池、业务流量防护等级划分、边界安全服务规则库、边界服务链生成模块四部分组成。模型是我们所提机制的实现途径, 可以不唯一, 在我们文献调研范围内, 暂无同类型模型和机制设计。

(2) 针对动态安全边界防护机制要解决的目标优化问题, 建立数学模型, 作为理论分析的基础。其中我们提出了安全设备/系统的安全能力量化指标-安全贡献度, 这是综合安全设备的安全防护能力、风险评估和性能(计算、存储和通信)实时计算得到的数值, 通过分析对比相关文献[4-18], 该指标属首次提出。

(3) 动态安全边界生成算法。首次提出适配业务防护等级和边界安全服务能力的可变安全服务功能链生成算法, 在满足业务防护等级需求和最小化处理时延目标下计算出部署优化解, 生成相应的边界安全服务规则。

后续章节安排如下: 第 2 节介绍相关研究工作和仿真工具, 包括安全域及安全边界、NFV/SDN 及服务功能链和 SDN 仿真工具三个小节; 第 3 节阐述动态安全边界防护模型细节; 第 4 节是动态安全边界防护机制, 包括数学模型、动态安全边界生成算法和轨道交通行业实例; 第 5 节是实验验证; 第 6 节和第 7 节分别是讨论和总结。

2 相关工作

2.1 安全域及安全边界

IEC 62443 系列标准[19]描述了安全区域的概念, 即共享公共安全需求的物理、信息和应用程序资产的逻辑分组。安全域是指在同一系统内具有相同安全保护需求、相互信任需求、并且具有相同安全访问控制和边界控制的子网或网络。安全域的划分是保障网络和基础设施稳定正常工作的基础, 也是保障业务信息安全的基础。宋杨在《网络安全域划分及边界整合研究与规划》[20]中提出, 现有安全域的划分采用向日葵结构, 即花心: 统一的核心承载网, 提供 IP 可达性或受限 IP 可达性; 花环: IP 承载网边界; 花萼: 业务模块与承载网的交互区域; 花瓣: 明确单一的业务功能模块。李旺在《网络边防关键技术研究》[21]中提出了以保障云计算业务安全的安全域划分架构, 把安全域划分为不同的安全子域, 如生产区、非生产区、堡垒区、DMZ 等, 从而进行纵深防护。郭睿等在《安全域划分在企业中的实际应用研究》[22]中提出了动态安全域划分的方案, 实现一个系统的动态安全域划分, 从纵深的角度, 全盘考虑安全的部署和应用, 提高网络安全性。Ao 在《Quarantine Region Scheme to Mitigate Spam Attacks in Wireless-Sensor Networks》[23]中提出以间歇的身份验证方式划分隔离区方案, 抵御无线传感器网络中的垃圾邮件攻击, 动态检测节点的状态, 根据状态的不同将其划分到隔离区或非隔离区, 同时设置缓冲区, 通过减少状态保持时间提高警戒性为边界增加厚度, 更高效地保障域内安全。

安全域中的交互网络域与互联网、专线和内网的边界是安全域的重要边界, 安全子域之间也存在相应的边界, 如计算域、服务域、维护域之间的边界[24]。网络安全边界的主要作用是把一个大规模复杂系统的安全问题化解为更小区域的安全问题, 以实现大规模复杂网络系统的安全等级保护。林育凯在《浅析隔离网闸与防火墙在网络安全中的综合利用》[25]中提出的传统的边界安全防护机制, 综合应用了隔离网闸和防火墙, 利用防火墙的入侵检测和防病毒系统与网闸隔离定位准确的优势, 通过隔离网闸技术中的链路层断开技术阻断 TCP/IP 穿透, 补充防火墙存在的漏洞, 有效阻止外部程序的恶意入侵。这种边界防护机制的网络功能由不同的硬件设备提供, 网络服务提供商(Network Service Provider, NSP)需要在用户请求新服务时部署大量新设备, 价格昂贵且灵活性差, 并且对业务流量采取的防护措施只有隔离和非隔离两种状态, 不能根据业务流量

的安全需求为其定制动态的防护措施, 因此业务流量在安全设备上的通过率很低。SDN 和 NFV 技术的产生解决了网络功能部署灵活性差且价格昂贵的问题[26]。李天龙在《多域网络安全服务编排系统的设计与实现》[27]中提出一种在多域数据中心环境下按需部署网络安全服务的方法, 基于SDN和NFV技术, 使用 Docker 容器封装网络安全服务, Open vSwitch 软件交换机配置路由寻址, 为网络安全服务添加特定报头封装, 完成从单网络域到多网络域的分层拓展, 减少数据流量延迟的同时降低中间件频繁扩容和管理困难的问题。本文在此多域网络安全服务功能编排方法基础之上, 考虑以边界安全设备的安全功能为元素, 提出一种动态的边界防护机制, 根据业务流量的防护等级为其定制服务功能链, 在保证隔离恶意流量的同时提高防护等级需求较高的业务流量在边界设备上的通过率。

2.2 NFV/SDN 及服务功能链

新一代的网络主要基于 SDN 和 NFV 实现[28-29]。SDN 将网络设备的控制层和数据层分开, 网络不仅可以完成数据传输的任务, 还可以成为一种灵活的资源, 经过虚拟化后作为计算和存储资源进行部署。NFV 使软件和硬件脱钩, 网络设备功能不再依赖于特殊的硬件, 从而实现了基于实际业务需求的网络功能软件、新业务的快速生成和部署、故障隔离自我修复等功能[30]。将 SDN 及 NFV 技术应用到 5G 网络架构中, 可让 5G 移动通信网络达到良好的虚拟化效果, 并采用编程开发的形式对通信目标相同的网络硬件进行组合, 为新的 5G 业务开发以及软件革新等工作提供足够便利, 同时, 也可以让 5G 网络软件达到集中化管理的效果, 使其管理效率得以显著提升。另外, 通过 SDN 与 NFV, 能够控制 5G 网络中的全网流量, 充分满足其数据传输过程中的带宽需求, 实现 5G 网络资源的灵活调用, 使其利用效率显著提高[31-32]。支敏慧等在《5G 网络架构中 SDN 和 NFV 的应用策略》[32]中指出通过 SDN 的应用, 可以简化网络管理、快捷部署应用, 同时也可以实现网络的自动化配置。借助 SDN, 用户可在云服务中进行所需资源的选择和功能应用, 以此来实现网络、储存以及计算机等资源的智能化控制和利用, 使其达到最佳配置, 并实现更具直观性的服务部署。NFV 主要是依托网络优势, 实现服务的有效简化。利用网络中的自动系列处理器, 实现压缩负荷、加密、虚拟化硬件加速以及多核计算性能的集成。

NSP 提供的服务可以通过 SFC 来实现。SFC 是指引导流量按序通过一组虚拟网络功能(Virtual Network Function, VNF)以提供端到端服务的过程。当 SFC 请求到达目标网络时, NFV 控制器需要根据优化目标(如最大化资源利用率、最小化设备总能耗、最小网络时延、数据中心负载均衡等), 将 VNF 部署在特定的服务器上并为其分配资源。近年来, 关于 SFC 部署的研究已成为一个热门话题, 但现有研究主要关注静态 SFC 编排, 未考虑服务请求的动态变化[33-34], 对应用而言, 动态服务功能链优化部署是亟待解决的问题。由于服务链部署属于 NP 难问题[35], 已展开的工作主要集中在设计启发式算法来获取近似最优解。Tajiki 等在《Joint Energy Efficient and QoS-Aware Path Allocation and VNF Placement for Service Function Chaining》[36]中提出了整数线性规划模型来降低 SFC 的部署成本, 并提出了一种启发式算法来提供近似模型的解决方案; 陈卓等在《MEC 中基于改进遗传模拟退火算法的虚拟网络功能部署策略》[37]中提出将遗传算法与模拟退火算法相结合的求解策略, 通过判断个体约束性与纠正遗传的方法避免局部最优的出现, 大幅降低了端到端时延; 文献[38-39]使用机器学习部署 VNF 能够提高 SFC 的优化效果, 但又依赖于利用大量准确的数据集训练模型。然而, 以上 SFC 部署的研究大多只考虑单域内 SFC 的动态部署, 没有考虑边界安全设备的动态 SFC 部署。本文工作侧重设计云边端管多层次防护架构下的边界安全服务功能链的动态编排和部署, 保证业务流量不过载的同时, 实现满足业务流防护等级需求和最小化处理时延的多目标联合优化 SFC 部署策略。

2.3 SDN 仿真工具

Mininet 是由 Lantz 等人创建的开源网络虚拟仿真平台, 其特点是能为 SDN 提供虚拟测试和开发环境, 它支持在计算机或服务器上进行 SDN 相关内容的开发, 并且SDN设计可以在Mininet和实时部署中进行无缝移动, 通过指令“sudo mn”即可快速创建 SDN 网络。

由日本NTT公司实验室发布和维护的SDN控制器开源项目 Ryu 是用 Python 编写的软件定义网络控制器平台。其特点是简单易用、灵活且可扩展、支持多种 OpenFlow 协议版本和高性能。Ryu 控制器可以与SDN交换机通过OpenFlow协议进行通信, 并对交换机进行控制。通过指令“ryu-manager your_app.py”可以启动 Ryu 控制器, 用于加载已经编写好的应用程序。

3 动态安全边界防护模型

基于 SDN 和 NFV 技术设计的动态安全边界防

护模型主要由以下几个部分构成:

(1) 边界安全功能资源池

在工业控制系统中, 为了保证业务系统的可靠性和稳定性, 需要将网络分割成不同的安全域, 并在安全域之间部署边界安全防护设备或系统, 通过虚拟化技术将这些设备或系统组织成安全边界功能资源池, 采用软件定义控制器对虚拟化资源进行有效调度。在 5G 网络中, 基于 NFV 的软件定义安全, 采用虚拟化的网络安全功能网元。这些网元以独立形态的虚拟化软件形式运行在服务器上, 通过服务器、内部的虚拟网络进行通信, 构成一个可平滑扩展的网元集群, 并通过统一的管控平台管理承载运行的虚拟机并实现相互之间的隔离。

由此可以看出, 基于 5G 的工业互联网具备建立边界安全功能资源池的基础和应用需求, 为定义本文提出的动态安全边界提供了可调度的安全功能集合。

为了量化资源池中的安全功能能力, 我们依托信息系统安全性评价方法对每个安全功能进行评估。信息系统安全性评价是指对信息系统的安全风险进行评估和分析, 以确定安全措施是否足够保护系统免受攻击和威胁[40]。我们将安全设备在保护信息系统安全方面所起到的作用和贡献定义为安全设备的安全贡献度, 包括其可靠性、性能、安全性的多层次综合评估, 结果用等级数值表示。

安全设备的安全贡献度综合评估模型如图 1 所示, 结构和评估流程是:

a. 根据网络安全设备的工作原理和特性与常见的攻击类型, 建立关于评估对象的信息库 [41-42];

b. 建立基于安全性、性能和可靠性的安全贡献度评估指标体系;

c. 使用风险叠加(Cumulative Incidence of Maintenance, CIM)模型评估可靠性, 使用 ROC 曲线(Receiver Operating Characteristic curve), 基于检测率和误警率的线性叠加评估性能指标, 使用综合安全评估模型, 借鉴“木桶效应”的概念, 考虑安全设备各方面的表现, 选择最薄弱的表现评估安全设备的安全性指标[43-44];

d. 使用主客观结合的确权算法, 得到三项一级指标的权重;

e. 考虑指标包含主客观因素, 可采用模糊综合评估方法计算网络安全设备的安全贡献度得分。

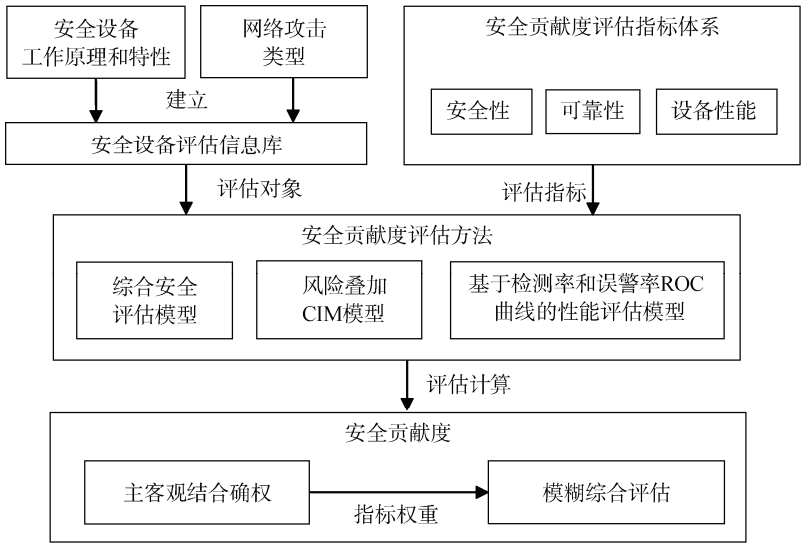

图 1 安全贡献度综合评估模型

Figure 1 Integrated assessment model for security contribution degree

风险叠加模型是一种用于评估系统可靠性的方法。对于安全设备, 我们可以将其作为系统的一部分, 使用 CIM 模型来评估其可靠性指标。首先, 需要识别与安全设备相关的各种可能的风险因素, 例如环境条件、使用频率、制造质量等; 对于识别的风险因素, 需要确定它们对安全设备可靠性的影响程度, 通过专家评估和历史数据分析的方法确定风险权重 I 和风险影响程度 W, 则对于每种风险其风险叠加值 $s = i \times w$; 将所有风险叠加值进行汇总, 得到综合的风险叠加值 S, 从而得出安全设备的可靠性水平。

计算网络安全设备的检测率(True Positive Rate, TPR)和误警率(False Positive Rate, FPR), 收集网络安全设备的检测结果数据, 包括真阳性(True Positive, TP)、假阳性(False Positive, FP)、真阴性(True Negative, TN)、假阴性(False Negative, FN)的比例; 检测率使用公式(1)计算,

$$\mathrm{TPR}=\frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \tag{1}$$

误警率使用公式(2)计算,

$$\mathrm{FPR}=\frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \tag{2}$$

以误警率为横轴, 检测率为纵轴, 绘制 ROC 曲线。计算 ROC 曲线下的面积(Area Under the Curve, AUC)。AUC 值是 ROC 曲线下的面积, 用于量化网络安全设备在不同误警率下的整体性能。AUC 值越接近 1, 表明网络安全设备性能越好。

选择响应时间、漏洞修复速度和性能稳定性代表安全设备的安全性指标, 基于专家意见和历史数据分析为每个指标分配权重, 以体现其在安全性评估中的重要程度。对收集到的网络安全设备的实际响应时间、漏洞修复速度和性能稳定性数据进行标准化处理, 将不同量纲的数据统一到相同的尺度上, 以便综合评估各项指标的表现。按照权重对各项指标进行加权计算, 最低值所对应的指标即为安全性的最薄弱环节, 以其评估安全设备的安全性指标。

利用基于熵权的客观确权方法修正基于指标关联性排序的主观权重的偏差, 进而基于模糊综合评价方法进行计算[43], 依据最大隶属度原则得到目标安全设备的安全贡献度。基于指标关联性评价排序的确权方法, 利用马尔可夫链的基本原理和指标间的关联性, 根据专家的集体评价结果确定指标间的影响程度, 不断迭代计算最终达到稳定的状态以确定指标的权重。这样的确权方式集合了众专家的评价结果, 达到评价人数越多、评价结果越客观的效果, 消除了单一专家评价的主观性问题。客观权重的计算采用熵权法, 信息熵的取值范围为(0,1], 在实际情况中信息熵等于 1 表示该指标对安全设备未提供任何有价值的信息, 信息熵等于 0 表示只需要该指标就可以完成对安全设备安全贡献度的度量。因此, 指标的权重设置遵循公式 $\omega_i=\partial\omega_{ai}+\beta\omega_{bi}$。其中 ω_i 表示新权重, ω_{ai} 表示主观权重, ω_{bi} 表示客观权重, $\partial+\beta=1$。最后, 利用模糊综合评价方法得出安全设备的安全贡献度。

(2) 业务流量防护等级

要实现动态地调整安全策略, 为不同业务配置不同的边界安全功能, 首先需要明确每个业务流的防护等级需求。5QI(5G Quality of Service Identifier)是 5G 定义的质量指标, 用于评估和度量用户体验和网络性能, 5QI 值作为衡量 5G 网络性能的指标反映出网络的延迟、丢包率、吞吐量等方面的情况。业务流量的防护等级代表了不同业务流量所需要的保护级别, 较高的防护等级通常要求网络提供更高的带宽、更小的处理时延。基于这种理解, 同时兼顾参数获取的可实施性和便利性, 我们考虑将 5QI 值作为定义业务流量防护等级的依据, 通过映射关系将 5QI 值与防护等级进行对应。

(3) 边界安全服务规则库

边界安全服务规则库是一个服务链编排规则数据库, 用于根据业务流量的防护等级需求动态调整边界服务链[44-47]。边界规则库的构建需要结合实际应用场景, 设定相应的触发条件和预制规则, 包含规则名称、触发条件和规则动作。规则名称用来标识每个规则的唯一性。触发条件是业务流量防护等级需求。规则动作用于描述当为满足触发条件应采取何种动作, 即生成为不同等级的业务流定制的边界安全功能服务链。

(4) 边界服务链生成

边界安全服务规则库中的规则来源于边界服务链生成模块。它根据业务流量的变化动态生成边界服务链。

上述四个部分结合起来, 构成了一个动态的安全边界防护体系, 如图 2 所示。

图 3 为系统处理流程图, 包含如图 3(a)所示的系统初始化流程和图 3(b)所示的业务处理流程。

系统初始化阶段的主要步骤如下:

a. 通过虚拟化技术将安全域之间部署的边界安全防护设备或系统虚拟化;

b. 评估安全设备在保护信息系统安全方面所起的作用和贡献, 计算各自的安全贡献度;

c. 输出带有安全功能贡献度的可平滑扩展的虚拟化的网元集合, 并将这些虚拟化的网元写入安全功能资源池;

d. 输入防护等级定义模板及预制规则。

业务处理流程主要有:

a. 业务流量到达安全边界网关, SDN 数据平面根据流源/目的 IP 和 5QI 对流量进行解析, 映射到各自的防护等级;

b. 将业务流量防护等级与边界规则库中的触发条件进行匹配;

c. 匹配产生规则动作, 生成边界服务功能链;

d. 利用 SDN 数据平面和虚拟网桥构建边界设备之间的连接, 调度边界安全功能;

e. 若边界设备无法满足业务流的防护等级需求, 则跨域调用域内安全设备的安全功能;

f. SDN 控制器控制 SDN 交换机和虚拟网桥上的转发流表, 以此实现业务流量按照指定的顺序经过指定类型的边界安全设备。

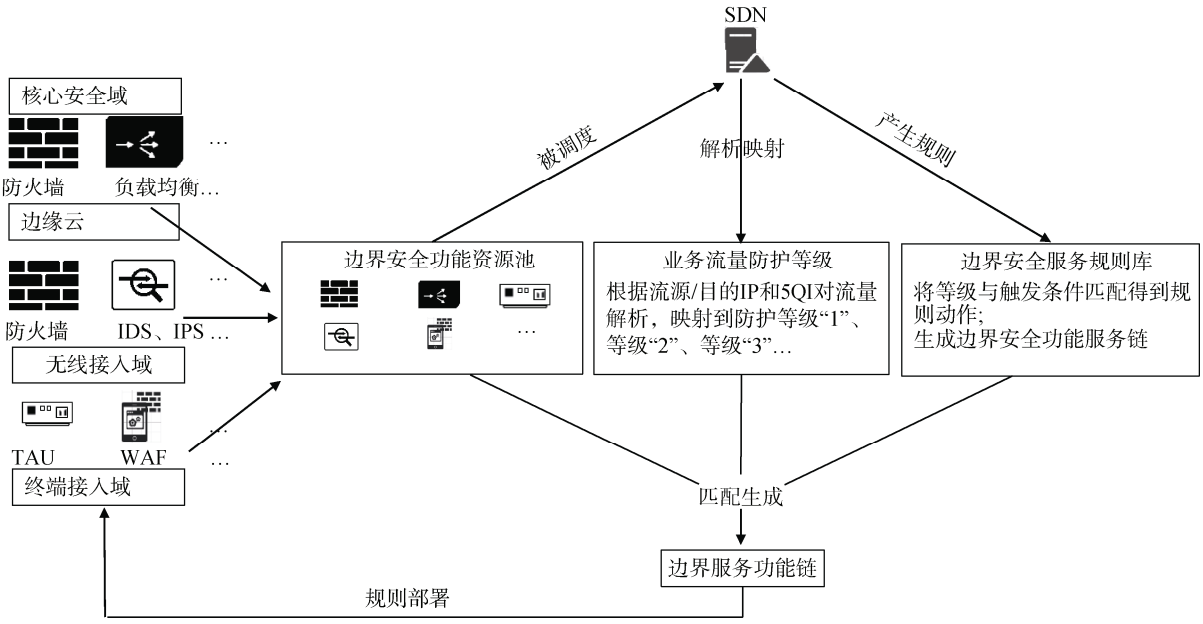

图 2　动态安全边界防护体系结构图

Figure 2　Dynamic security perimeter protection architecture

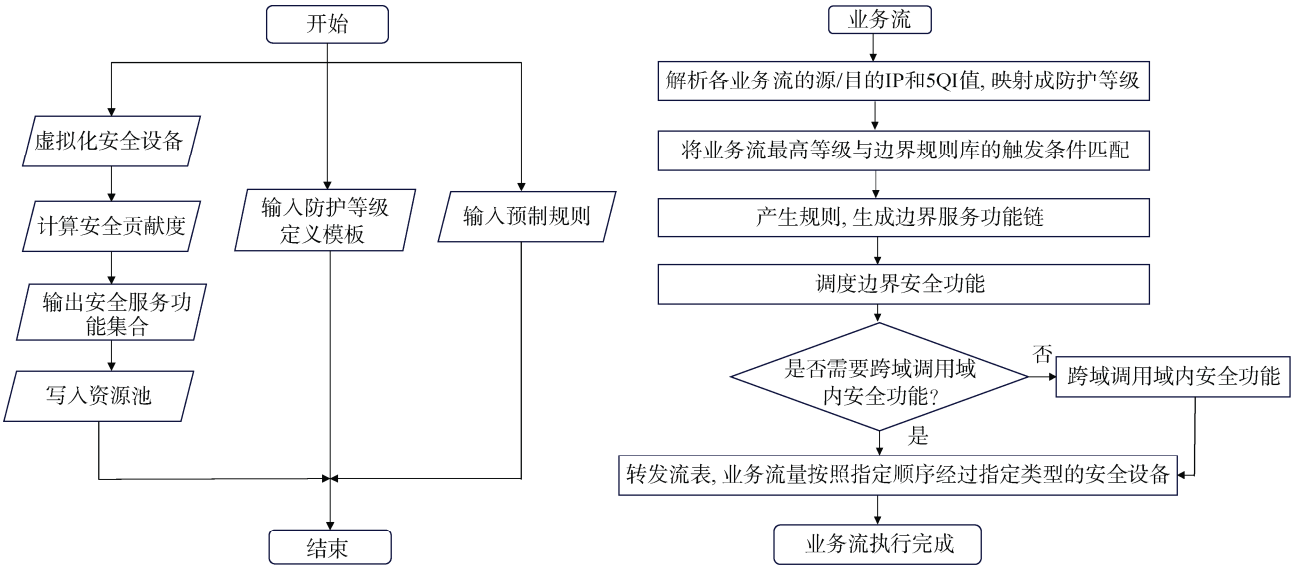

图 3　系统处理流程图

Figure 3　System processing flow chart

该体系可以根据业务流量的特点和防护等级需求, 动态地调整安全策略和服务功能链, 从而实现网络安全防护的细粒度控制、提高业务流在边界设备上的通过率。

4　动态安全边界防护机制

4.1　数学模型

接下来这一节将介绍动态安全边界防护的数学模型, 包括定义边界节点的网络安全贡献度、约束条件和优化目标函数的具体表达公式, 并详细描述建模过程。

4.1.1　边界安全功能模型

本节介绍在系统模型中创建边界安全服务功能链并优化边界安全服务功能链的过程。

论文中使用的符号列表见表 1。

我们用 N 表示边界的节点集合, 边界节点的数量用 n 表示, F 表示业务流的防护等级集合, 某个流量的防护等级用 f 表示。M 表示业务流量的集合,

单个业务流量用 m 表示, ∂^m 表示业务流 m 的分组数量。K 表示每个节点上的网络安全功能的集合, 节点上的某个安全功能用 k 表示。

表 1 符号列表

Table 1 List of symbols

符号	定义描述
n,N	边界节点数量和边界节点集合
f,F	业务流量防护等级数值和业务流防护等级集合
m,M	业务流和业务流集合
∂^m	业务流 m 的分组数量
k,K	节点上的安全功能和节点安全功能集合
L	边界节点间的链路
$l_{i,j}$	节点 i 到节点 j 之间的链路
B	链路带宽的集合
$B_{i,j}$	节点 i 到节点 j 之间可以传输的最大流量
C	边界节点的安全贡献度
$C_f(i)$	节点 i 对防护等级为 f 的流量的安全贡献度
$C^s(z)$	安全域 s 中某设备 z 的安全贡献度
X	边界节点上的虚拟化安全功能是否有效
$X_f(i,k)$	节点 i 的安全功能 k 对防护等级为 f 的流量是否有效
P	边界服务功能链
$P_f(j\|i,k)$	链路 $l_{i,j}$ 是否可以作为安全功能 k 对防护等级为 f 的业务流提供安全服务的一条链路
D	边界节点使用安全功能时的处理时延
$D_f(i,k)$	节点 i 使用安全功能 k 对等级 f 的流量的处理时延
T	边界节点传输流量的链路时延
$t_{i,j}$	节点 i 到节点 j 传输时的链路时延
ProcessDelay	处理时延
LinkDelay	链路时延
R	安全域的集合
Z	安全域内设备的集合
$R_s(z)$	某安全域 s 中的某个安全设备 z

L 表示边界节点间的链路, 节点 i 到节点 j 之间的链路表示为 $l_{i,j}$, B 表示链路带宽的集合, 则节点 i 到节点 j 之间可以传输的最大流量为 $B_{i,j}$。C 表示边界节点的安全贡献度, 即流量经过此节点后产生的防护效果的数值表示, 则节点 i 对等级为 f 的流量的安全贡献度为 $C_f(i)$。集合 X 表示边界节点上的虚拟化安全功能是否有效, 则节点 i 的安全功能 k 对等级为 f 的流量是否有效可表示为 $X_f(i,k)$, 且有表达式

$$X_f(i,k)=\begin{cases}1 & \text{if} \quad k\in K \quad \text{is} \quad \text{active}\\ 0 & \text{otherwise}\end{cases} \tag{1}$$

流量经过的各个边界节点之间的链路组成了一条边界安全服务功能链, 流量依特定的顺序到达不同的边界节点, 我们引入公式(2)来表示流量的服务功能链。

$$P_f(j\,|\,i,k)=\begin{cases}1 & \text{若} l_{i,j}\text{是服务链的一条边}\\ 0 & \text{其他}\end{cases} \tag{2}$$

其中, $j\,|\,i$ 表示流量从节点 i 离开前往节点 j, k 表示节点 j 的安全功能。该公式取 0 或 1, 若公式等于 1, 则表示流量从节点 i 到节点 j 后节点 j 上的安全功能 k 可以为等级为 f 的流量提供安全服务, 即链路 $l_{i,j}$ 可以作为服务功能链的一条链路。

为了简化问题, 认为流的流速恒定。当安全服务功能链创建且存在时, 假设业务流量到达的速率不能造成网络阻塞, 那么只需要关心单个流量的延迟即可。D 表示边界节点使用安全功能时的处理时延, 则节点 i 使用网络安全功能 k 对等级为 f 的流量进行处理的时延可以表示为 $D_f(i,k)$。T 表示边界节点传输流量的链路时延, 则流量在节点 i 到节点 j 传输时的链路时延为 $t_{i,j}$。

4.1.2 约束条件

业务流量经过的网络边界节点形成了一条边界安全服务功能链, 按照边界规则库中的规则定义, 该业务流量必须经过至少一个边界安全设备 i 上某种安全功能 k 的处理, 因此有

$$\sum_{i\in N}\left(\sum_{k\in K}X_f(i,k)\right)\geqslant 1 \tag{3}$$

我们使用的网络拓扑模型为非全连接网络拓扑模型, 这必然会导致动态边界安全边界生成算法中计算路径时产生链路的使用重叠, 我们要保证每一条链路的容量不过载, 因此有

$$\sum_{(i,j)\in L}\left(\sum_{m\in M}\left(\sum_{i,j\in N}\partial_m P_f(j\,|\,i,k)\right)\right)\leqslant B_{i,j} \tag{4}$$

4.1.3 优化模型

本模型的优化目标是在满足特定防护等级需求的服务链路上, 降低流量从源节点到目的节点的平均时延。该时延包含两个主要组成部分: 第一部分是边界设备对业务流量进行安全功能处理所需的时延; 第二部分是传输流量经过链路所需的链路时延。

第一部分, 处理时延是某防护等级为 f 的业务流量经过满足其防护等级需求的边界安全设备提供的网络安全功能处理所需的总时延。可以用以下公

式表示:

$$\text{ProcessDelay}_f = \sum_{i\in N}\left(\sum_{k\in K} X_f(i,k)\cdot D_f(i,k)\right) \quad f \in F \tag{5}$$

第二部分, 链路时延是某防护等级为 f 的业务流量途经满足其防护等级需求的边界安全设备组成的链路的总时延。可以用以下公式表示:

$$\text{LinkDelay}_f = \sum_{(i,j)\in L}\left(\sum_{k\in K} P_f(j\,|\,i,k)\cdot t_{i,j}\right) \quad f \in F \tag{6}$$

所以该业务流量的分组平均时延可以表示为

$$\begin{aligned}\text{TotalDelay}_f &= \frac{\text{ProcessDelay}_f + \text{LinkDealy}_f}{\partial^m} \\ &= \frac{\sum_{i\in N}\left(\sum_{k\in K} X_f(i,k)\cdot D_f(i,k)\right) + \sum_{(i,j)\in L}\left(\sum_{k\in K} P_f(j\,|\,i,k)\cdot t_{i,j}\right)}{\partial^m}\end{aligned} \tag{7}$$

本模型的优化目标是满足特定防护等级需求流量的平均时延相对最低, 且要满足模型中的约束条件, 最后得到 $X_f(i,k)$ 和 $P_f(j\,|\,i,k)$。

4.1.4 跨安全域模型

SDN 数据平面对到达边界处的流量信息进行解析后, 根据预定义的防护等级映射规则, 将输入流量划分为不同的防护等级, 然后利用 SDN 控制器中的动态边界生成算法, 根据约束条件和优化目标对边界设备的安全功能进行编排生成边界服务功能链。当动态边界生成算法在当前边界设备的安全功能池中找不到无法生成满足当前流量防护等级需求的服务功能链时, 会向控制器发出请求, 向安全域间设备寻求帮助。

我们用 R 表示安全域的集合, 假设共有 r 个安全域, R_1, R_2, ..., R_r 分别表示不同的安全域, 用 Z 表示安全域内设备的集合, 则 $R_s(0<s\le r)$ 中安全设备 z 可表示为 $Z_s(z)$, 某安全域 s 中的某个安全设备 z 可表示为 $R_s(z)$。用 C 表示各安全域中设备安全贡献度的集合, 分别用 C^1, C^2, ..., C^r 表示不同安全域中设备安全贡献度的集合, 则某安全域 s 中某设备 z 的安全贡献度可表示为 $C^s(z)$。我们令 R_r 对应的防护等级为最高级, 域内安全设备的类型最丰富, 安全贡献度最高, 即

$$C^1 < C^2 < C^3 < \ldots < C^r \tag{8}$$

4.2 安全边界防护生成算法

上一节, 我们对动态安全边界防护模型所需要的内容进行了数学建模, 得到了解决 SDN 控制器处理不同防护等级需求的流量的最优边界服务功能链的优化模型。本模型使用安全边界防护生成算法来驱动各边界设备的安全功能, 为不同等级的流量提供不同的安全策略。算法分为两部分实现。

第一部分, 安全边界防护生成算法。该算法运行在 SDN 控制平面, 主要实现为不同等级的流量定制满足其需求的安全功能服务链。

蚁群算法(Ant Colony Optimization, ACO)是一种模拟蚂蚁行为来寻找优化路径的概率型启发式算法, 该算法具有分布式、信息正反馈和启发式搜索的特征, 可以通过减少迭代次数找到满足条件的最优解。蚁群算法通常用于解决旅行商问题(Traveling Salesman Problem, TSP)。在 TSP 问题中, 蚂蚁需要分布在不同的节点上, 并选择路径以找到遍历所有节点的最短路径。

然而, TSP 问题与本文中提出的优化目标问题是有一些不同的, 由系统模型的内容可知, 公式(7)为优化目标, 公式(3)和公式(4)为约束条件, 为使蚁群算法更符合本文中提出的模型来实现边界设备安全功能为不同等级的流量定制满足其需求的服务链的需求, 需要对蚁群算法进行改进。首先, 我们要将蚂蚁部署在同一个起始节点上的, 蚂蚁从起始节点出发遍历可以到达目的节点的所有路径, 然后通过比较选择最优路径。此外, 由于本模型中蚂蚁部署在同一个起始节点, 必然会有重复的路径, 因此必须要在算法中对重复路径进行特殊处理, 否则重复路径会更新两次信息素, 会导致路径的信息素浓度很可能超过时间更短的信息素浓度。

基于上述改进, 本模型中的蚁群算法伪代码如算法 1 所示。算法 1 中, 启发函数对应于根据流量信息、防护等级需求、带宽资源和链路时延等因素计算节点的选择概率。这个概率会影响蚂蚁在路径选择过程中的决策。信息素浓度表示了路径的好坏程度, 可以根据路径时延信息来更新信息素, 较高浓度的信息素对应于更好的路径选择。

算法 1 基于改进蚁群算法的安全边界防护生成算法

输入: 多个防护等级的流量的源节点和目的节点、带宽资源、链路时延、边界设备安全能力的安全贡献度、边界设备安全能力处理的时延

输出: 最佳路径、最佳路径时延

1 初始化参数和蚂蚁位置
2FOR a=1 TO 总数
3 FOR b=1 TO 迭代总数
4 FOR c=1 TO 蚂蚁总数
5 选择下一跳节点
6 根据启发函数和信息素浓度计算节点的选择概率
7 更新蚂蚁的位置和路径信息
8 更新信息素浓度
9 根据路径时延信息更新信息素
10 END FOR
11 END FOR
12 FOR d=1 TO 路径总数
13 根据路径时延以及链路的安全贡献度选择最佳路径时延
14 IF 没有路径可以到达目的节点
15 报告给控制层决策节点向安全域内的设备请求对应的网络安全功能来实现防护
16 END IF
17 END FOR
18END FOR

第二部分, 跨域安全设备调度算法。

第一部分的边界防护生成算法可以利用边界设备的安全功能对不同防护等级的流量定制满足其需求的服务功能链, 当算法 1 中已有的边界设备的安全功能无法满足某防护等级的流量的安全需求时, 我们可以调度跨安全域的安全设备为流量定制服务功能链以满足其安全需求。因此, 我们设计了第二部分的调度算法, 当边界防护生成算法无法处理某等级的业务流量时, 会给 SDN 控制器发送信息请求调度跨安全域的设备的安全功能为流量服务。控制器收到算法 1 的请求信息后, 调用算法 2 进行跨域安全设备调度。

本模型的跨域安全设备调度算法如算法 2 所示。

算法 2 跨域安全设备调度算法

输入: R , Z, C
输出: $R_s(z)(0<s\le a)$
1 FOR e=1 TO r
2 量化各个安全域中安全设备的安全贡献度
3END FOR
4 调度合适的安全域中的安全设备编排到服务功能链

4.3 应用实例

针对轨道交通行业数据采集传输中面临的数据安全、网络安全问题, 我们将本文提出的机制与行业场景对应, 进一步解释和检验所提机制的可行性和实现方式。图 4 是轨交行业基于 5G 的云边端管多层

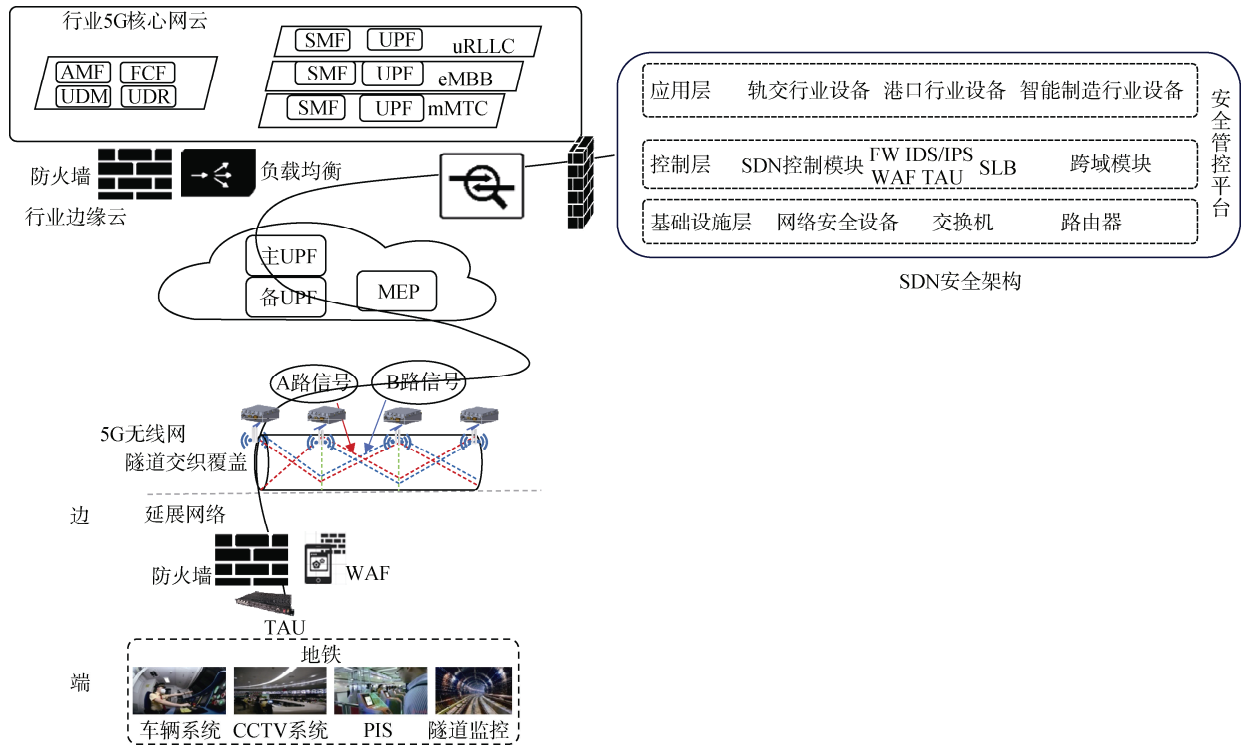

图 4 云边端管多层次安全防护框架图

Figure 4 A multi-level security protection framework for cloud, perimeter, terminal and management

次安全防护框架示意图, 融合软件定义安全架构设计, 将网络划分为相互隔离的安全域的形式, 在各安全域的边界处部署着不同类型的边界安全设备。通常在核心网与边缘云之间部署具有防火墙、负载均衡等功能的安全设备, 在边缘云与无线接入侧之间部署具有防火墙、IDS/IPS 等功能的安全设备, 而无线接入侧与终端之间部署着行业5G设备车载接入单元(Train Access Unit, TAU)、具有防火墙功能的安全设备等。通过虚拟化技术将这些设备组织成安全边界功能资源池, 采用软件定义控制器对虚拟化资源进行有效调度。根据安全设备在保护信息系统安全中的作用范围、安全功能、防御能力、响应能力、稳定性和成本效益等方面的综合评估定义其安全贡献度, 并将评估结果用数值来表示。

本模型根据 5QI 值作为调整业务流量防护等级的依据, 通过映射关系将 5QI 值与防护等级进行对应。例如, 当 5QI=1 时, 可以将业务流量的防护等级调整为“1”级别; 当 5QI 值=9 时, 可以将业务流量的防护等级调整为“9”级别。如表 2 所示, 根据轨交各业务系统的网络需求总结归纳出 5 大类轨交业务及其对应的5QI取值, 将业务流量的防护等级映射为 1、2、3、6、8、9 共 6 种级别。对于不同类别的业务流量, 配置不同的安全策略和服务功能链, 以实现细粒度网络安全防护。业务流量按源 IP 地址到达边界处, SDN 数据平面根据预置映射规则分析其防护等级。SDN 控制器将业务流量等级与事先预置好的边界规则库中的触发条件进行匹配得到规则动作, 即根据不同边界设备的安全贡献度将边界安全设备编排为边界安全服务功能链, 以满足不同等级业务的防护需求。利用 SDN 交换机和虚拟网桥构建边界设备之间的连接, 并通过 SDN 控制器控制 SDN 交换机和虚拟网桥上的转发流表, 依次实现业务流量按照指定的顺序经过指定类型的边界设备。

表 2 轨交业务系统的 5G 网络的 5QI 值

Table 2 5QI value of 5G network in subway traffic system

行车控制类	5QI	运营保障类	5QI	维修维护类	5QI	乘客服务类	5QI	安全防护类	5QI
列车运行控制	3	车站和区间视频监控	6	车辆状态实时监测	6	车载播放控制	6	X 射线设备智能视频分析	6
集群语音对讲	1	车载视频监控	6	信号智能运维列车状态监测	6	车站乘客信息显示	9	定位	9
集群视频对讲	2	火灾报警、环境与设备监控	8	扶梯预警	8	自动售检票专业	8	便携移动安检设备	8
紧急文本下发	6	供电运行安全生产管理	8	大型钢轨探伤车	9	广播业务	6	防洪防汛监测	8
				工程车智慧维修管理	9				
				钢轨打磨	9				
				车载网轨监测	9				

假设有多个业务流同时到达边界设备处, 且业务流中混有恶意攻击的流量, 未启动边界安全防护机制的情况下, 当前行业采取的安全策略是使用网闸功能对边界进行硬隔离, 此时, 所有的业务流都不能通过安全设备, 业务流的通过率为 0。而启动边界安全防护机制后, SDN 数据平面会对流量信息进行解析, 可以检测出恶意流量攻击的业务流量中防护等级最高的数值, 然后控制器根据流量的防护等级调度边界安全功能资源池中的安全功能为其定制相应的服务功能链。相较于使用网闸直接切断业务流的方式, 本文提出的边界安全防护机制可以提高业务流的通过率。

5 实验验证

在这一部分, 我们基于上一节提出的安全边界防护生成算法在 MATLAB 和 Mininet 中做了模拟仿真, 评估其算法性能是否符合预期。安全边界防护生成算法由蚁群优化算法以及跨安全域算法组成。本文将 MATLAB 部署在 16GB 内存, 4 核处理器, 64 位 Windows 操作系统上, 将 Mininet 部署在 4GB 内存, 2 核处理器, 64 位 Ubuntu 操作系统上。

5.1 安全边界生成算法仿真

首先我们根据上一节中建立的轨交行业基于云边端管多层次安全防护框架图创建一个非全连接的边界安全设备拓扑图, 如图 5 所示。

每条路径上的数据表示通过该路径的时延, 单位为 ms, 以及该路径能承受的最大带宽, 单位为 Mbps。橙色表示动态边界防护生成算法的起始节点和目的节点, 蓝色代表边界设备安全贡献度数值为“1”的安全功能, 绿色代表边界设备安全贡献度数

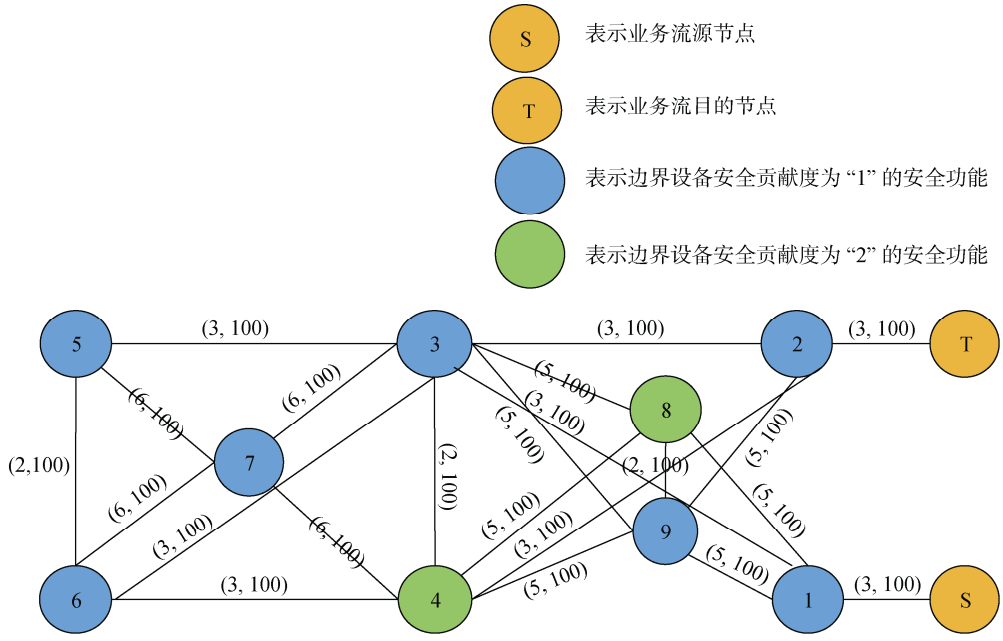

图 5　边界安全设备拓扑图

Figure 5　Topology of perimeter security devices

值为“2”的安全功能。流量从起始节点“S”流入边界处，经过边界安全设备后，传输到目的节点“T”。在核心网与边缘云之间的边界部署着若干具有防火墙、负载均衡功能的边界设备，边缘云与无线接入侧之间的边界部署着具有防火墙和 IDS 功能的边界设备，在无线接入侧和终端域之间的边界部署着若干具有防火墙功能的边界设备以及5G设备车载接入单元 TAU，同时，安全域内还部署着具有负载均衡、访问控制和 WAF 功能的安全设备。

假设有多个业务流同时到达边界设备处，且业务流中混有恶意攻击的流量。启动边界安全防护机制后，利用蓝色、绿色的边界设备的安全功能对恶意流量攻击的业务流量进行安全防护，链路带宽需求为 30Mbps。

评估改进蚁群算法应用在轨交行业基于云边端管多层次的防护框架中是否有效，在此次仿真模拟中，我们假设恶意流攻击的地铁业务流中防护等级的最高数值为“6”，算法运行结果如表 3 和图 6 所示。

表 3　算法输出最佳路径

Table 3　Algorithm output optimal path

	路径	时延(ms)	防护等级等效值
用时最短路径	S ->1 -> 3 -> 6-> 4 -> 2 ->T	18	6
防护等级最高路径	S ->1 -> 3 -> 5 -> 6 -> 4 -> 2 ->T	20	7
算法选择最优路径	S ->1 -> 3 -> 6-> 4 -> 2 ->T	18	6

为了更好地评估改进蚁群算法运行的稳定性以及跨安全域算法是否可以有效，我们进行了另一组实验。假设恶意流攻击的地铁业务流中防护等级的最高数值为“9”，得到表 4 和图 6。

表 4　算法输出最佳路径

Table 4　Algorithm output optimal path

	路径	时延(ms)	防护等级等效值
用时最短路径	S ->1 -> 3 -> 5 -> 6 -> 4 -> 8 -> 9 -> 2 ->T	29	9
防护等级最高路径	S ->1 -> 3 -> 5 -> 6 -> 7 -> 4 -> 8 -> 9 -> 2->T	38	11
算法选择最优路径	S ->1 -> 3 -> 5 -> 6 -> 7 -> 4 -> 8 -> 9 -> 2 ->T	38	11

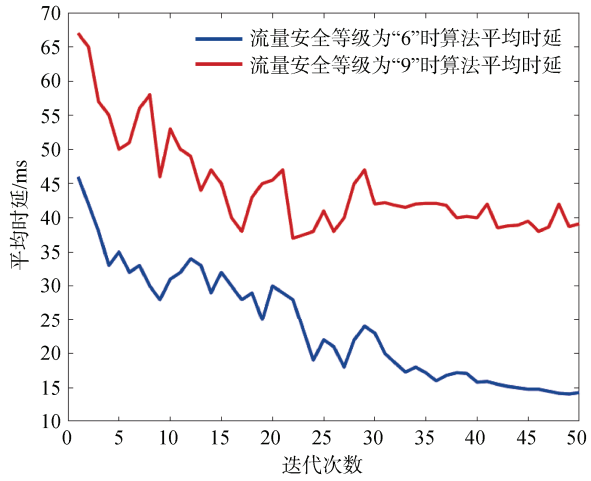

图 6　算法输出路径平均时延

Figure 6　Average latency of algorithm output path

由表 3、表 4 的结果可以看出, 在得到最优解的过程中, 算法会获得几个较优解, 结合时延和防护等级等效值共同进行判断。对时延和防护等级赋权值, 安全需求较高时, 例如, 恶意流攻击的某个业务流量的防护等级的数值超过“6”, 则对防护等级赋较高权值; 当安全需求较低时, 对时延赋较高权值, 以此来判断算法最终采用哪个较优解为最终解。由图 6 可以看出, 随着迭代次数的增加, 蚂蚁爬行的路径平均时延呈下降趋势, 符合改进蚁群算法设计的初衷, 可以更快地得到满足条件的最优解。

5.2 安全防护机制实现仿真

接下来我们采用 Mininet 和 Ryu 控制器进行模拟仿真。我们根据图 4 建立好的边界安全设备拓扑图, 在 Mininet 中建立了一个仿真拓扑图, 如图 7 所示。

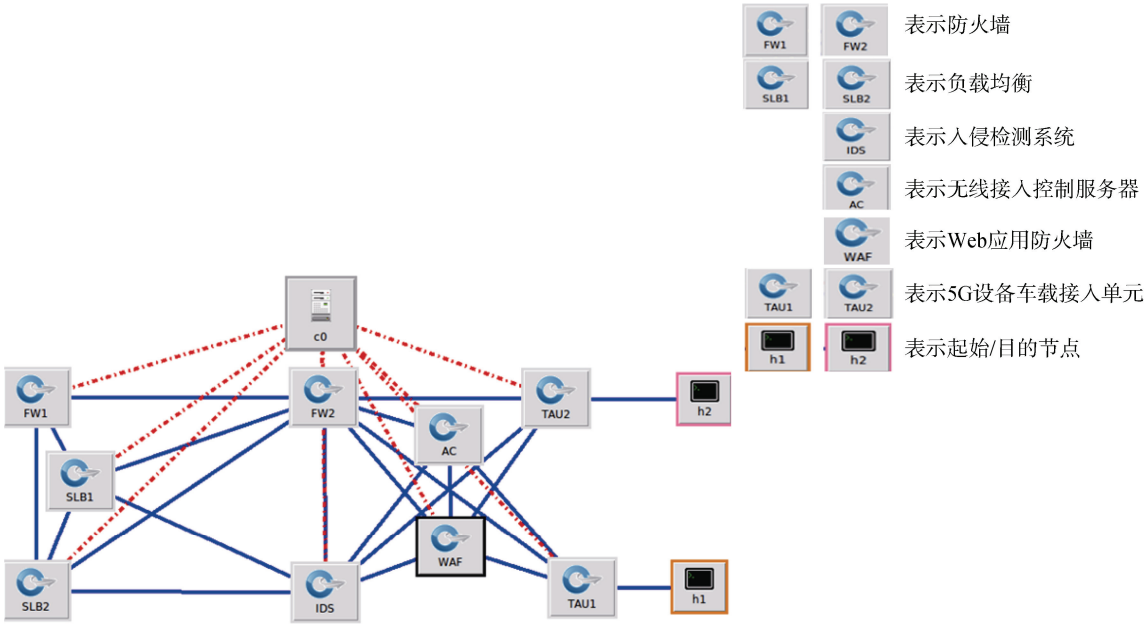

图 7 Mininet 仿真拓扑图

Figure 7 Mininet simulation topology

将上一节设计好的安全边界防护生成算法写入 Ryu 控制器中。将“TAU1”的节点 ID 设置“1”, “TAU2”的节点 ID 设置为“2”, “FW2”的节点 ID 设置为“3”, “DS”的节点 ID 设置为“4”,“FW1”的节点 ID 设置为“5”, “SLB2”的节点 ID 设置为“6”, “SLB1”的节点 ID 设置为“7”, “AC”的节点 ID 设置为“8”, “WAF”的节点 ID 设置为“9”。

启动该 Mininet 边界安全设备拓扑的同时, 启动已经写入安全边界防护生成算法的 Ryu 控制器。模拟边界安全设备拓扑连接到 Ryu 控制器后, Ryu 控制器首先获得模拟边界安全设备拓扑内的设备连接情况, 然后执行 Ryu 控制器中的基于改进蚁群算法的边界防护生成算法。本次实验的目的是验证边界防护生成算法下防护等级数值为“3”的流量从节点“h1”流经边界安全设备到“h2”所需要最优路径, 由于业务流防护等级小于“6”, 说明安全需求较低, 因此算法最终选择的最优解由时延决定, 实验预期最佳路径为“[1, 3, 2]”, 即依次经过 TAU1、FW2、TAU2 后到达目的节点。我们得到的实验结果如图 8 所示, 第 1～4、7～10 行表示算法给出的满足业务流防护等级要求的可行路径的时延和边界设备的安全防护等级等效值, “10.0.0.1”为源节点的 IP 地址, “10.0.0.2”为目的节点的 IP 地址, 红框标注的 5～6、11～12 行表示算法最终选择的最佳路径为“[1, 3, 2]”, 该路径时延为 12ms, 路径中安全设备的安全防护等级等效值为“3”。经过最终验证可以发现该结果符合预期, 并且通过拓扑图可以看出这条路径是可行的, 因此边界防护生成算法是可以正常在 SDN 网络场景中运行的。

```
Ant 1: Current node: 2, Path: [1, 3, 4, 2], Delay: 14 ms, Security Level: 5
Ant 2: Current node: 2, Path: [1, 3, 6, 4, 2], Delay: 18 ms, Security Level: 6
Ant 3: Current node: 2, Path: [1, 3, 2], Delay: 12 ms, Security Level: 3
Ant 4: Current node: 2, Path: [1, 3, 5, 6, 4, 2], Delay: 20 ms, Security Level: 7
Find Path:  [1, 3, 2]  Delay: 12  ms, Security Level:  3
path from 10.0.0.1 to 10.0.0.2:10.0.0.1 ->1 ->3 ->2 ->10.0.0.2
Ant 1: Current node: 2, Path: [2, 3, 1], Delay: 12 ms, Security Level: 3
Ant 2: Current node: 2, Path: [2, 4, 3, 1], Delay: 14 ms, Security Level: 5
Ant 3: Current node: 2, Path: [2, 4, 6, 5, 3, 1], Delay: 20 ms, Security Level: 7
Ant 4: Current node: 2, Path: [2, 4, 6, 3, 1], Delay: 18 ms, Security Level: 6
Find Path:  [2, 3, 1]  Delay: 12  ms, Security Level:  3
path from 10.0.0.2 to 10.0.0.1:10.0.0.2 ->2 ->3 ->1 ->10.0.0.1
```

图 8 Mininet 模拟边界设备寻路仿真结果

Figure 8 Mininet simulation boundary device routing simulation results

接下来验证恶意流量攻击的情况下, 边界防护生成算法及跨域安全设备调度算法是否可以正常运

行。当业务流中混有恶意攻击的流量防护等级中最高的数值为“8”时，边界设备的安全功能无法满足防护等级为“8”的流量的安全需求，需要启动跨域安全设备调度算法为流量定制服务功能链，由于业务流防护等级大于“6”，说明防护等级需求较高，因此算法最终选择的最优解由边界设备的安全防护等级等效值决定，实验预期结果为[1, 3, 5, 6, 7, 4, 8, 9, 2]，即依次经过 TAU1、FW2、FW1、SLB2、SLB1、IDS、AC、WAF、TAU2 后到达目的节点得到实验的部分结果如图 9 所示，第 1～61 行表示算法给出的满足防护等级要求的可行路径的时延和边界设备的安全防护等级等效值，红框标注的第 62～63 行表示算法最终选择的最佳路径为[1, 3, 5, 6, 7, 4, 8, 9, 2]，该路径时延为 38ms，路径中安全设备的安全防护等级等效值为“11”。经过最终验证可以发现该结果符合预期，并且通过拓扑图可以看出这条路径是可行的，因此跨域安全设备调度算法是可以正常在 SDN 网络场景中运行的。

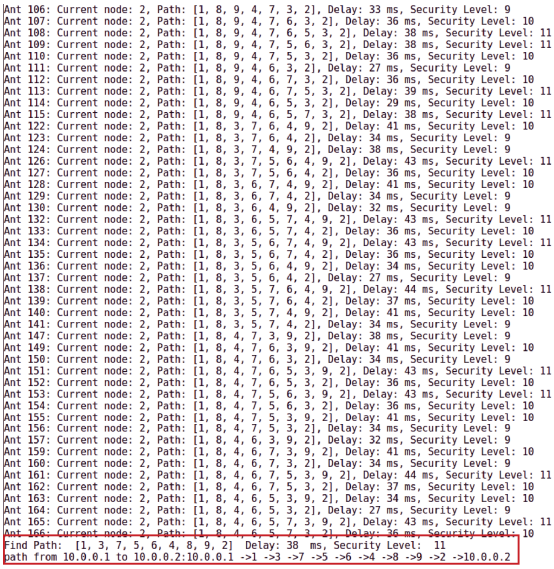

图 9　Mininet 模拟安全域内寻路仿真结果

Figure 9　Mininet simulation of path finding in the security domain simulation results

5.3　业务流通过率仿真

为了更直观地反映动态边界防护机制提高了业务流在边界设备上的通过率，我们进行了另一组实验。该实验将传统边界防护机制和动态边界防护机制的边界业务流通过情况做了对比，边界设备安全功能仍采用图 7 的拓扑结构，传统的边界防护机制综合应用隔离网闸和防火墙功能对业务流过滤，动态边界防护机制则根据业务流防护等级为其提供满足安全需求的服务功能链。实验结果如图 10 和图 11 所示。图 10 的第 1、2 行表示传统边界防护机制下，等级为“9”的业务流无法通过边界，类似地，第 3～14 行表示等级为“8”和“6”的业务流不能通过边界，红框标注的第 15～20 行表示等级为 3 的业务流可以通过边界，可以看出，传统边界防护机制无法通过防护等级大于“3”的业务流，而启动动态边界防护机制后，图 11 的红框标注显示防护等级为“6”的业务流可以通过边界设备，即可以让等级大于“3”的业务流通过边界设备到达目的地址。

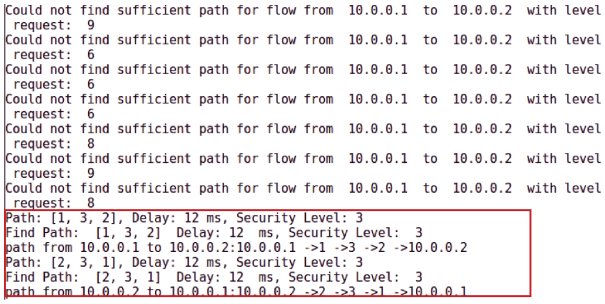

图 10　传统边界机制下业务流路径

Figure 10　Business flow path of traditional boundary mechanism

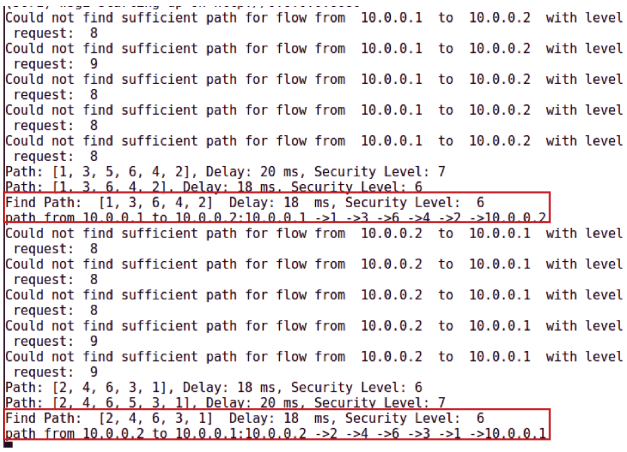

图 11　动态边界机制下业务流路径

Figure 11　The business flow path of dynamic boundary mechanism

动态边界生成算法以满足业务流量防护等级、最小化延迟为优化目标，通过处理被恶意流量攻击的业务流量，解决了以往采用网闸网关直接切断业务流的方式而导致的正常业务流无法正常运行的影响，相较于传统边界防护机制，提高了业务流在边界设备上的通过率。

6　讨论

本文工作依托国家重点研发计划项目(2020YFB1808100)，针对 5G 网络应用于典型垂直行

业中的网络安全和数据安全保障挑战, 设计一种云边端管多层次安全防护框架。其中典型行业之一是轨道交通行业, 在对其安全现状进行调研后, 行业反馈当前亟需解决的就是边界防护问题。我们根据 5G 安全框架和 SDN/NFV 技术特点, 提出了一种动态安全边界防护机制。

我们在本文中详述了机制的实现方式即动态安全边界防护模型、通用数学表达模型、核心算法, 并结合轨交行业实际, 将所提机制实例化, 以服务于工程实践。但在实验验证方面我们暂时仅做了基本验证, 并缺少与同类型工作的横向比较。经过文献调研, 暂时没有找到同类型研究成果。我们将在后续工作中搭建更完整的仿真环境, 将由 Matlab 模拟的安全边界生成算法改进为在 Ryu 中实现, 并设计更接近实际业务流和安全设备组成的网络拓扑和验证机制性能的相关实验, 通过具体的数值分析显示机制运行效果。

7 总结

本文提出了一种动态边界防护机制, 该机制包含边界防护生成算法和跨域安全设备调度算法。该机制以满足业务流量防护等级、最小化延迟为优化目标, 通过处理被恶意流量攻击的业务流量, 解决了以往采用网闸网关直接切断业务流的方式而导致的正常业务流无法正常运行的影响, 提高了业务流在边界设备上的通过率。我们还提出了一种云边端管多层次安全防护框架, 该框架根据工业场景的网络需求来部署动态安全边界防护机制。最后, 我们通过对所提出的动态安全边界防护机制和云边端管多层次安全防护框架进行实验模拟评估, 该机制能够有效地动态生成边界服务功能链并且达到控制不同防护等级业务流量通过的目标。

参考文献

[1] 5G-ACIA white paper “Security Aspects of 5G for Industrial Networks”, https://5g-acia.org/whitepapers/security-aspects-of-5G-for-industrial-networks/, Feb 2021.

[2] 3GPP TS 33.501. Security Architecture and Procedures for 5G System[S], 3GPP.

[3] Huawei Technologies Co., Ltd., White Paper on 5G Security Architecture, 2017.
(华为技术有限公司, 5G 安全架构白皮书, 2017.)

[4] Angermeier D, Wester H, Beilke K, et al. Security Risk Assessments: Modeling and Risk Level Propagation[J]. *ACM Transactions on Cyber-Physical Systems*, 2023, 7(1): 1-25.

[5] Varadharajan V, Tupakula U, Karmakar K K. Techniques for Enhancing Security in Industrial Control Systems[J]. *ACM Transactions on Cyber-Physical Systems*, 2024, 8(1): 1-36.

[6] Seeba M, Oja T, Murumaa M P, et al. Security Level Evaluation with F_4SLE[C]. *The 18th International Conference on Availability, Reliability and Security*, 2023: 1-8.

[7] Mancini F, Bianchi G. ScasDK - a Development Kit for Security Assurance Test in Multi-Network-Function 5G[C]. *The 18th International Conference on Availability, Reliability and Security*, 2023: 1-8.

[8] Fei W, Ohno H, Sampalli S. A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions[J]. *ACM Computing Surveys*, 2023, 56(5): 1-40.

[9] Kebande V R, Awad A I. Industrial Internet of Things Ecosystems Security and Digital Forensics: Achievements, Open Challenges, and Future Directions[J]. *ACM Computing Surveys*, 2024, 56(5): 1-37.

[10] Barrera D, Bellman C, Van Oorschot P. Security Best Practices: A Critical Analysis Using IoT as a Case Study[J]. *ACM Transactions on Privacy and Security*, 2023, 26(2): 1-30.

[11] Bansal A, Kandikuppa A, Hasan M, et al. System Auditing for Real-Time Systems[J]. *ACM Transactions on Privacy and Security*, 2023, 26(4): 1-37.

[12] Gao D L, Zhang Q M, Sun S J, et al. The Design of Holistic Vulnerability Measure Method Integrated with Topological Properties and Security Capabilities for Smart Grid Control System[C]. *2021 7th International Conference on Computer and Communications*, 2021: 1415-1419.

[13] Alavizadeh H, Alavizadeh H, Jang-Jaccard J. Cyber Situation Awareness Monitoring and Proactive Response for Enterprises on the Cloud[C]. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications*, 2020: 1276-1284.

[14] Degefa M Z, Sanchez S, Borgaonkar R. A Testbed for Advanced Distribution Management Systems: Assessment of Cybersecurity[C]. *2021 IEEE PES Innovative Smart Grid Technologies Europe*, 2021: 1-5.

[15] Simpson J J, Endicott-Popovsky B. 3.2.1 System Security Capability Assessment Model Development and Application[J]. *INCOSE International Symposium*, 2010, 20(1): 323-338.

[16] Lyu X R, Ding Y L, Yang S H. Safety and Security Risk Assessment in Cyber-Physical Systems[J]. *IET Cyber-Physical Systems: Theory & Applications*, 2019, 4(3): 221-232.

[17] Shangguan X L, Liu C. Analysis of EU’s National Network Security Capability Assessment Framework[J]. *Secrecy Science and Technology*, 2021(7): 53-59.
(上官晓丽, 刘畅. 欧盟《国家网络安全能力评估框架》解析[J]. *保密科学技术*, 2021(7): 53-59.)

[18] He H, Liu H F, Cheng J A. Research on Evaluation System and Index of Cloud Computing Platform Security Capability[J]. *Journal of Information Security Research*, 2020, 6(11): 990-995.
(贺海, 刘海峰, 成金爱. 云计算平台安全能力评估体系和评估指标研究[J]. *信息安全研究*, 2020, 6(11): 990-995.)

[19] IEC 62443-3-3:2013, Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels.

[20] Song Y. Research and Planning of Network Security Domain Divi-

sion and Boundary Integration[J]. *New Technology & New Products of China*, 2017(6): 147-148.
(宋杨. 网络安全域划分及边界整合研究与规划[J]. *中国新技术新产品*, 2017(6): 147-148.)

[21] Li W. *A research of network border protection*[D]. Chengdu: University of Electronic Science and Technology of China, 2018.
(李旺. 网络边防关键技术研究[D]. 成都: 电子科技大学, 2018.)

[22] Guo Rui, Chen Tao Research on the Practical Application of Security Domain Division in Enterprises [C]. *Information Network Security 2016 Supplement*, 2016: 163-168.
(郭睿, 陈涛. 安全域划分在企业中的实际应用研究[C].*信息网络安全 2016 增刊*, 2016: 163-168.)

[23] Ao L. Design and Deployment of Border Security in Multimedia Network[C]. *2022 IEEE 4th International Conference on Power, Intelligent Computing and Systems*, 2022: 195-198.

[24] Douglas Jacobson. Translated by Yang Liyou, Zhao Hongyu, et al. Fundamentals of Network Security. Beijing: Electronic Industry Press.
(Douglas Jacobson. 网络安全基础[M]. 仰礼友, 赵宏宇等译. 北京: 电子工业出版社.)

[25] Lin Y K. Analysis on the Comprehensive Utilization of Isolation Gateway and Firewall in Network Security[J]. *Network Security Technology & Application*, 2020(1): 14-15.
(林育凯. 浅析隔离网闸与防火墙在网络安全中的综合利用[J]. *网络安全技术与应用*, 2020(1): 14-15.)

[26] Wu Y T, Zhou J H. A Dynamic Orchestration and Deployment of Service Function Chaining Using NFV[J]. *Telecommunication Engineering*, 2022, 62(10): 1506-1513.
(吴宇彤, 周金和. 一种采用 NFV 架构的服务功能链动态编排与部署[J]. *电讯技术*, 2022, 62(10): 1506-1513.)

[27] Li T L. *The design and implement of multi-domain network security service orchestration system*[D]. Beijing: Beijing Jiaotong University, 2018.
(李天龙. 多域网络安全服务编排系统的设计与实现[D]. 北京: 北京交通大学, 2018.)

[28] Zhang C K, Cui Y, Tang H Y, et al. State-of-the-Art Survey on Software-Defined Networking (SDN)[J]. *Journal of Software*, 2015, 26(1).

[29] Alsmadi I, Xu D X. Security of Software Defined Networks: A Survey[J]. *Computers & Security*, 2015, 53: 79-108.

[30] Cao X, Fan G J, Wang H C. Network Security Architecture Based on SDN and NFV Technologies[J]. *Microcomputer Applications*, 2022, 38(1): 114-116.
(曹鑫, 范国璠, 王昊辰. 基于 SDN 和 NFV 技术的网络安全架构[J]. *微型电脑应用*, 2022, 38(1): 114-116.)

[31] IMT-2020 (5G) Promotion Group. White Paper. 5G Vision and Needs. 2014, 5.
(IMT-2020 (5G) 推进组. 白皮书. 5G 愿景与需求. 2014, 5.)

[32] Zhi M H, Yuan X, Zhang H W. Application Strategy of SDN and NFV in 5G Mobile Communication Network Architecture[J]. *Digital Communication World*, 2023(1): 66-68.
(支敏慧, 元鑫, 张华伟. 5G 网络架构中 SDN 和 NFV 的应用策略[J]. *数字通信世界*, 2023(1): 66-68.)

[33] Sun G, Li Y Y, Liao D, et al. Service Function Chain Orchestration across Multiple Domains: A Full Mesh Aggregation Approach[J]. *IEEE Transactions on Network and Service Management*, 2018, 15(3): 1175-1191.

[34] Huin N, Tomassilli A, Giroire F, et al. Energy-Efficient Service Function Chain Provisioning[J]. *Electronic Notes in Discrete Mathematics*, 2018, 64: 265-274.

[35] Kim S, Park S, Kim Y, et al. VNF-EQ: Dynamic Placement of Virtual Network Functions for Energy Efficiency and QoS Guarantee in NFV[J]. *Cluster Computing*, 2017, 20(3): 2107-2117.

[36] Tajiki M M, Salsano S, Chiaraviglio L, et al. Joint Energy Efficient and QoS-Aware Path Allocation and VNF Placement for Service Function Chaining[J]. *IEEE Transactions on Network and Service Management*, 2019, 16(1): 374-388.

[37] Chen Z, Feng G, Liu Y J, et al. Virtual Network Function Deployment Strategy Based on Improved Genetic Simulated Annealing Algorithm in MEC[J]. *Journal on Communications*, 2020, 41(4): 70-80.
(陈卓, 冯钢, 刘怡静, 等. MEC 中基于改进遗传模拟退火算法的虚拟网络功能部署策略[J]. *通信学报*, 2020, 41(4): 70-80.)

[38] Wei D S L, Xue K P, Bruschi R, et al. Guest Editorial Leveraging Machine Learning in SDN/NFV-Based Networks[J]. *IEEE Journal on Selected Areas in Communications*, 2020, 38(2): 245-247.

[39] Qu L, Assi C, Khabbaz M J, et al. Reliability-Aware Service Function Chaining with Function Decomposition and Multipath Routing[J]. *IEEE Transactions on Network and Service Management*, 2020, 17(2): 835-848.

[40] Wang Z N, Li J H, Tan C H, et al. Design and Analysis of Intelligent Service Chain System for Network Security Resource Pool[J]. *Chinese Journal of Network and Information Security*, 2022, 8(4): 175-181.
(王泽南, 李佳浩, 檀朝红, 等. 面向网络安全资源池的智能服务链系统设计与分析[J]. *网络与信息安全学报*, 2022, 8(4): 175-181.)

[41] Zhu X G. Network security equipment and technology[M]. Beijing: Tsinghua University Press, 2004.
(祝晓光. 网络安全设备与技术[M]. 北京: 清华大学出版社, 2004.)

[42] JIANG Jian chun, MA Heng tai, REN Dang en, et al. A Survey of Intrusion Detection Research on Network Security[J]. *Journal of Software*, 2000, 11(11): 1460-1466.
(蒋建春, 马恒太, 任党恩, 等. 网络安全入侵检测: 研究综述[J]. *软件学报*, 2000, 11(11): 1460-1466.)

[43] Zuo J X. *Research on key technologies of information system security evaluation*[D]. Beijing: Beijing University of Posts and Telecommunications, 2022.
(左金鑫. 信息系统安全性评价关键技术研究[D]. 北京: 北京邮电大学, 2022.)

[44] Xiao W D, Zhang X, Wang D B. Cross-Security Domain Dynamic Orchestration Algorithm of Network Security Functions[C]. *2022 7th IEEE International Conference on Data Science in Cyberspace*, 2022: 413-419.

[45] Xie R J, Cao J H, Li Q, et al. Disrupting the SDN Control Channel *via* Shared Links: Attacks and Countermeasures[J]. *IEEE/ACM*

Transactions on Networking, 2022, 30(5): 2158-2172.

[46] Cui Y J, Li H, Ruan H W, et al. Service Function Chain Deployment of Users' QoS and Network Resource-Awareness[J]. *Journal of Chinese Computer Systems*, 2021, 42(9): 1931-1937.
(崔雅君, 李华, 阮宏玮, 等. 用户 QoS 与网络资源感知的服务功能链部署方法[J]. *小型微型计算机系统*, 2021, 42(9): 1931-1937.)

[47] Mu Z P. On Algorithm of Functions Dynamic Orchestration in Virtualized Network[J]. *Journal of Southwest China Normal University* (*Natural Science Edition*), 2019, 44(6): 92-102.
(母泽平. 一种虚拟化网络功能启发式动态编排算法[J]. *西南师范大学学报(自然科学版)*, 2019, 44(6): 92-102.)

张莹(1999-), 于 2020 年在北京邮电大学通信工程专业获得学士学位。现在北京邮电大学信息与通信工程专业攻读硕士。主要研究方向为新一代无线网络架构与安全。Email: 2629355177@qq.com

王东滨(1978−), 黑龙江哈尔滨人, 博士。现在北京邮电大学担任教授、博士生导师, 主要研究方向为软件定义网络与安全、区块链、网络流量分析与模拟等。Email: dbwang@ bupt.edu.cn

陆月明(1969−), 江苏苏州人, 博士, 北京邮电大学教授, 博士生导师, 主要研究方向为网络安全防护、信任体系等。Email: ymlu@bupt. edu.cn

张勖(1973−), 上海人, 博士。现在北京邮电大学网络空间安全学院担任副教授, 主要研究方向为移动自组织网络安全、信息物理融合系统。Email: selina_zhangx@bupt.edu.cn

蔡昌俊(1965−), 湖北宜昌人, 博士, 广州地铁集团有限公司副总经理, 全国轨道交通设备管理创新“领军人物”, 交通部轨道交通领域专家, 主要研究方向为城市轨道交通智能运行、装备技术管理和工程应用。Email: caichangjun@gzmtr.com