基于马尔可夫过程的 5G 网络功能信任预测机制

张奕鸣[1], 刘彩霞[1], 刘树新[1], 潘 菲[1]

[1]中国人民解放军战略支援部队信息工程大学 郑州中国 450001

摘要 第五代移动通信网络(The 5th generation mobile network, 5G)已成为全球新一轮科技革命和产业革命的重要驱动力量, 服务功能日益完善, 面临的安全挑战更加复杂多样。传统防御方法主要通过创建网络边界保护网络内部安全, 所应用的网络形态较为单一。基于软件定义网络和虚拟化技术的 5G 网络愈加开放灵活, 网络边界逐渐消失, 需要新的安全理念。零信任理论适用于开放性网络的数据安全防护, 5G 核心网络是由网络功能组成的动态系统, 网络功能通信行为可抽象为马尔可夫过程, 网络功能信任模型是实现 5G 零信任安全的重要技术手段。针对此问题, 本文提出了基于马尔可夫过程的 5G 网络功能信任预测机制(Markov Network Function Trust Prediction, MNFTP), 此机制包含网络功能信任评估和信任预测。信任评估机制依据行为方式将网络功能分类为合法、伪装、非法, 层次分析访问请求安全威胁性并得出信任评分, 采用 k-means++算法将信任评分归类为五种信任状态。信任预测机制基于马尔可夫过程构建网络功能访问请求信任状态链, 结合时间因子和自适应奖惩因子计算马尔可夫状态转移矩阵, 通过求解转移矩阵平稳分布得出预测信任状态。最后, 网络功能基于预测信任状态抵御不可信的访问请求。实验表明, MNFTP 机制相对于现有信任预测机制对伪装网络功能和非法网络功能有更好的抑制效果和信任状态分类能力。

关键词 5G 网络功能; 信任模型; 零信任; 马尔可夫; 信任预测

中图法分类号 TP309 DOI 号 10.19363/J.cnki.cn10-1380/tn.2023.07.04

5G network function trust prediction mechanism based on Markov process

ZHANG Yiming[1], LIU Caixia[1], LIU Shuxin[1], PAN Fei[1]

[1] PLA Information Engineering University, Zhengzhou 450001, China

Abstract The 5th generation mobile network (5G) has become an important driving force for a new round of technological and industrial revolutions in the world, with increasingly improved service functions and more complex and diverse security challenges. The traditional defense method mainly protects the internal security of the network by creating network boundaries, and the applied network form is relatively simple. 5G based on software-defined network and virtualization technology are becoming more open and flexible, and the network boundaries are gradually disappearing, requiring new security concepts. Zero trust theory is suitable for data security protection of open networks. The 5G core network is a dynamic system composed of network functions. The communication behavior of network functions can be abstracted into Markov process. The network function trust model is an important technology to realize 5G zero trust security. In response to this problem, this paper proposes Markov Network Function Trust Prediction (MNFTP) mechanism, which includes network function trust evaluation and trust prediction. The trust evaluation mechanism classifies the network functions into legal, fake, and illegal according to the behavior mode, performs hierarchical analysis on the security threat of network function access requests and obtains the trust score. The k-means++ algorithm is used to classify the trust score into five trust states. The trust prediction mechanism constructs the network function access request trust state chain based on the Markov process, calculates the Markov state transition matrix by combining the time factor and the adaptive reward-punishment factor, and solves the stable distribution of the transition matrix to obtain the predicted trust state. Finally, the network function defends against untrusted access requests based on the predicted trust state. Experiments show that the MNFTP mechanism has a better suppression effect and trust status classification ability than the existing trust prediction mechanism for fake and illegal network functions.

Key words 5G network function; trust model; zero trust; markov; trust prediction

通讯作者: 张奕鸣, 硕士研究生, Email:zym913914944@163.com。

本课题得到国家科技重大专项(No. 2018ZX03002002)资助。

收稿日期: 2022-01-03; 修改日期: 2022-03-10; 定稿日期: 2023-04-18

1 引言

当前 5G 网络的商业化建设正在全球范围内开展, 新一代移动通信网络给人们带来更大的连接容量、更高的数据传输速率和更低的数据传输时延。随着 5G 网络的快速发展, 5G 网络引入的新架构、新技术、新场景对于 5G 网络安全而言成为了新挑战, Jing Qiu 等人分析了 5G 人工智能应用面临的对抗性样本扰动的安全威胁, 通过实验证明白盒攻击和黑盒攻击都能使 5G 深度学习模型失效[1]。5G 网络引入的 HTTP/2 协议给攻击者带来了新的攻击面, 易引发拒绝服务攻击, 造成网络瘫痪[2-5]。Hu 等人研究分析了 5G 核心网络身份认证协议和非接入层协议存在的安全缺陷[6-8]。Alotaibi 分析了 5G 网络切片面临的资源隔离和移动管理方面的安全挑战[9]。高安全性的 5G 网络越来越成为运营商和用户的迫切需要。如何针对 5G 网络诸多新特性构建 5G 网络安全防护能力成为亟待解决的问题。

传统网络安全机制通过建立网络物理边界来防护网络内设备和应用的安全, 主要使用防火墙[10-11]、边界关防[12]等划分边界的技术对外来用户或者设备的访问进行检查过滤, 其所应用的主要网络场景特点是网络较为封闭, 网络边界突出, 网络与网络之间的交互较少。5G 网络瞄准的移动增强带宽、大规模机器连接和高可靠低时延三大应用场景皆是对传统网络的一次颠覆, 5G 网络的虚拟化[13-14]和软件定义网络[15-16]等技术使网络物理边界更加模糊甚至消失, 传统网络安全机制现已不再适应于 5G 网络, 需要新的理念和技术。

2010 年 Forrester 研究公司分析师 John Kindervag 首次提出了零信任理念[17], 其核心内容是不再以物理边界作为网络信任边界, 而是以身份验证为基础, 通过对网络内外所有用户、设备、业务的持续信任评估检测、动态访问控制和最小化主动授权来保护网络信息数据安全。信任模型是实现零信任中持续信任评估的一项重要机制, 通过对用户行为方式画像并建立用户信任模型实现用户的持续信任评估, 并将信任评分作为对用户实施访问控制的依据。基于零信任思想, 对 5G 网络功能所在网络环境和访问请求行为持续监控并对网络功能行为进行信任评分, 建立 5G 网络功能的信任模型, 无疑是 5G 网络实施新型访问控制的重要技术思路。当前有部分研究者对 5G 网络信任模型开展了研究, Niu 等人提出基于云模型的 5G 网络切片信任计算模型[18], 将用户评价、历史信任和动态奖惩机制综合分析来计算网络切片信任度。Baker 等人提出了零信任增强加密模型[19], 对 5G 网络中所有数据提供端到端的加密。Wong 分析了 2G 到 5G 信任模型的演变, 提出基于贝叶斯网络的 5G 网络信任模型[20]。Surridge 等人介绍了通过 5G-ENSURE 项目中的 Trust Builder 工具分析 5G 网络威胁、依赖关系和信任关系的方法[21]。Han 等人提出了信任区概念作为 5G 网络身份认证和授权的解决方案[22], 信任区包含一组同一地理区域的网络功能, 信任区内自主实施不同的访问策略来保证数据安全。综上所述, 将零信任理念和信任模型应用于 5G 网络切片安全和数据安全已有理论基础, 如何利用信任模型实现 5G 网络功能安全仍处于研究探索阶段。

5G 网络可以视为由网络功能组成的系统, 网络功能依据访问请求安全威胁性的差异具有不同的信任状态, 通信过程中的网络功能可以视为处于动态信任状态空间, 并在其中进行信任状态转换, 马尔可夫过程是研究离散事件动态系统状态空间的重要理论, 可以刻画描述 5G 网络功能在通信过程中的信任状态转换。基于上述分析, 本文立足于 5G 网络功能安全领域, 针对如何构建 5G 网络功能信任模型并对网络功能行为进行信任预测的问题, 基于零信任思想, 设计提出了基于马尔可夫过程的网络功能信任预测机制 MNFTP。该机制包含 5G 网络功能信任评估和信任预测两个子机制, 信任评估机制对网络功能的一次访问请求根据其安全风险性的高低给出合适的信任评分, 信任预测机制基于网络功能历史访问请求信任评分并结合信任评分“缓增加、快降低、随时间衰减”的特征得出网络功能预测信任状态, 基于预测信任状态拒绝安全风险性高的访问请求从而保护 5G 网络功能。

本文主要贡献可以概括如下:

(1)提出一种针对 5G 网络功能的信任预测机制 MNFTP, MNFTP 包含信任评估机制和信任预测机制。信任评估机制基于行为将 5G 网络功能分为合法、伪装和非法三类, 分析每一类网络功能所具备的行为特点, 将网络功能的访问请求分为请求方法、请求服务、请求内容三个元素, 使用层次分析法细粒度分析访问请求三个元素的安全风险性, 计算访问请求三个元素的信任评分从而得出访问请求信任评分, 将 5G 网络功能信任状态从完全可信到完全不可信分为五种, 采用 k-means++算法对合法网络功能访问请求信任评分集合聚类得出信任评分到信任状态的映射关系从而得出访问请求所属信任状态。

(2)信任预测机制基于时间尺度构建网络功能访

问请求信任状态链, 将网络功能通信过程视为马尔可夫过程, 将访问请求信任状态链映射于马尔可夫链建立网络功能通信行为信任模型, 结合时间因子和奖惩因子计算马尔可夫平稳分布, 动态预测 5G 网络功能信任度, 从而过滤或拒绝不可信的 5G 网络功能请求, 保障 5G 网络功能的安全可信运行。

本文的结构如下: 第 2 节介绍了 5G 网络信任模型研究现状; 第 3 节介绍了 MNFTP 中信任评估和信任预测机制框架; 第 4 节介绍了 MNFTP 机制仿真实验流程和结果并与相关信任机制进行对比; 第 5 节为讨论; 第 6 节对文章总结。

2 相关工作

当前, 基于信任模型的 5G 网络安全防护领域, 具有代表性的研究工作总结如表 1 所示。现有研究所针对的重点领域是 5G 网络数据完整性保护和网络恶意实体检测, 随着区块链技术和人工智能的快速发展, 有研究学者利用区块链的去中心化特性和共识机制保护 5G 网络数据完整性并达到数据可追溯的目的, 然而区块链技术共识阶段带来的时间开销大、可扩展性较低的痛点问题还未得到充分解决, 对于 5G 网络海量数据场景的应用仍有待研究。也有研究学者基于人工智能的强化学习技术检测识别 5G 网络恶意节点, 绕过恶意丢弃数据的节点, 提高 5G 数据包在传送链路中的转发效率, 而当前研究工作重点在于识别以丢弃数据为主要行为的恶意节点, 节点行为较单一, 且面临人工智能模型可解释性较差的问题。

在 5G 网络技术相关领域, 如云计算、物联网、边缘计算等也有相关信任模型研究, Ritu 和 Sushma Jain 提出了使用服务质量(Quality of Service, QoS)衡量云计算提供商信任值[23], Fenglian Jiang 等人着眼于边缘计算中网络节点服务器之间的安全问题, 建立了基于移动边缘计算基站节点的信任机制, 提出了基于信任机制的数据传输模式[24], Adewuyi 等人针对物联网的安全威胁管理设计了信任管理框架[25]。Ning Hu 等人基于边缘计算和分散计算思想提出了一种物联网的节能计算范式, 有效降低了云服务器计算负载[26], 也为 6G 网络提出了一种高效的网络计算模式, 将集成网络功能的计算平台代替传统网络设备[27]。

表 1 5G 网络信任模型相关技术研究

Table 1 Research on related technologies of 5G network trust model

研究领域	论文题目	发表时间	研究内容	存在问题
5G 网络设备到设备(D2D)通信	Trust-based and social-aware coalition formation game for multihop data uploading in 5G systems[28]	2016	为 5G 网络 D2D 内容上传建立信任约束模型, 将设备间通联关系和历史信任作为衡量标准	仅针对恶意设备丢弃数据的行为进行防护, 未考虑恶意设备修改或损坏数据的情况
5G 网络恶意实体检测	A Hybrid Reinforcement Learning-Based Trust Model for 5G Networks[29]	2020	基于强化学习构建 5G 网络混合信任模型, 检测识别 5G 网络恶意实体	仅检测识别恶意丢弃数据包的实体, 未考虑实体其他恶意行为
超 5G(B5G)网络信息安全	Blockchain and AI Empowered Trust-Information-Centric Network for Beyond 5G[30]	2020	基于区块链和人工智能为 B5G 节点设计信息流通方案, 动态量化 B5G 节点信任度	随着 B5G 节点数目的增加, 区块链共识阶段消耗的时间成指数级增长
5G 网络数据保护	Trust in 5G and Beyond Networks[31]	2021	使用区块链分块存储 5G 网络流量数据哈希值, 以保证数据完整性和可追溯	区块链共识协议的去中心化的特点限制了数据交易吞吐量和速度, 增加了处理数据的计算、存储和通信开销
	5G Intelligent Network Trust Model Based on Subjective Logic[32]	2021	通过扩展 J sang 等人提出的主观逻辑使其应用于 5G 智能网络, 判断数据可信度	时空消耗相对于传统模型有所增加

5G 网络功能作为 5G 核心网的控制节点和数据节点, 承担了用户认证、信令下发、数据传输、数据存储等重要任务, 其面临的安全考验不容忽视。当前针对 5G 网络功能信任评估和预测的研究仍有待开展, 本文基于 5G 网络功能访问请求行为安全性设计了 5G 网络功能信任评估模型, 依据信任评估模型的评估结果对 5G 网络功能信任度进行动态预测, 实现网络功能信任的实时监测, 以达到防护 5G 网络安全的目的。

3 基于马尔可夫过程的网络功能信任预测机制 MNFTP

5G 网络使用虚拟化技术将各个网络功能从以往的固定物理设备中抽离出来, 将物理设备中的硬件资源编排整合以实现网络功能从创建到销毁的生命周期软件化管理, 虚拟化技术提高了 5G 网络功能编排的灵活性和物理资源的利用率, 然而这也为 5G 网络功能安全防护提出了更高的挑战, 恶意攻击者可以通过木马病毒和软件漏洞入侵 5G 网络功能编排管理器[33-34], 从而将精心设计的恶意网络功能安插于网络之中, 造成数据泄漏和拒绝服务等不良后果。

MNFTP 定义 5G 网络功能处于两种状态之中, 一是未被攻击者控制的网络功能即能够正常提供服务, 发送正常的访问请求; 二是已被攻击者控制的网络功能, 在此状态中的网络功能通常表现为两种行为模式, 第一种行为模式是伪装模式, 即攻击者希望被控制的网络功能具有良好的隐蔽性, 通常情况下保持原有网络功能的行为特征, 当网络环境或网络功能状态达到预期后攻击者再控制网络功能发送具有严重威胁性的非法请求企图对网络造成严重破坏。第二种行为模式是非法模式, 当攻击者并不了解当前网络的弱点和漏洞时, 攻击者通常会控制网络功能发送各种非法请求以探测网络中存在的安全漏洞, 因此网络功能的非法行为模式是发送各种类型、严重性各异的非法请求。

鉴于上述分析, 本文提出了基于马尔可夫过程的 5G 网络功能信任预测机制 MNFTP, 包括网络功能信任评估机制和网络功能信任预测机制。信任评估机制拆解分析网络功能访问请求的三个信任元素(请求方法、请求服务、请求内容), 综合计算每个信任元素的信任值得出访问请求的信任值并基于信任值等级聚类的方法得出网络功能一次访问请求的信任状态。信任预测机制将网络功能历史所有访问请求视为马尔可夫过程, 结合时间因子和奖惩因子计算马尔可夫信任状态预测矩阵, 通过求解预测矩阵平稳分布进而预测网络功能未来访问请求的信任状态, MNFTP 整体框架如图 1 所示。5G 网络中网络存储功能(Network Repository Function, NRF)和统一数据存储功能(Unified Data Repository, UDR)都担任着信息数据管理者的角色, NRF 存储并管理各类网络功能的实例信息, UDR 存储并管理用户的鉴权向量等结构化数据。由于 NRF 和 UDR 管理着 5G 网络和用户的重要数据, 因此成为攻击者的重点攻击对象, 本文以 NRF 和 UDR 为基础设计实现 5G 网络功能信任预测机制, 评估预测 5G 网络中访问 NRF 和 UDR 服务的网络功能的信任度。

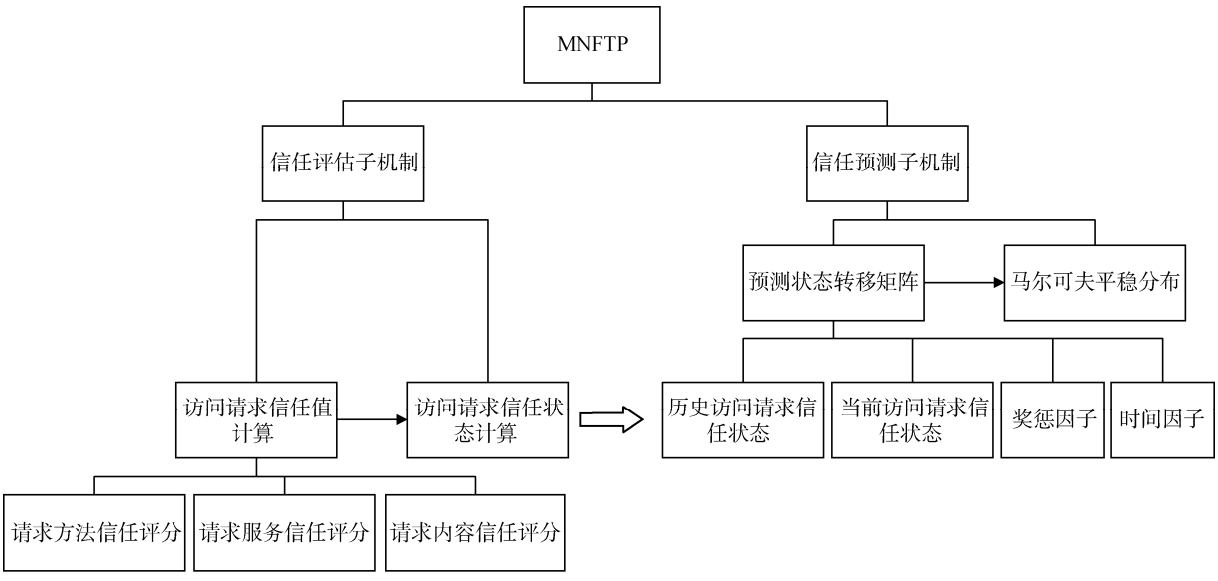

图 1 零信任马尔可夫过程的网络功能信任预测机制框架

Figure 1 The framework of MNFTP

3.1 网络功能信任评估机制

5G 网络基于服务化架构设计, 网络功能间通过服务化接口发送访问请求, 服务化接口的通信协议在最上层是由 Restful API 封装[35]。Restful API 形式的访问请求由三种元素组成, 分别是请求方法、请求服务和请求内容。因此访问请求信任值的计算包含三部分, 请求方法信任评分、请求服务信任评分和请求内容信任评分。

3GPP 协议 TS.29501[36]中规定的 5G 网络功能 Restful API 的请求方法包含四种, 分别是 POST、DELETE、PUT 和 GET, 对应于网络功能的新增、删除、修改、查询四种操作。对请求方法的安全威胁性进行分析, 5G 网络功能使用 GET 请求方法查找 NRF 中指定网络功能实例的具体信息或 UDR 中指定用户的鉴权向量, GET 方法无法对数据造成破坏和污染, 但有可能造成数据泄漏, 安全威胁相对较低。5G 网络功能使用 POST 和 PUT 请求方法在 NRF 中注册新的网络功能实例或者修改现有网络功能实例信息, 两种请求方法皆可使 NRF 网络功能数据变动, 造成数据污染, 安全威胁相对中等。5G 网络功能使用 DELETE 请求方法删除 NRF 中指定的网络功能实例信息或是 UDR 中指定的用户鉴权向量信息, 当 DELETE 方法被攻击者利用时可能会造成 5G 网络数据不可逆的破坏, 安全威胁相对较高。因此 MNFTP 所构造的请求方法信任评分如表 2 所示, 分值越高表示请求方法的安全威胁越小。

表 2 请求方法信任评分

Table 2 Request method trust score

请求方法	信任评分
GET	1.0
PUT	0.9
POST	0.9
DELETE	0.8

5G 网络的 NRF 和 UDR 网络功能将自身服务以 Restful API 的形式对外提供, 本文分析的 5G 网络功能请求服务包含四种, 分别是 NRF 的网络功能实例发现服务、网络功能实例管理服务、令牌获取服务和 UDR 的数据管理服务。对请求服务的安全威胁性进行分析, NRF 的网络功能实例发现服务支持 5G 网络功能使用查询操作在 NRF 中查找指定类型或指定 ID 的网络功能, 有可能造成网络功能实例信息泄漏, 不会产生数据破坏, 安全威胁较低。NRF 网络功能实例管理服务支持 5G 网络功能注册、修改原实例信息和删除原实例信息, 当被攻击者利用时易造成数据损坏, 难以修复, 安全威胁相对较高。NRF 的令牌获取服务支持网络功能通过 NRF 获取访问其他网络功能服务的令牌, 令牌敏感性较高, 在遭到中间人攻击时令牌可能会被攻击者窃取导致非法访问服务, 安全威胁相对较高。UDR 的数据管理服务支持对用户身份鉴权数据的查询和修改, 有使用户数据遭到泄漏和污染的风险, 安全威胁相对较高。鉴于上述分析 MNFTP 所构造的请求服务信任评分如表 3 所示, 分值越高表示请求服务的安全威胁越小。

表 3 请求服务信任评分

Table 3 Request service trust score

请求服务	信任评分
NRF-网络功能实例发现	1.0
NRF-网络功能实例管理	0.9
NRF-令牌获取	0.9
UDR-数据管理	0.9

基于以上对 NRF 和 UDR 网络功能服务的分析, 依据 3GPP 协议 TS.29510[37]中描述的 NRF 网络功能服务正常访问请求内容和 3GPP 协议 TS.29504[38]描述的 UDR 网络功能正常访问请求内容, 设计了恶意请求匹配项表(见表 4)用于计算请求内容信任评分, 请求内容信任评分满分为 1.0, 当请求内容满足表中匹配项, 则扣除相应惩罚分数, 最终得出请求内容信任评分, 分值越高表示请求内容的安全威胁越小。

网络功能信任评估机制通过层次分析法对 5G 网络功能访问请求进行细粒度分析, 将访问请求分解为请求方法、请求服务和请求内容三个部分分别计算信任评分, 对访问请求的每个部分进一步拆解, 研究其被攻击者利用时所能够造成的安全威胁严重性, 由此赋予信任评分, 最终三个部分信任评分相乘得出网络功能一次访问请求的信任评分, 网络功能访问请求信任评估机制框架如图 2 所示。

3.2 网络功能信任预测机制

基于网络功能信任评估机制, 可计算得出 5G 网络中所有访问 NRF 和 UDR 服务的网络功能访问请求的信任评分, 网络功能信任预测机制使用马尔可夫过程对网络功能的访问请求过程建模, 能够结合历史请求信任评分对网络功能未来的信任状态进行动态预测, 更好地体现网络功能相邻访问请求之间的信任相关性。信任预测机制将网络功能的信任状态分为五种, 分别是完全可信、可信任、一般可信、不可信和完全不可信, 使用 k-means++聚类算法将信任评估机制得出的访问请求信任评分映射到五种信任状态中。MNFTP 对来访的网络功能建立其访问请

求马尔可夫预测向量, 计算其状态转移矩阵, 将时间因子和奖惩因子与状态转移矩阵相结合构建预测状态转移矩阵, 最终基于预测状态转移矩阵得出当前时刻来访的网络功能信任状态平稳分布, 将平稳分布中取得最大概率的状态作为网络功能的预测信任状态。

表 4　恶意请求匹配项

Table 4　Malicious request matches

请求服务	请求操作	恶意请求内容匹配项	惩罚分数
NRF-网络功能实例发现	注册网络功能实例	恶意匹配项 1: 同一个网络功能 ID 创建多个网络功能实例	0.3
NRF-网络功能实例管理	查询网络功能实例	恶意匹配项 2: 请求内容中源 IP 未在 NRF 中注册	0.6
		恶意匹配项 3: 请求内容中网络功能类型与源 IP 所注册的网络功能类型不符	0.3
	修改/删除网络功能实例	恶意匹配项 4: 请求内容中源 IP 未在 NRF 中注册	0.6
		恶意匹配项 5: 请求服务中网络功能 ID 与请求内容源 IP 所注册的网络功能 ID 不符	0.3
NRF-令牌获取	获取网络功能访问令牌	恶意匹配项 6: 源网络功能类型不属于 UDM、PCF、NEF	0.3
UDR-数据管理	查询 UDR 中用户鉴权数据	恶意匹配项 7: 请求内容中网络功能类型与源 IP 所注册的网络功能类型不符	0.6

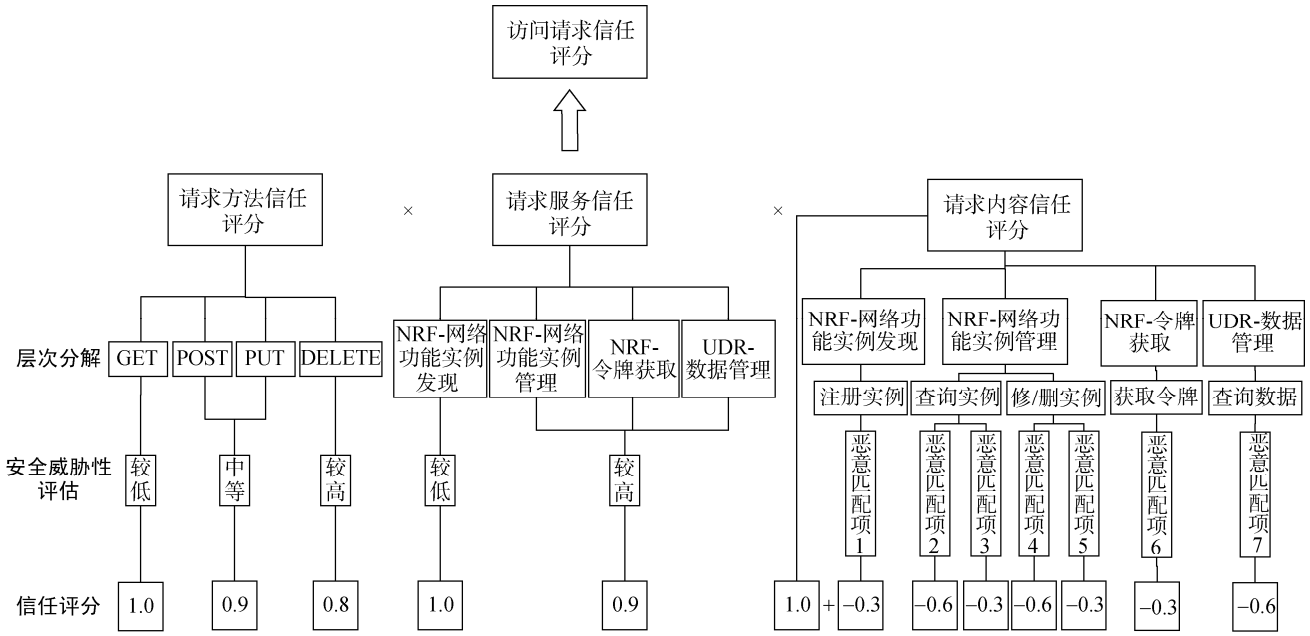

图 2　信任评估机制框架

Figure 2　The framework of Trust evaluation mechanism

3.2.1　建立网络功能马尔可夫预测向量

本文基于 NRF 和 UDR 网络功能进行信任预测机制设计, 信任预测机制位于 5G 网络服务化架构的数据总线之中, NRF 和 UDR 网络功能位于信任预测机制之后, 如图 3 所示。信任预测机制对于访问 NRF 和 UDR 的网络功能建立其马尔可夫预测向量, 马尔可夫预测向量包括网络功能标识符、网络功能历史访问请求信任状态、当前访问请求信任状态和奖惩因子。信任预测机制对于来访的每一个网络功能都给予其唯一的标识符, 历史访问请求信任状态是信任评估机制对来访的网络功能上一次访问请求作出的信任状态评估, 当前访问请求信任状态是信任评估机制对来访的网络功能本次访问请求的信任状态评估。在人类认知中信任值具有缓慢上升, 快速下降

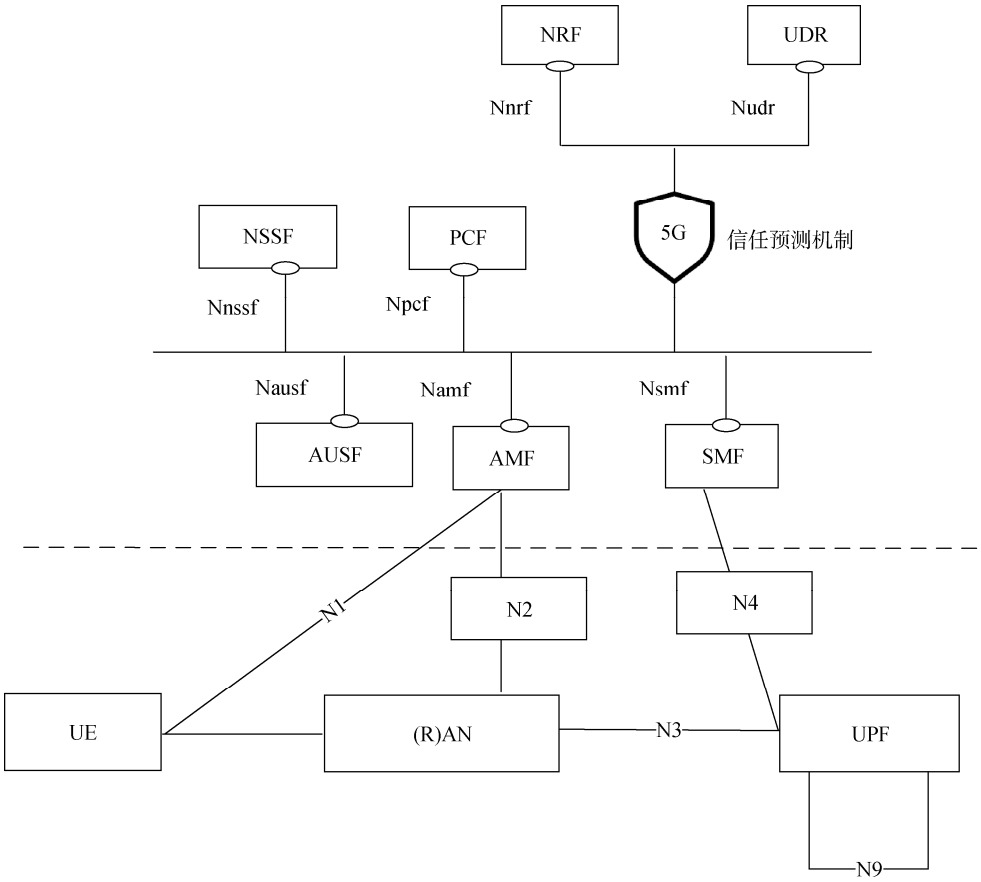

图 3　5G 网络中信任预测机制

Figure 3　Trust prediction mechanism in 5G network

的特性, 网络功能通过大量合法正常的访问请求建立的高信任值在少数非法访问请求之后就会消失, 信任值还具有随着时间延续衰减的特征, 网络功能近期访问请求的信任状态更应受到重视, 在预测未来信任状态时应对更早的访问请求给予更多的衰减, 为了实现信任值“慢上升、快下降、随时间衰减”的特征并有效抑制被攻击者控制的网络功能的访问请求行为, 本文引入了奖惩因子和时间因子。基于马尔可夫过程的无后效性, 奖惩因子依据网络功能的历史访问请求信任状态和当前访问请求信任状态自适应动态调整。

设 C_i 为网络功能第 i 次访问请求的奖惩因子, h 为网络功能历史访问请求信任状态, l 为网络功能当前访问请求信任状态, 使用数字 0,1,2,3,4 分别表示完全可信, 可信任, 一般可信, 不可信, 完全不可信五种信任状态, 奖惩因子的计算公式如(1)所示, 本文使用 sigmoid 函数作为奖惩因子基本调整函数, 其优点是奖惩梯度较为平滑, 避免因子剧烈变化导致信任预测值较难收敛, 其中 d_1, d_2 为调整因子, d_3 为奖惩因子的默认值。

$$C_i = F(C_{i-1},h,l) = \begin{cases} \dfrac{d_1}{1+e^{-C_{i-1}}} & h \in \{0,1\}, l \in \{3,4\} \\ \dfrac{1}{C_{i-1}} & h \in \{2,3,4\}, l \in \{0,1\} \\ \dfrac{d_2}{1+e^{-C_{i-1}}} & h \in \{3,4\}, l \in \{3,4\} \\ d_3 & others \end{cases} \tag{1}$$

3.2.2　构建网络功能预测状态转移矩阵

信任预测机制对访问 NRF 和 UDR 的网络功能基于其马尔可夫预测向量建立状态转移矩阵, 状态转移矩阵记录网络功能在以往的访问请求中从一个信任状态转移到另一个信任状态的频率, MNFTP 将网络功能的五种信任状态设定为马尔可夫过程的五种状态, 转移矩阵中的元素表示此网络功能从矩阵相应行所代表的信任状态转移到矩阵相应列所代表的信任状态的频率。MNFTP 结合奖惩因子和马尔可夫预测向量计算状态转移矩阵, 结合时间因子和状态转移矩阵计算预测状态转移矩阵, 算法如下。

表 5 算法主要参数符号定义

Table 5 Definition of the algorithm parameter symbol

参数	定义
$\boldsymbol{V}(id, h, l, C_i)$	网络功能的马尔可夫预测向量
id	网络功能标识符
hs	网络功能历史访问请求信任状态, 初始化为 4(完全不可信)
ls	网络功能当前访问请求信任状态
$R=(R[1], R[2], ..., R[n])$	网络功能访问请求序列
T	信任评估机制, 输出访问请求信任状态
F	奖惩因子计算函数, 如公式(1)所示
C_i	网络功能第 i 次请求的奖惩因子
t	时间因子
$\boldsymbol{M}_{id}$	网络功能状态转移矩阵, 矩阵元素初始化为 $1/v$, v 是状态数, 本文中为 5
$\boldsymbol{PM}_{id}$	网络功能预测状态转移矩阵

算法 1. MNFTP 机制网络功能预测状态转移矩阵算法

输入: $\boldsymbol{V}, R, C_i, t$

输出: $\boldsymbol{M}_{id}, \boldsymbol{PM}_{id}$

1) FOR $i = 1$ TO n DO

2) $ls = T(R[i])$

3) $C_i = F(C_{i-1}, hs, ls)$

4) $\boldsymbol{PM}_{id} = t * \boldsymbol{M}_{id}$

5) $\boldsymbol{PM}_{id}[h][l] = \boldsymbol{PM}_{id}[h][l] + C_i$

6) $\boldsymbol{M}_{id}[h][l] = \boldsymbol{M}_{id}[h][l] + C_i$

7) $hs = ls$

8) END

9) RETURN $\boldsymbol{M}_{id}, \boldsymbol{PM}_{id}$

通过上述算法得出网络功能预测状态转移矩阵 $\boldsymbol{PM}_{id}$ 后, 计算预测状态转移矩阵的马尔可夫平稳分布 $\boldsymbol{X}$, 将平稳分布 $\boldsymbol{X}$ 作为网络功能的信任预测向量, 选择平稳分布中取得最大概率的信任状态作为网络功能的预测信任状态, 计算方法如下。

算法 2.网络功能预测信任状态算法

输入: $\boldsymbol{PM}_{id}$

输出: 网络功能预测信任状态 $State_{id}$

1) $$\boldsymbol{PM}_{id}=\begin{bmatrix} P_{11},P_{12},P_{13},P_{14},P_{15} \\ P_{21},P_{22},P_{23},P_{24},P_{25} \\ P_{31},P_{32},P_{33},P_{34},P_{35} \\ P_{41},P_{42},P_{43},P_{44},P_{45} \\ P_{51},P_{52},P_{53},P_{54},P_{55} \end{bmatrix}$$

2) 设平稳分布 $\boldsymbol{X}=(x_1, x_2, x_3, x_4, x_5)$

3) 根据平稳分布定义可得

$$\boldsymbol{X}\cdot\boldsymbol{PM}_{id}=(x_1,x_2,x_3,x_4,x_5)\begin{bmatrix} P_{11},P_{12},P_{13},P_{14},P_{15} \\ P_{21},P_{22},P_{23},P_{24},P_{25} \\ P_{31},P_{32},P_{33},P_{34},P_{35} \\ P_{41},P_{42},P_{43},P_{44},P_{45} \\ P_{51},P_{52},P_{53},P_{54},P_{55} \end{bmatrix}$$

$$=\boldsymbol{X}$$

$$=(x_1, x_2, x_3, x_4, x_5)$$

4) 展开得

$$\begin{cases} P_{11}x_1+P_{21}x_2+P_{31}x_3+P_{41}x_4+P_{51}x_5=x_1 \\ P_{12}x_1+P_{22}x_2+P_{32}x_3+P_{42}x_4+P_{52}x_5=x_2 \\ P_{13}x_1+P_{23}x_2+P_{33}x_3+P_{43}x_4+P_{53}x_5=x_3 \\ P_{14}x_1+P_{24}x_2+P_{34}x_3+P_{44}x_4+P_{54}x_5=x_4 \\ P_{15}x_1+P_{25}x_2+P_{35}x_3+P_{45}x_4+P_{55}x_5=x_5 \\ x_1+x_2+x_3+x_4+x_5=1 \end{cases}$$

5) 求解方程组得 $x_i=F_i(P_{11}, P_{12}, ..., P_{55})$, i=1,2,3,4,5, 其中 F_i 是 x_i 的解函数

6) $max = 0$

7) FOR $i = 1$ TO 5 DO

8) IF $x_i > max$ THEN

9) $max = x_i$

10) $State_{id} = i$

11) RETURN $State_{id}$

4 实验描述及分析

为了避免危害真实 5G 网络的安全性, 同时评估所提信任预测机制的性能指标, 进行仿真实验, free5gc 是一款开源的 5G 核心网实验平台, 实现了(Access and Mobility Management Function, AMF)、(Authentication Server Function, AUSF)、NRF、UDR 等网络功能的基础服务, 本文将 free5gc 平台部署于 10GB 内存, 8 核处理器, 64 位 ubuntu 操作系统之上。实验在 free5gc 平台上设置了 1000 个网络功能对 NRF 和 UDR 进行访问, 其中 800 个网络功能是未被攻击者控制的, 100 个网络功能是被攻击者控制并处于伪装行为模式, 100 个网络功能是被攻击者控制并处于非法行为模式, 为了简洁方便, 将这三种网络功能分别命名为合法网络功能、伪装网络功能和非

法网络功能。

实验针对 NRF 的网络功能实例发现、网络功能实例管理、令牌获取服务和 UDR 的数据管理服务设计了相应的正常访问请求和具有不同安全威胁性的非法访问请求。为了模拟真实网络功能行为, 在仿真实验中, 合法网络功能有 95%的可能性向 NRF 和 UDR 发送合法访问请求, 有 5%的可能性由于配置错误或者链路噪声故障而发送非法请求; 伪装网络功能为了隐蔽自身有 80%的可能性向 NRF 和 UDR 发送合法请求, 有 20%的可能性发送安全威胁性较高的非法请求; 非法网络功能为了寻找网络漏洞有 80%的可能性发送各类非法请求, 有 20%的可能性发送合法请求。实验中每个网络功能发送 500 次访问请求, 通过信任评估机制对每个网络功能的每次访问请求进行信任评分, 得到每个访问请求的信任评分 s 和信任评分向量(信任评分向量包括请求方法评分 a, 请求服务评分 b, 请求内容评分 c), 之间的关系是 $s=a*b*c$。为了将信任评分与五种信任状态进行映射, 使用 k-means++聚类算法对合法网络功能的访问请求信任评分向量集合进行聚类, 具体步骤如下。

Step1.构建合法网络功能的访问请求信任评分向量集合 $G=\{\boldsymbol{v_1},\boldsymbol{v_2},\ldots,\boldsymbol{v_n}\}$, 其中 $\boldsymbol{v_k}$ 代表第 k 个信任评分向量, $\boldsymbol{v_k}=(a_k,b_k,c_k)$,$1\leqslant k\leqslant n$。

Step2.对集合 G 的信任评分向量按照其总信任评分的大小进行排序, 由于实验中合法网络功能有 95%的概率发送合法访问请求, 因此选择排序后信任评分在前 95%的信任评分向量构建子集合 $G_1=\{\boldsymbol{v_1},\boldsymbol{v_2},\ldots,\boldsymbol{v_m}\}$, 选择信任评分在后 5%的信任评分向量构建子集合 $G_2=\{\boldsymbol{v_{m+1}},\boldsymbol{v_{m+2}},\ldots,\boldsymbol{v_n}\}$。

Step3.使用 k-means++聚类算法分别对 G_1, G_2 集合进行聚类, 使用欧式距离作为算法距离计算方法, 算法最大迭代次数为 100, 聚类质心误差容忍最小值为 0.001, 对 G_1 聚类时算法类别数 k=3, 对 G_2 聚类时算法类别数 k=2。G_1 聚类结果 $G_1=\{G_{11},G_{12},G_{13}\}$, G_2 聚类结果 $G_2=\{G_{21},G_{22}\}$。

Step4.计算 $G=\{G_{11},G_{12},G_{13},G_{21},G_{22}\}$每一类中包含的信任评分范围, 由高至低排序, 排序后的结果映射到完全可信, 可信任, 一般可信, 不可信, 完全不可信五种信任状态, 最终映射结果如表 6 所示。

表 6 信任状态映射表

Table 6 Trust states mapping

信任状态	0(完全可信)	1(可信任)	2(一般可信)	3(不可信)	4(完全不可信)
信任评分范围	[1.0, 0.86)	[0.86, 0.71)	[0.71, 0.64)	[0.64, 0.34)	[0.34, 0]

为了评估信任预测机制的性能, 实验将 MNFTP 机制与文献[18]提出的动态历史信任评估算法(Dynamic history, DH)和文献[20]提出的基于贝叶斯网络的 5G 网络实体信任预测算法(Bayes network, BN)进行对比。动态历史评估算法依据网络功能历史所有访问请求信任状态并结合历史权重系数预测未来请求信任状态。贝叶斯网络是刻画随机变量相关性的数学理论, 能够描述通信过程中网络功能行为的信任相关性。贝叶斯网络信任模型基于贝叶斯公式 $P(e\,|\,h)=\dfrac{P(e)\cdot P(h\,|\,e)}{P(h)}$ 和全概率公式 $P(y)=\sum_{i=1}^{n}P(v_i)P(y\,|\,v_i)$, 其中 h 作为网络功能历史访问请求信任状态, e 为网络功能的未来预测信任状态, y 为最终分类的信任状态, v_i 为第 i 种信任状态, n 为状态类别数。一个网络功能历史访问请求序列可看作贝叶斯网络中的一条路径, 如图 4 所示, 箭头中数字代表网络功能标识符, 圆圈中数字代表网络功能信任状态, 箭头的指向表示该网络功能从一个信任状态转换为另一个信任状态。贝叶斯网络基于网络功能历史请求信任状态序列, 选择可使 $P(e\mid h)$取值达到最大的状态 e 作为预测状态, 选择可使 $P(y)$取值到达最大的状态 y 作为最终状态。

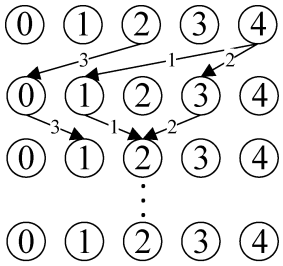

图 4 贝叶斯网络

Figure 4 Bayes network

4.1 网络功能访问请求成功率分析

信任评估向量记录了网络功能当前访问请求的信任状态, 信任评估向量是 1×5 的矩阵, 矩阵五个元素分别对应五种信任状态, 当前访问请求信任状态为 k 时, 矩阵第 k 个元素为 1, 其余元素为 0。本文将网络功能每次访问请求的信任评估向量和此次访问请求前经信任预测机制得出的信任预测向量的夹角加权余弦作为评判信任预测向量与信任评估向量相似程度的衡量标准, 计算公式如下:

$$score_i=\frac{\boldsymbol{hv_i}\cdot\boldsymbol{pv_i}}{|\boldsymbol{hv_i}|\cdot|\boldsymbol{pv_i}|}=\frac{\sum_{j=1}^{v}h_{ij}\cdot p_{ij}}{\sqrt{\sum_{j=1}^{v}h_{ij}^2}\cdot\sqrt{\sum_{j=1}^{v}p_{ij}^2}}$$ ，其中

$score_i$ 是网络功能第 i 次访问请求的信任预测向量相似度, $\boldsymbol{hv_i}$ 是第 i 次访问请求的加权信任评估向量, $\boldsymbol{pv_i}$ 是第 i 次访问请求的信任预测向量, v 是网络功能信任状态数目(在本文中为 5), h_{ij}、p_{ij} 分别是 $\boldsymbol{hv_i}$、$\boldsymbol{pv_i}$ 的第 j 个分量, $\boldsymbol{hv_i}$ 与信任评估向量的映射关系如下表:

信任评估向量	$\boldsymbol{hv_i}$
(1, 0, 0, 0, 0)	(1, 0.5, 0, 0, 0)
(0, 1, 0, 0, 0)	(0.5, 1, 0, 0, 0)
(0, 0, 1, 0, 0)	(0, 0, 1, 0, 0)
(0, 0, 0, 1, 0)	(0, 0, 0, 1, 0.5)
(0, 0, 0, 0, 1)	(0, 0, 0, 0.5, 1)

MNFTP 设置相似度阈值 *Threshold*, 如果 $score_i > Threshold$ 且预测信任状态在{0, 1, 2}之中, 则接受网络功能此次访问请求, 否则拒绝此次访问请求。定义网络功能集合单次访问请求成功率

$$success_j = \frac{\sum_{i=1}^{n} score_{ji} > Threshold}{n}$$

, 其中 $succuss_j$ 表示第 j 次请求中信任预测机制所接受网络功能的数量占网络功能总数量的比率, n 是网络功能总数量, $score_{ji}$ 是第 i 个网络功能第 j 次请求的信任预测向量相似度。

实验将奖惩因子默认值 d_3 设定为 1.0, 为了确定最佳调整因子 d_1,d_2、时间因子 t 和阈值 *Threshold*, 最大程度抑制伪装和非法网络功能访问请求并使合法网络功能请求通过, 定义最大平均请求成功率指标

$$msavg = \max \frac{\sum_{i=1}^{m}(success_{i,1} - (success_{i,2} + success_{i,3}))}{m},$$

其中 m 是所有网络功能发送访问请求总次数, $success_{i,1}$ 是合法网络功能集第 i 次访问请求的成功率, $success_{i,2}$ 是伪装网络功能集第 i 次访问请求的成功率, $success_{i,3}$ 是非法网络功能集第 i 次访问请求的成功率, 使 *msavg* 达到最大值的 d_1,d_2,t,*Threshold* 即为最佳参数组合。调整因子 d_1 是在历史信任状态 $h \in \{0,1\}$, 当前信任状态 $l \in \{3,4\}$ 的情况下上调奖惩因子, d_2 是在历史信任状态 $h \in \{3,4\}$, 当前信任状态 $l \in \{3,4\}$ 的情况下上调奖惩因子, 在相邻两次的信任状态都不可信的情况下, 惩罚力度加大, 奖惩因子上调的幅度应更高, 故 $d_1 \geqslant d_2$,。实验选取了 d_1,d_2 为(2,3)、(3,3)、(3,4)、(4,4)、(4,5)五种组合, 测试了当 t 取值 1.0, *Threshold* 在[0.9,1.0]区间上变化时 *msavg* 取值情况, 如图 5 所示。由此得出当 d_1 取 3, d_2 取 4, *Threshold* 取 0.97 时 *msavg* 达到最大值。

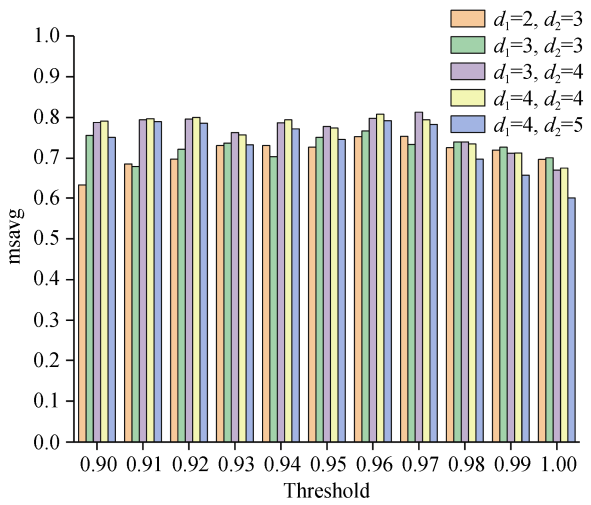

图 5 *msavg* 随参数组合的变化

Figure 5 *msavg* changes with combination of parameters

实验在 d_1=3.0, d_2=4.0, d_3=1.0, *Threshold*=0.97 的条件下测试了 *msavg* 随时间因子 t 取值的变化情况, 如图 6 所示。可以看出 t 取 0.8 时 *msavg* 达到最大值。

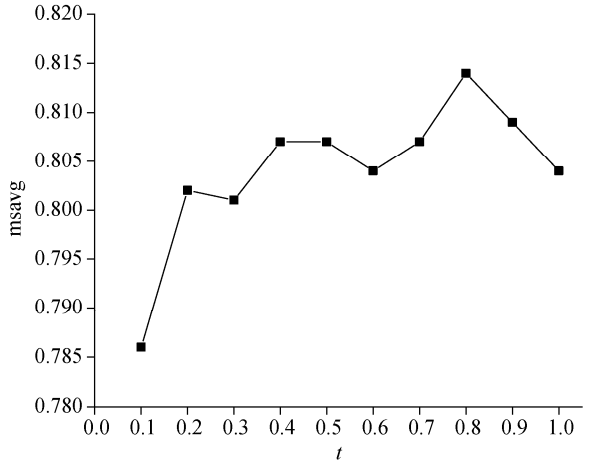

图 6 *msavg* 随 *t* 变化

Figure 6 *msavg* changes with *t*

实验将奖惩因子公式中 d_1,d_2,d_3 分别设为 3.0,4.0,1.0, 时间因子 t 设为 0.8, 相似度阈值 *Threshold* 设为 0.97, 图 7 至图 9 展示了三类网络功能集合分别在马尔可夫、贝叶斯网络和动态历史信任预测机制下随着访问请求次数的增加请求成功率的变化。表 7 展示了三类网络功能集合在三种信任预测机制下第 50 次至 500 次、第 100 次至 500 次、第 200 次至 500 次、第 300 次至 500 次和第 400 次至 500 次的访问请求平均请求成功率的数值。由图可以看出合法网络功能集在 MNFTP 机制和 BN 机制

下收敛速度相似, 在 DH 机制下收敛速度较快。在请求数量较少时, DH 机制下的请求成功率相对更高, 三种机制最终都达到 91 %左右的请求成功率。在伪装网络功能访问请求方面, DH 和 BN 机制始终在 50%和 60%之间震荡, 无法收敛, 对伪装网络功能的抑制效果较差, MNFTP 机制相对而言始终将伪装网络功能的请求成功率保持在 12%以下的低水平, 最终收敛到 2%到 3%之间, 证明 MNFTP 机制相对于 BN 和 DH 机制能够大幅降低伪装网络功能的请求成功率, 有效抵御其行为。在非法网络功能访问请求方面, 三种信任预测机制都能够将非法网络功能请求成功率维持在 4%以下的低水平, 最终都能够收敛到 0, DH 机制平均成功率较低, BN 机制相对而言平均成功率和收敛速度有所欠缺。由表可以看出在 400 次访问请求之后 MNFTP 机制将合法网络功能集的平均请求成功率提高到 90.7%, BN 机制将其提高到 91.2%, DH 机制提高到 92%。伪装网络功能集在 MNFTP 机制下随着访问请求次数的增加, 请求成功率持续降低, 400 次访问请求后下降到 2.2%的水平, 而在 BN 和 DH 机制下随着访问请求次数的增加, 平均成功率仍保持在 53%左右。非法网络功能集在发送 100 次访问请求之后, 三种机制都将其请求成功率降低到 0。

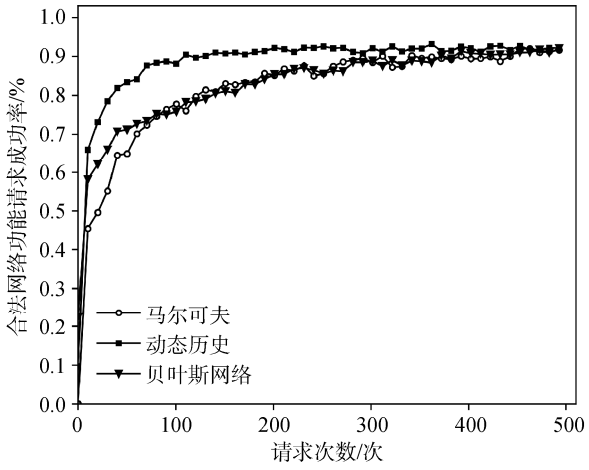

图 7 合法网络功能集在三种信任预测机制下请求成功率

Figure 7 The success rate of requests for legitimate network functions in the three trust prediction mechanisms

根据实验结果分析得出:

1. 合法网络功能集的访问请求在三种机制下都具有较高的请求成功率。DH 机制在对网络功能进行信任预测时关注于历史请求状态变化, 由于合法网络功能历史可信状态占据较大比例, 因此DH机制下

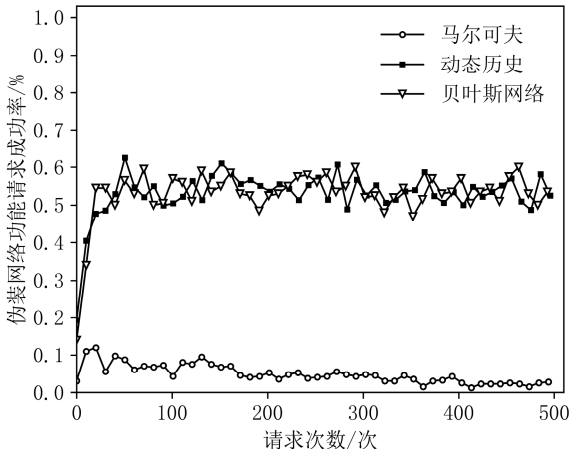

图 8 伪装网络功能集在三种信任预测机制下请求成功率

Figure 8 The success rate of requests for fake network functions in the three trust prediction mechanisms

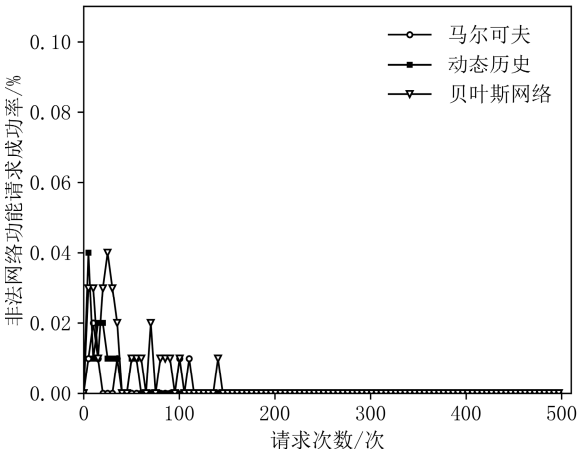

图 9 非法网络功能集在三种信任预测机制下请求成功率

Figure 9 The success rate of requests for illegal network functions in the three trust prediction mechanisms

合法网络功能请求成功率较高。BN 机制关注于信任状态的条件概率, 由于合法网络功能历史请求信任状态通常在完全可信和可信之间转换, 因此BN机制能够保证较高的合法网络功能请求成功率。MNFTP 机制由于加入了奖惩因子和时间因子, 对于信任状态由可信到不可信的转变有较高的敏感性, 对于合法的历史请求也有一定程度的忽略, 当访问请求数量较少时, 合法网络功能在 MNFTP 机制下的请求成功率有所下降。当请求数量增加到 300 附近时, 合法网络功能集在三种机制下的请求成功率几乎相同。

2. 在预测伪装网络功能访问请求时, 由于伪装网络功能有大概率发送合法访问请求, 仅有小概率

发送安全威胁性较高的访问请求。DH 机制在预测时伪装网络功能的大多数合法访问请求将历史信任评分提高, 导致DH机制下伪装网络功能请求成功率较高。BN 机制基于贝叶斯公式进行预测, 在预测时伪装网络功能的大多数合法访问请求提升了可信任状态所占比例, 导致BN机制倾向于将伪装网络功能预测为可信任状态, 因此请求成功率较高。MNFTP 机制通过引入奖惩因子对伪装网络功能从可信状态到不可信状态的行为进行惩罚, 通过时间因子削减伪装网络功能的历史高信任状态, 因此降低了请求成功率。

3. 在预测非法网络功能访问请求时, 三种机制都能达到较低的成功率且最终收敛至 0, 对于非法网络功能都有较好的抑制效果。

表 7　三种预测机制平均请求成功率随请求次数变化

Table 7　The average request success rate of the three prediction mechanisms varies with the number of requests

预测机制 \ 请求次数		50	100	200	300	400
MNFTP	合法网络功能	85.4%	87.1%	88.7%	89.6%	90.7%
	伪装网络功能	4.4%	4.1%	3.4%	2.9%	2.2%
	非法网络功能	0.04%	0.03%	0	0	0
BN	合法网络功能	85.5%	86.9%	89.0%	90.3%	91.2%
	伪装网络功能	53.4%	53.3%	53.2%	53.2%	53.7%
	非法网络功能	0.1%	0.04%	0	0	0
DH	合法网络功能	91.0%	91.5%	91.7%	92.0%	92.0%
	伪装网络功能	53.8%	53.6%	53.5%	53.2%	53.3%
	非法网络功能	0.01%	0	0	0	0

4.2　网络功能预测信任状态分析

实验所设置的 1000 个网络功能分别发送 500 次访问请求后, 两种预测机制分别对每个网络功能得出最终的信任状态, 图 10、图 11、图 12 和表 8 显示了 MNFTP 机制、BN 机制和 DH 机制对三类网络功能集在 500 次访问请求后计算得出的信任状态分布。

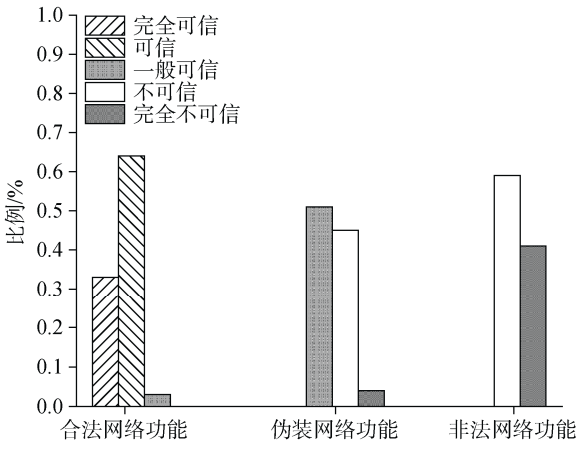

图 10　MNFTP 机制网络功能信任状态分布

Figure 10　Network function trust status distribution in MNFTP mechanism

从图表中可以看出 MNFTP 机制将 97%合法网络功能分类为完全可信和可信任之中, 将 3%的合法网络功能和 51%的伪装网络功能分类为一般可信, 将其余 49%的伪装网络功能分类为不可信和完全不可信; 将 59%的非法网络功能分类为不可信, 其余41%的非法网络功能分类为完全不可信。可以看出MNFTP机制所分类的伪装网络功能与合法网络功能相同信任状态的重叠部分较少, 非法网络功能与合法网络功能的信任状态完全不重叠, 分类效果较好。

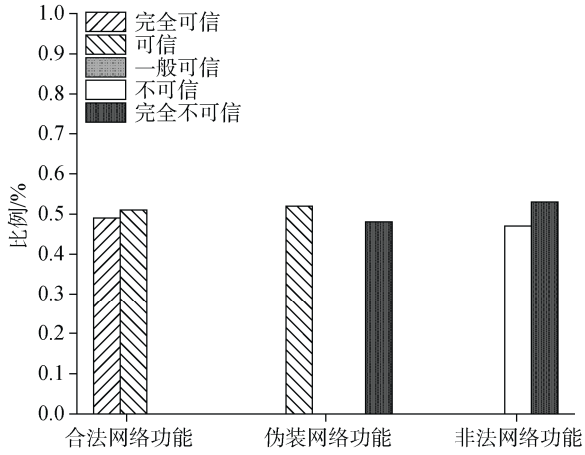

图 11　BN 机制网络功能信任状态分布

Figure 11　Network function trust status distribution in BN mechanism

BN机制将49%的合法网络功能分类为完全可信, 将其余 51%分类为可信任; 将 52%的伪装网络功能

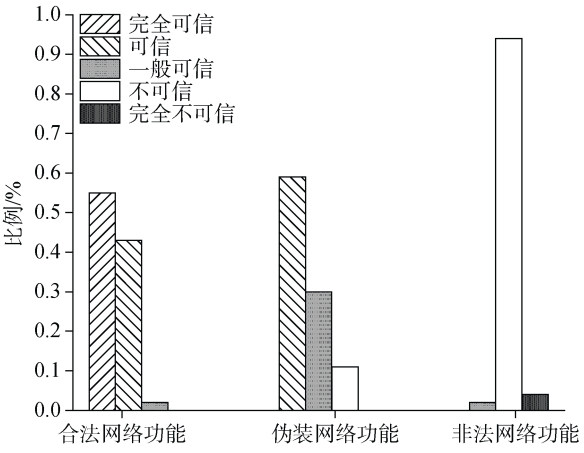

图 12 DH 机制网络功能信任状态分布

Figure 12 Network function trust status distribution in DH mechanism

分类为可信任, 将其余 48%分类为完全不可信; 将47%的非法网络功能分类为不可信, 将其余 53%的非法网络功能分类为完全不可信。可以看出 BN 机制所分类的合法网络功能集和伪装网络功能集的相同信任状态(可信任)重叠部分较大且倾向于将伪装网络功能分类为可信任状态, 造成伪装网络功能在 BN 机制下信任状态两极分化的原因是 BN 机制基于全概率公式 $P(y)=\sum_{i=1}^{n}P(v_i)P(y\mid v_i)$ 计算网络功能最终信任状态, 伪装网络功能历史请求信任状态大部分位于可信任及以上, 少部分位于不可信任及以下, 处于中等信任状态的概率很小, 因此BN机制在选择使得 $P(y)$取得最大概率的 y 过程中倾向于选择较高信任状态或者较低信任状态。

DH 机制将 55%的合法网络功能分类为完全可信, 将 43%的合法网络功能分类为可信任, 将其余2%分类为一般可信; 将 59%的伪装网络功能分类为可信任, 将30%的伪装网络功能分类为一般可信, 将其余 11%分类为不可信; 将 2%的非法网络功能分类为一般可信, 将 94%的非法网络功能分类为不可信, 将其余 4%分类为完全不可信。DH 机制倾向于将伪装网络功能分类为高信任值, 这是由于伪装网络功能在多数情况下发送的是高信任值的访问请求, 其预测信任值被历史高信任值请求所提升。

合法网络功能在三种信任预测机制下都能够被分类为高等级的信任状态, 相对而言 BN 和 DH 机制因为考虑到所有历史访问请求序列从而给予合法网络功能更高的预测信任值。

伪装网络功能在BN和DH机制下的预测信任状态大部分位于可信中, 容易和可信状态的合法网络功能相混淆, 导致伪装网络功能隐蔽于网络中造成安全威胁。本文提出的 MNFTP 机制针对伪装网络功能隐蔽性的问题, 基于马尔可夫过程理论建立网络功能请求行为信任模型, 引入奖惩因子, 当网络功能的相邻信任状态发生跳转时, 奖惩因子根据跳转前信任状态、跳转后信任状态和历史奖惩因子进行自适应调整, 从而打击伪装网络功能信任状态跳变的行为特性; 引入时间因子, 在预测未来网络功能信任值时对网络功能的历史信任值权重进行衰减, 进一步减小伪装网络功能历史高信任值访问请求对预测的影响, 从网络功能预测信任状态分布结果可以得出, MNFTP 机制在分类效果上优于 BN 和 DH 机制, 具有较高的伪装网络功能识别能力。

非法网络功能在三种信任预测机制下都能够被分类为低等级的信任状态, 相对而言 BN 机制是以网络功能历史访问请求序列各类信任状态出现的条件概率作为预测信任状态的计算基础, 由于非法网络功能历史请求序列中低信任状态出现的频率高, 在 BN 机制下被授予更低的预测信任值。

表 8 网络功能在三种信任预测机制下信任状态分布

Table 8 Distribution of trust status of network functions in three trust prediction mechanisms

预测机制 \ 信任状态		完全可信	可信任	一般可信	不可信	完全不可信
MNFTP	合法网络功能	33%	64%	3%	0	0
	伪装网络功能	0	0	51%	45%	4%
	非法网络功能	0	0	0	59%	41%
BN	合法网络功能	49%	51%	0	0	0
	伪装网络功能	0	52%	0	0	48%
	非法网络功能	0	0	0	47%	53%
DH	合法网络功能	55%	43%	2%	0	0
	伪装网络功能	0	59%	30%	11%	0
	非法网络功能	0	0	2%	94%	4%

4.3 计算时间复杂度对比分析

实验测试了三种机制的计算时间复杂度，当网络功能数量为 1000 时，随着每个网络功能请求数量的增加，三种机制预测出所有网络功能未来信任状态所消耗的时间如图 13 所示。

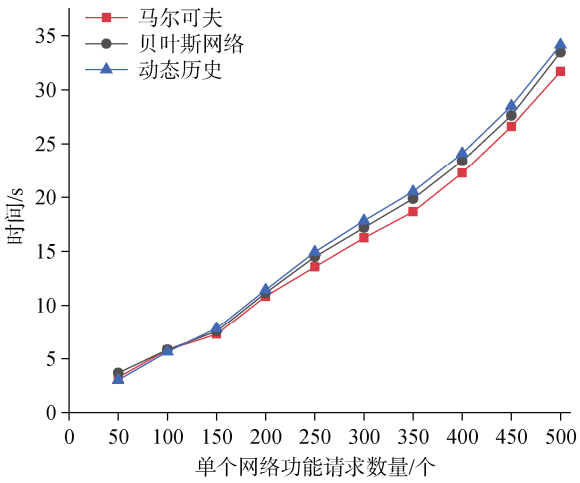

图 13 三种信任预测机制计算时间对比

Figure 13 Comparison of calculation time of three trust prediction mechanisms

由图看出 MNFTP 机制在计算时间上略优于 BN 和 DH 机制，这是因为 BN 和 DH 机制在预测网络功能未来信任状态时考虑其所有历史信任状态的条件转移概率或分布情况，MNFTP 机制重点在于处理相邻信任状态转换过程和计算状态转移矩阵平稳分布，所处理的数据量小于 BN 和 DH 机制。MNFTP 机制更适用于时延敏感性高的 5G 网络。

5 讨论

本文定义了 5G 网络功能三类行为模式，提出的 MNFTP 机制基于网络功能行为模式对访问 5G 网络 NRF 和 UDR 的网络功能进行信任评估和动态信任预测，MNFTP 的信任评估机制依据访问请求安全威胁性的大小给予访问请求不同的信任评分，MNFTP 的马尔可夫信任预测机制为了模拟现实社会信任值特性，引入了信任奖惩因子和时间衰减因子，相对于 5G 信任模型领域的贝叶斯网络和动态历史预测机制可以更好地降低恶意攻击者所控制的伪装网络功能和非法网络功能的访问成功率，虽然当访问请求数量较少时合法网络功能在 MNFTP 机制下的访问成功率有所减小，但相比于 MNFTP 机制对伪装网络功能的大幅抑制，合法网络功能访问成功率的损失能够被接受，且在请求数量增加时三种预测机制的访问成功率几乎相同，也可以通过提高合法网络功能鲁棒性和数据链路容错性进一步提升合法网络功能的请求成功率。在网络功能信任状态分类方面，MNFTP 机制能够将伪装网络功能和非法网络功能的信任状态分布与合法网络功能的信任状态分布较为明显的区分开，分类效果更好。

本文以层次分析作为网络功能访问请求的信任评估方法，除此之外可以基于传统机器学习和人工智能方法对网络功能行为进行评估，从而实现信任评估自动化，减少人为经验对评估结果的影响。

6 结束语

5G 网络商业化的快速发展给予攻击者更大的利益驱动发起网络攻击，网络功能的正常运行是保障 5G 网络各项服务指标的重要前提，本文立足于 5G 网络功能行为安全领域，针对如何为网络功能行为进行信任评分和预测的问题，提出了一种基于马尔可夫过程的 5G 网络功能信任预测机制 MNFTP。该机制首先使用层次分析法分层拆解网络功能行为要素，分析行为要素的安全威胁性并赋予信任评分；其次，基于马尔可夫过程构建网络功能行为信任状态转移矩阵，引入自适应奖惩因子和时间因子计算预测状态转移矩阵和其马尔可夫平稳分布；最后，得出网络功能的预测信任状态。实验表明 MNFTP 在抑制伪装网络功能和非法网络功能行为方面具有较好的效果。

致 谢 本文工作受到国家科技重大专项(No. 2018ZX03002002)资助。

参考文献

[1] Qiu J, Du L, Chen Y Y, et al. Artificial Intelligence Security in 5G Networks: Adversarial Examples for Estimating a Travel Time Task[J]. *IEEE Vehicular Technology Magazine*, 2020, 15(3): 95-100.

[2] Praseed A, Thilagam P S. Multiplexed Asymmetric Attacks: Next-Generation DDoS on HTTP/2 Servers[J]. *IEEE Transactions on Information Forensics and Security*, 2020, 15: 1790-1800.

[3] Tripathi N, Hubballi N. Slow Rate Denial of Service Attacks Against HTTP/2 and Detection[J]. *Computers & Security*, 2018, 72: 255-272.

[4] Ling X, Wu C, Ji S, et al. H_2DoS: An Application-Layer DoS Attack Towards HTTP/2 Protocol[C]. *International Conference on Security and Privacy in Communication Systems*, 2017: 550-570.

[5] Beckett D, Sezer S. HTTP/2 Tsunami: Investigating HTTP/2 Proxy Amplification DDoS Attacks[C]. *2017 Seventh International Conference on Emerging Security Technologies*, 2017: 128-133.

[6] Hu X X, Liu C X, Liu S X, et al. A Vulnerability in 5G Authentica-

tion Protocols and Its Countermeasure[J]. *IEICE Transactions on Information and Systems*, 2020, E103.D(8): 1806-1809.

[7] Hu X X, Liu C X, Liu S X, et al. A Security Enhanced 5G Authentication Scheme for Insecure Channel[J]. *IEICE Transactions on Information and Systems*, 2020, E103.D(3): 711-713.

[8] Liu C X, Hu X X, Liu S X, et al. Security Analysis of 5G Network EAP-AKA' Protocol Based on Lowe's Taxonomy[J]. *Journal of Electronics & Information Technology*, 2019, 41(8)1800-1807
(刘彩霞, 胡鑫鑫, 刘树新, 等. 基于 Lowe 分类法的 5G 网络 EAP-AKA'协议安全性分析[J]. *电子与信息学报*, 2019, 41(8)1800-1807)

[9] Alotaibi D. Survey on Network Slice Isolation in 5G Networks: Fundamental Challenges[J]. *Procedia Computer Science*, 2021, 182: 38-45.

[10] Neupane K, Haddad R, Chen L. Next Generation Firewall for Network Security: A Survey[C]. *SoutheastCon*, 2018: 1-6.

[11] LUO F, HOU S, 0148-7191 [R]: SAE Technical Paper, 2019.

[12] Felemban E. Advanced border intrusion detection and surveillance using wireless sensor network technology[J]. *International Journal of Communications, Network and System Sciences*, 2013, 6(5): 251-259.

[13] Han B, Gopalakrishnan V, Ji L S, et al. Network Function Virtualization: Challenges and Opportunities for Innovations[J]. *IEEE Communications Magazine*, 2015, 53(2): 90-97.

[14] Barakabitze A A, Ahmad A, Mijumbi R, et al. 5G Network Slicing Using SDN and NFV: A Survey of Taxonomy, Architectures and Future Challenges[J]. *Computer Networks*, 2020, 167: 106984.

[15] Ordonez-Lucena J, Ameigeiras P, Lopez D, et al. Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges[J]. *IEEE Communications Magazine*, 2017, 55(5): 80-87.

[16] Yousaf F Z, Bredel M, Schaller S, et al. NFV and SDN—Key Technology Enablers for 5G Networks[J]. *IEEE Journal on Selected Areas in Communications*, 2017, 35(11): 2468-2478.

[17] Kindervag J. Build security into your network's dna: The zero trust network architecture[J]. *Forrester Research Inc*, 2010: 1-26.

[18] Niu B, You W, Tang H, et al. 5G network slice security trust degree calculation model[C]. *IEEE 3rd International Conference on Computer and Communications*, 2017: 1150-1157.

[19] Baker J, Waldron K. 5G and zero trust networks[J]. *R Street Institute*, 2020.

[20] Wong S. The Fifth Generation (5G) Trust Model[C]. *2019 IEEE Wireless Communications and Networking Conference*, 2019: 1-5.

[21] Surridge M, Correndo G, Meacham K, et al. Trust Modelling in 5G Mobile Networks[C]. *The 2018 Workshop on Security in Softwarized Networks*: *Prospects and Challenges*, 2018: 14–19.

[22] Han B, Wong S, Mannweiler C, et al. Security Trust Zone in 5G Networks[C]. *2017 24th International Conference on Telecommunications*, 2017: 1-5.

[23] Ritu, Jain S. A Trust Model in Cloud Computing Based on Fuzzy Logic[C]. *2016 IEEE International Conference on Recent Trends in Electronics*, *Information & Communication Technology*, 2017: 47-52.

[24] Jiang F L, Tseng H W. Trust Model for Wireless Network Security Based on the Edge Computing[J]. *Microsystem Technologies*, 2021, 27(4): 1627-1632.

[25] Adewuyi A A, Cheng H, Shi Q, et al. CTRUST: A Dynamic Trust Model for Collaborative Applications in the Internet of Things[J]. *IEEE Internet of Things Journal*, 2019, 6(3): 5432-5445.

[26] Hu N, Tian Z H, Du X J, et al. Deep-Green: A Dispersed Energy-Efficiency Computing Paradigm for Green Industrial IoT[J]. *IEEE Transactions on Green Communications and Networking*, 2021, 5(2): 750-764.

[27] Hu N, Tian Z H, Du X J, et al. An Energy-Efficient In-Network Computing Paradigm for 6G[J]. *IEEE Transactions on Green Communications and Networking*, 2021, 5(4): 1722-1733.

[28] Militano L, Orsino A, Araniti G, et al. Trust-Based and Social-Aware Coalition Formation Game for Multihop Data Uploading in 5G Systems[J]. *Computer Networks*, 2016, 111: 141-151.

[29] Ahmad I, Yau K L A, Loong Keoh S. A Hybrid Reinforcement Learning-Based Trust Model for 5G Networks[C]. *2020 IEEE Conference on Application*, *Information and Network Security*, 2021: 20-25.

[30] Pan Q Q, Wu J, Li J H, et al. Blockchain and AI Empowered Trust-Information-Centric Network for beyond 5G[J]. *IEEE Network*, 2020, 34(6): 38-45.

[31] Benzaïd C, Taleb T, Farooqi M Z. Trust in 5G and beyond Networks[J]. *IEEE Network*, 2021, 35(3): 212-222.

[32] Diao Z M, Wang Y, Fan Y G, et al. 5G Intelligent Network Trust Model Based on Subjective Logic[C]. *2021 IEEE International Conference on Power Electronics*, *Computer Applications*, 2021: 541-545.

[33] Dehnel-Wild M, Cremers C. Security vulnerability in 5G-AKA draft[J]. *Department of Computer Science, University of Oxford, Tech. Rep*, 2018: 14-37.

[34] Dao N N, Dinh N T, Pham Q V, et al. Vulnerabilities in fog/edge computing from architectural perspectives[M]. *Fog/Edge Computing For Security, Privacy, and Applications. Springer, Cham*, 2021: 193-212.

[35] 3GPP. Technical Realization of Service Based Architecture [M]. Stage 3 3GPP TS29500. 2020.

[36] 3GPP. 5G System Principles and Guidelines for Services Definition [M]. Stage 3 3GPP TS29501. 2019.

[37] 3GPP. Network Function Repository Services [M]. Stage 3 3GPP TS29510. 2020.

[38] 3GPP. Unified Data Repository Services [M]. Stage 3 3GPP TS29504. 2021.

张奕鸣 于 2019 年在北京理工大学软件工程专业获得学士学位。现在战略支援部队信息工程大学网络空间安全专业攻读硕士学位。研究领域为网络空间安全。研究兴趣包括: 移动通信安全、网络风险感知。Email: zym913914944@163.com

刘彩霞 于 2004 年在战略支援部队信息工程大学通信与信息系统专业获得博士学位。现任国家数字交换系统工程技术研究中心研究员。研究领域为移动通信网络。研究兴趣包括: 新型网络体系结构。Email: lcxtxr@163.com

刘树新 于 2016 年在战略支援部队信息工程大学网络空间安全专业获得博士学位。现任国家数字交换系统工程技术研究中心助理研究员。研究领域为链路预测。研究兴趣包括: 通信网络安全。Email: liushuxin11@126.com

潘菲 于 2017 年在战略支援部队信息工程大学信息与通信工程专业获得硕士学位。现任国家数字交换系统工程技术研究中心研究实习员。研究领域为移动通信网络。研究兴趣包括: 通信网络安全。Email: roc_0@163.com