

电子科技大学
UNIVERSITY OF ELECTRONIC SCIENCE AND TECHNOLOGY OF CHINA

硕士学位论文

MASTER THESIS



论文题目 面向大模型推理服务的攻击检测研究

学科专业 信息与通信工程

学 号

作者姓名

指导教师

学 院 信息与通信工程学院

分类号 TN828.6 密级 公开
UDC^{注 1} 621.39

学 位 论 文

关于我的杀父仇人疑似是名震天下的大侠时 该如何报仇

(题名和副题名)

(作者姓名)

指导教师 古墓派 活死人墓

(姓名、职称、单位名称)

申请学位级别 硕士 学科专业 玉女素心剑法
专业学位领域 剑道
提交论文日期 论文答辩日期
学位授予单位和日期 中华武林
答辩委员会主席
评阅人

注 1：注明《国际十进分类法 UDC》的类号。

How to Take Revenge When My Father's Murderer is Suspected to Be a Famous Hero

A Master Thesis Submitted to
University of Electronic Science and Technology of China

Discipline Jade Lady Soul Sword Technique Jade Lady Soul

Sword Technique

Student ID _____

Author _____

Supervisor _____

School Ancient Tomb Sect Ancient Tomb Sect Ancient

Tomb Sect Ancient Tomb Sect

独创性声明

本人声明所呈交的学位论文是本人在导师指导下进行的研究工作及取得的研究成果。据我所知,除了文中特别加以标注和致谢的地方外,论文中不包含其他人已经发表或撰写过的研究成果,也不包含为获得电子科技大学或其它教育机构的学位或证书而使用过的材料。与我一同工作的同志对本研究所做的任何贡献均已在论文中作了明确的说明并表示谢意。

作者签名: _____ 日期: _____ 年 _____ 月 _____ 日

论文使用授权

本学位论文作者完全了解电子科技大学有关保留、使用学位论文的规定,同意学校有权保留并向国家有关部门或机构送交论文的复印件和数字文档,允许论文被查阅。本人授权电子科技大学可以将学位论文的全部或部分内容编入有关数据库进行检索及下载,可以采用影印、扫描等复制手段保存、汇编学位论文。

(涉密的学位论文须按照国家及学校相关规定管理,在解密后适用于本授权。)

作者签名: _____ 导师签名: _____

日期: _____ 年 _____ 月 _____ 日

摘 要

杨过少年时期母亲染病而亡，随后他便过着四处流浪的生活。

关键词：练武；离经叛道；复仇；抗敌；练武；离经叛道；复仇；抗敌；练武；离经叛道；复仇；抗敌；**注意：2025 年 09 月 03 日修订的研究生论文撰写规范要求改用“；”分隔关键词；（双学位）学士论文撰写规范尚未调整，仍使用“，”分隔关键词**

ABSTRACT

When Yang was a teenager, his mother contracted a disease and died,

Keywords: Martial arts; Apostasy; Revenge; Fighting against the enemy; Martial arts;
Apostasy; Revenge; Fighting against the enemy

目 录

第一章 绪论	1
第二章 相关技术基础和方法	2
2.1 大语言模型 LLM 推理机制	2
2.2 vLLM 与内存管理机制	2
2.3 异常检测算法基础	2
第三章 基于多维资源特征的拒绝服务攻击	3
第四章 基于缓存侧信道的攻击检测研究	4
第五章 总结和展望	5
5.1 工作总结	5
5.2 后续工作展望	5
致 谢	6
参考文献	7
附录 A 九阴真经原本	7
A.1 总纲（核心心法）	7
A.1.1 梵文总纲（后由郭靖、黄蓉译解）:	7
攻读硕士学位期间取得的成果	8

主要符号表

符号	说明	页码
a	加速度 (acceleration)	1
A	振幅 (amplitude)、面积 (Area)、磁场矢量势 (magnetic vector potential)	2
B	磁场、磁感应强度、核结合能	3
c	真空中光速	4
C	比热容 (heat capacity)、电容	5
d	长度 (distance)、直径 (diameter)、微分 (differential, 如 dx)	6
D	电位移矢量 (electric displacement)	7

缩略词表

英文缩写	英文全称	中文全称
4G	Fourth Generation Mobile Communication Technology	第四代移动通信技术
5G	Fifth Generation Mobile Communication Technology	第五代移动通信技术
B5G	Beyond 5G	超五代移动通信技术
LP	Linear Programming	线性规划
mMIMO	massive Multiple Input Multiple Output	大规模多输入多输出
NLP	non-linear programming	非线性规划
NSA	Non-Standalone	非独立组网
PLE	Path Loss Exponent	路径损失指数
QoS	Quality of Service	服务质量
SLA	Service Level Agreement	服务水平协议

第一章 绪论

第二章 相关技术基础和方法

2.1 大语言模型 LLM 推理机制

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad (2-1)$$

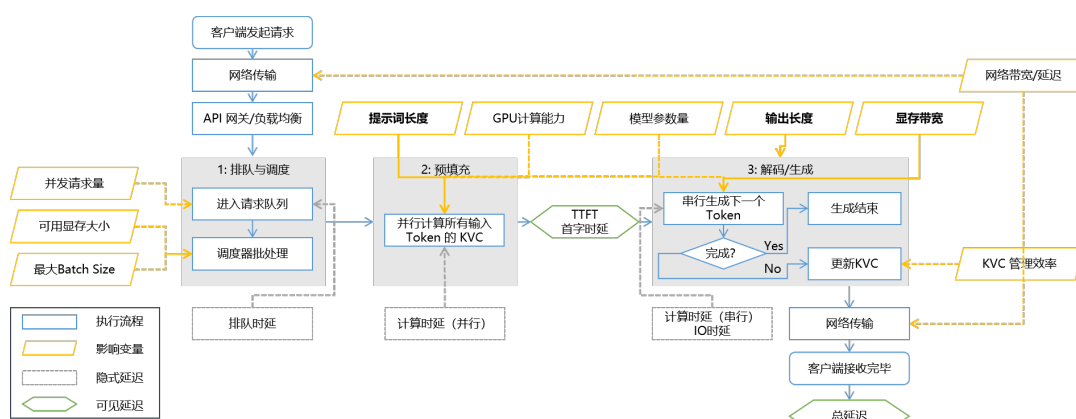


图 2-1 请求的生命周期

2.2 vLLM 与内存管理机制

2.3 异常检测算法基础

第三章 基于多维资源特征的拒绝服务攻击

第四章 基于缓存侧信道的攻击检测研究

第五章 总结和展望

5.1 工作总结

5.2 后续工作展望

致 谢

杨过一介狂生，半生漂泊，蒙诸位不弃，屡次仗义相助，此恩此情，铭刻五内。今日斗胆执笔，聊表寸心，若有疏漏，还望海涵。

附录 A 九阴真经原本

A.1 总纲（核心心法）

A.1.1 梵文总纲（后由郭靖、黄蓉译解）：

原版《九阴真经》的总纲以梵文写成，蕴含武学至高哲理，强调“阴阳互济、刚柔并重”，是化解经中武功戾气的关键。

关键理念：“天之道，损有余而补不足”（出自《道德经》），主张内力修炼需顺应自然，调和阴阳。

攻读硕士学位期间取得的成果

发表论文：

- [1] 作者 1, 作者 2*, 作者 3, 作者 4. Domain decomposition method based on integral equation for solution of scattering from very thin, conducting cavity. *IEEE Transactions on Antennas and Propagation*, 2014, 62(10): 5344–5348. (CCF 评级, 中科院分区, IF: 98.8)
- [99] 作者 1, 作者 2*, 作者 3, 作者 4. Domain decomposition method based on integral equation for solution of scattering from very thin, conducting cavity. *IEEE Transactions on Antennas and Propagation*, 2014, 62(10): 5344–5348. (CCF 评级, 中科院分区, IF: 98.8)

发明专利：

[1] 作者 1, 作者 2*, 作者 3, 作者 4。一种基于 xxxxx 的真气运转方法:
ZL201120846830.0. 2023-02-20.

参与项目：

- 项目号. 项目名称. 项目级别, 2020.01-2022.12.