Ningke Li

Wuhan, China | zmlnk001@gmail.com | +86 18856461861 | ningke-li.github.io |

Education

Huazhong University of Science and Technology 2022 – Present

- M.E. in Cyber Science and Engineering, *GPA: 89.88, rank 10/133*
- Supervisor: Prof. Haoyu Wang, Dr. Kailong Wang

Beijing University of Posts and Telecommunications 2018 – 2022

- B.E. of Information Security, *GPA: 88.63, rank 7/93*

Publications (*Co-first authors)

[1] Drowzee: Metamorphic Testing for Fact-conflicting Hallucination Detection in Large Language Models
Ningke Li, Yuekang Li, Yi Liu, Ling Shi, Kailong Wang, Haoyu Wang

Object-Oriented Programming, Systems, Languages & Applications (OOPSLA), 2024.

[2] Large language models for cyber security: A systematic literature review
Hanxiang Xu, Shenao Wang, ***Ningke Li***, Yanjie Zhao, Kai Chen, Kailong Wang, Yang Liu, Ting Yu, Haoyu Wang

Under Review (Preprint arXiv:2405.04760), 2024.

[3] MalWuKong: Towards Fast, Accurate, and Multilingual Detection of Malicious Code Poisoning in OSS Supply Chains

Ningke Li, Shenao Wang, Mingxi Feng, Kailong Wang, Meizhen Wang, Haoyu Wang

IEEE/ACM International Conference on Automated Software Engineering (ASE), Industry Challenge Track, 2023.

[4] Understanding and Tackling Label Errors in Deep Learning-based Vulnerability Detection

Xu Nie*, ***Ningke Li****, Kailong Wang, Shangguang Wang, Xiapu Luo, Haoyu Wang

ACM SIGSOFT International Symposium on Software Testing and Analysis (ISSTA 2023).

[5] How About Bug-Triggering Paths? - Understanding and Characterizing Learning-Based Vulnerability Detectors

Xiao Cheng, Xu Nie, ***Ningke Li***, Zheng Zheng, Haoyu Wang, Yulei Sui

IEEE Transactions on Dependable and Secure Computing (TDSC), 2022, Vol.8.

Research Experience

Research on Temporal Logic Augmented Generation for LLMs
2024.05 – Present

- **Research Background:** Investigated how large language models (LLMs), such as GPT-4, struggle with temporal reasoning due to their sequential processing nature and lack of formal temporal understanding. Explored integrating formal temporal logic (e.g., Finally, Globally operators) into LLMs to enhance their temporal reasoning abilities.
- **My Contribution: Main Contributor** to implement the temporal logic formulas and the whole pipeline.
- **Techniques Used:** Metric Temporal Logic, Prolog, Datalog, Python.
- **Collaborations:** Worked with Dr. Yahui Song, a research fellow at the National University of Singapore who is expertise in temporal logic and formal reasoning.

Research on Overconfidence Phenomenon for LLMs
2024.08 – Present

- **Research Background:** Investigated the overconfidence phenomenon in LLMs, where models present overly confident responses even when incorrect, which can mislead users in critical decision-making tasks.
- **My Contribution: Main Contributor** to implement the automatic testing pipeline.
- **Techniques Used:** Python.
- **Collaborations:** Advised by Prof. Lorenz GOETTE, a professor and provost's chair of the Department of

Economics in the National University of Singapore who is expertise in behavioral economics.

Research on Prolog-aided Test Cases Generation and Metamorphic Testing for Alleviating LLM Hallucination
2023.10 – 2023.04

- **My Contribution: First author in one top-tier paper**. Designed and implemented a Prolog-aided test case generator that covered various knowledge domains. Developed a metamorphic testing strategy to detect hallucinations.
- **Techniques Used:** Prolog, Python.
- **Key Outcomes:** Conducted a comprehensive benchmark for LLM hallucination testing. Presented a novel metamorphic testing framework that highlights fact-inconsistencies in LLMs.
- **Collaborations:** Collaborated with Dr. Yuekang Li, an ARC DECRA Fellow and a lecturer at the University of New South Wales who is expertise in software testing techniques (fuzzing) and software quality assurance techniques.

Research on C/C++ Program Analysis and Vulnerable/Malicious Source Code Detection
2022.09 – 2023.08

- **My Contribution: Co-authored three top-tier papers (1st, co-1st, and 3rd author).** Contributed to empirical studies on deep learning-based vulnerability detection tools and techniques for de-noising vulnerability labels. Led research on backdoor detection in software supply chains, and designed a malicious code detection tool using static analysis and heuristic rules.
- **Techniques Used:** PyTorch, Scala, Kotlin, Python, C/C++.
- **Collaborations:** Advised by Dr. Kailong Wang and Prof. Haoyu Wang, a tenured associate professor and a full professor in the School of CSE at Huazhong University of Science and Technology, with expertise in AI+Security.

Projects and Internship

Research Intern, Sangfor Technologies (Shenzhen, China) 2023.08 – 2023.09
- **Participant**
- *Key Technology Research on Vulnerability Detection and Repair Based on LLM*

Huawei Collaboration Project 2022.11 – 2023.06
- **Group Leader & Main Developer**
- *Research on Open-Source Malicious Code Detection Technology*

Ant Group Collaboration Project 2023.09 – 2024.08
- **Participant**
- *Research on Automated Discovery of Backdoor Poisoning in the Software Supply Chain*

China Telecommunication Technology Lab (CTTL) Collaboration Project 2024.06 – 2024.09
- **Main Developer**
- *Research and System Development for LLM Algorithm Security and Data Security*

Honors and Awards

China National Scholarship ×2 (Top 1%), Ministry of Education of PRC 2019, 2023
Outstanding Graduates of Beijing, Beijing Municipal Education Commission 2022
First Prize of University Scholarship ×3 (Top 5%) 2020, 2022, 2024

Services

Sub-reviewer – ASE 2024, FSE 2024, MSR 2024, Internetware 2024, EMSE 2024, ICECCS 2024
Invited Talks – Seminar Security of Large Language Models (LLMs) - 03 **TUM Germany** 2024.11.12

Skills

Programming Languages: Python, Prolog, Java, Kotlin, C/C++

Language Level – Mandarin (Native), English (C1, **IELTS 7.5, GRE 324+3.5**)