Ke He

Updated November 12, 2025

Email: ke.he@canterbury.ac.nz
Phone: (+64) 021 253-4346

GitHub: Kihy
LinkedIn: ke-he-353682276

Research interests

Network Intrusion Detection System, Adversarial Learning, Deep Learning

Education

University of Auckland — Auckland, New Zealand
Ph.D in Computer Science — August 2010 – Jun 2024
Supervisors: Assoc. Prof. Rizwan Asghar, Assoc. Prof. Dan Kim.

University of Canterbury — Christchurch, New Zealand
B.Sc. (Hon) — Feb 2015 – Nov 2019
GPA: 8.5/9

Publications

LAGER: Layer-wise Graph Feature Extractor for Network Intrusion Detection
Ke He, Dan Kim, Rizwan Asghar.
IEEE/IFIP International Conference on Dependable Systems and Networks, 2025. CORE A

MTD-AD: Moving Target Defence as Adversarial Defence
Ke He, Dan Kim, Rizwan Asghar.
IEEE Transactions on Dependable and Secure Computing, 2025. Impact Factor 7.3

NIDS-Vis: Improving the Generalized Adversarial Robustness of Network Intrusion Detection System
Ke He, Dan Kim, Rizwan Asghar.
Computers & Security, 2024. Impact Factor 5.9

Adversarial machine learning for network intrusion detection systems: a comprehensive survey
Ke He, Dan Kim, Rizwan Asghar.
IEEE Communications Surveys & Tutorials, 2023. Impact Factor: 35.6

Malware Detection with Malware Images using Deep Learning Techniques
Ke He, Dan Kim.
IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2019. CORE A

Under Review

Liuer Mihou: A Practical Framework for Generating and Evaluating Grey-box Adversarial Attacks against NIDS
Ke He, Dan Kim, Jing Sun, Jeong Do Yoo, Young Hun Lee, Huy Kang Kim.

IEEE Transactions on Emerging Topics in Computing, 2025. Impact Factor: 5.4

Research experience

Ph.D. Candidate

Mentors: Dan Kim (University of Queensland) and Rizwan Asghar (University of Surrey) August 2020 – Jun 2024

Adversarial Attacks on NIDS Developed practical adversarial attacks targeting NIDS by employing heuristic search algorithms, such as Particle Swarm Optimization (PSO), to craft manipulated network packets using Scapy. This work focuses on generating packets that successfully evade detection by NIDS.

Adversarial Defenses for NIDS Enhanced the robustness of NIDS against packet-level attacks through strategic modifications to their decision boundaries, significantly increasing the difficulty of successful attacks.

Interpretability of NIDS Advanced the understanding of NIDS decision-making processes by applying feature attribution methods including SHAP, LIME, and Integrated Gradients (IG). This research involved tracing and visualizing the decision boundaries to identify adversarial regions within the system.

Concept Drift in NIDS Investigated and designed NIDS capable of adapting to dynamic threat environments, using state-of-the-art techniques such as Transformers, Self-supervised Contrastive Autoencoders, Graph Neural Networks, and Diffusion Models. This approach addresses the limitations of static offline threat models and enhances real-time, online detection capabilities.

Research Intern at Cybersecurity Lab

Mentors: Dan Kim (University of Queensland) Dec 2017 – Feb 2018

Wrote a plugin in Python to calculate risk based on Bayesian networks on the Hierarchical Attack Representation Model (HARM) for the University of Canterbury Dependability and Security Lab.

Teaching experience

Lecturer (Teaching and Admin)

University of Canterbury Oct 2024 – Now

Program/Course Coordinator/ Facilitator for Postgraduate Certificate in Cybersecurity

The Postgraduate Certificate in Cybersecurity is an online program offered by UC Online, and I hold several roles within this program. As the Program Coordinator, I am responsible for answering students' questions about the program. As the Course Coordinator, I oversee the course content, labs, and assessments. As the facilitator, I am responsible for delivering the course to the students.

Graduate Teaching Assistant

University of Auckland — Semester 1 and 2, 2022
Open Lab Tutor
The open lab is a general help-desk-like lab that all undergraduate students can attend. My responsibilities mainly include answering assignment questions or lecture material for all undergraduate students in any courses related to computer science.

Graduate Teaching Assistant, School
University of Auckland — Semester 2, 2021
COMPSCI 316: Cybersecurity
COMPSCI 316 features a range of security topics, including encryption, network security, and software security. My responsibilities mainly include Preparing tutorials, marking assignments, and answering students' questions.

Marker, School of Computer Science
University of Auckland — Summer school, 2022
COMPSCI 1000MC: Cybersecurity
COMPSCI 1000MC is an online course on cybersecurity designed for working professionals. My responsibilities include marking assignments and exams.

Industry experience

Huayun Electric Power Co., Ltd. — Hangzhou, China
Software Intern — Dec 2018 - Feb 2019
Intern at object detection team. The main task involves using CNN (YOLO, PVANet, RetinaNET, *etc.*) to detect whether workers are wearing helmets on construction sites.

Huayun Electric Power Co., Ltd. — Hangzhou, China
Software Intern — Dec 2016 - Feb 2017
Worked on fault detection project and developed a Naive Bayes Classifier with Python to classify faulty equipment based on descriptions. The classifier was deployed on an internal server with REST API.

Honors and scholarships

UoA Doctoral Scholarship (University of Auckland)	2020
Summer Scholarship (University of Canterbury)	2016
UC Undergraduate Entrance Scholarship (University of Canterbury)	2015

Skills

Programming
Languages: Python, Java, C, Latex
Packages: Pytorch, Tensorflow, Scikit-learn, Numpy, Pandas, Matplotlib
Development Platforms: Docker, VSCode, Git, Linux

Languages
Chinese (native), English (fluent/native)