

Tran Duc Le

Assistant Professor | Computer Networking & Cybersecurity

let@uwstout.edu | 715-440-5754 | tranducle.github.io
tinyurl.com/GoogleScholarTranLe | ORCID: 0000-0003-3735-0314
linkedin.com/in/tranducle

Academic Profile

Assistant Professor at the University of Wisconsin-Stout Polytechnic specializing in computer networking and cybersecurity. Research builds on a background in wireless networking and networked systems and now focuses on network security, malware and intrusion analytics, and practical cybersecurity solutions for small and medium-sized enterprises (SMEs) and other resource-constrained organizations. Recent work also explores AI-enabled approaches to cyber defense. Teaching experience includes computer networking, network administration, network security, malware analysis, and penetration testing.

Research Interests

- **Network and systems security:** intrusion detection, malware behavior and propagation, IoT/IIoT security, network telemetry, explainable intrusion triage, wireless security, SDN security, and defensive experimentation.
- **Applied security analytics:** security analytics for SMEs and resource-constrained organizations, user behavior analytics, lightweight zero-trust architectures, malicious-content detection, and enterprise cybersecurity.
- **Agentic AI for cybersecurity:** multi-agent security, prompt-injection resilience, AI-assisted cyber defense, autonomous triage, and human-in-the-loop security operations.

Academic Appointments

Assistant Professor

University of Wisconsin-Stout Polytechnic

Department of Mathematics, Statistics & Computer Science

Aug. 2024–Present

Menomonie, Wisconsin, USA

- Teach undergraduate computer networking and cybersecurity courses in in-person and online formats; current/recent courses include CNIT-133 Network Fundamentals I, CNIT-134 Network Fundamentals II, and CNIT-383 Introduction to Network Security.
- Develop hands-on laboratories, network simulations, practical troubleshooting activities, semester projects, and supplemental instructional resources.
- Conduct research in network security, malware/intrusion analytics, cybersecurity analytics, IoT/IIoT security, and AI-enabled cyber defense.
- Contribute to academic advising, ABET-related course evidence, faculty searches, and departmental/university service.

Postdoctoral Researcher

Université du Québec à Trois-Rivières

Jan. 2023–Jul. 2024

*Trois-Rivières, Québec,
Canada*

- Conducted cybersecurity research for SMEs, including user behavior analytics, malicious-content threats, enterprise cybersecurity, and human-centered AI.
- Worked with Prof. Thang Le-Dinh and Prof. Sylvestre Uwizeyemungu on interdisciplinary research connecting cybersecurity with organizational and enterprise contexts.

Full-Time Lecturer

University of Science and Technology, The University of Danang

Dec. 2018–Dec. 2022

Danang, Vietnam

- Taught Malware Analysis, Network Security, Penetration Testing, Computer Networking, Network Administration, and Network Technologies; contributed to laboratory instruction and curriculum development.
- Supervised master's students, undergraduate course projects, and capstone projects; historically supervised approximately eight undergraduate capstone students per semester.
- Guided undergraduate scientific research and supported industry–university engagement activities.

Education

Doctoral Degree, Electronics, Radio Engineering and Communication Systems

2018

The Bonch-Bruевич Saint Petersburg State University of Telecommunications, Saint Petersburg, Russia

- **U.S. equivalency:** Ph.D. in Electrical Engineering
- **Original credential:** Candidate of Technical Sciences (Kandidat Nauk)
- **Doctoral focus:** Telecommunication Systems, Networks, and Devices
- **Dissertation:** *Mechanisms for Ensuring QoS in Unlicensed Frequencies for High-Density Wi-Fi Networks*
- **Supervisor:** Assoc. Prof. Olga Simonina

Degree of Engineer, Multi-Channel Telecommunication Systems

2014

The Bonch-Bruевич Saint Petersburg State University of Telecommunications, Saint Petersburg, Russia

Final project: *Analysis of Interconnection in SDN Technology*

Teaching Expertise

Current/recent U.S. courses taught:

- CNIT-133: Network Fundamentals I
- CNIT-134: Network Fundamentals II
- CNIT-383: Introduction to Network Security

Additional courses previously taught: Malware Analysis; Network Security; Penetration Testing; Computer Networking; Network Administration; Network Technologies.

Instructional methods and technical environments: hands-on network/security laboratories, network simulation and emulation, packet/protocol analysis, routing and switching, network troubleshooting, firewall/VPN/IDS concepts, Linux/network administration, attack/defense exercises, practical projects, and research-informed cyber scenarios.

Cybersecurity Education, Outreach, and Technical Resources

- *Malicious Traffic Analysis Agent (MTA-Agent):* Developed a PCAP analysis and reporting workflow that combines **tshark**-based extraction, structured analysis, reproducible Wireshark procedures, and educational Markdown/LaTeX reports for students and security analysts. <https://malicious-traffic-analysis.vercel.app/>
- *Cyber Security University:* Created a free learn-by-doing cybersecurity resource hub organized around foundational skills, red-team and blue-team learning paths, CTF practice, labs, certification resources, and career development. <https://csuc-website.vercel.app/>
- *Le-Puchin Cybersecurity Blog:* Author of a technical blog covering network security, malware analysis, digital forensics, security fundamentals, and practical cybersecurity learning resources. <https://lepuchin.com/>

Selected Publications and Scholarly Outputs

This list emphasizes work in cybersecurity, network and systems security, and enterprise/SME security. The full publication record is available on Google Scholar and the personal academic website.

Refereed Journal Articles

- J1. Le, Tran Duc**, Dinh, T. D., Nguyen, T. L. Q., and Nguyen, C. D. "Cross-layer contagion of prompt injections in multi-agent swarms: a multiplex microscopic Markov chain approach." *Cybersecurity*, 9, article 191, 2026. DOI: 10.1186/s42400-026-00628-w.
- J2. Le, Tran Duc**, Arifuzzaman, M., and Bao, Y. "TRACE: Feature-Space Feasible Action Contracts for Explainable Intrusion Triage." *Electronics*, 15(15), 3291, 2026. DOI: 10.3390/electronics15153291.
- J3. Le, Tran Duc**, Bao, Y., and Arifuzzaman, M. "X-GATE: Attribution-Aware Distillation and Hardening for Compressed Edge-IIoT Intrusion Detection." *Electronics*, 15(11), 2284, 2026. DOI: 10.3390/electronics15112284.
- J4. Le, Tran Duc**, Le-Dinh, T., and Uwizeyemungu, S. "A cybersecurity framework for enhancing small and medium-sized enterprises (SMEs) security posture using user behaviour analytics." *Enterprise Information Systems*, 19(10), article 2529282, 2025. DOI: 10.1080/17517575.2025.2529282.
- J5. Le, Tran Duc**, Le-Dinh, T., and Uwizeyemungu, S. "Cybersecurity Analytics for the Enterprise Environment: A Systematic Literature Review." *Electronics*, 14(11), 2252, 2025. DOI: 10.3390/electronics14112252.
- J6. Do, P. H., Le, Tran Duc**, Dinh, T. D., and Pham, V. D. "Classifying IoT Botnet Attacks with Kolmogorov-Arnold Networks: A Comparative Analysis of Architectural Variations." *IEEE Access*, 13, 16072–16093, 2025.
- J7. Le, Tran Duc**, Le-Dinh, T., and Uwizeyemungu, S. "Search Engine Optimization Poisoning: A Cybersecurity Threat Analysis and Mitigation Strategies for Small and Medium-sized Enterprises." *Technology in Society*, 76, 102470, 2024.

- J8.** Do, P. H., **Le, Tran Duc**, Vishnevsky, V., Berezkin, A., and Kirichek, R. “A Horizontal Federated Learning Approach to IoT Malware Traffic Detection: An Empirical Evaluation with N-BaIoT Dataset.” *ICACT Transactions on Advanced Communications Technology*, 12(3), 1494–1506, 2024.
- J9.** **Le, Tran Duc**, Tran, T. T., Dang, K. Q., Alkanhel, R., and Muthanna, A. “Malware spreading model for routers in Wi-Fi networks.” *IEEE Access*, 10, 61873–61891, 2022.
- J10.** **Le, Tran Duc**, Dang, K. Q., Nguyen, Q. L. T., Alhelaly, S., and Muthanna, A. “A Behavior-based Malware Spreading Model for Vehicle-to-Vehicle Communications in VANET Networks.” *Electronics*, 10(19), 2403, 2021.
- J11.** **Le, Tran Duc**, Dao, M. H., and Nguyen, Q. L. T. “Comparison of Machine Learning Algorithms for DDoS Attack Detection in SDN.” *Informatsionno-Upravliaiushchie Sistemy*, 3(106), 59–70, 2020.

Accepted / Forthcoming Journal Articles

- A1.** **Le, Tran Duc** and Dinh, Truong Duy. “Security-by-Transformation: A Capability Prioritization Framework for Resource-Constrained SMEs.” *Journal of Telecommunications and the Digital Economy*, accepted for publication, 2026.

Current Journal Manuscript Pipeline

In Revision

- R1.** **Le, Tran Duc**, Dinh, Truong Duy, Do, Phuc Hao, and Pham, Van Dai. “SAINT: Semantic Attention for Interpretable Insider Threat Detection.” *Journal of Universal Computer Science*, in revision, 2026.
- R2.** **Le, Tran Duc**, Dinh, Truong Duy, Nguyen, Cong Danh, and Nguyen, Thi Thu Ha. “Runtime Threat Modeling for Enterprise GenAI: A DATM Governance Formulation.” *Information Technology and Management*, in revision, 2026.
- R3.** **Le, Tran Duc**, Dinh, Truong Duy, Nguyen, Cong Danh, and Ninh, Thi Thu Trang. “Post-Hoc Explainable AI for Learning-Based Phishing Detection: A Systematic Literature Review and Evidence-Maturity Taxonomy.” *Applied Intelligence*, major revision, 2026.
- R4.** **Le, Tran Duc**, Arifuzzaman, Mohammad, Bao, Yida, and Dinh, Truong Duy. “DNSAGuard: Leakage-Aware Evaluation of Identifier-Stripped Packet-Size and Inter-Arrival-Time Sequences for DNS over HTTPS Tunneling Detection.” *Computer Networks*, in revision, 2026.
- R5.** Do, Phuc Hao, Nguyen, Van Long, **Le, Tran Duc**, and Dinh, Truong Duy. “What Federated KANs Cost and What They Actually Buy: A Controlled Study for NetFlow Intrusion Detection at Gateway Scale.” *IEEE Internet of Things Journal*, Revision 1 under review, 2026.

Selected Manuscripts Under Review

- U1.** **Le, Tran Duc** and Dinh, Truong Duy. “MalPhylo: A Typed-Edge DAG Framework for Malware Phylogeny from Interpretable Binary Features.” *IEEE Transactions on Information Forensics and Security*, under review, 2026.
- U2.** **Le, Tran Duc**, Dinh, Truong Duy, Nguyen, Thi Le Quyen, and Do, Phuc Hao. “Denial-of-Wallet Contagion in LLM Systems Using the Model Context Protocol: A Bipartite Stochastic Delay Model.” *Journal of Computer Security*, under review, 2026.
- U3.** **Le, Tran Duc**, Dinh, Truong Duy, Do, Phuc Hao, and Pham, Van Dai. “Indirect Prompt Injection in Model Context Protocol Networks: A Fractional Bipartite SEIQ Model.” *Computer Communications*, under review, 2026.
- U4.** Dinh, Truong Duy, **Le, Tran Duc**, Do, Phuc Hao, and Pham, Van Dai. “X-ZTA: An Explanation-Aware Policy Decision Layer for Zero Trust Network Access Management.” *Journal of Network and Systems Management*, under review, 2026.
- U5.** **Le, Tran Duc**, Dinh, Truong Duy, Nguyen, Cong Danh, Alkanhel, Reem Ibrahim, and Muthanna, Ammar. “Protocol-Prior Causality: Deterministic Network Malware Tracking via Epidemiological State Machines.” *ACM Transactions on AI Security and Privacy*, under review, 2026.
- U6.** Dinh, Truong Duy, **Le, Tran Duc**, Do, Phuc Hao, and Pham, Van Dai. “Predictive Risk Association Profiler: A SHAP Pipeline for SME Cybersecurity.” *Information Security Journal: A Global Perspective*, under review, 2026.
- U7.** **Le, Tran Duc**, Dinh, Truong Duy, Nguyen, Dac Cu, and Pham, Van Dai. “A Phase-Aware Socio-Technical Framework for Cybersecurity Awareness in Digital Transformation.” *Information Security Journal: A Global Perspective*, under review, 2026.

Conference Papers and Book Chapters

- C1.** Do, P. H., **Le, Tran Duc**, Dinh, T. D., and Pham, V. D. “Mind the Gap: On the Practical Utility of SHAP for Deep Learning-Based Intrusion Detection.” In *RIVF International Conference on Computing and Communication Technologies*, IEEE, 364–369, 2025.
- C2.** Do, P. H., **Le, Tran Duc**, Dinh, T. D., Pham, V. D., and Nguyen, T. L. Q. “GT-FID: A Graph-Temporal Fusion Network for Host-Based Intrusion Detection from System Call Sequences.” In *CCIoT '25: 10th International Conference on Cloud Computing and Internet of Things*, ACM, 7–14, 2025.

- C3.** Tran, T. C. G., Le-Dinh, T., and **Le, Tran Duc**. “Agentic AI Across Technologies, Applications, and Development Domains: A Systematic Literature Review.” In *International Conference on Data Analytics & Management (ICDAM 2025)*, Lecture Notes in Networks and Systems, vol. 1603, Springer, 587–601, 2025.
- C4.** **Le, Tran Duc**, Le-Dinh, T., Uwizeyemungu, S., Doan, X. H., and Dinh, T. D. “SafeDocs: A Machine Learning-Based Framework for Malicious PDF Detection Tailored for SMEs.” In *RIVF International Conference on Computing and Communication Technologies*, IEEE, 295–300, 2024.
- C5.** **Le, Tran Duc**, Do, P. H., Nguyen, D. T., Phung, V. T., Nguyen, C. D., and Dinh, T. D. “Federated Learning for Linux Malware Detection: An Experimental Study.” In *EAI/Springer Innovations in Communication and Computing*, Springer, 63–75, 2023.
- C6.** Le, V. T., Do, P. H., Uwizeyemungu, S., Le-Dinh, T., and **Le, Tran Duc**. “Utilizing InfoGAN and PE Header Features for Synthetic Ransomware Image Generation: An Experimental Study.” In *Future Data and Security Engineering (FDSE 2023)*, CCIS vol. 1925, Springer, 226–239, 2023.
- C7.** **Le, Tran Duc**, Dinh, T. D., Nguyen, P. H. T., Muthanna, A., and Abd El-Latif, A. A. “Exploring Common Malware Persistence Techniques on Windows Operating Systems for Enhanced Cybersecurity Management: Detection and Mitigation Strategies.” In *Cybersecurity Management in Education Technologies*, Taylor & Francis, 107–149, 2023.
- C8.** Truong, C. K., Do, P. H., and **Le, Tran Duc**. “A Comparative Analysis of E-mail Phishing Detection Methods: A Deep Learning Perspective.” In *Artificial Intelligence for Biometrics and Cybersecurity*, IET, 149–174, 2023.
- C9.** **Le, Tran Duc**, Le, B. L., Dinh, T. D., and Pham, V. D. “Classification of Ransomware Families Based on Hashing Techniques.” Lecture Notes in Networks and Systems, vol. 734, Springer, 37–49, 2023.
- C10.** Do, P. H., **Le, Tran Duc**, Vishnevsky, V., Berezkin, A., and Kirichek, R. “A Horizontal Federated-Learning Model for Detecting Abnormal Traffic Generated by Malware in IoT Networks.” In *25th International Conference on Advanced Communication Technology (ICACT)*, IEEE, 28–36, 2023.
- C11.** Nguyen, H. H., Nguyen, T. G., Hoang, D. T., **Le, Tran Duc**, and Phan, T. V. “CARS: Dynamic Cyber-attack Reaction in SDN-based Networks with Q-learning.” In *International Conference on Advanced Technologies for Communications (ATC)*, IEEE, 156–161, 2021.
- C12.** **Le, Tran Duc**, Tai, N. D., Luong, L. B., Pham, V. D., and Kirichek, R. “Analysis of Network Security Issues in the Join Procedure of LoRaWAN.” In *24th International Conference on Distributed Computer and Communication Networks*, 468–476, 2021.

Datasets and Preprints

- D1.** **Le, Tran Duc**. “LWDED: Large-scale Website Defacement Evaluation Dataset (v2).” Zenodo dataset, 2026. DOI: 10.5281/zenodo.22051074.
- P1.** **Le, Tran Duc**. “Research Methodologies for Cybersecurity in Enterprise Environments: A Narrative Review, Synthesis and Executable Guide.” arXiv preprint, 2026. arXiv:2608.24850.
- P2.** **Le, Tran Duc**, Dinh, T. D., Do, P. H., Pham, V. D., and Nguyen, S. N. “Beyond the Flag: A Framework for Integrating Cybersecurity Competitions into K-12 Education for Cognitive Apprenticeship and Ethical Skill Development.” arXiv preprint, 2026. arXiv:2602.16921.

Selected Research Funding

Young Researcher Grant (T2021-02-06), Principal Investigator	<i>2020–2021</i>
University of Science and Technology, The University of Danang; approximately \$1,500. Project: <i>Malware Spreading Model for Wi-Fi Networks</i> .	
NAFOSTED Grant (102.01-2019.322)	<i>2019–2022</i>
National Foundation for Science and Technology Development, Vietnam; approximately \$40,800. Project: <i>AI-Driven Cyberattack Detection for Future SDN-Based Networks</i> . Role: core project member; research ideas and manuscript development.	
Science and Technology Research Grant (41/HDKHCN/2021)	<i>2021–2023</i>
Funded by Quang Nam Province, Vietnam; approximately \$120,500. Project: <i>Construction of a Database and Intelligent Management System for Biodiversity of Plant Communities in Special Forest Areas of Quang Nam Province</i> . Role: core project member; network/server configuration, technical contributions, and reporting.	
Science and Technology Research Grant (36/HDKHCN/2020)	<i>2020–2023</i>
Funded by Danang City, Vietnam; approximately \$70,500. Project: <i>Research on the Development of an Intelligent Biodiversity Management System for Plant Communities in Danang City</i> . Role: core project member; network/server configuration, technical contributions, and reporting.	

Research Leadership and Student Mentoring

Founder, NetSec-ITDUT Lab

2020–Dec. 2022

University of Science and Technology, The University of Danang.

- Founded and led a student-centered network-security research group involving senior undergraduates, collaborators from other universities, and R&D engineers.
- Supervised research in network security, malware analysis, IoT/LoRa security, intrusion detection, and related applied cybersecurity topics.
- Supervised master's work, undergraduate scientific research, course projects, and capstone projects; supported student participation in cybersecurity activities and CTF-style learning.

Honors and Awards

- Outstanding Paper Award, ICACNGC 2022.
- Outstanding Paper Award, International Conference on Advanced Communication Technology (ICACT), 2020.

Professional and Academic Service

Selected Journal Reviewer Service: ACM Computing Surveys; IEEE Access; Engineering Applications of Artificial Intelligence; The Journal of Supercomputing; Transactions on Emerging Telecommunications Technologies; PeerJ Computer Science; Journal of Computer Virology and Hacking Techniques; Journal of Cybersecurity; Journal of Cybersecurity and Privacy; SN Computer Science; Journal of Telecommunications and the Digital Economy; Wireless Networks.

Conference / Program Committee Service:

- Program Committee, ACM Conference on Computer and Communications Security (CCS) Poster/Demonstration Sessions, 2025.
- Reviewer: AMCIS 2025; CITA 2025 and 2024; DCCN 2024; RIVF 2023; CITA 2023 and 2022; FDSE 2023; MaDaIN 2021 and 2020; and other networking/computing venues.
- Organizing Committee, MaDaIN 2021 and MaDaIN 2020.

Institutional Service, University of Wisconsin-Stout Polytechnic:

- Faculty search committees for computer networking / computing positions.
- ABET-related course evidence and accreditation support.
- Academic advising and student career preparation.
- Departmental colloquium and program-support activities.

Professional Certifications and Selected Technical Training

- Cisco Certified Specialist, Enterprise Core (350-401 ENCOR), Cisco, 2025.
- Cisco Certified Network Associate (CCNA), Cisco, 2024.
- Certified in Cybersecurity (CC), ISC2, 2024.
- Penetration Testing, Incident Response and Forensics, IBM Skills Network, 2023.
- Splunk Search Expert 101, Splunk, 2023.
- Hands-on Introduction to Linux Commands and Shell Scripting, IBM, 2023.

Technical Expertise

Cybersecurity: network security, intrusion detection, malware analysis, malware traffic analysis, penetration testing, security analytics, IoT/IIoT security, zero-trust concepts, cyber defense, explainable AI for security, agentic/multi-agent security.

Networking and systems: TCP/IP, routing and switching, WLAN, SDN, IoT/LoRa, network administration, Linux, network simulation/emulation, packet analysis, troubleshooting.

Research methods: machine learning/deep learning, federated learning, graph learning, quantitative experimentation, systematic/narrative literature synthesis, model evaluation, and applied cybersecurity analytics.