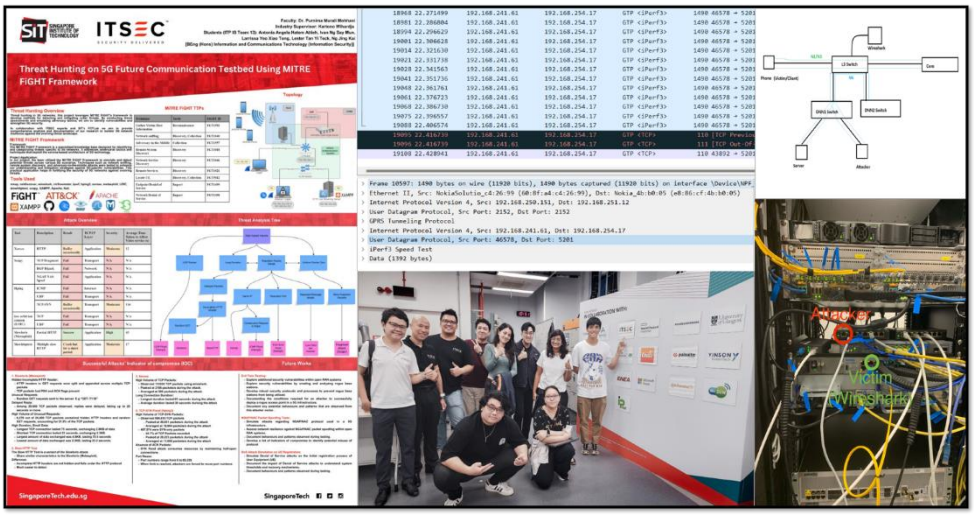
AI-Driven Fuzzing for 5GA/6G Security

As the development of 5G continues with advanced releases such as Release 17 and the upcoming Release 18, ensuring the robustness, reliability, and security of network protocols is increasingly critical [1]. These releases aim to enhance mobile broadband, ultra-reliable low-latency communications (URLLC), and massive machine-type communications (mMTC), for wide-ranging applications from autonomous driving, industrial automation, and smart cities.

Traditional methods of protocol testing can fail to identify complex vulnerabilities due to their limited ability to generate diverse or comprehensive test cases [2]. To address these challenges, we aim to leverage AI-driven fuzzing techniques facilitated by Large Language Models (LLMs) [3] and the MITRE FiGHT (5G Iterative Framework for Hunting Threats) framework [4]. This promises to enhance vulnerability detection, optimize protocol performance, and support dynamic resource allocation & management in OpenRAN and 5G core network elements.



The integration of AI-driven fuzzing techniques + MITRE FiGHT will significantly enhance the robustness and security of 5G and future network protocols [5]. By leveraging AI and LLMs to generate diverse and comprehensive test cases, this project addresses complex vulnerabilities that traditional methods often miss. This ensures that critical network infrastructures are protected against sophisticated cyber threats, thus enhancing network reliability/performance for applications ranging from autonomous driving, industrial automation, future applications such as smart cities, and telemedicine. Collaboration with industry leaders such as Viavi, Palo Alto, and ITSEC will ensure that project findings contribute to global standards and best practices.

[1] M. Mahyoub, A. AbdulGhaffar, E. Alalade, E. Ndubisi, and A. Matrawy, “Security analysis of critical 5g interfaces,” IEEE Communications Surveys & Tutorials, 2024.
[2] C. Daniele, S. B. Andarzian, and E. Poll, “Fuzzers for stateful systems: Survey and Research Directions,” ACM Computing Surveys, vol. 56, no. 9, pp. 1–23, 2024.
[3] L. Huang, P. Zhao, H. Chen, and L. Ma, “Large language models based fuzzing techniques: A survey,” arXiv preprint arXiv:2402.00350, 2024.
[4] MITRE, “MITRE FiGHT: 5G Iterative Framework for Hunting Threats,” Tech. Rep., 2020, online; accessed 12-July-2024. [Online]. Available: https://www.mitre.org/publications/technical-papers/ mitre-fight-5g-iterative-framework-for-hunting-threats
[5] “Future Communications Translation Lab (FCTLab), SIT,” Tech. Rep., 2024. [Online]. Available: https://www.singaporetech.edu.sg/research/FCTLab