Researcher Profile: Dr. Shangqing Zhao  
Affiliation: School of Computer Science, University of Oklahoma

|  |  |
| --- | --- |
| Category | Content |
| Research Domains | - Mobile and Wireless Security- Machine Learning & Artificial Intelligence- Signal Processing- Quantum Computing- Internet of Things (IoT) Security |
| Techniques Used | - Machine Learning Algorithms: Siamese Neural Networks (SNN), Support Vector Machines (SVM), Decision Tree (DT) classification, Multi-layer perceptron (MLP) classifiers, Variational Quantum Algorithms (VQA), Quantum Support Vector Machines (QSVM), Quantum Convolutional Neural Networks (QCNN)- Signal Processing and Analysis: Audio Fingerprinting, Dynamic Time Warping (DTW), Channel State Information (CSI), Symbol Timing Offset (STO)- Other: Location Lookup Table (LLT) Inference Attack, Identification Override (IDO) to inject signals to another tag’s reflected signal to override unique info of transmitted tag for RFID. |
| Data & Platforms | - Self collected data: Human Study music, Public AP’s, SNN Model Training Dataset- Public Datasets: Alzheimer’s Disease Dataset (<https://www.kaggle.com/dsv/8668279)-> Software: scikit-learn library, IBM Qiskit software stack, Google Geolocation API, Mozilla Location Service- Hardware: Universal Software Radio Peripheral (USRP) X310 for Radio Frequency Identification (RFID) Analysis. |
| Application Areas | - Audio Copyright Detection- Machine Learning Security- Wi-Fi Spoofing Attack- Quantum Machine Learning |

Key Research Thinking Patterns

|  |  |
| --- | --- |
| Aspect | Detail |
| Adversarial Modeling | Analyzes systems through the perspective of a potential attacker and constructs threat models (e.g., Evading copyright detection, Wi-Fi Spoofing, Crowd counting in wireless signals, IDO to spoof RFID tags). |
| Reverse Engineering | Deconstructs complex systems to uncover hidden functionalities (e.g., Emulating YouTube copyright detection system, unveiling Google Wi-Fi positioning system) |
| Comparative Evaluation | Assesses different approaches and conducts comparisons analytically over baselines and metrics of different approaches to determine success rates (e.g., Music Copyright Different Attack Types, Quantum Machine Learning vs. Classical Machine Learning, Wi-Fi Spoofing Attack via Geolocation API vs. Traditional Wi-Fi Spoofing Attack). |
| Black-Box System Approach | Analyzing a system’s behavior solely by observing inputs and outputs without any knowledge of internal workings (e.g., YouTube’s copyright detection system, Google Wi-Fi positioning system). |

Knowledge Graph Sketch (Hierarchical View)

TBD

Summary Description (for use as a KG node or metadata tag)

Dr. Shangqing Zhao’s research mainly focuses on cybersecurity, with a speciality towards mobile and wireless security within realms of machine learning and quantum computing. They employ adversarial modeling and reverse engineering to analyze vulnerabilities and enhance the security in applications such as audio copyright detection to Wi-Fi spoofing and RFID systems. They introduce different types of attacks to find exploits and vulnerabilities within public systems, also emphasizing the practicality of attacks and operating within a black-box system or environment. Their contributions reflect understanding security vulnerabilities across modern technologies to fortify systems.