Taibiao Zhao

☎ +1(225)441-5041 ✉ taibiaozhao2020@gmail.com linkedin.com/taibiao-zhao-234baa23a/ github.com/ztb-35

EDUCATION

Louisiana State University **Aug. 2021 – Jun. 2026 (Expected)**
Ph.D. in Computer Science *Baton Rouge, United States*

Northeastern University **Sep. 2016 – Jun. 2020**
B.S. in Information and Computation Science *Shenyang, China*

EXPERIENCE

Louisiana State University **Aug. 2021 – Present**
Research Assistant (Machine Learning Engineer) *Baton Rouge, United States*

- Designed a spatiotemporal fault-injection framework (STAFI) for ADAS, integrating Progressive Metric-guided Bit Search and context-aware timing to reveal safety-critical vulnerabilities in OpenPilot–CARLA autonomous driving simulations.
- Proposed a multi-level text-aligned time-series forecasting framework that decomposes signals into trend, seasonal, and residual components to enhance LLM multimodal reasoning and forecasting.
- Proposed a practical backdoor attack that swaps in a malicious attention head, achieving 99.5% attack success rate with minimal clean-accuracy impact and strong resilience to modern defenses.

Northeastern University **Sep. 2020 – Jul. 2021**
Research Assistant (Computer Vision / Applied Machine Learning) *Shenyang, China*

- Implemented and optimized semantic segmentation models for industrial predictive-maintenance applications in collaboration with Ansteel Group.
- Reduced system downtime by 30% through image-based defect detection and automated data labeling pipelines.

PROJECTS

Spatiotemporal-Aware Fault Injection on ADAS **Jan. 2025 – Oct. 2025**

- Proposed a PMBS pipeline that leverages gradient-based importance ranking to discover bit-flip vulnerabilities causing unsafe autonomous driving behaviors.
- Developed a temporal fault-activation module (CFTI + H-Net) that identifies risk-amplifying contexts and predicts hazard likelihood and time-to-hazard for each bit site.
- Achieved 7.16× higher induced hazards than random or TGFI baselines, demonstrating superior precision in triggering safety-critical faults.

Multimodal Time-Series Forecasting with LLMs **Aug. 2023 – Dec. 2024**

- Developed a unified forecasting framework aligning decomposed time-series components with language embeddings for interpretable prediction (*DASFAA 2025*).
- Introduced multi-level alignment between time-series anchors and word tokens to enhance LLM reasoning.
- Outperformed SOTA benchmarks by up to 26% while maintaining interpretability.

Pruning and Malicious Injection for Robust Transformer Analysis **Sep. 2022 – Jul. 2023,**

- Proposed a retraining-free backdoor attack (HPMI) injecting malicious heads into pre-trained transformers without degrading clean accuracy.
- Exposed hidden robustness flaws in ViT and BERT architectures with minimal computation cost.
- Achieved 99.5% attack success and full evasion of four major defense methods across CV and NLP tasks.

TECHNICAL SKILLS

Languages: Python, C++, Java, MATLAB
Machine Learning: PyTorch, TensorFlow, Hugging Face, Scikit-learn, ONNX Runtime, OpenCV
Optimization & Experimentation: Gradient-based Optimization, Causal Inference, A/B Testing, Simulation
Tools: NumPy, Pandas, Docker, AWS, Git, Jupyter, Linux, GPU Cluster Automation

SELECTED PUBLICATIONS

- **Zhao, T.**, Zhang, X., Ding, R., Zhou, X., and Sun, M. (2025). Spatiotemporal-Aware Bit-Flip Injection on DNN-based Advanced Driver Assistance Systems. Under review, *Proceedings of the Design Automation Conference (DAC)*, Nov. 2025.
- **Zhao, T.**, Chen, X., and Sun, M. (2025). Enhancing Time Series Forecasting via Multi-Level Text Alignment with Large Language Models. In *Proceedings of the International Conference on Database Systems for Advanced Applications (DASFAA)*, May 2025.
- **Zhao, T.**, Sun, M., Hao, W., Chen, X., and Zhou, X. (2025). Pruning and Malicious Injection: A Retraining-Free Backdoor Attack on Transformer Models. Under review, *Knowledge and Information Systems (KAIS)*, 2025.