Xiang Cheng

+1(626)877-1252 xiangcheng@vt.edu https://xiangcheng.link

Education

Virginia Tech Blacksburg, VA
Ph.D. in Computer Science, Advisor: Yaling Yang *Aug.2018 – May.2023(expected)*

University of Electronics Science and Technology of China Chengdu, China
B.Eng., Electronic and Electrical Engineering, ranking 1/240 *Aug.2014 – May.2018*

University of Glasgow Glasgow, UK
B.Eng., Electronic and Electrical Engineering, with Honors of the First Class *Aug.2014 – May.2018*

Technical Skills

Programming: Python/MATLAB (proficient), C/C++/Java/JavaScript (Prior experience)
Tools & Frameworks: React Native, Node.js, Firebase, TensorFlow, PyTorch, Git, GNURadio

Work Experience

Intelligent Data Analytics Lab, visiting scholar Jul.2017 – Sep.2017
Michigan State University *East Lansing, MI*

- Mild Cognitive Impairment (MCI) Diagnosis: built an NLP pipeline based on daily conversations to diagnose MCI. The pipeline is built with python using TensorFlow, the model can assist MCI diagnosis with over 70% accuracy.
- Traffic data synthesis: helped to build generative neural networks (GAN) to synthesize urban traffic data, implemented a data preprocessing pipeline, and integrated it into the GAN model.

Research Projects

Privacy-Friendly Digital Contact Tracing System, Team Leader May.2020 – Present

- Designed a digital contact tracing system by encoding geolocation and Bluetooth data together, the system protects users' privacy using crypto algorithms like homomorphic encryption, k-anonymity, and multi-party computation.
- Built an **Android app** and a **backend server** based on the design. The app is implemented under React Native framework in JavaScript, and the server is built using Google Firebase.
- Optimized the system to reduce the system's computation time **by 50%**, and make the app's memory usage **less than 30MB**.

Robust GPS Spoofing Detection, Co-Leader Oct.2019 – Oct.2020

- Proposed a GPS spoofing detection system that works for off-the-shelf GPS chipsets, the method **reduce the cost** of spoofing detection from thousands of dollars **to almost 0**.
- Built a data collection app and an analytic toolset. The app is built based on the Android GNSSLogger framework in Java, the analytic toolset is implemented with Matlab.
- The system is tested in various environments, it can achieve **over 95%** detection accuracy **within 5 seconds**.

Attack and Defense with GAN, Team Member Aug.2018 – Jul.2019

- Neural translation for attacks on the medical image domain: proposed and implemented custom generative neural networks (GAN) in adversarial settings to mislead medical diagnostics. The work revealed a realistic threat to the healthcare system posed by deep learning.
- Detecting GAN-synthesized deepfakes: developed a fingerprint-based clustering algorithm to detect deepfake images. The algorithm detects GAN-synthesized fake images with 99% accuracy under an unsupervised setting.

Publications

[USENIX Security'21]Shinan Liu, Xiang Cheng(co-first author), Hanchao Yang, Yuanchao Shu, Xiaoran Weng, Ping Guo, Kexiong (Curtis) Zeng, Gang Wang, Yaling Yang. "Stars Can Tell: A Robust Method to Defend against GPS Spoofing Attacks using Off-the-shelf Chipset". USENIX Security, 2021. [Paper Link]

[arXiv] Xiang Cheng, Hanchao Yang, Archanaa S Krishnan, Patrick Schaumont, Yaling Yang."KHOVID: Interoperable Privacy Preserving Digital Contact Tracing". [Paper Link].

[IEEE Access] Jialin Tian, Yazhou Ren, Xiang Cheng. "Stratified Feature Sampling for Semi-Supervised Ensemble Clustering ". in IEEE Access, 2019. [Paper Link]