Side-channel Attacks Against Mobile Users: Singularity Detection, Behavior Identification, and Automated Rectification

Award#: 1815636

Dr. Guan-Hua Tu, Michigan State University

Dr. Jiliang Tang (tangjili@msu.edu), Michigan State University

MICHIGAN STATE UNIVERSITY

Side-channel attacks have been proven effective in inferring mobile user activities. This research aims to discover side-channel information leakage issues threatening mobile users, including

- various cellular network services (Packet-Switched based, Circuit-Switched based or IP Multimedia Subsystem based),
- cellular network control-plane protocol events (e.g., changing current bearer QoS prole) by analyzing mobile users' encrypted data including control-plane signalings and data-plane data packets, and
- diversified Internet applications and activities.

Key Challenges:

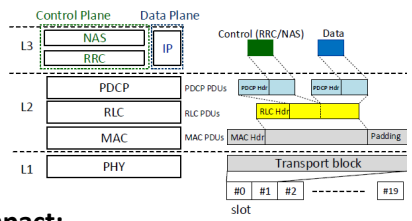
- Control-plane and data-plane traffic are transmitted by the same physical channels
- All cellular network operations are initiated by encrypted signalings
- Detecting the singularity and identify user and network behaviors is challenging since the data is sequential, high-dimensional, and limited

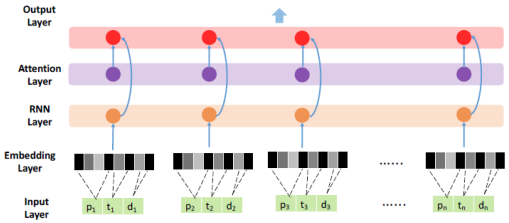
Scientific Impact:

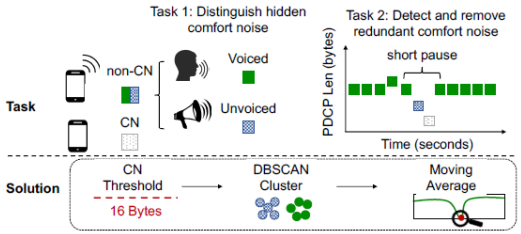
- Extend the state-of-the-art side-channel attack research to a new frontier of mobile networks, investigates original problems that entreat innovative data collection, data labeling, data mining, deep learning solutions.
- Pave the way for a new research endeavor to effectively tame diversified traffic for discovering insightful singularities

Solutions:

- Develop new techniques for mobile data collection and labeling
- Develop singularity detection and behavior identification
- Develop mobile/cellular-friendly automated rectification







Broader Impact:

- Lay a solid foundation for researching novel methodologies for detecting singularities of mobile big data, discovering the hidden association between singularities and user behaviors and network events, rectifying the side-channel information in a mobile-specific context (e.g., limited resources, volume-based charging/billing model)
- Accelerate the understanding of mobile big data. As an important preprocessing step for secure the mobile ecosystem from a variety of side-channel attacks, the successful completion of this project will benefit billions of mobile users