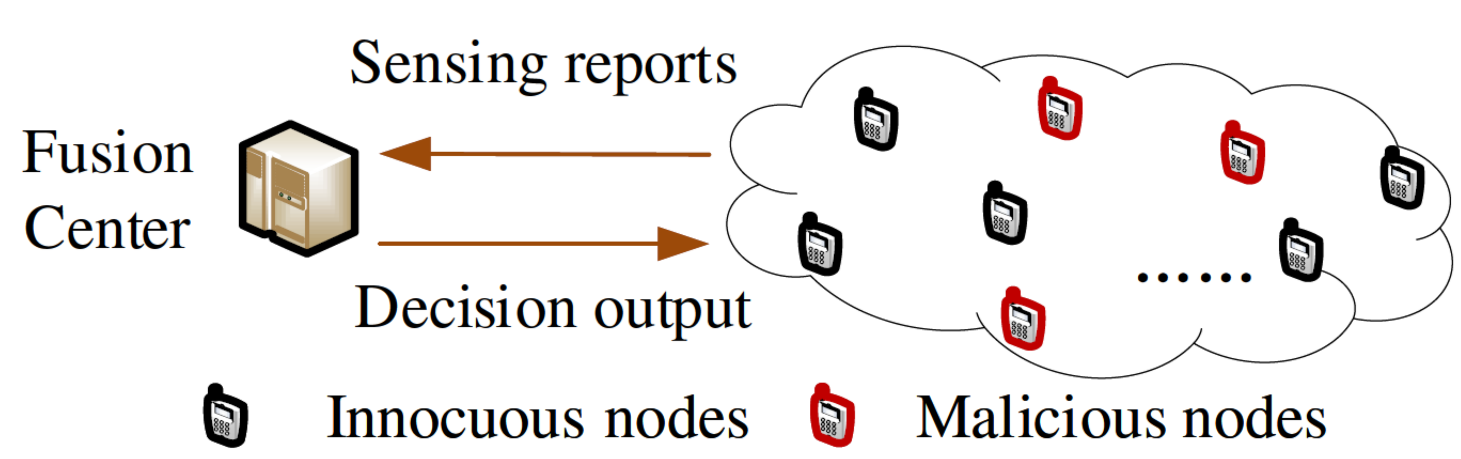
Collaborative Research: SWIFT: SMALL: Understanding and Combating Adversarial Spectrum Learning towards Spectrum-Efficient Wireless Networking

PIs: Zhuo Lu and Yasin Yilmaz at University of South Florida (Project# 2029875)
Jie Xu at University of Miami (Project# 2029858)

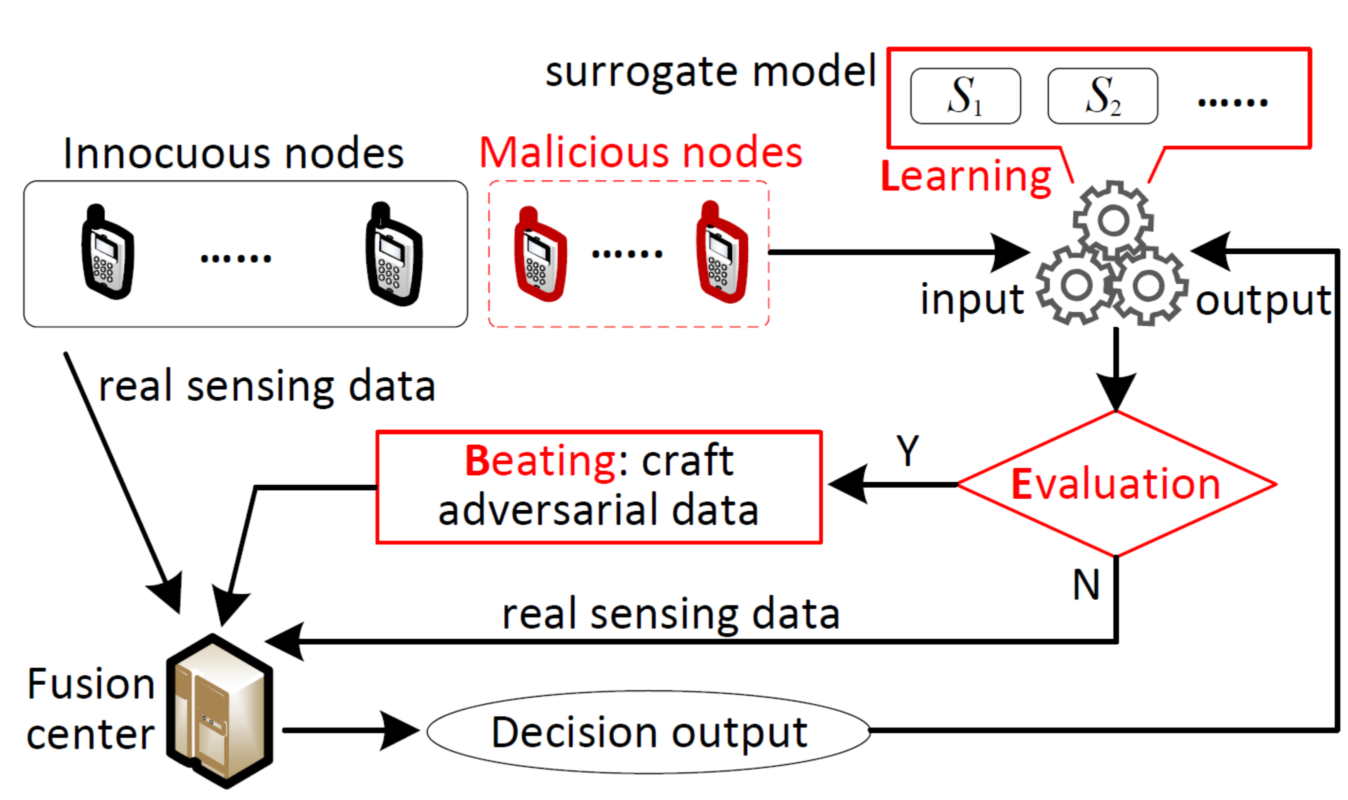
Project Objectives

This goal of this project is to identify and investigate new security vulnerabilities associated with existing cooperative spectrum sensing designs, called **adversarial spectrum learning**, and create new adversarial spectrum learning **mitigation, defense and management** mechanisms for wireless networks.

Background



- Malicious nodes know both spectrum data used for the spectrum access decision and the final decision at the same time. So they train a machine learning model by using the spectrum data as the input and the decision as the output to steal the defense model
- Threat Model: The attacker builds multiple surrogate models {*Si*} to learn and decide how to create adversarial examples based on internal accuracy for each model.



Broader Impacts

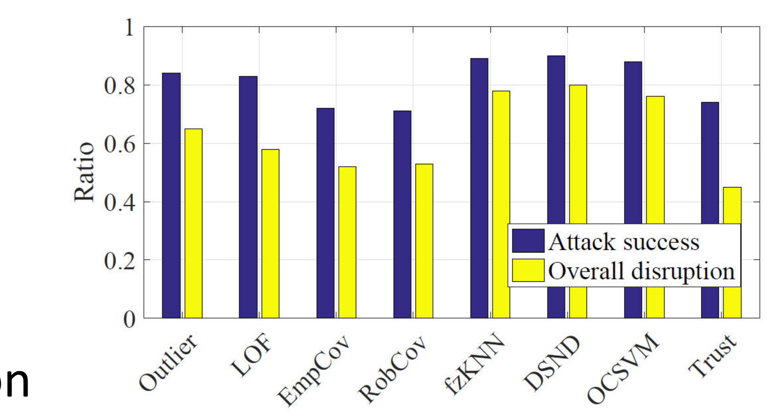
Course materials of machine learning / adversarial machine learning and adversarial spectrum learning in wireless networking

Results at IEEE/ACM SEC -EdgeComm, ACM WiSec-WiseML, IEEE DySPAN, IEEE INFOCOM, and IEEE Trans Mobile Computing

Two female Ph.D. students have been involved. Organized lab tour for HBCU undergraduate visitors.

Impact and Detection

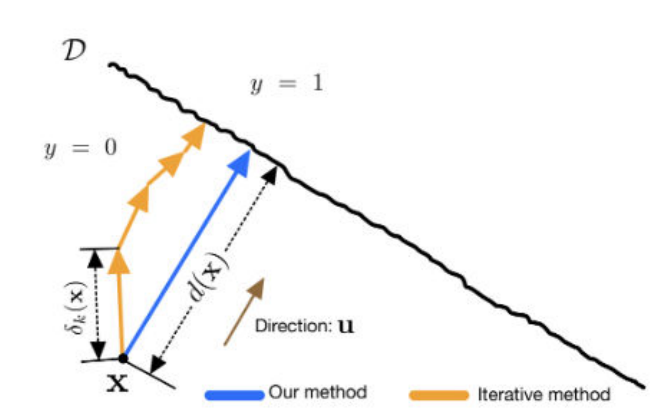
Attack success ratio:
\# Attack successes / # attack attempts
Overall distribution ratio:
\# Attack successes / # time slots elapsed
- as attacker may decide not to attack due to low accuracy evaluation



Attack detection intuition: a falsified sensing report created by adversarial spectrum would be close to the decision boundary. Thus, its distance to the decision boundary would be small.
Attack detection idea: design a decision to decision boundary (DDB) statistic over a time period as an indicator measure for attack detection.

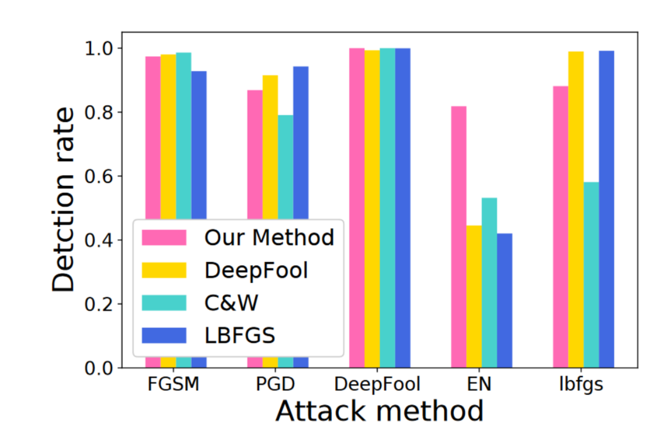
It is unclear what is a decision boundary in an AI-based spectrum sensing availability detector. Existing machine learning approaches to iteratively find the DDB: (i) DeepFool, (ii) LBFCG, and (iii) C&W
- In machine learning domain to handle image data generally
- Not optimized for wireless/spectrum applications

Our detection approach is to combine machine learning and wireless modeling to approximate the DDB by searching along a direction predicted by an LLR test built upon the wireless sensing data modeling.



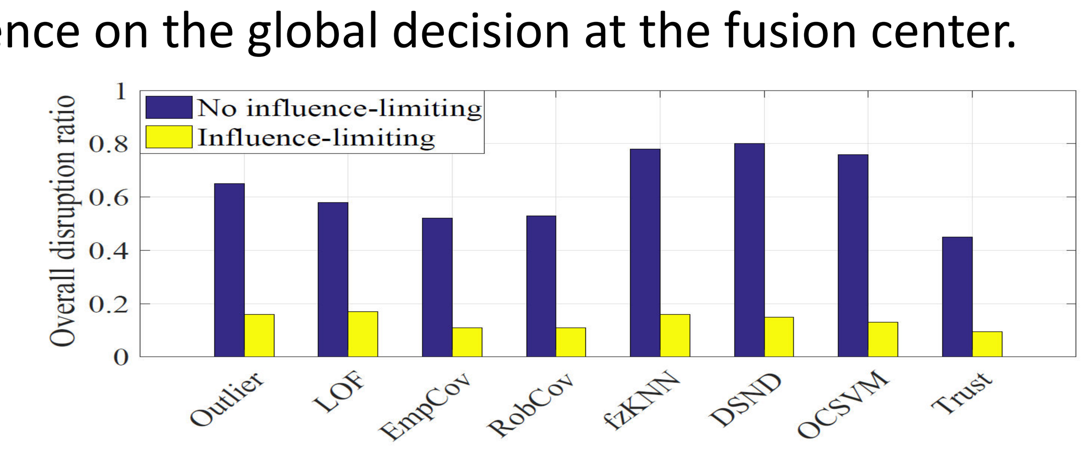
Detection Performance:
- Comparable performance to DeepFool, C&W, and LBFGS.

Computational Efficiency (Time used to find the DDB):
- 71% DeepFool, 8% C&W, and 2% LBFGS.



Mitigation and Management

- **Influence Limiting**: instead of offering a hard decision rule to clearly classify a node into either innocuous or malicious, we design a soft rule to discriminate certain nodes in the final decision by the fusion center.
  - When a node's signal strengths exhibit different properties during the training and testing (or decision) phases, we aim to limit its influence on the global decision at the fusion center.



- **Multi-Armed Bandit based Adversarial Spectrum Management**: instead of using a predetermined threshold function for the influence-limiting policy, we use multi-armed bandits to learn the optimal threshold function
  - In each timeslot when a set of nodes send their sensing data to the fusion center, the fusion center picks a threshold function depending on the contextual information of the data.