SysNetS

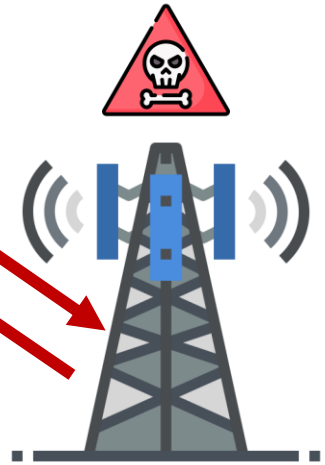
Gotta Detect'Em All: Fake Base Station and Multi-Step Attack Detection in Cellular Networks

Imtiaz Karim
Assistant Professor
Department of Computer Science
The University of Texas at Dallas

First OAI Foundation U.S. Hands-on Workshop, November 17

Fake Base Stations

Legitimate Base Station



Fake Base Station

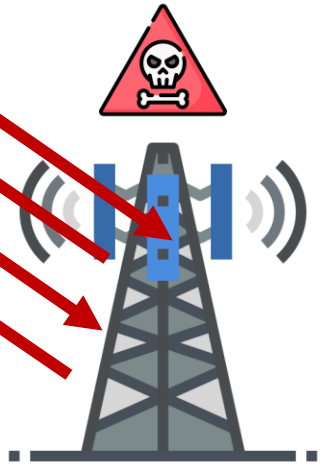
Are we connecting to a Legitimate Base Station?

Fake Base Stations and Multi-Step Attacks

Lack of authentication in initial broadcast messages

Legitimate Base Station

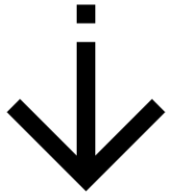
Connects naively to the strongest signal



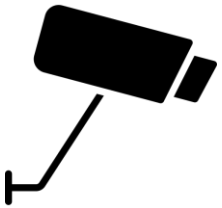
Fake Base Station

Location tracking

Denial-of-service



Downgrade



Activity monitoring

Motivation

CNN Politics SCOTUS Congress Facts First 2024 Elections Watch Listen

DHS confirms it has detected evidence of mobile snooping devices around DC

By Tal Kopan, CNN
2 minute read · Updated 9:11 AM EDT, Wed April 4, 2018

ELECTRONIC FRONTIER FOUNDATION

About Issues Our Work Take Action Tools Donate

Apple and Google Are Introducing New Ways to Defeat Cell Site Simulators, But Is it Enough?

BY COOPER QUINTIN | SEPTEMBER 13, 2023

SMS Blaster and IMSI-catcher News from Lebanon, Cambodia, Switzerland and the Philippines

By Eric Priezkalns 3 Nov 2025 Risk, Fraud & Security

Rogue radio communications devices are seemingly everywhere these days.

United States Secret Service

About Us Protection Investigations Mission Support Newsroom Careers Employee & Family Support Contact

U.S. Secret Service dismantles imminent telecommunications threat in New York tristate area

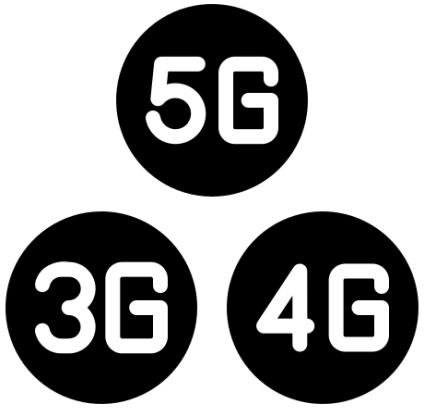
Published By U.S. Secret Service Media Relations
Published Date 2025-09-23

Technology

Gang Of Drivers Caught Using Stingrays To Send Fake Links And Steal Cash

May 25, 2023 *TNR Staff* Comments(3)

Motivation



A Persistent Problem

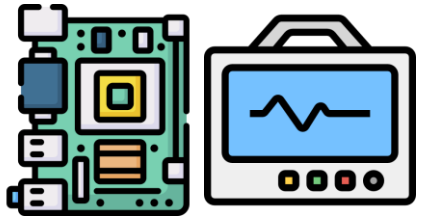
Billions of unprotected device

Impracticality and high cost of existing detection mechanisms

Solution – Goals?

Protect all the existing and new devices

No change in protocol



No additional hardware

Minimal Overhead

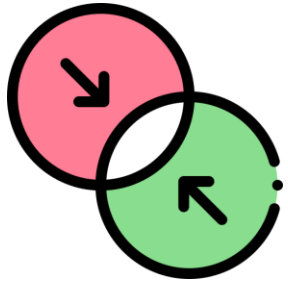
Supports Roaming

Challenges

Dataset availability and quality

Incorporating surrounding context

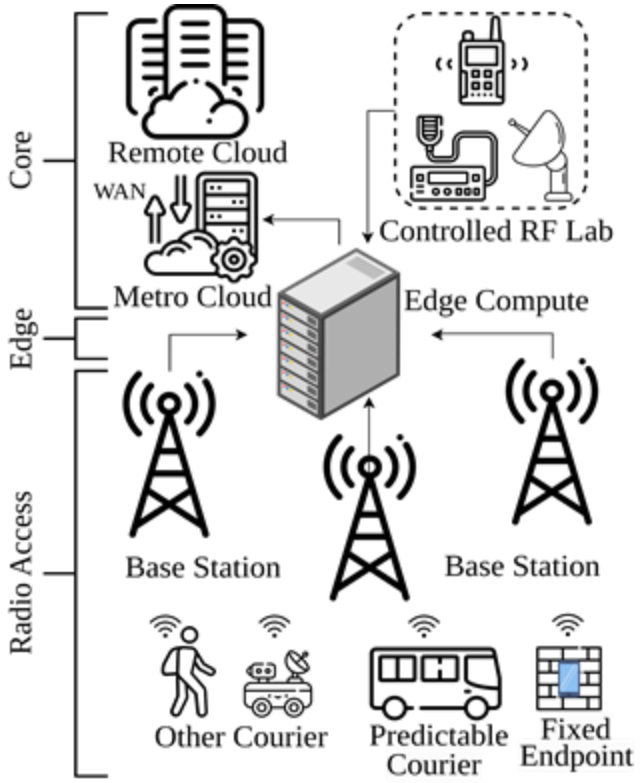
Learning MSA Characteristics

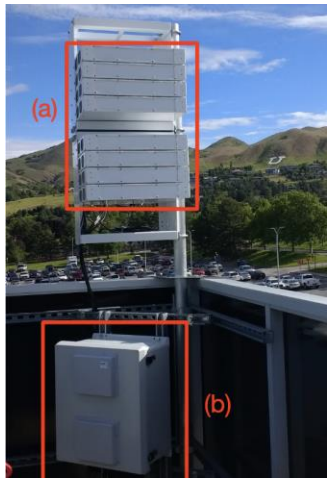


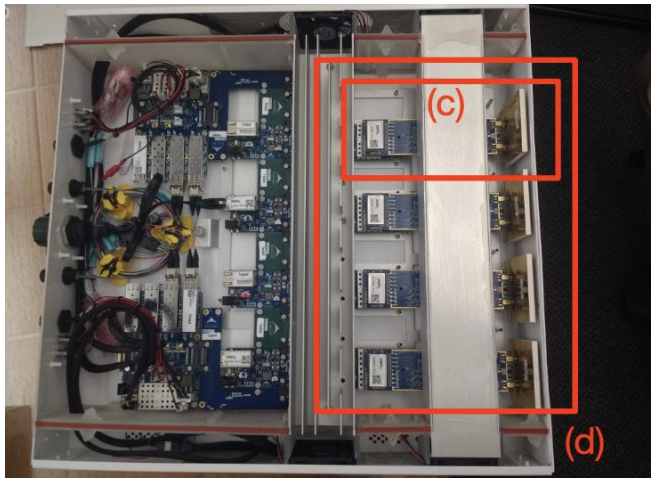
Combining Predictions

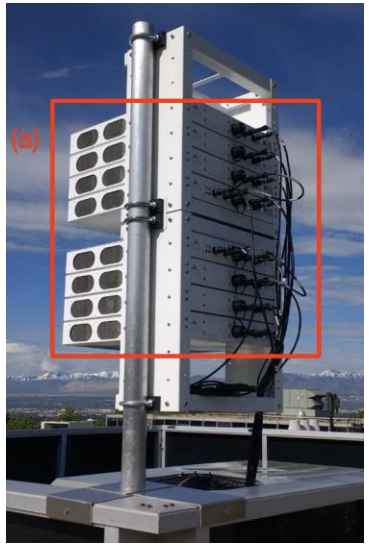
Real Time Detection

FBSDetector-POWDER







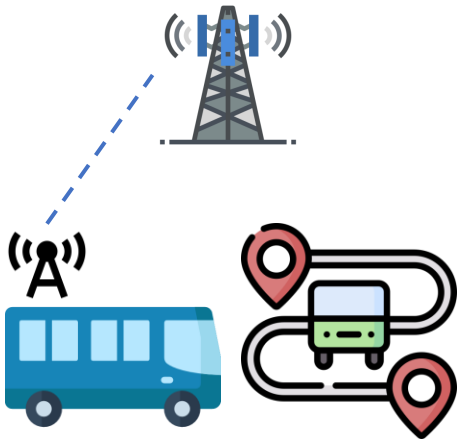


(a) Radio and antenna array; (b) Hub; © 2x2 Transceiver and antenna; (d) Transceiver chain

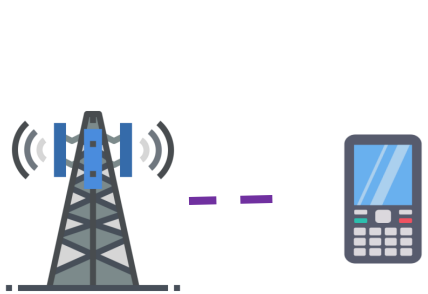
Capabilities leveraged:

- **P**latform for **O**pen **W**ireless **D**ata-drive **E**xperimental **R**esearch (POWDER)
- City-scale remote accessible large testbed by NSF
- Provides the capability to deploy FBS and attacks in real devices with actual packets following ethical guidelines
- Provides the capability to test mobility and signal overlapping

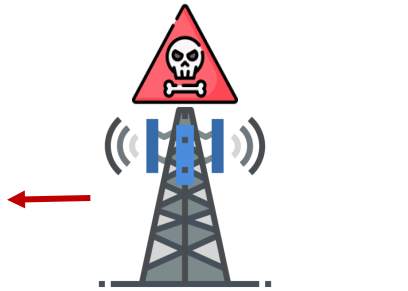
FBSDetector-Dataset Generation



Mobility



Legitimate Base Station



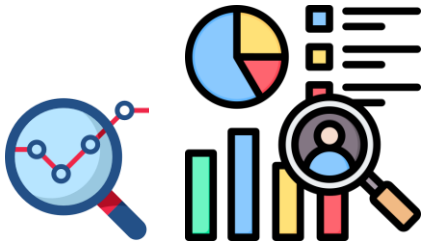
Fake Base Station

Attacker Level

Multi-step attacks

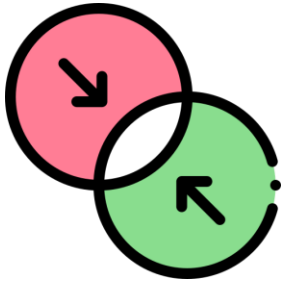
Challenges

Dataset availability and quality



Incorporating surrounding context

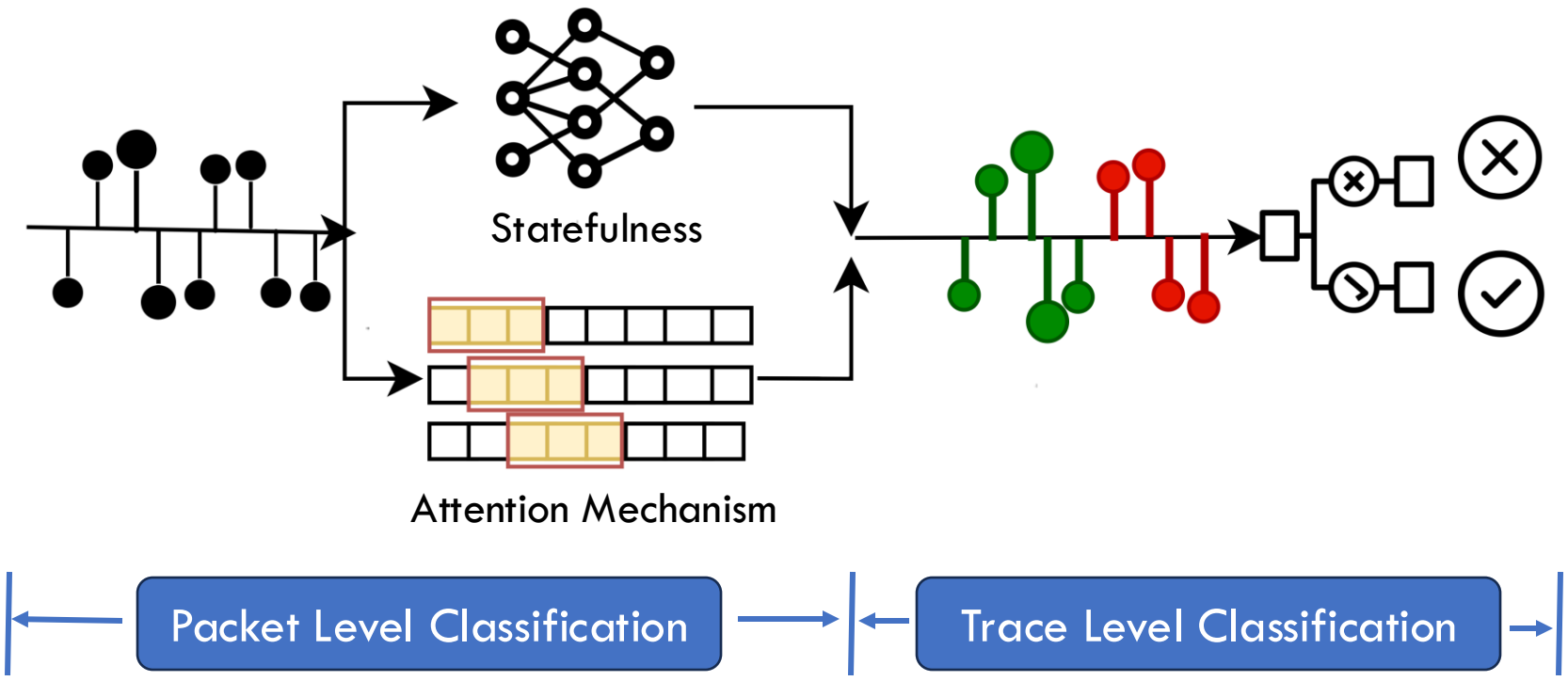
Learning MSA Characteristics



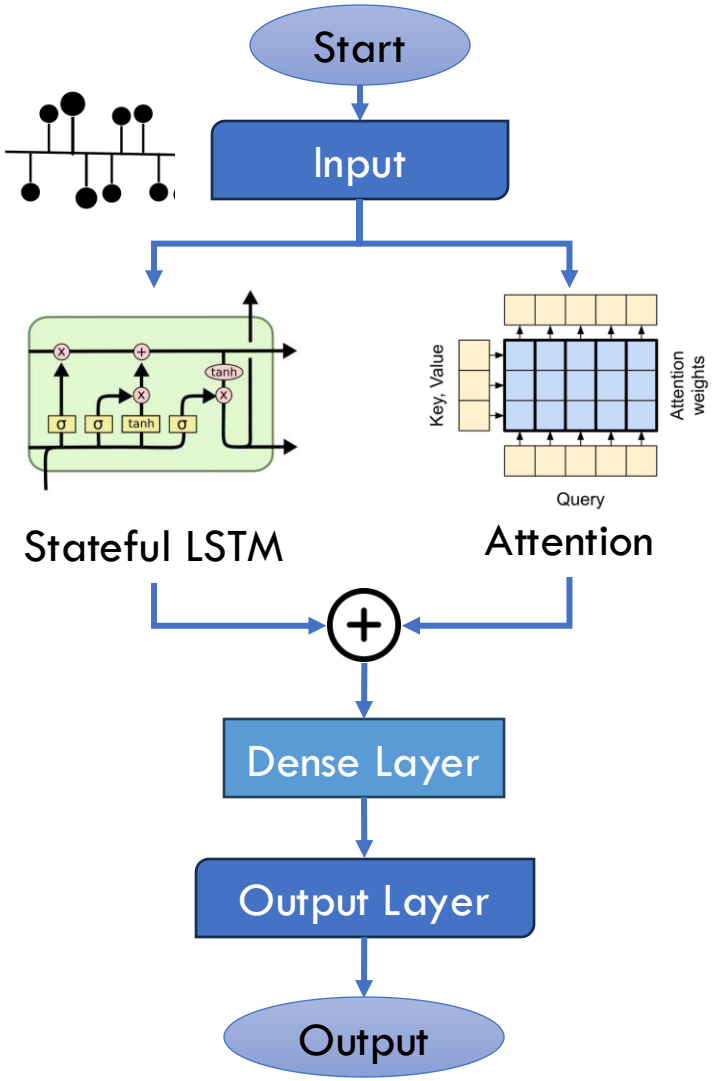
Combining Predictions

Real Time Detection

FBSDetector-FBS Detection



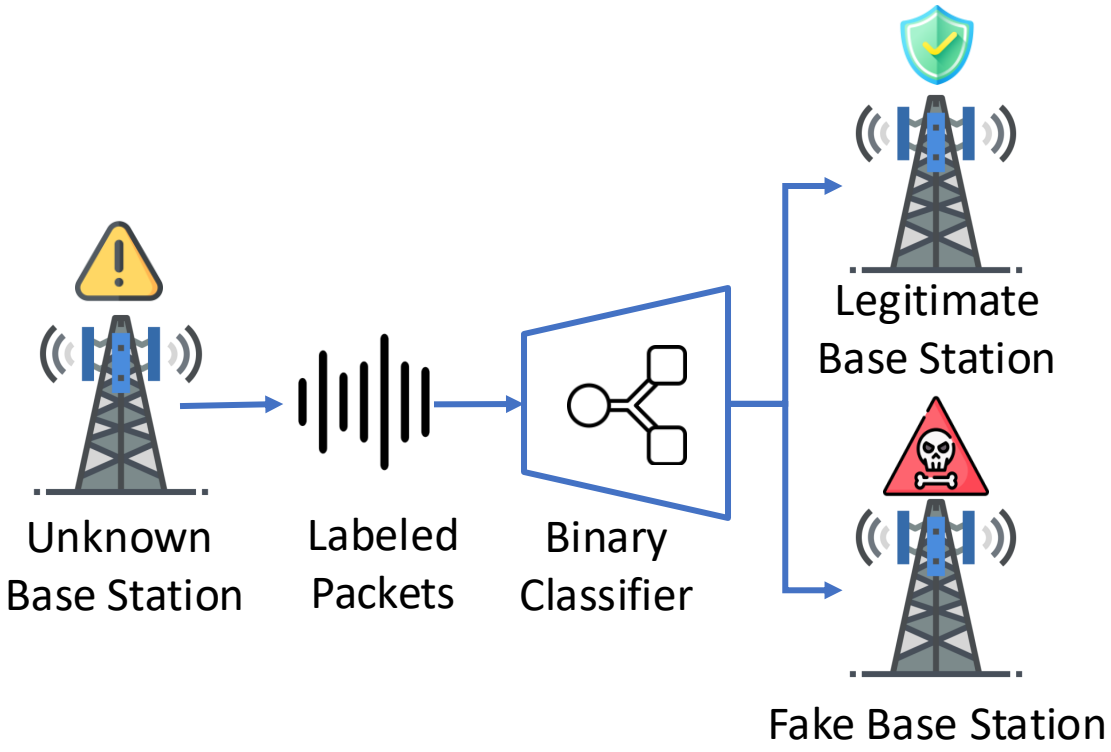
FBS Detection – Packet Level Classification



Advantages/ Strength:

- **Classifies each packet individually**
  - **Taking the context it was sent into consideration**
- **Statefulness models long-term dependencies**
  - **that span across sequences**
- **Attention mechanism focuses on the parts of each sequence**
  - **that affect the classification outcome the most**

FBS Detection – Trace Level Classification

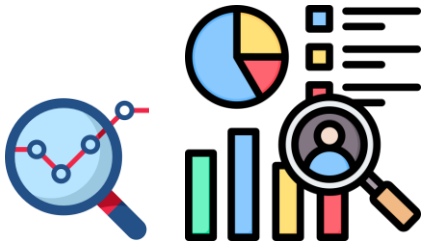


Advantages/ Strength:

- **Classifies the whole labeled trace from packet level classification**
- **Examines the order of packets and**
  - **sequence patterns**
  - **to discern characteristics indicative of FBS**

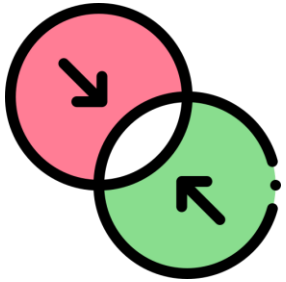
Challenges

Dataset availability and quality



Incorporating surrounding context

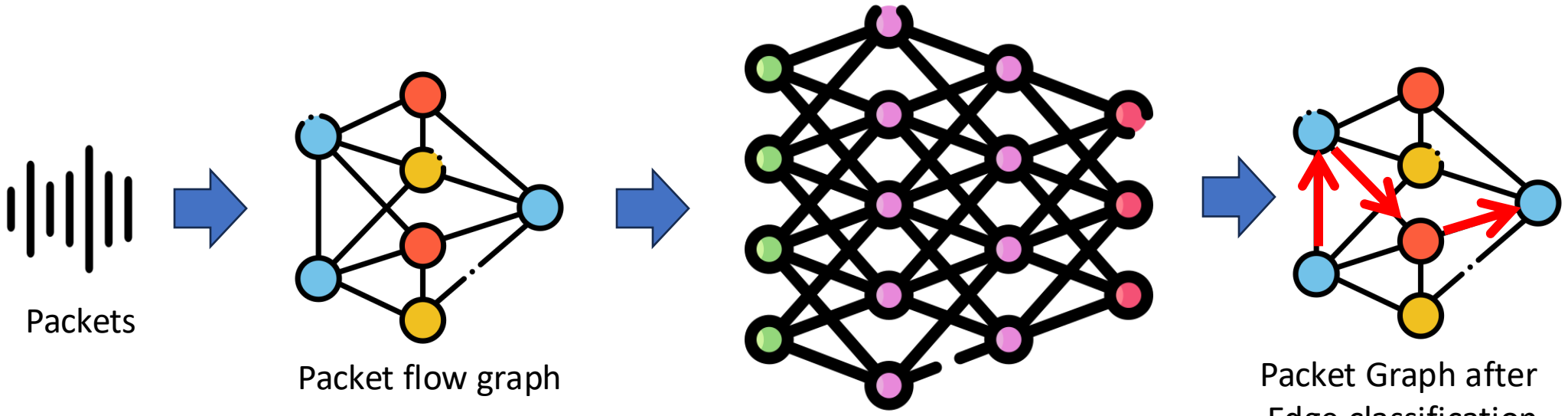
Learning MSA Characteristics



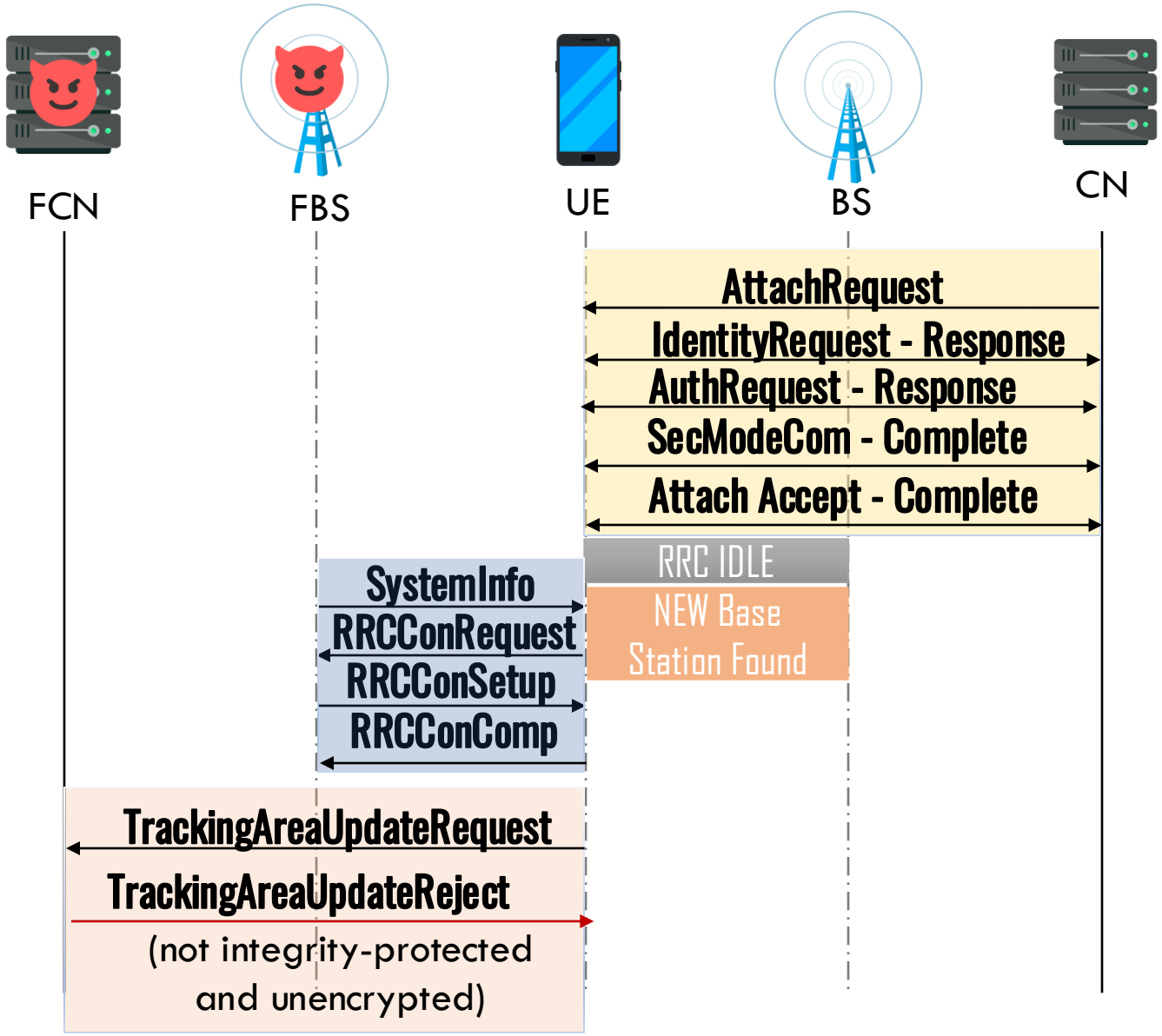
Combining Predictions

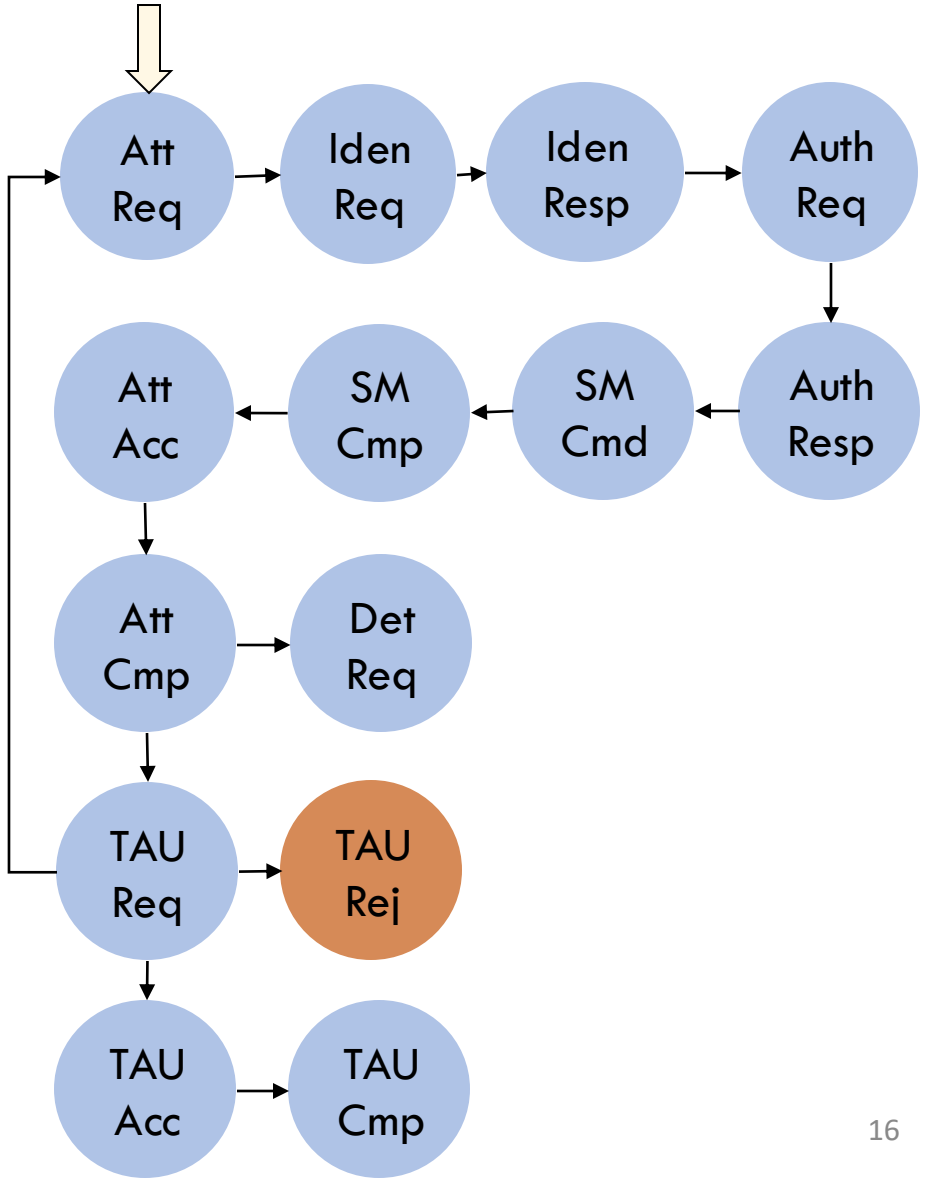
Real Time Detection

FBSDetector-MSA Recognition



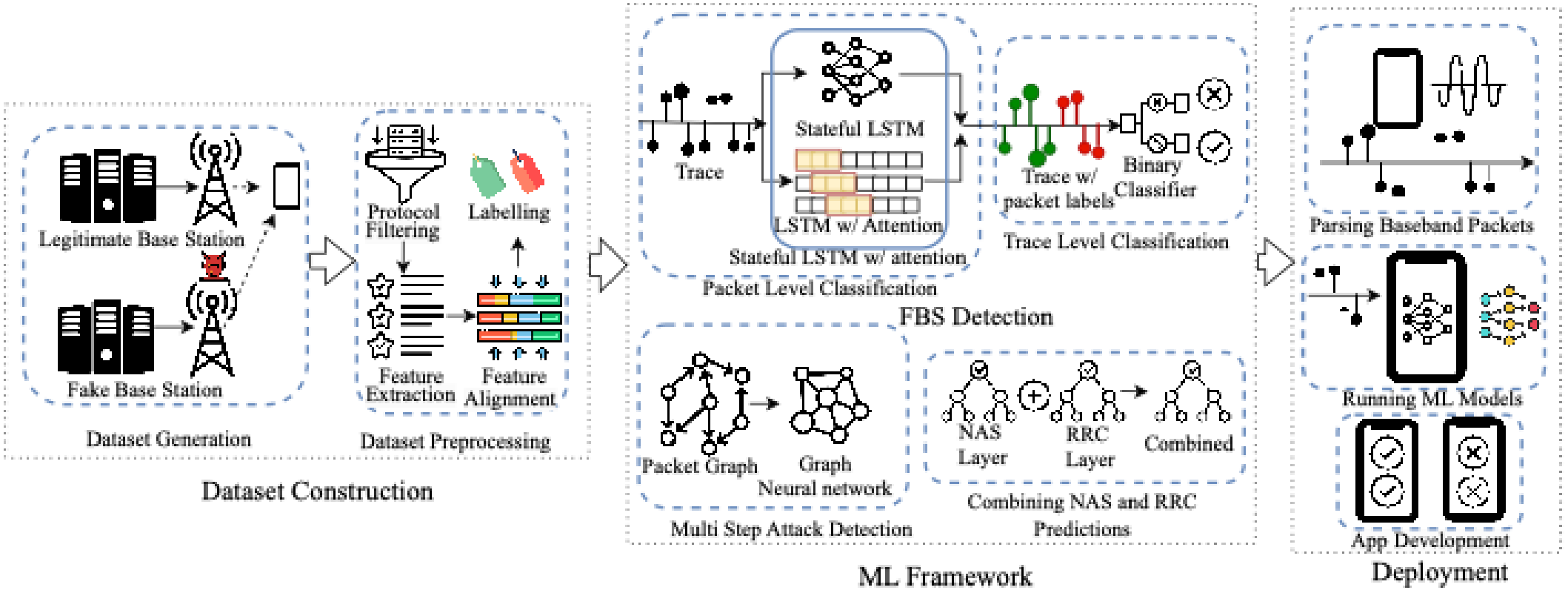
FBSDetector-MSA Recognition Example





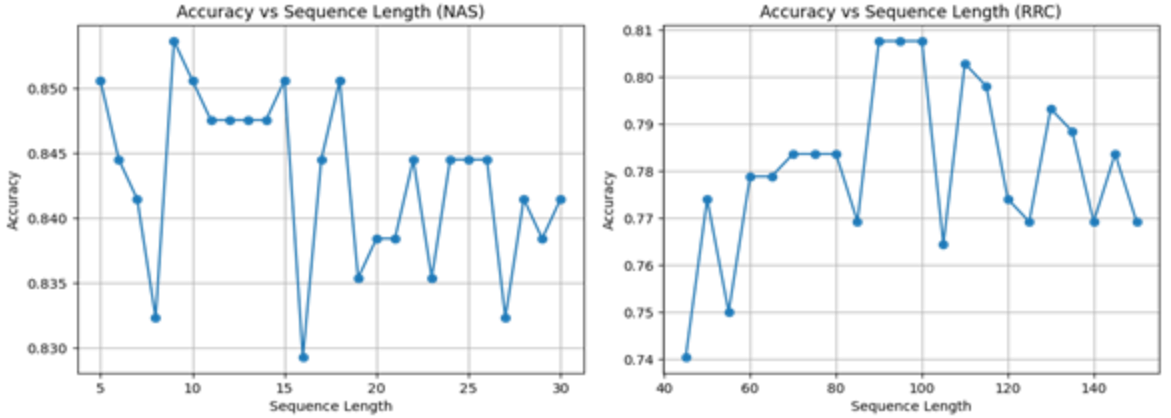
FBSDetector-Overall Solution

Overview of our end to end solution to detect FBSes and MSAs

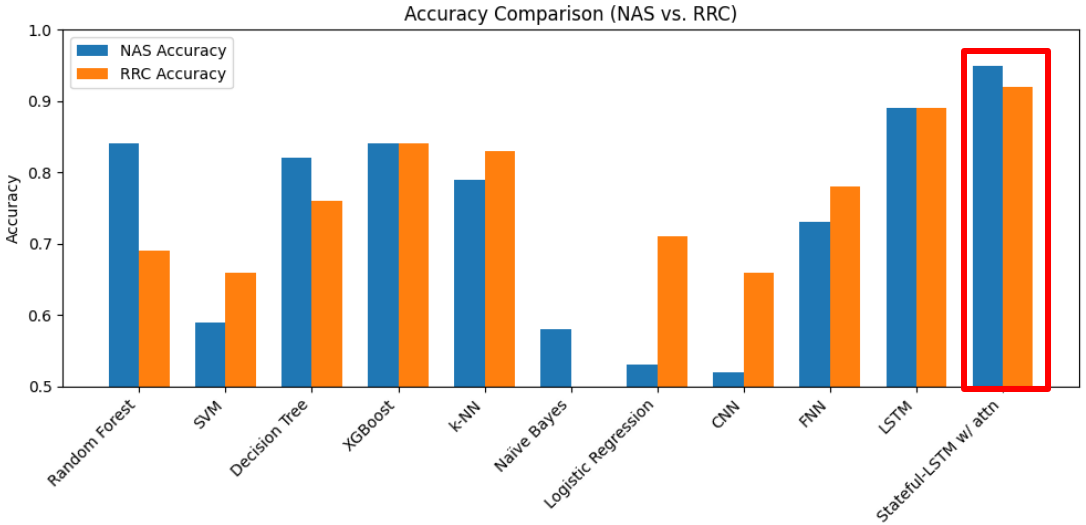


RQ1: FBS and MSA Detection Accuracy

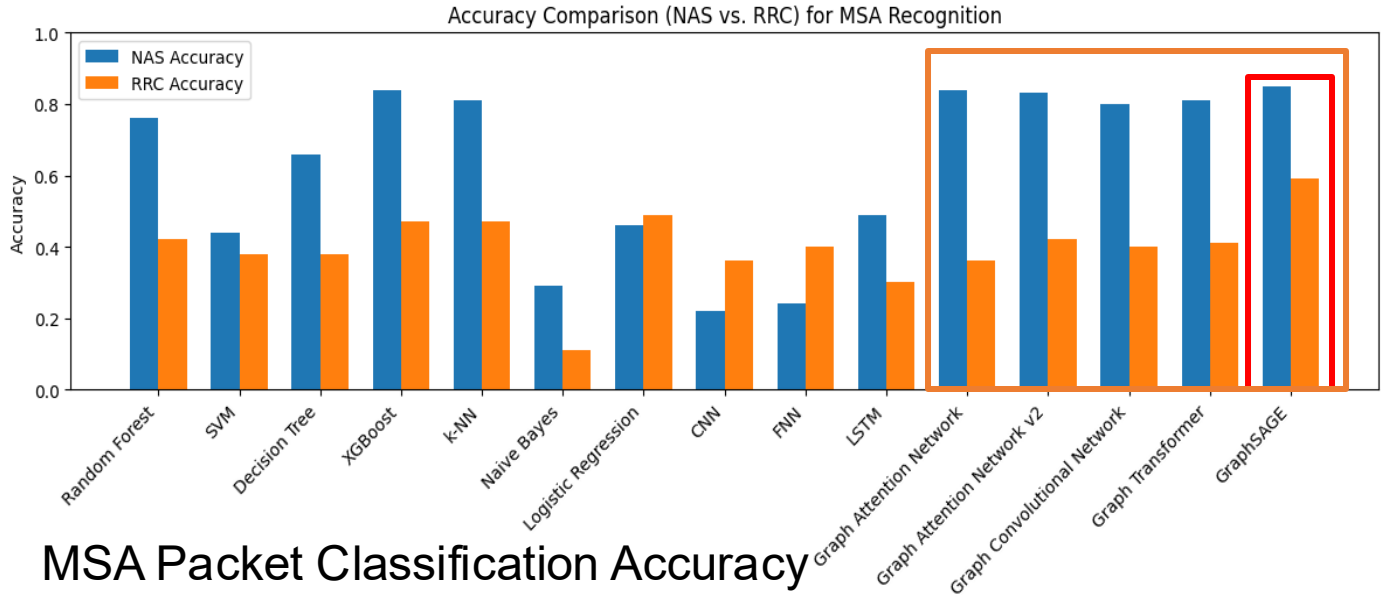
Criteria	Performance
FBS Detection Accuracy	96%
MSA Detection Accuracy	86%
False Positive Rate (FBS)	2.96%
False Positive Rate (MSA)	3.28%
# MSAs Detected	21



Acc vs seq length

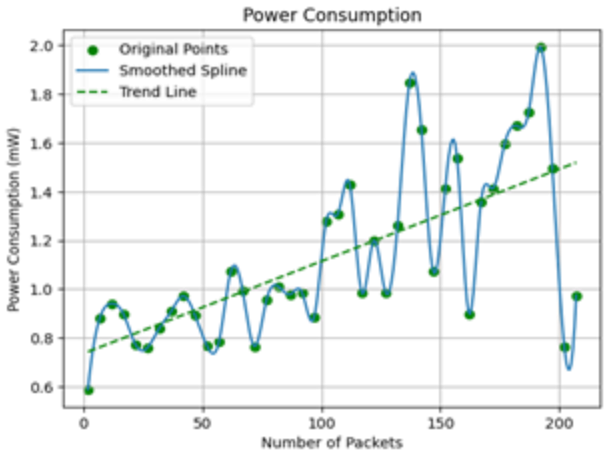


FBS Packet Classification Accuracy

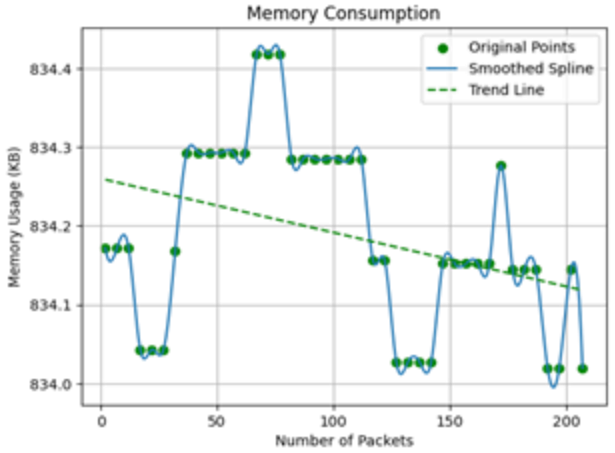


MSA Packet Classification Accuracy

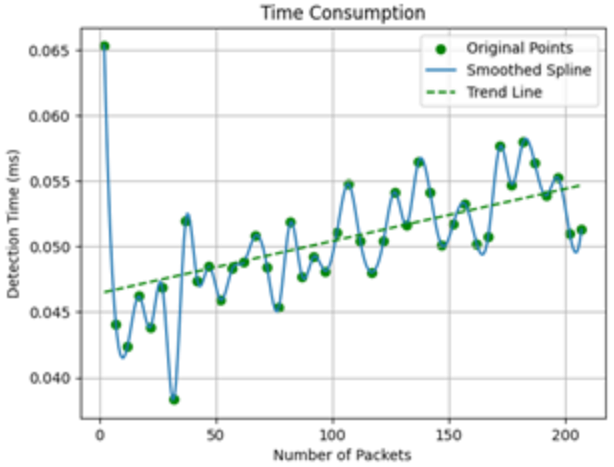
RQ2: Overhead Analysis



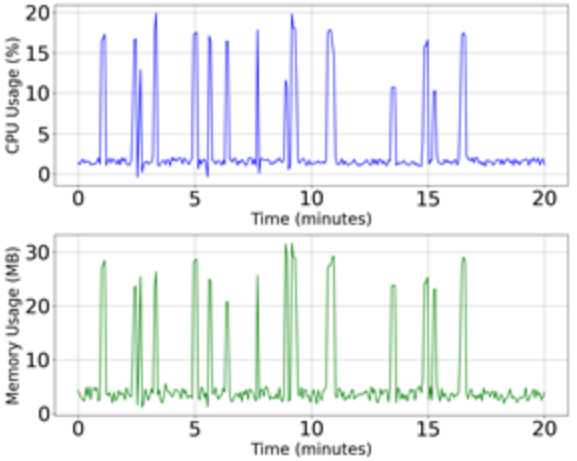
Power Consumption



Memory Consumption



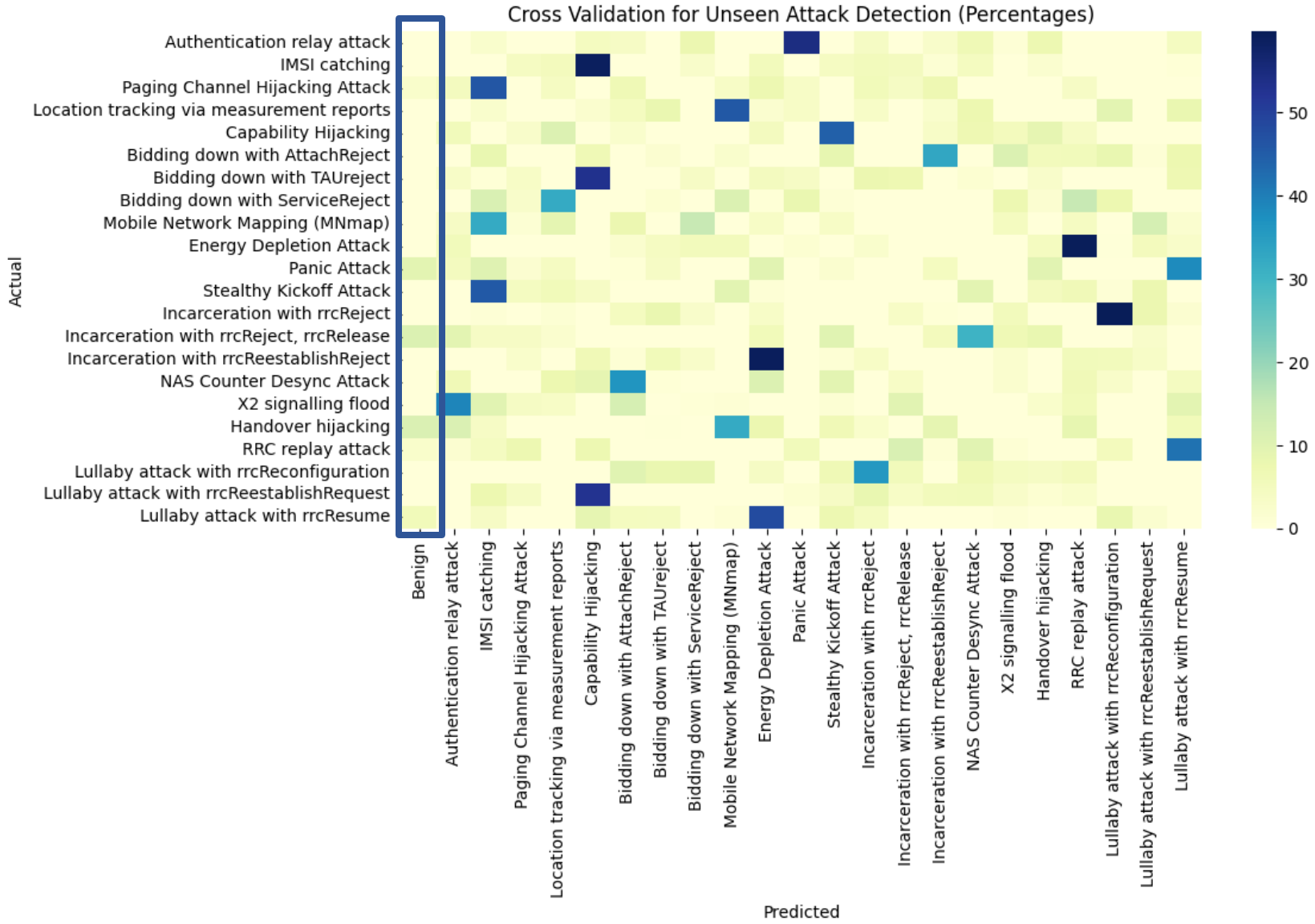
Time Consumption



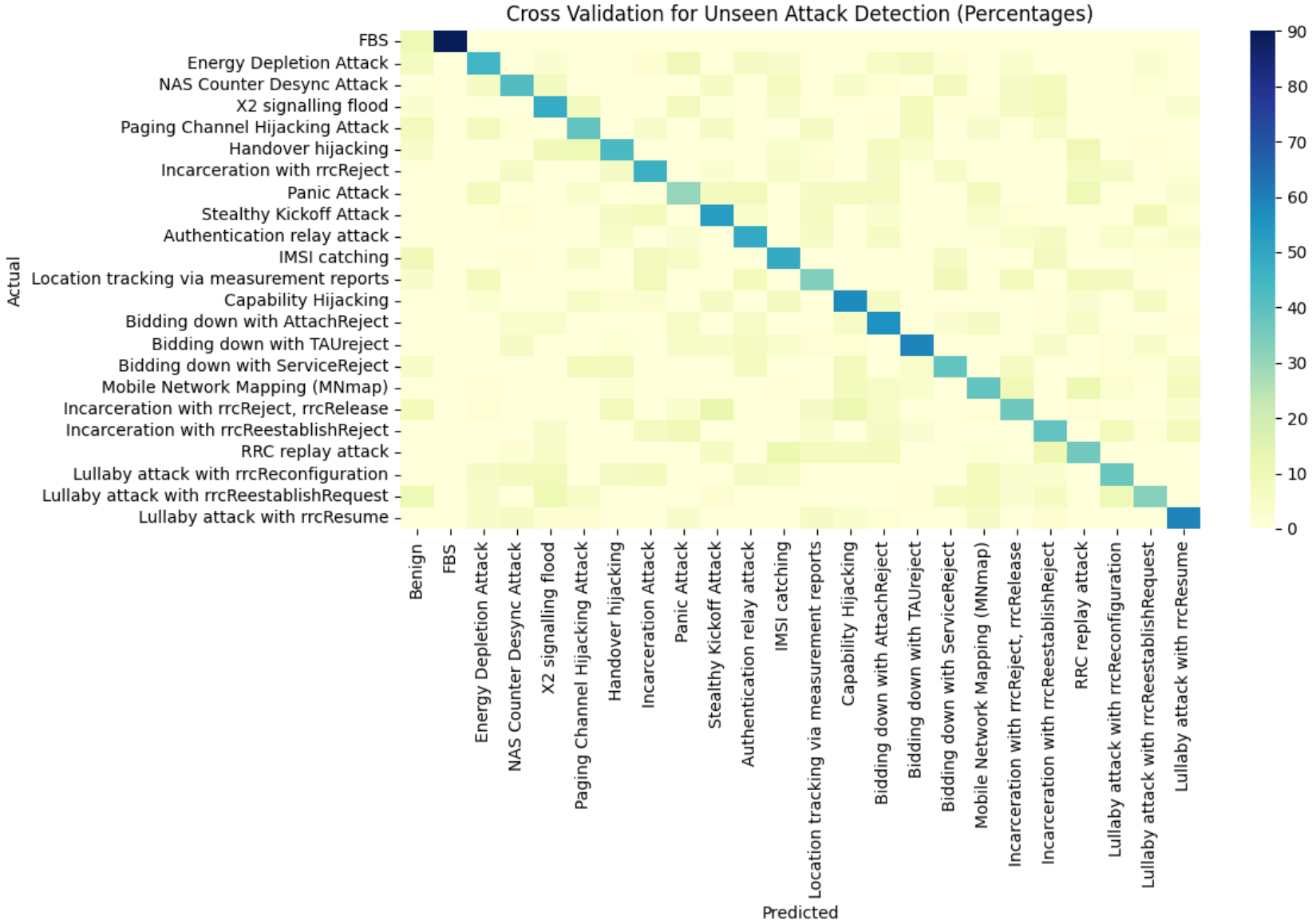
Memory and CPU usage by the mobile app

RQ3: Real world Validation

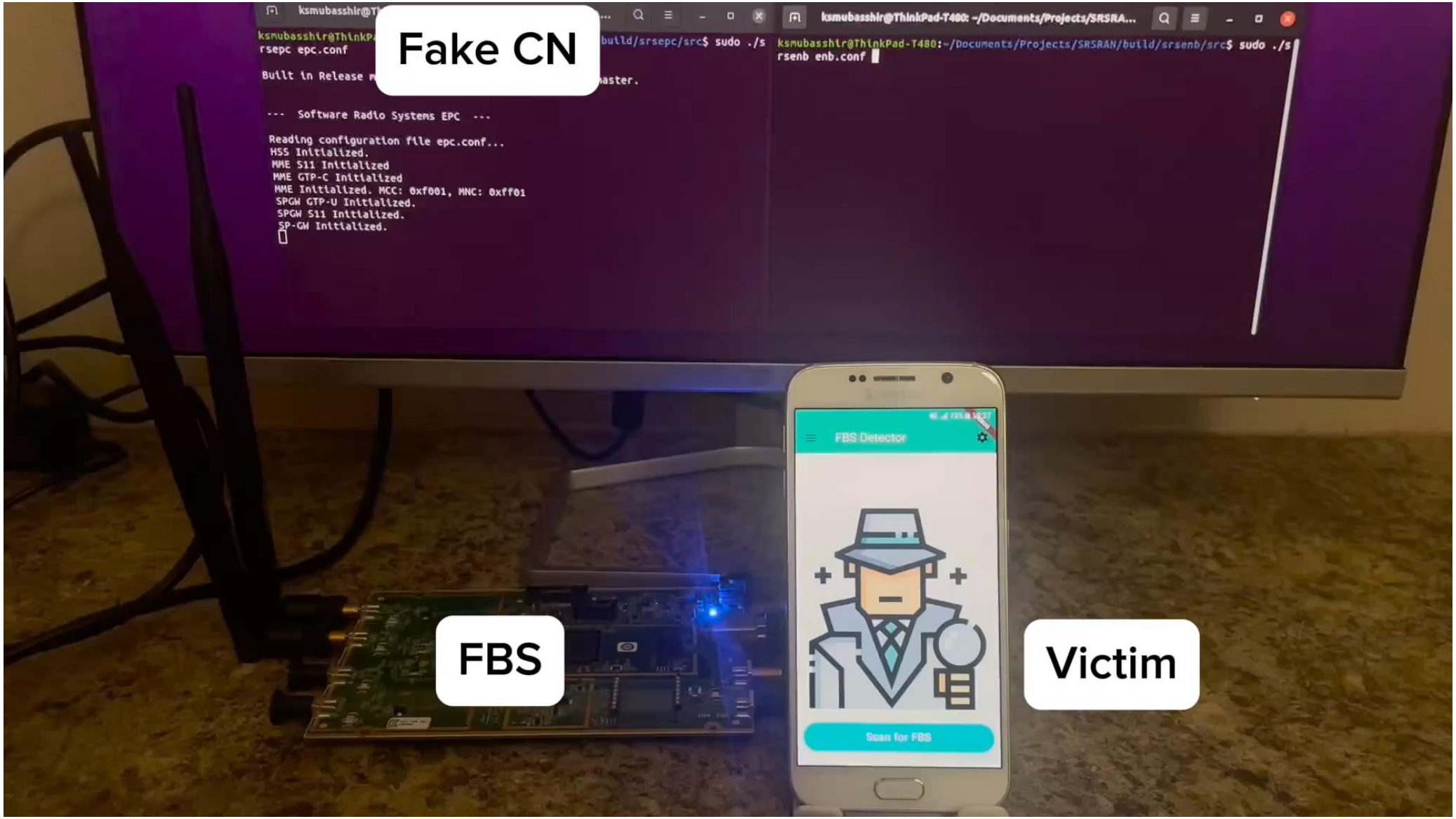
RQ4: Unseen and Reshaped Attack Evaluation



RQ4: Unseen and Reshaped Attack Evaluation



FBSDetector (Demo)



Summary and Impact of FBSDetector

FBSDetector- a framework to detect FBSes and MSAs from network traces using ML

The *first*-*ever* large real-world FBS and MSA datasets

Thanks, and Questions?

Our team is working with a company to deploy a version of the solution to core networks

https://fbsdetector.github.io/