Trust and Control with Multi-Network RF Devices

Wayne Phoel
Program Manager, Strategic Technology Office

ISART Panel on Regulatory Issues

2 August 2016

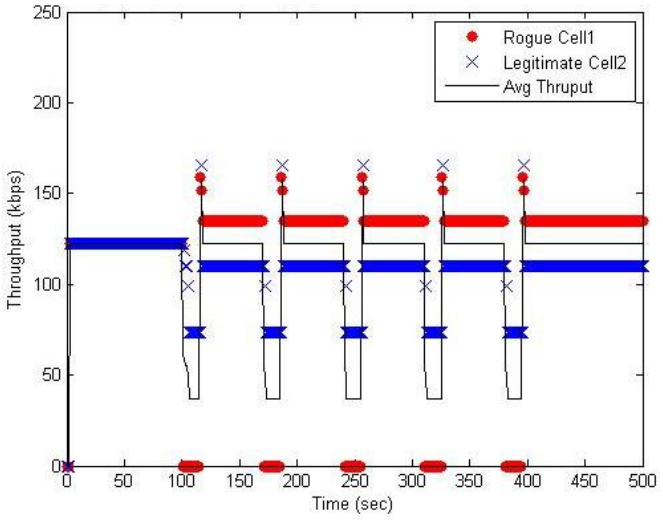
Toward Reliable Network Control

- RF devices no longer built single-band or even single function
  - Multiple simultaneous bands
  - Multiple simultaneous networks
  - Dynamically configurable
- Mechanisms implemented for system-level coordination present opportunities for bad actors to disrupt service
- Two developments are needed:
  - Protect wireless control protocols – LTE example
  - Dynamic security key generation and management

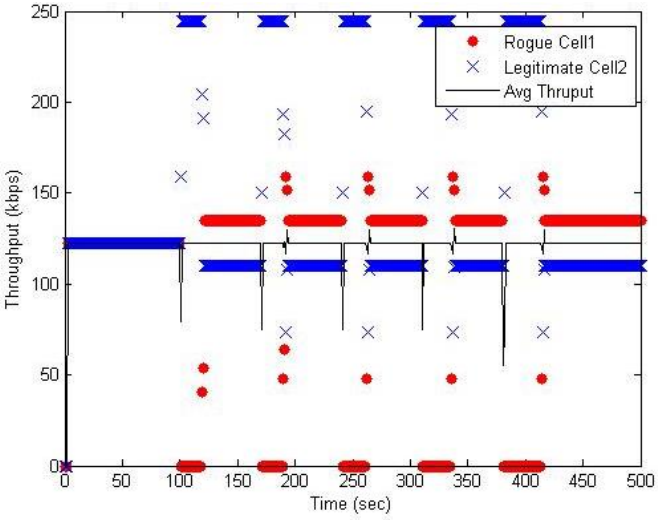
Determining Trust in the Network Control Plane

- Wireless networks increasingly use shared information to configure radios
- Bad information in the control can make the network unusable
- Insight: Multiple network observables provide context to determine trustworthiness of individual nodes
- Example: LTE eNodeB sensitivity to false/inaccurate load reports

Unprotected

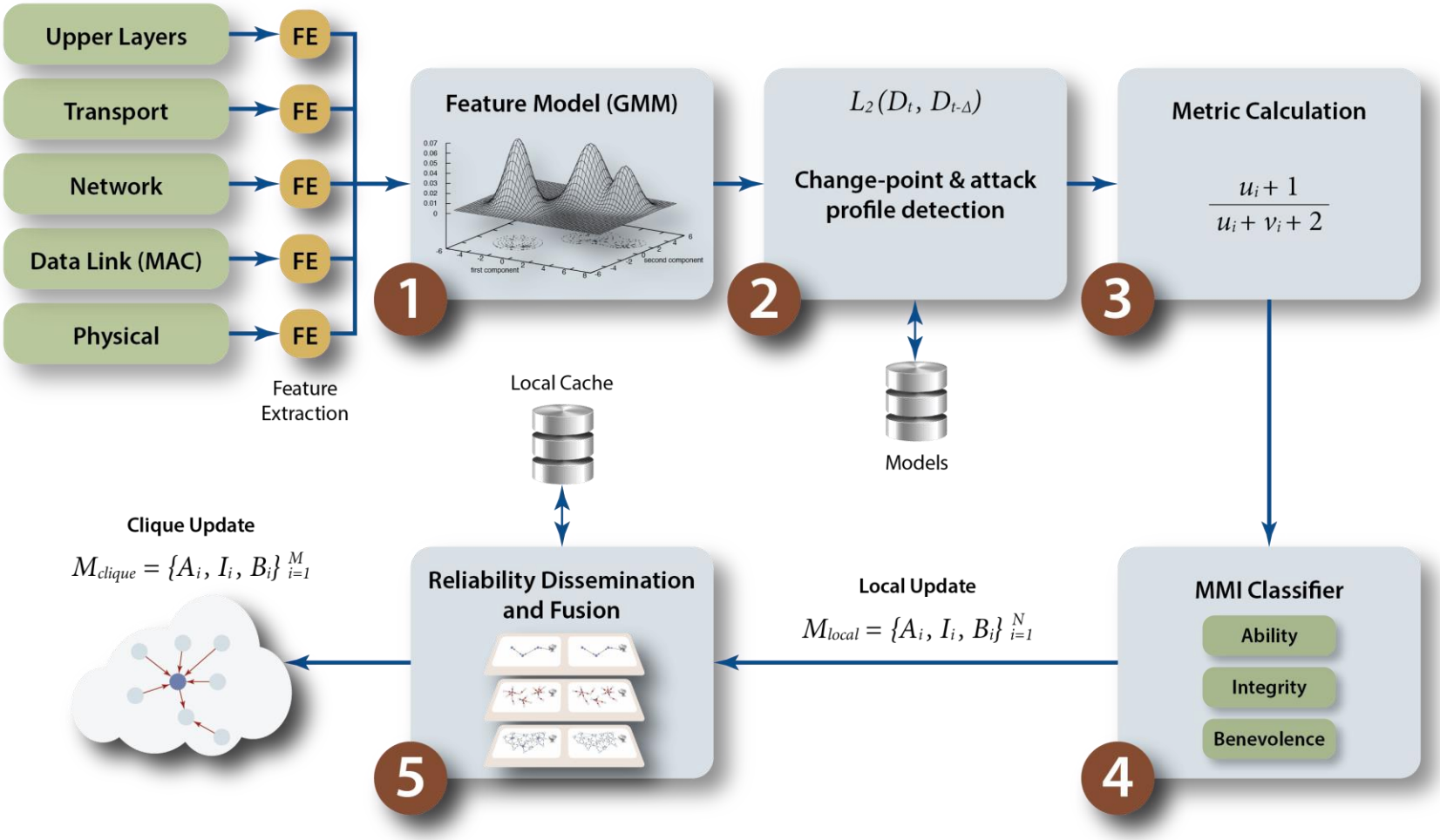


Mitigations Enabled

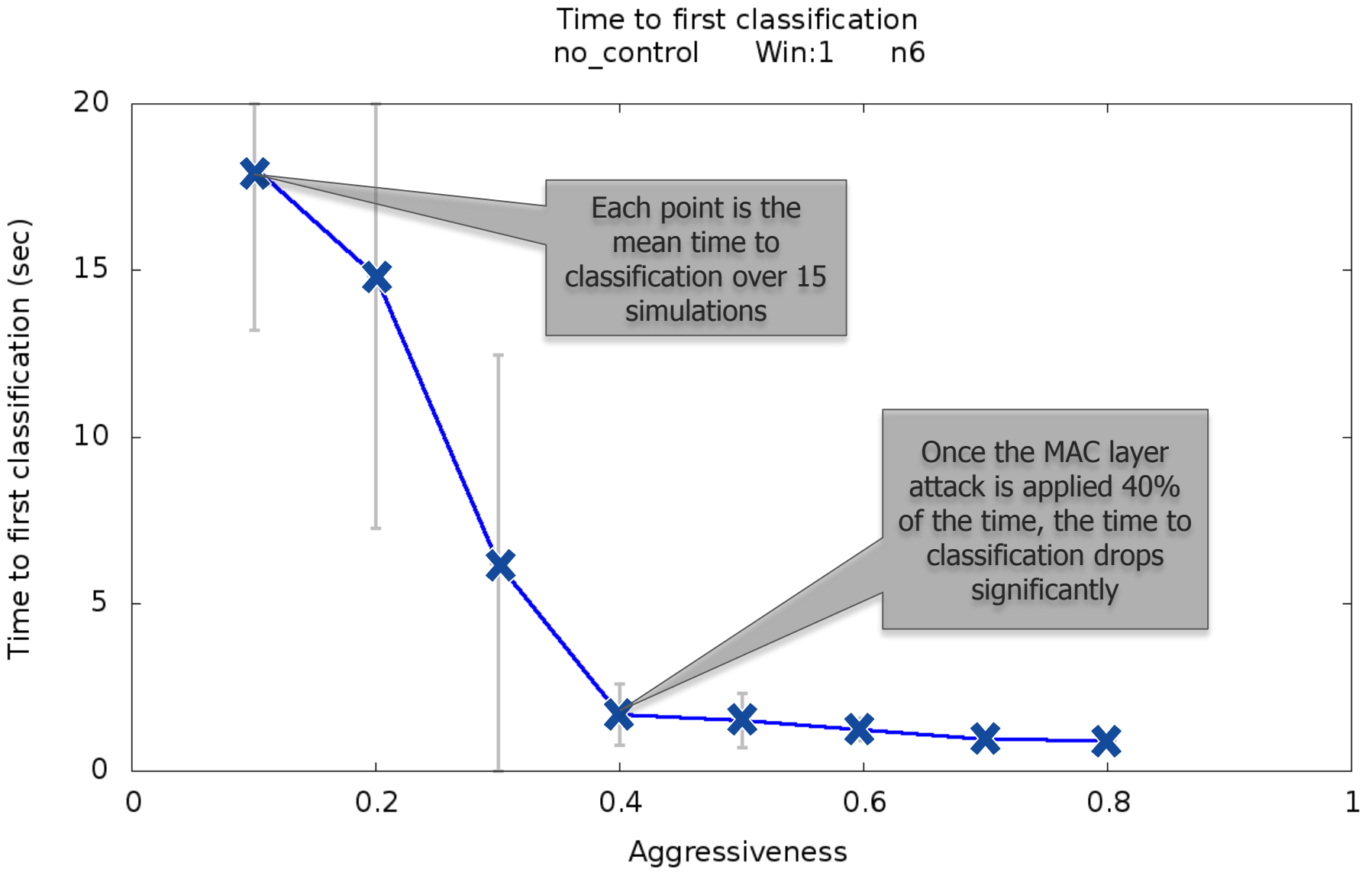


Cell1 sends periodic false load reports to Cell2, starting at 100s

Example Reliability Inference Approach

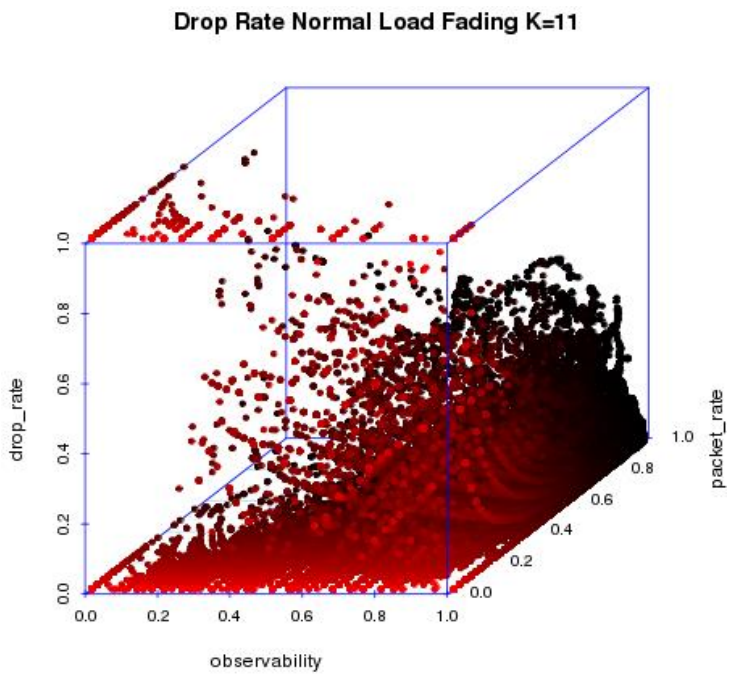


Example Time to First Classification: Wi-Fi MAC



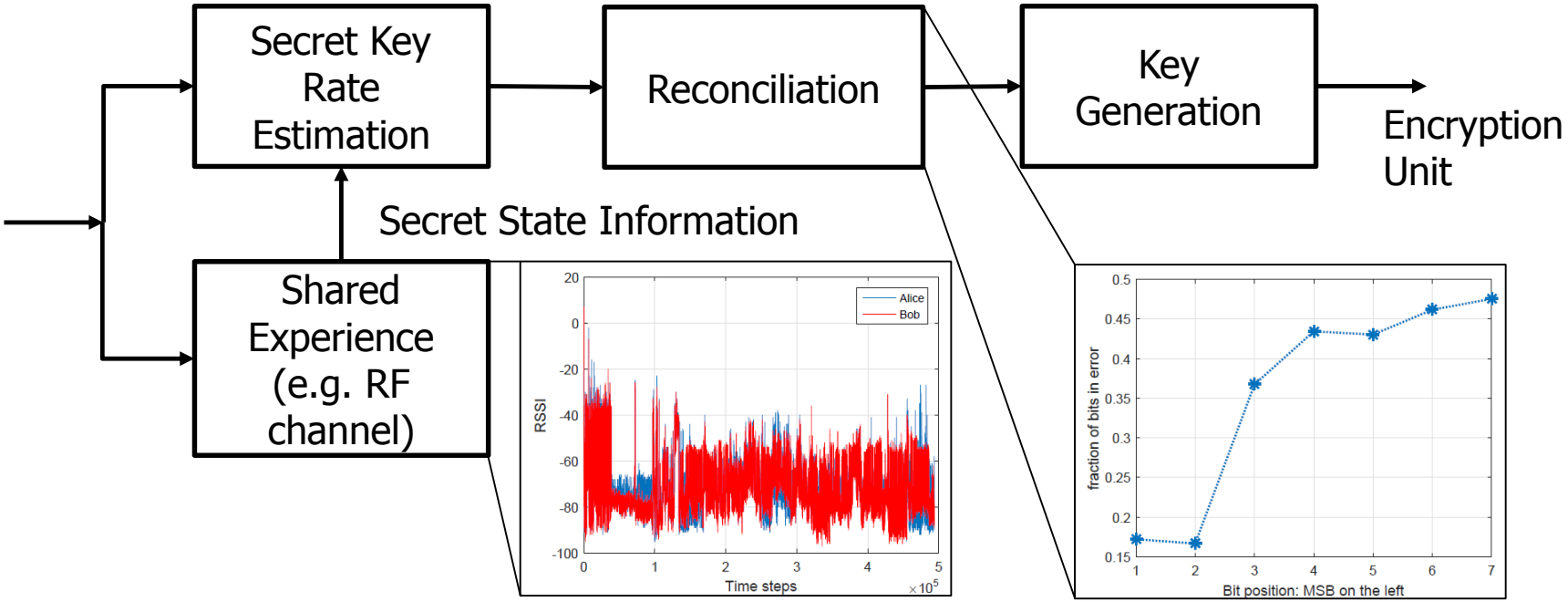
Unsupervised Learning Detects Packet Drops

- Goal: Find anomalies in node's forwarding behavior based on observation of features that are robust to network changes
- Approach: Statistical Detector
  - Peer nodes capture MAC frames in promiscuous mode and observe forwarding characteristics
  - Use cross-layer information to assess forwarding behavior, synthesized in three features that are robust to network changes:
    - Forward request packet rate
    - Observability ratio
    - Drop rate
  - Entirely local and passive



New Keying and Authentication Architectures

- Traditional authentication and encryption architectures don't scale for future dynamic, multi-network uses
  - Keys susceptible to loss
  - Don't handle the variable ways in which users will want to protect information
- Time-varying network statistics can support identification and authentication



Key is, these observations are happening all the time, enabling frequent updates to shared secret