STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

Machine Learning in Wireless Security

Founding Director, Stevens Institute of Artificial Intelligence

Prof. K.P. (Suba) Subbalakshmi

Dept. of Electrical and Computer Engineering

Jefferson Science Fellow

http://www.stevens.edu/siai

http://www.kpsuba.com

ksubbala@stevens.edu

Security Questions in Spectrum Agile Networks

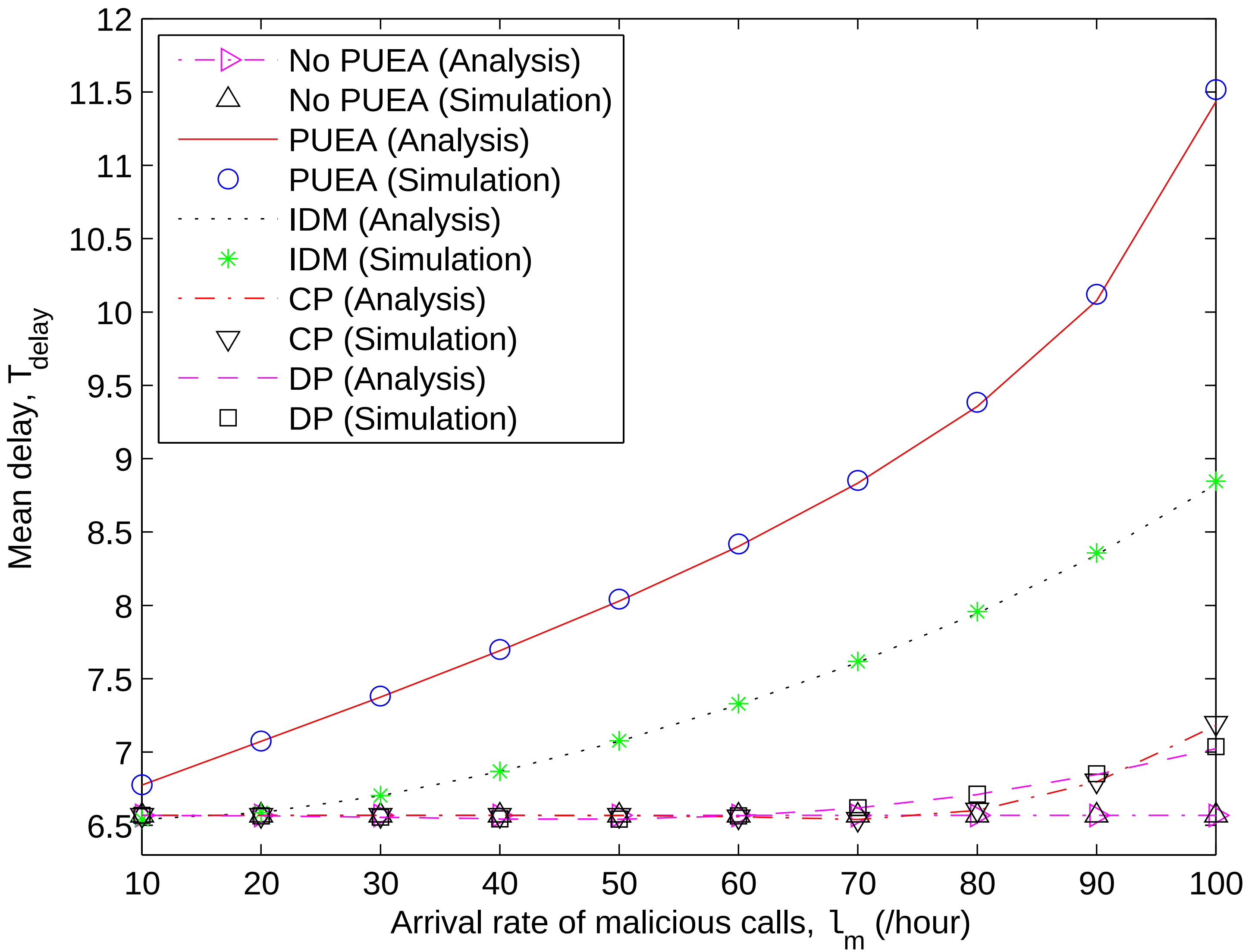
--- as distinct from general wireless network security

- Difference between “regular” wireless networks and spectrum aware networks lies in using spectrum “wisely and opportunistically”
- To use available spectrum “wisely”
  - Sense it (spectrum opportunity, and switch if necessary)
  - Store it (in a database)
  - Combine it (spectrum aggregation)
  - Use only what is needed, when needed (fragmentation)
- What are the vulnerabilities in these basic functions?
- How does ML play a role in both vulnerabilities and security measures?

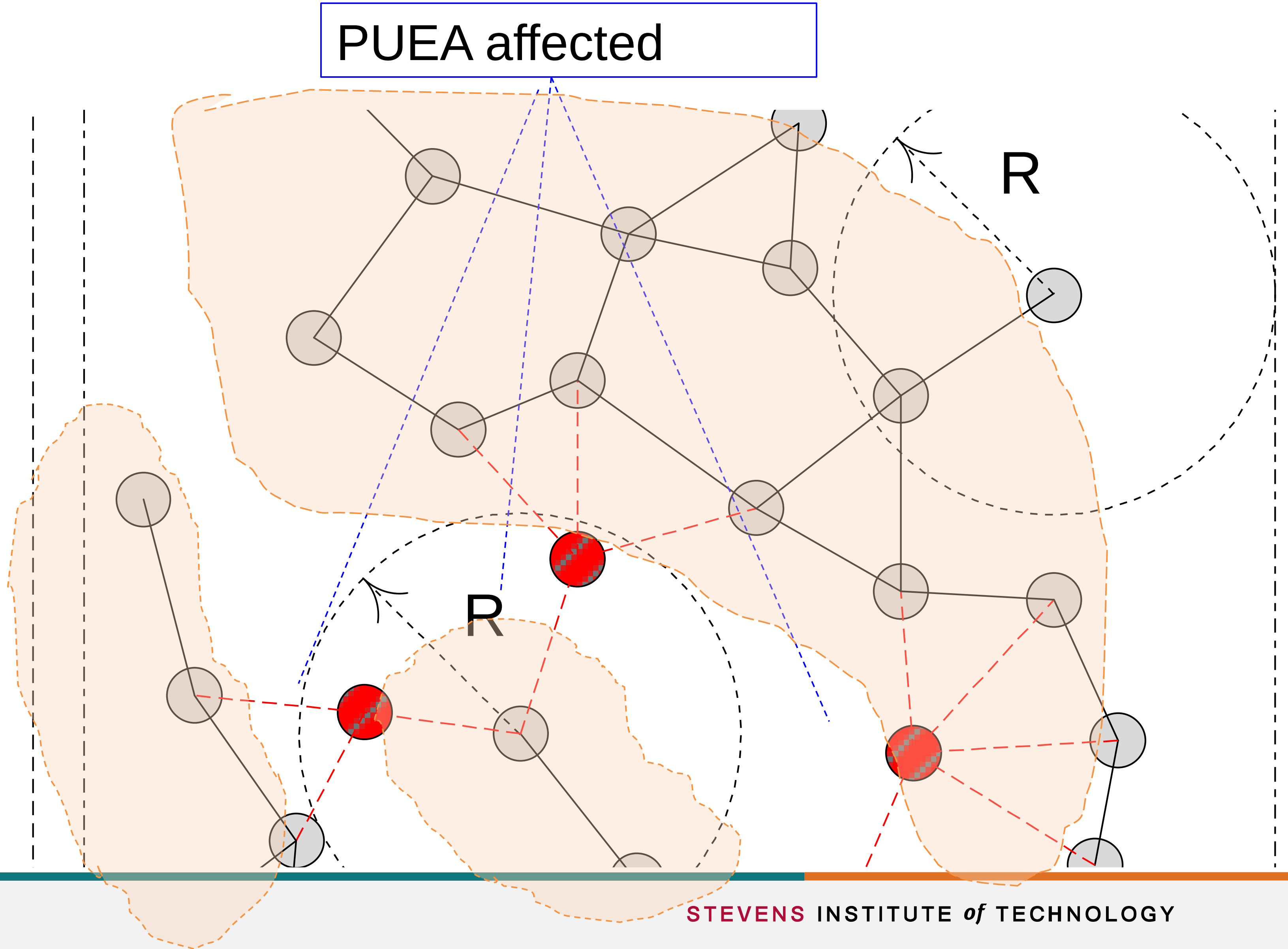
Attacks on Spectrum Agile Networks

- Thinking about attacks from
  - Impact perspective
  - Mechanics perspective
- Impact perspective (hitting at core value of spectrum agility – resource optimization)
  - Disrupting communication
    - Forced change of spectrum bands
      - Mechanisms:
        - PUEA
        - jamming attacks
        - spectrum data falsification attacks, etc.
      - Results: disconnected secondary networks, excessive delays in communications

Greedy PUEA can cause significant increase in delays



Network connectivity can be affected



Attacks on Spectrum Agile Networks

- Draining resources
  - Forced repeated change of spectrum bands
    - Mechanisms: Disrupting rendezvous mechanisms, PUEA and jamming attacks
    - Result: can cause rapid loss of battery power
  - Sybil like attacks
    - Multiple identities to grab more resources and disrupt fairness
- Privacy issues – location
- Secrecy issues – eavesdropping, leakage of information due to aggregation

ML in Attack and Defense

- Adverserial learning
  - Inference attacks: the attacker learns how the learning system works
    - Example effects: can learn sensitive information of the system
    - Another example: ML methods are used to learn when a primary is present or absent, this method can by unauthorized user to predict when the PU is present to launch a jamming attack (less power used)
  - Evasion attacks: Fooling the system to accept wrong results.
    - Useful when creating Sybil type attacks
    - Fooling decision mechanism to accept wrong results
  - Poisoning attacks: where false information is supplied to the learning mechanism
    - Useful in spectrum falsification type attacks

Impact of ML in Attack and Defense

- Reinforcement learning can be used to help deal with Byzantine attacks in crowd sensed systems
- ML can be used to help distinguish between unintentional “attacks” and intentional attackers
- Building uncertainty models for spectrum occupancy to predict future occupancy
    - Good models can be both an attack and a defense!
- Model based learning vs model free learning (like RL)

Open Questions/Challenges

- Deciding between a plethora of ML methods/approaches for specific applications
  - Difficult to compare apples to oranges
  - Combining strategies
  - Model stacking
- Data imbalance
  - Under representation of attacker data
- How to make the system “unlearn”
- Sample efficient learning – with very little data
- Robust defense against adverserial examples

The Networking and Information Technology Research and Development (NITRD) Program

Mailing Address: NCO/NITRD, 2415 Eisenhower Avenue, Alexandria, VA 22314

Physical Address: 490 L'Enfant Plaza SW, Suite 8001, Washington, DC 20024, USA Tel: 202-459-9674, Fax: 202-459-9673, Email: nco@nitrd.gov, Website: https://www.nitrd.gov