Potential Cognitive Radio Denial-of-Service Vulnerabilities and Countermeasures

Amita Sethi
Timothy X Brown
University of Colorado, Boulder

Presented at:
2007 International Symposium on Advanced Radio Technologies
Boulder, Colorado
February 27, 2007

UC-Boulder

Main Insight

Additional Protocols → **Additional Vulnerabilities**

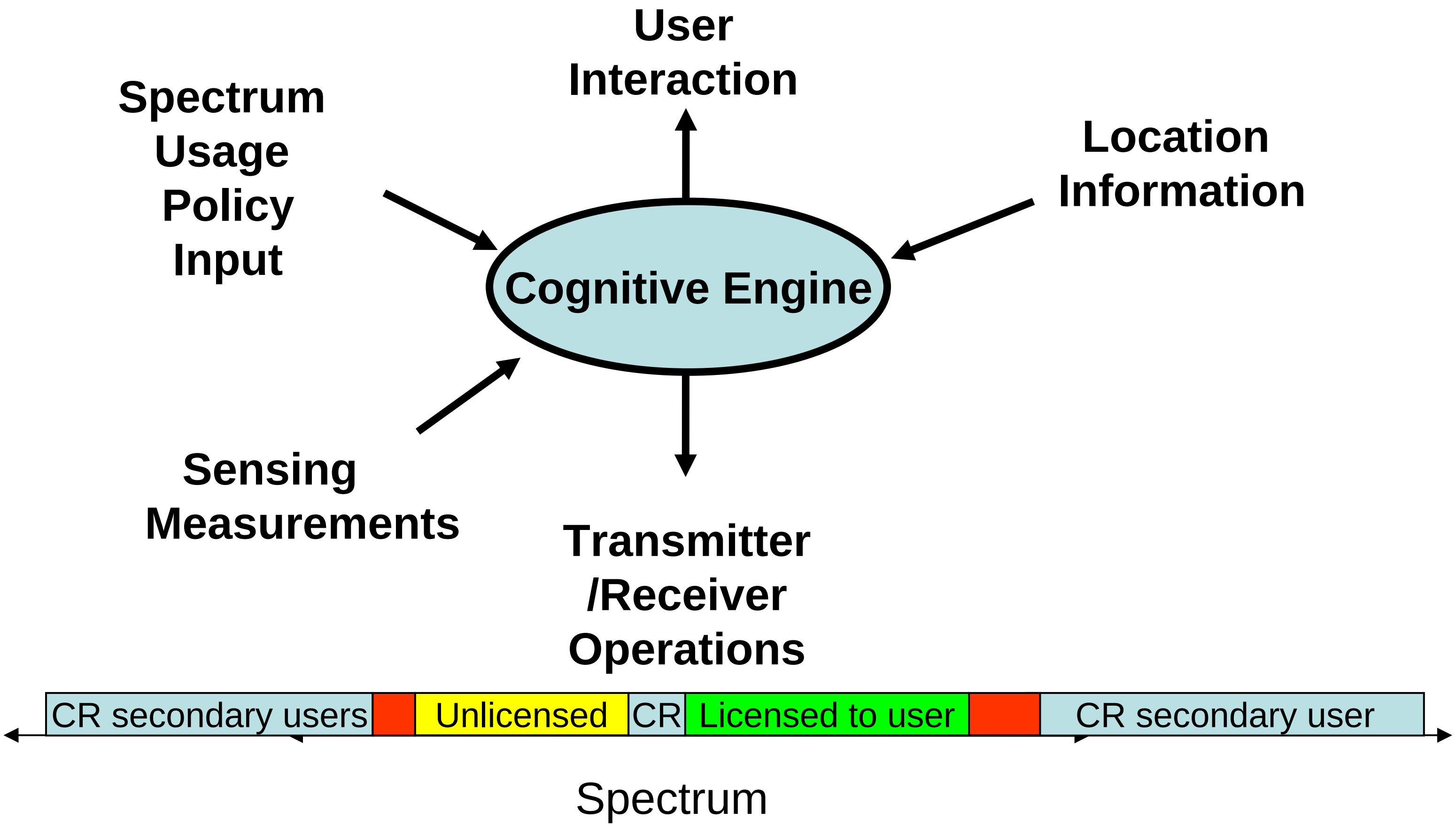
What are the additional vulnerabilities of Cognitive Radios?

Brown, James, Sethi, Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," in *MobiHoc* 2006.

Outline

- Traditional vs. Cognitive Radios
- Attack Taxonomy
- CR Architectures
- Potential CR DoS Attacks
- Conclusion

Traditional vs. Cognitive Radios



User Interaction

Spectrum Usage Policy Input

Location Information

Cognitive Engine

Sensing Measurements

Transmitter /Receiver Operations

CR secondary users	🟥	Unlicensed	CR	Licensed to user	🟥	CR secondary user

Spectrum

A CR does more than a traditional radio

Akyildiz et. al, NeXt Generation/Dynamic Spectrum Access/Cognitive Radio Wireless Networks: A survey, *Computer Networks*, 2006.

UC-Boulder

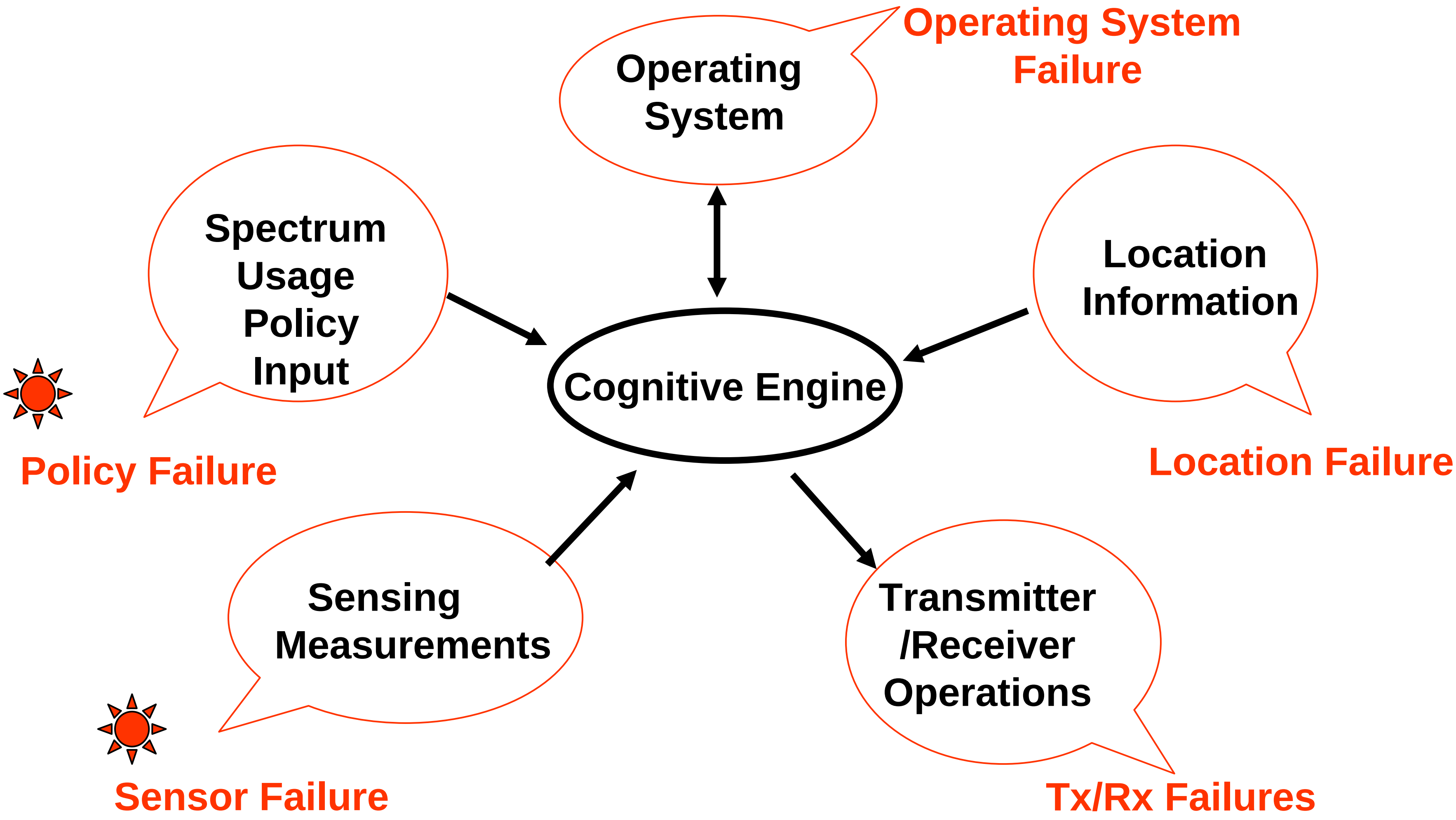
Outline

- Traditional vs. Cognitive Radios
- Attack Taxonomy
- CR Architectures
- Potential CR DoS Attacks
- Conclusion

Denial-of-Service (DoS)

- The prevention of authorized access to a system resource or the delaying of system operations and functions [RFC2828].
- Includes any effort to deny access to legitimate users.
- Attacker may be malicious, malfunctioning or misconfigured.

CR Points of Attack



Operating System

Operating System Failure

Spectrum Usage Policy Input

Location Information

Cognitive Engine

Policy Failure

Location Failure

Sensing Measurements

Transmitter /Receiver Operations

Sensor Failure

Tx/Rx Failures

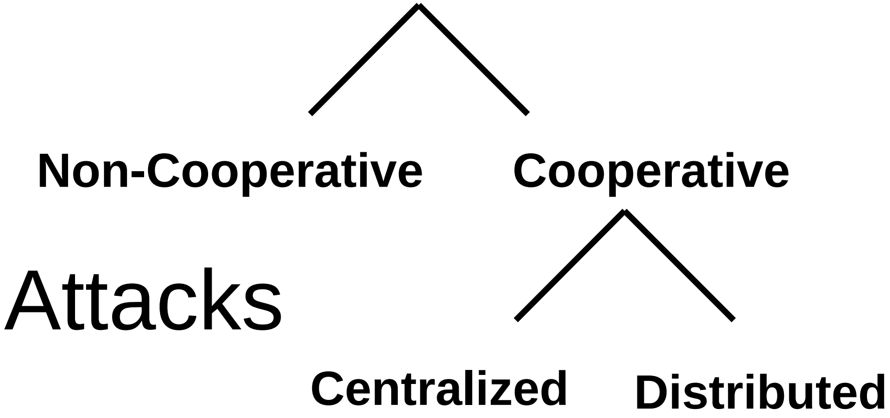
Failure = Denial / Induce

Deny Communication When Could

Induce Communication When Should Not

Outline

- Traditional vs. Cognitive Radios
- Attack Taxonomy
- CR Architectures



Non-Cooperative

Cooperative

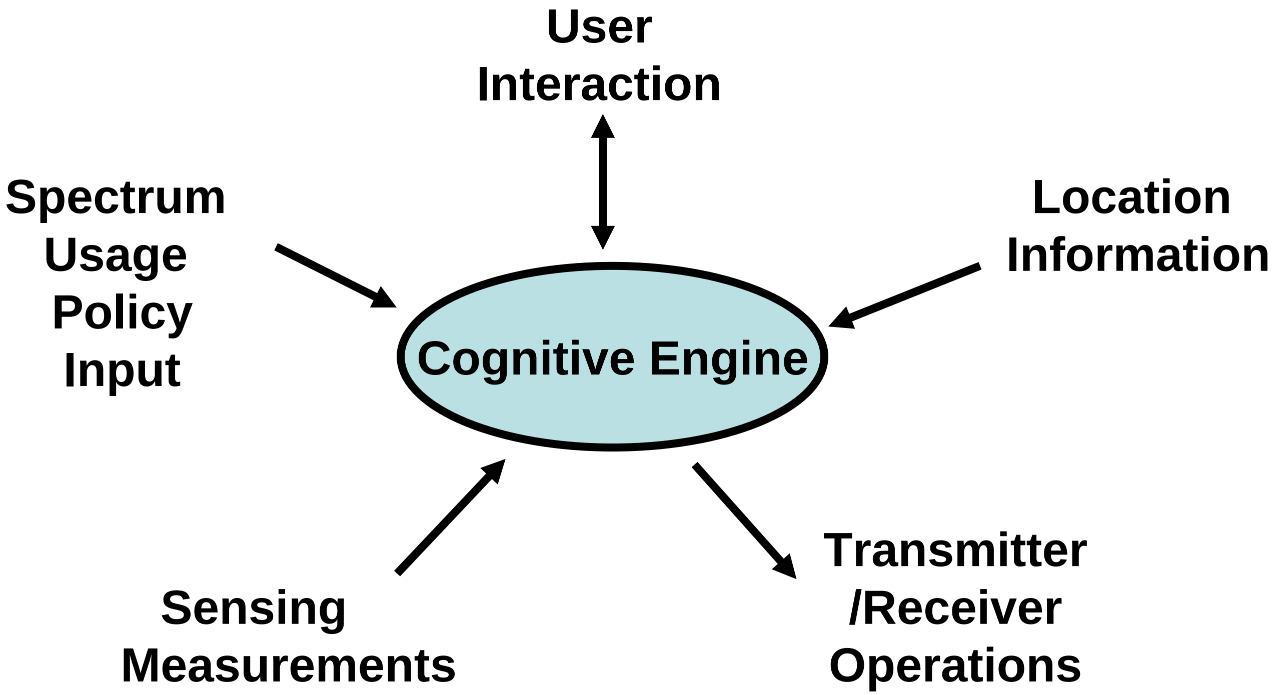
Centralized

Distributed

- Potential CR DoS Attacks
- Conclusion

UC-Boulder

CR Functions



User Interaction

Spectrum Usage Policy Input

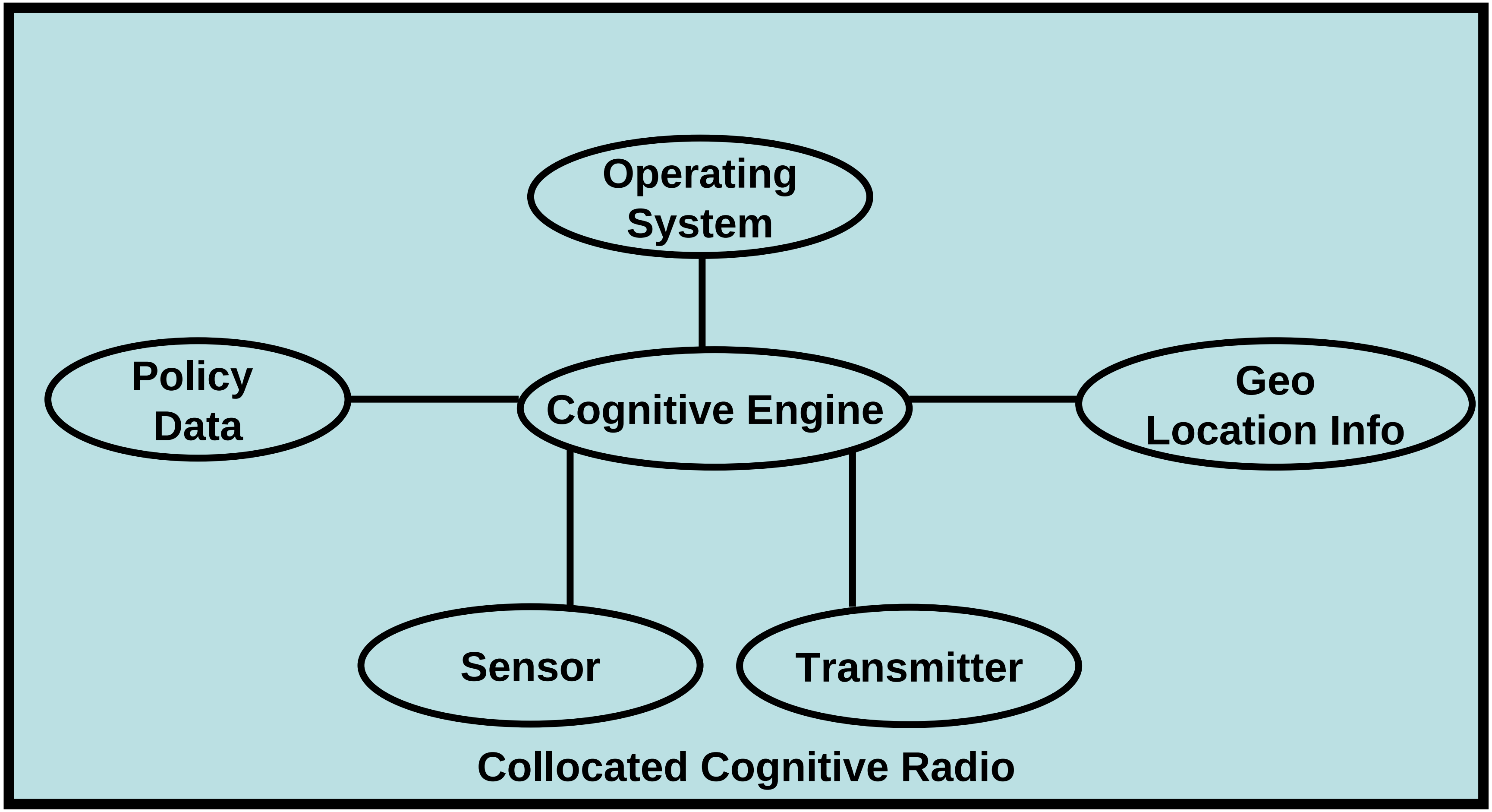
Location Information

Cognitive Engine

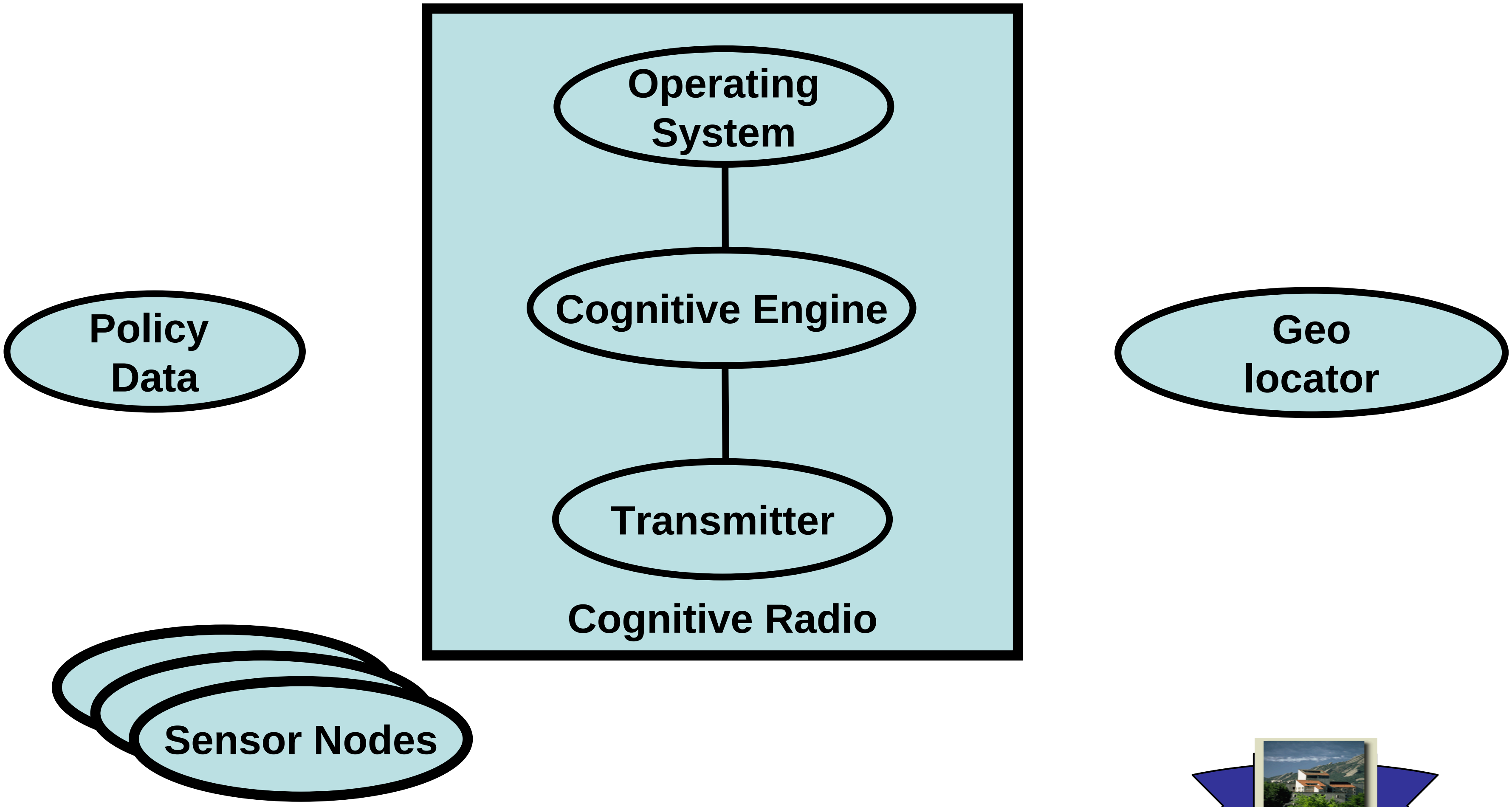
Sensing Measurements

Transmitter /Receiver Operations

CR Device Architectures – Collocated



CR Device Architectures - Distributed



Operating System

Cognitive Engine

Transmitter

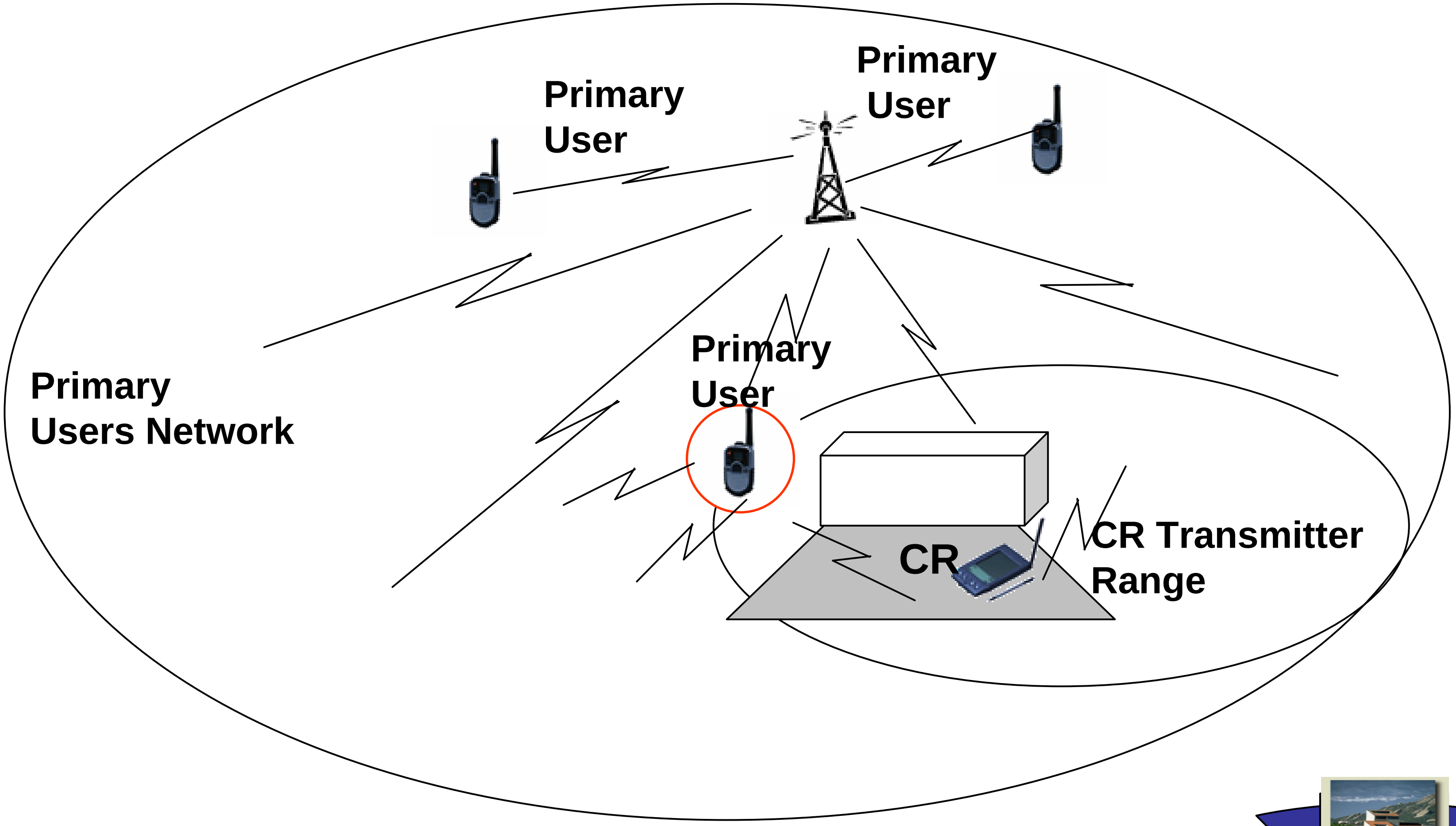
Cognitive Radio

Policy Data

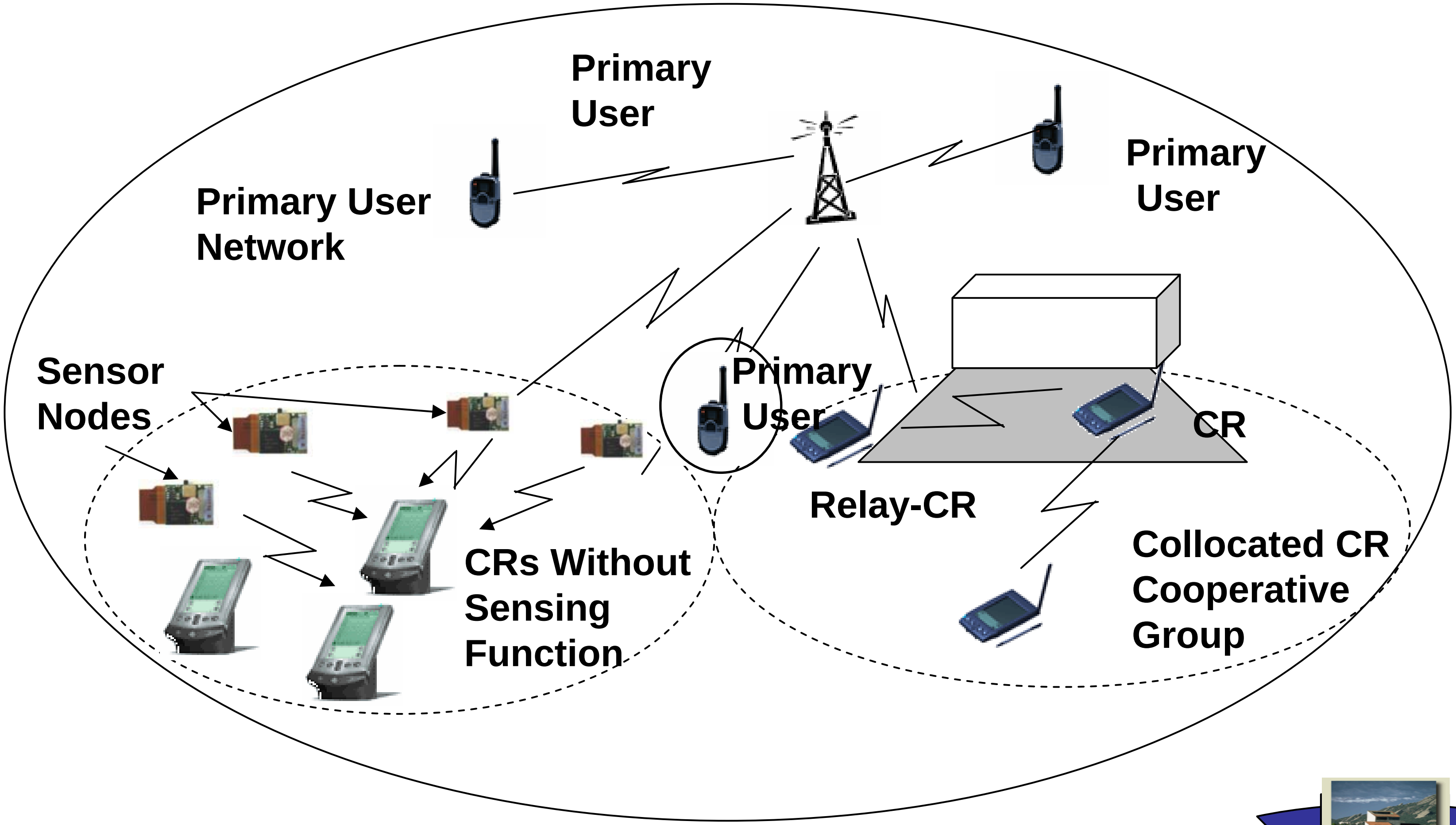
Geo locator

Sensor Nodes

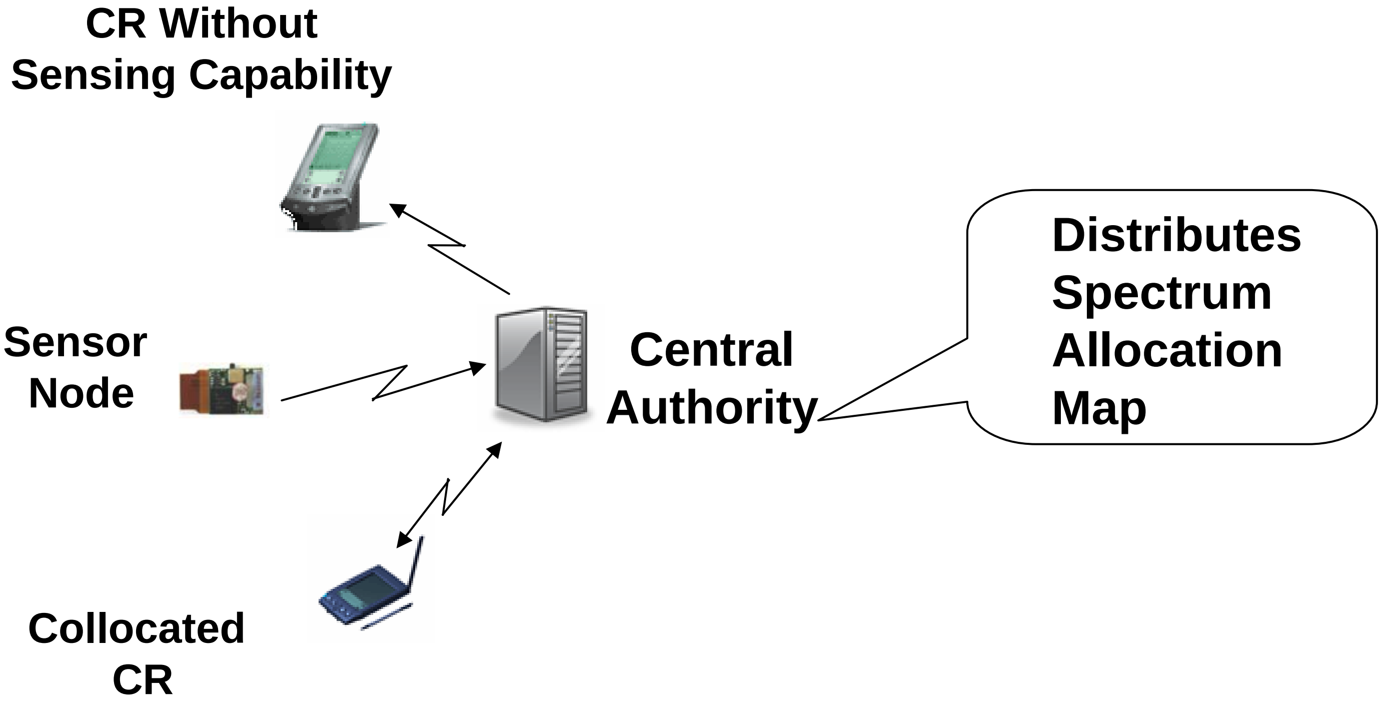
CR Mode of Operation – Non-cooperative



CR Mode of Operation – Distributed Cooperative



CR Mode of Operation – Centralized Cooperative



CR Without Sensing Capability

Sensor Node

Central Authority

Distributes Spectrum Allocation Map

Collocated CR

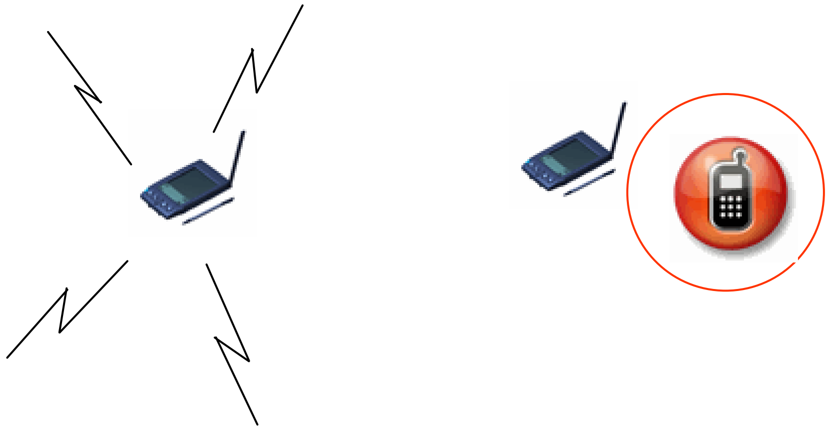
Outline

- Traditional vs. Cognitive Radios
- Attack Taxonomy
- CR Architectures
- Potential CR DoS Attacks
- Conclusion

Potential CR DoS Vulnerabilities

- Sensor Failures

  Scenario1: Attacker mimics licensed user.

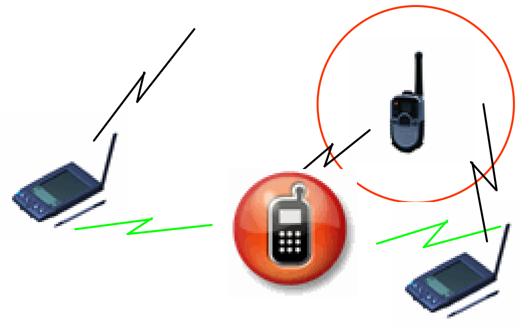


Attacker “denies” access

Potential CR DoS Vulnerabilities

- Sensor Failures

  Scenario2: Attacker masks a licensed user

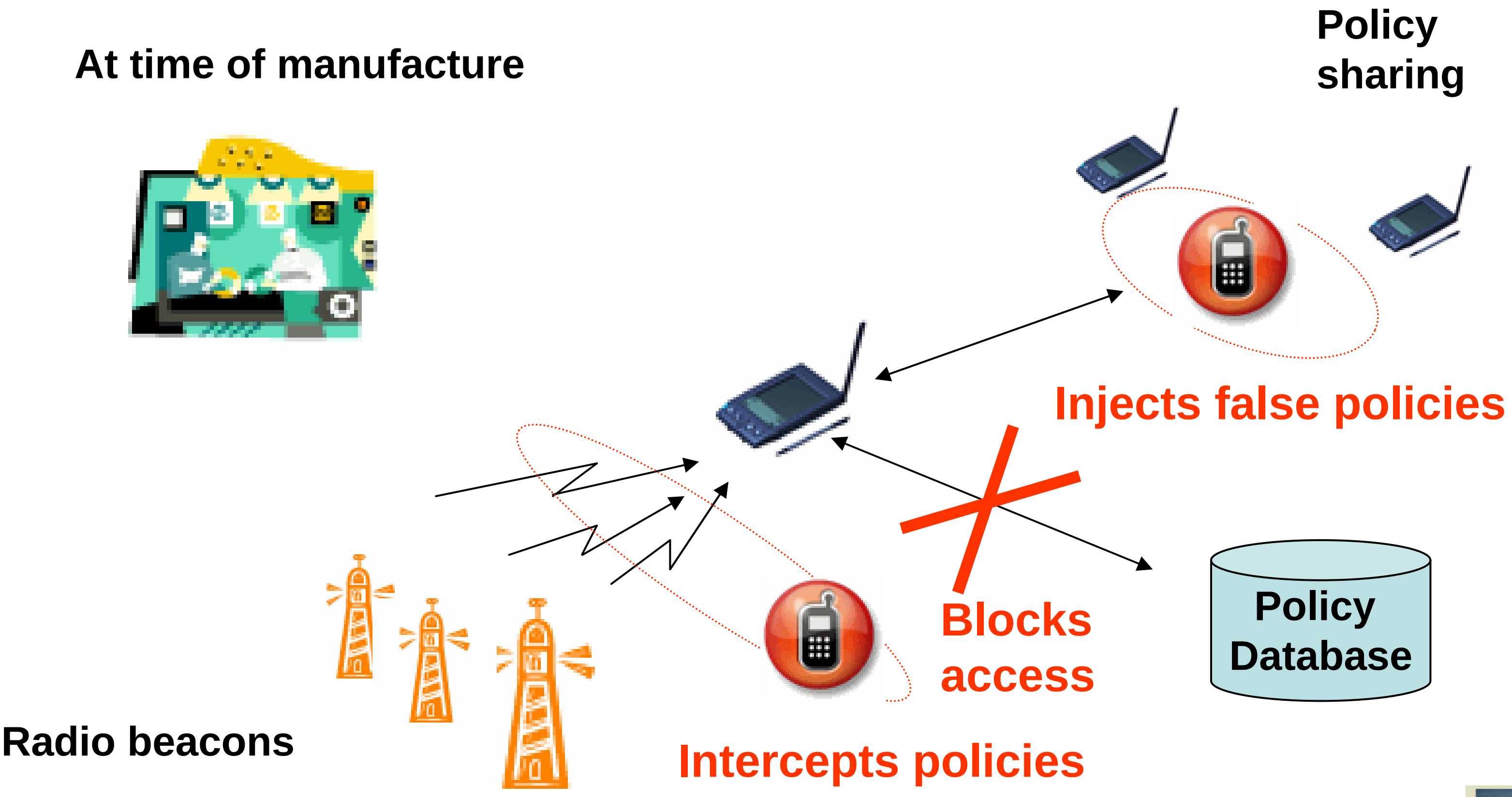


Attacker "induces" CRs to interfere with primary user

UC-Boulder

Potential CR DoS Vulnerabilities

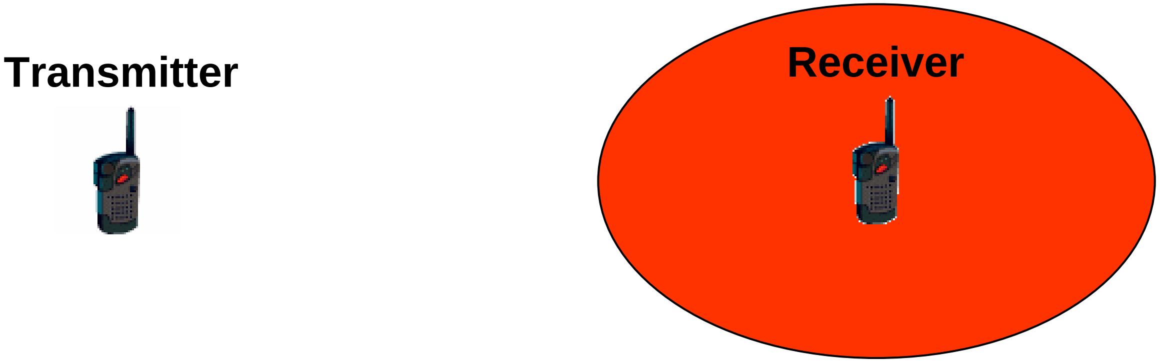
- Policy Failures



Outline

- Traditional vs. Cognitive Radios
- Attack Taxonomy
- CR architectures
- Potential CR DoS Attacks
- Conclusion

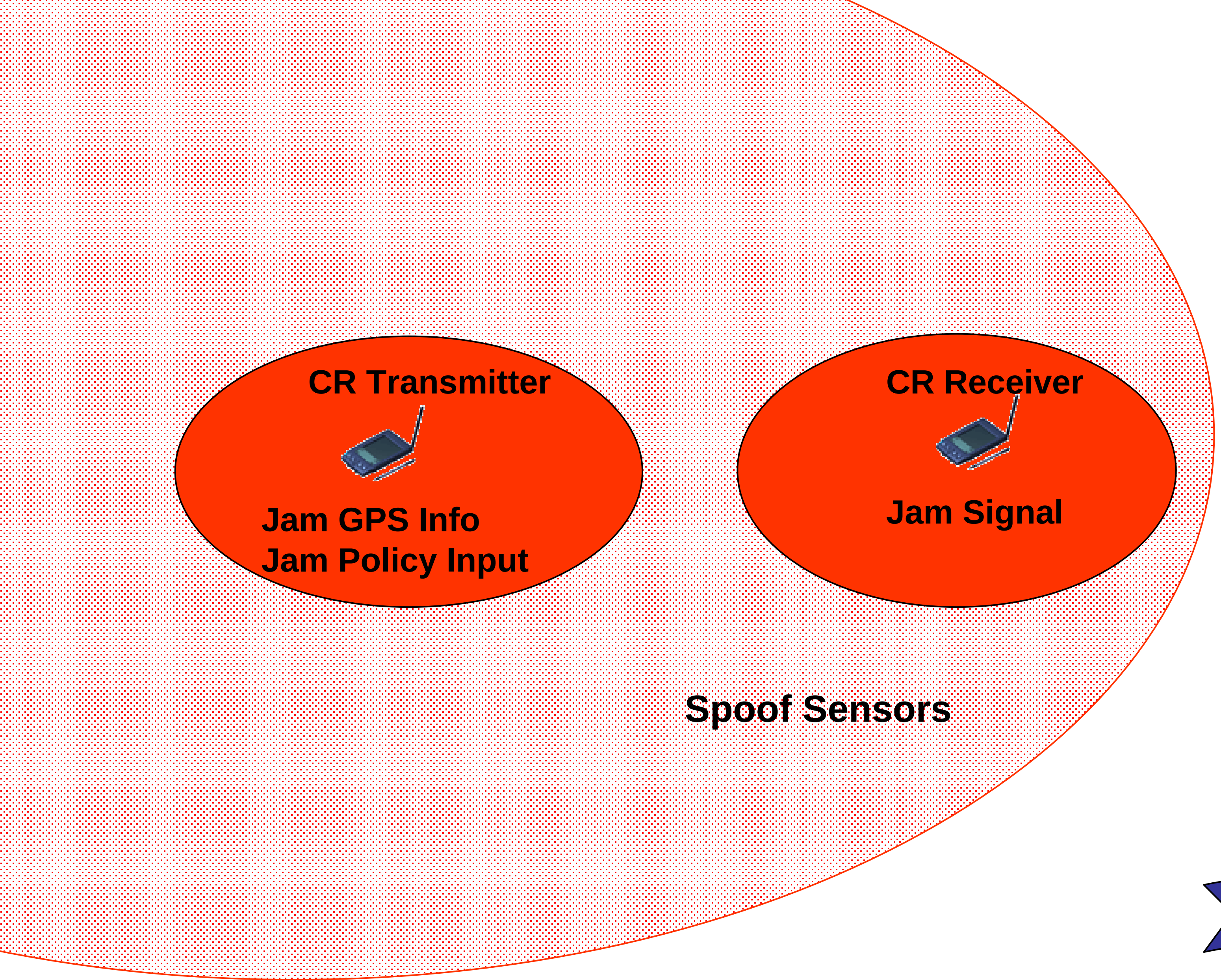
Traditional Points of Attack



Transmitter

Receiver

CR Points of Attack



CR Transmitter

Jam GPS Info
Jam Policy Input

CR Receiver

Jam Signal

Spoof Sensors

Should CRs be allowed?

- Potential DoS vulnerabilities need to be countered
- Always a risk of interference*
  - Potential for spectrum efficiency
- Can always revert to traditional radios

* T. X Brown, "A Harmful Interference Model for Unlicensed Device Operation in Licensed Service Bands," J. of Communications, 2006

Going forward..

Let`s learn from the past

Security Vulnerabilities in

- Computer Networks
- Wire-line Networks
- Encrypted Wireless Ad Hoc Access Networks

Conclusion

- CRs like every other radio are susceptible.

- CRs open new avenues of attack.

- NOW is the best time to devise countermeasures to reduce CR-specific vulnerabilities.

Thank you for your time and attention.
I welcome any questions
that you may have.