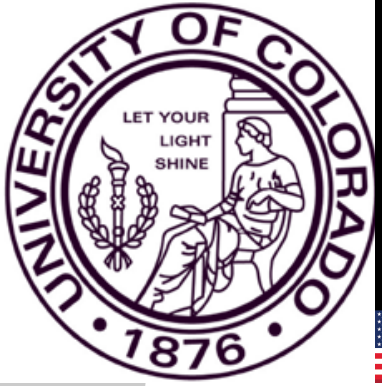


Carnegie Mellon University
Rwanda

Potential Denial-of-Service Threat Assessment for Cognitive Radios

Timothy X Brown*, Amita Sethi[+]

*,[+]Interdisciplinary Telecommunications

*Electrical, Computer, and Energy Engineering

University of Colorado, Boulder

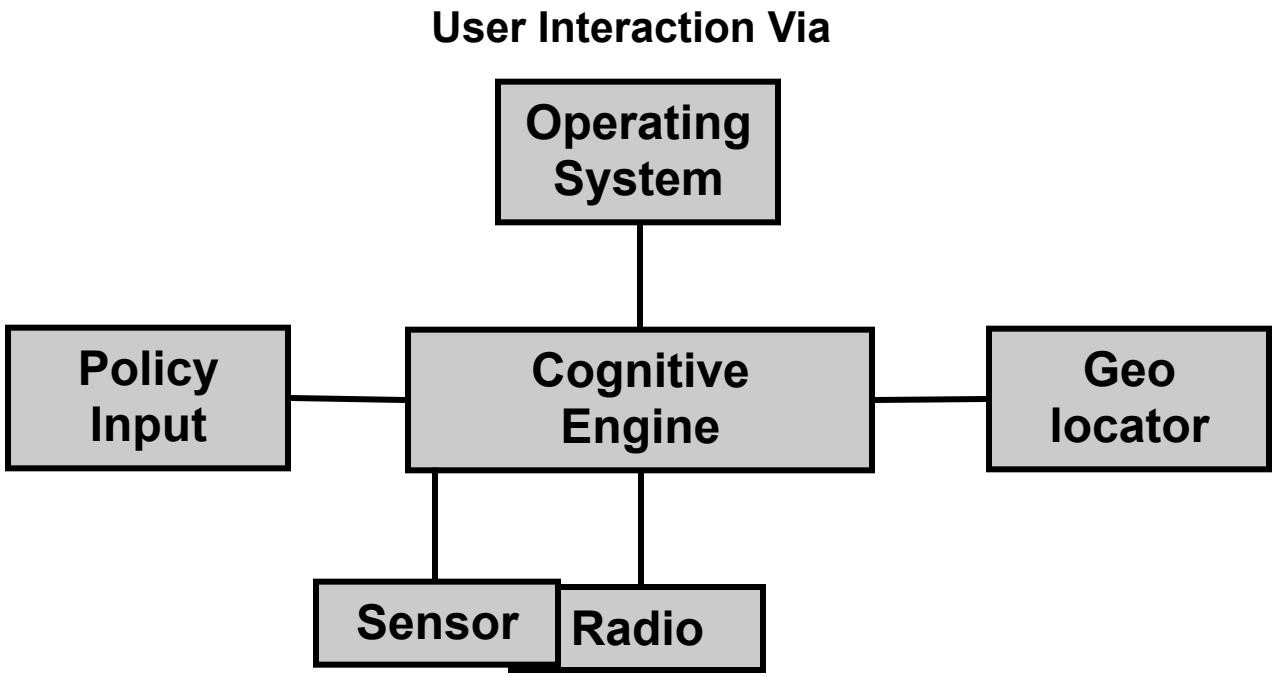
*Visiting Professor

Carnegie Mellon University, Rwanda

Presented at the ICTP School on Applications of Open Spectrum and White Spaces Technologies

March 10, 2014

Cognitive vs. Traditional Radios



A CR does more than a traditional radio

Cognitive Radios – a Secure Paradigm?

- Wireless
- Mobile
- Remotely Reconfigurable
- Opportunistic Transmission based on Spectrum Availability
- Device's Spectrum Access Control via Spectrum Policies

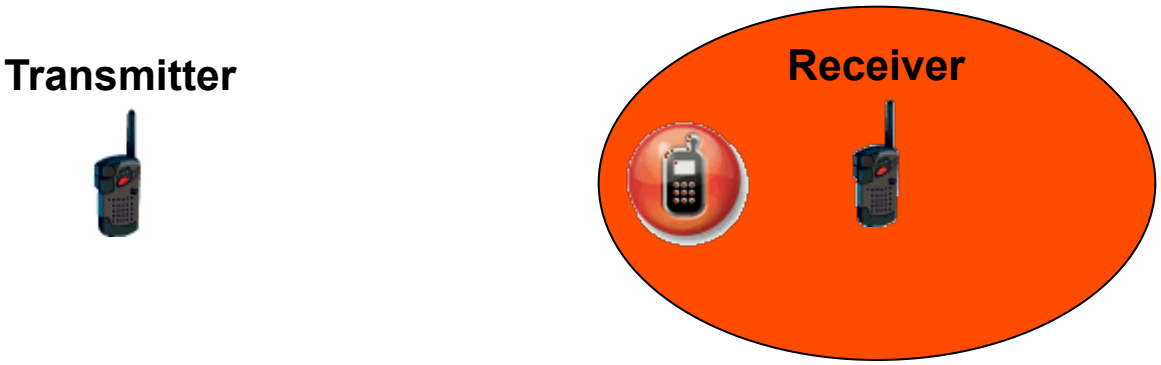
Research Question

Which potential denial-of-service (DoS) attacks are cognitive radios susceptible to, what are the risks they represent, which security mechanisms can be employed to forestall the high-priority risk attacks, and which cognitive radio (CR) designs are the most susceptible to these critical risks?

Denial-of-Service (DoS) Attacks

DoS is the prevention of authorized access to a system resource or the delaying of system operations and functions [RFC2828].

Traditional DoS Attack



Communications Receiver Jamming

DoS Attack Categories – Denial / Induce

Deny Communication When Could

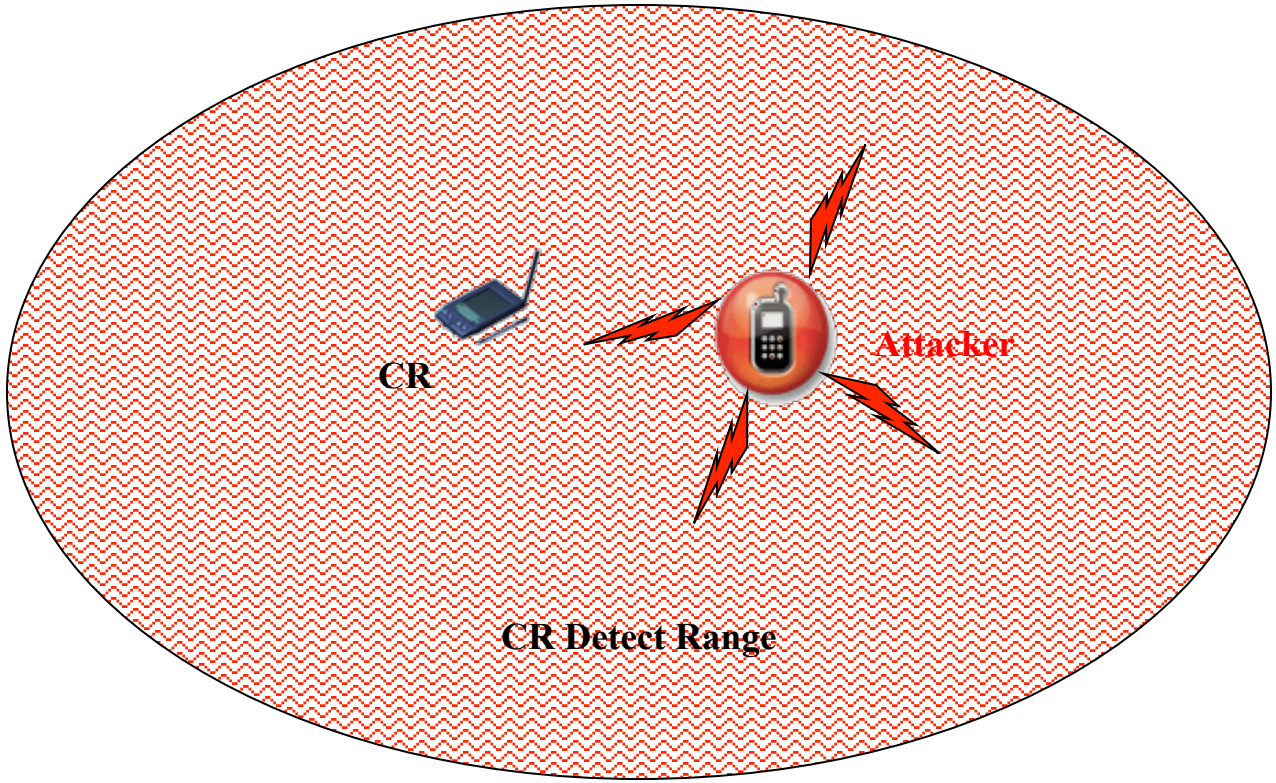
Immediate DoS

Induce Communication When Should Not

Long term DoS

Example Denial Attacks – Sensor Failures

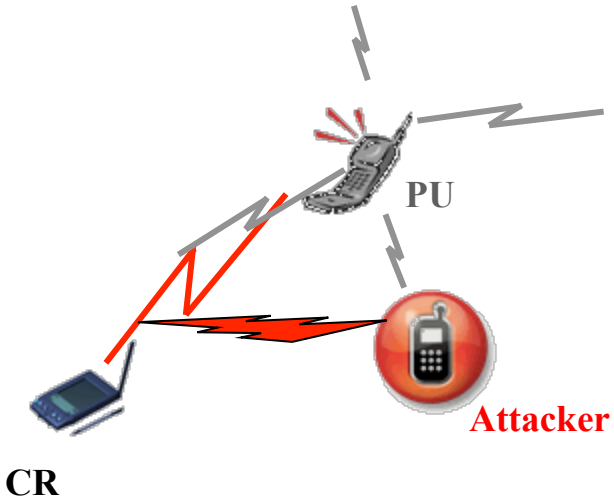
Scenario1: Attacker Emulates Primary User



Attacker "Denies" Access

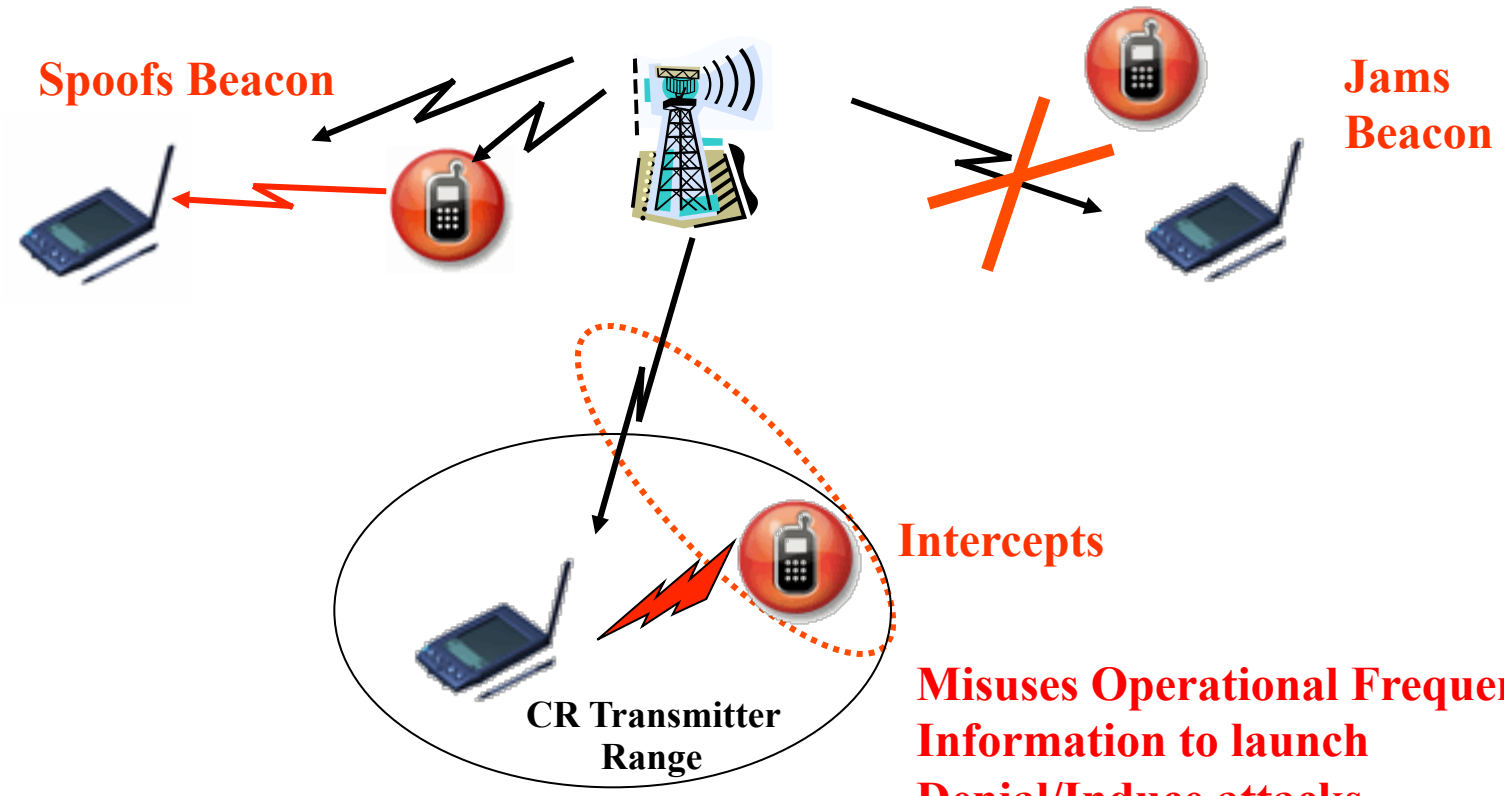
Example Induce Attacks – Sensor Failures

Scenario 2: Attacker Masks Primary User`s Signals.

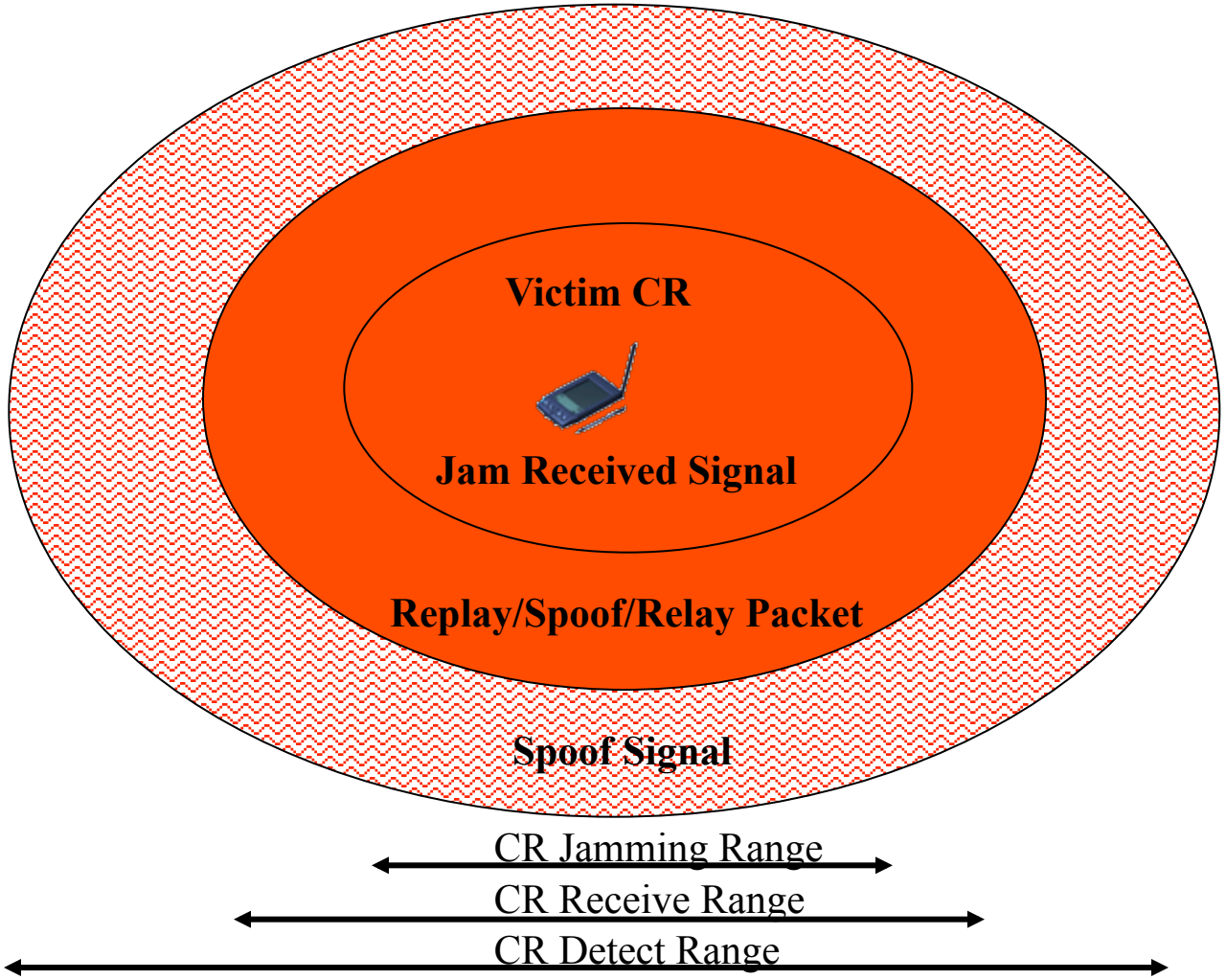


Attacker "Induces" CR to Interfere with Primary User

Example Denial/Induce Attacks – Policy Failure in Beaconing System



CR Avenues of Attack



Attack Analysis Methodology

- Hypothesize the Attack Scenario
- Identify the Associated Threats
- Organize the Associated Threats in a Hammer Model framework
- Assign a Quantitative Risk Value to the Attack based on its Likelihood and Impact (Risk Assessment)

Attack Analysis: Threat Categorization

- Initiating (Triggering Event)
- Associated (Other Causal Events)
  - Contributory
- Primary (Outcome)

Attack Analysis: Hammer Model Framework

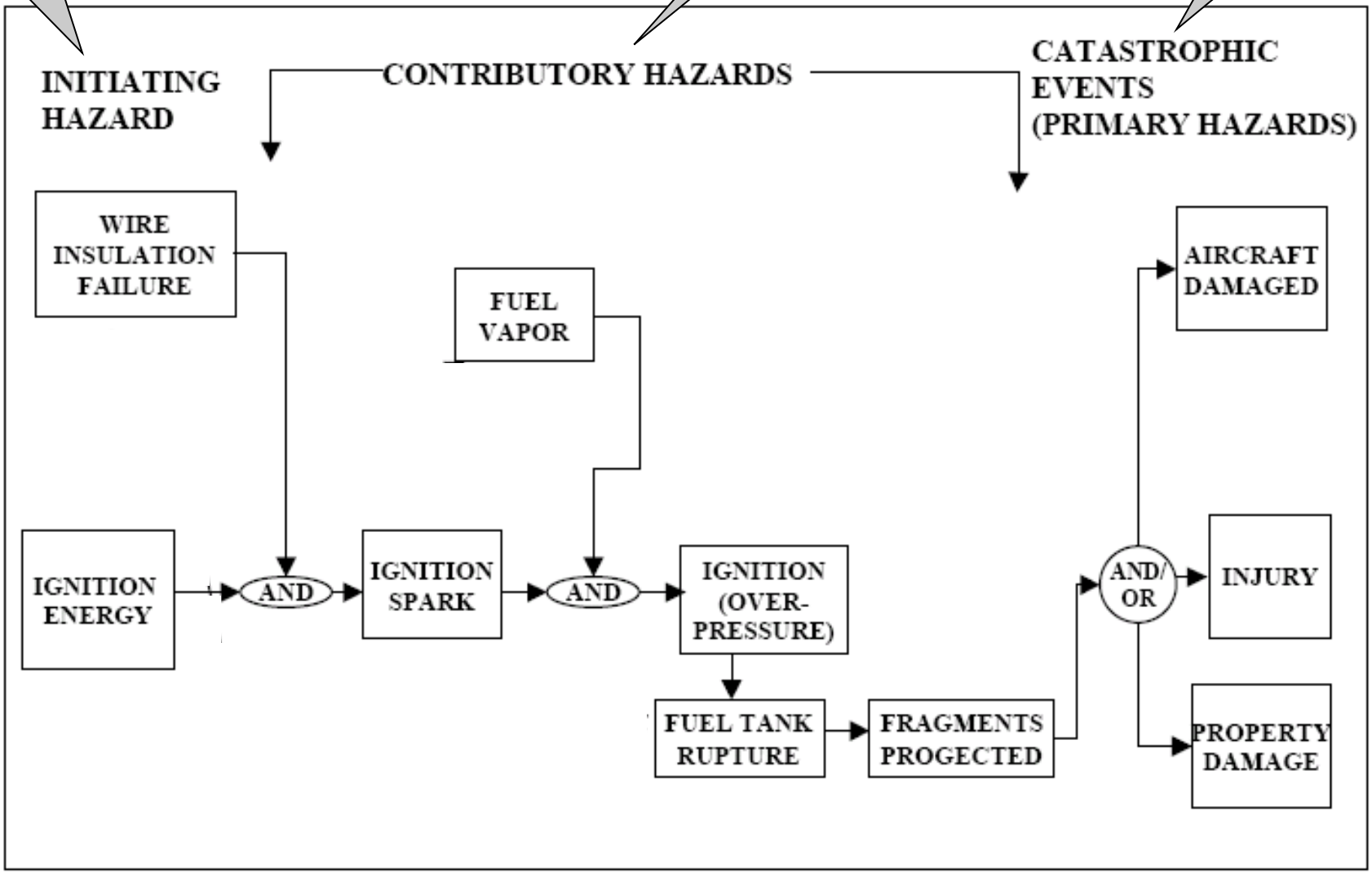
- Modeling tool to represent an attack scenario into a sequence of initiating and contributory threats that result in one of more primary threats.
- Primarily Used for Qualitative Scenario based Attack Analysis.
- Example Application in System Safety Hazard Analysis in Federal Aviation Administration.

Example Fuel Tank Rupt ario

Threats from Attackers Outside the CR system

Threats from Within the CR system

DoS Outcomes



Attack Analysis: Risk Assessment (1/3)

1. Assess the Technical Likelihood of the Attack

Rationale: Technical Problems to Attacker	Likelihood Case	Rank
Insolvable	Impossible	0
Strong	Low	1
Solvable	Medium	2
None	High	3

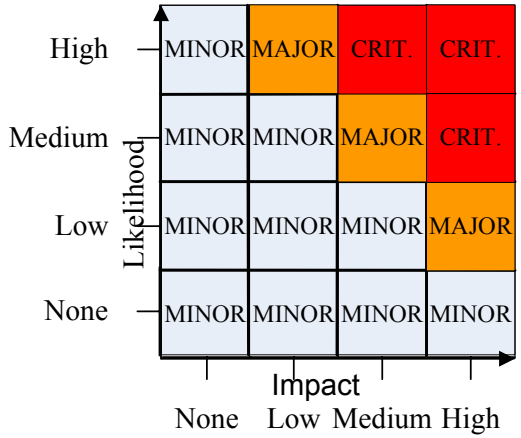
Attack Analysis: Risk Assessment (2/3)

2. Assess the Impact of the Attack

Rationale: Impact on Victim		**Impact Case**	**Rank**
Denial Attacks	**Induce Attacks**		
None	None	None	0
Perceptible but insignificant degradation in CR communication.	Perceptible but infrequent interference to active primary users	Low	1
Significant degradation but still operational CR communication.	Perceptible frequent interference to active primary users	Medium	2
Non-operational CR communication	Continuous interference to active primary users	High	3

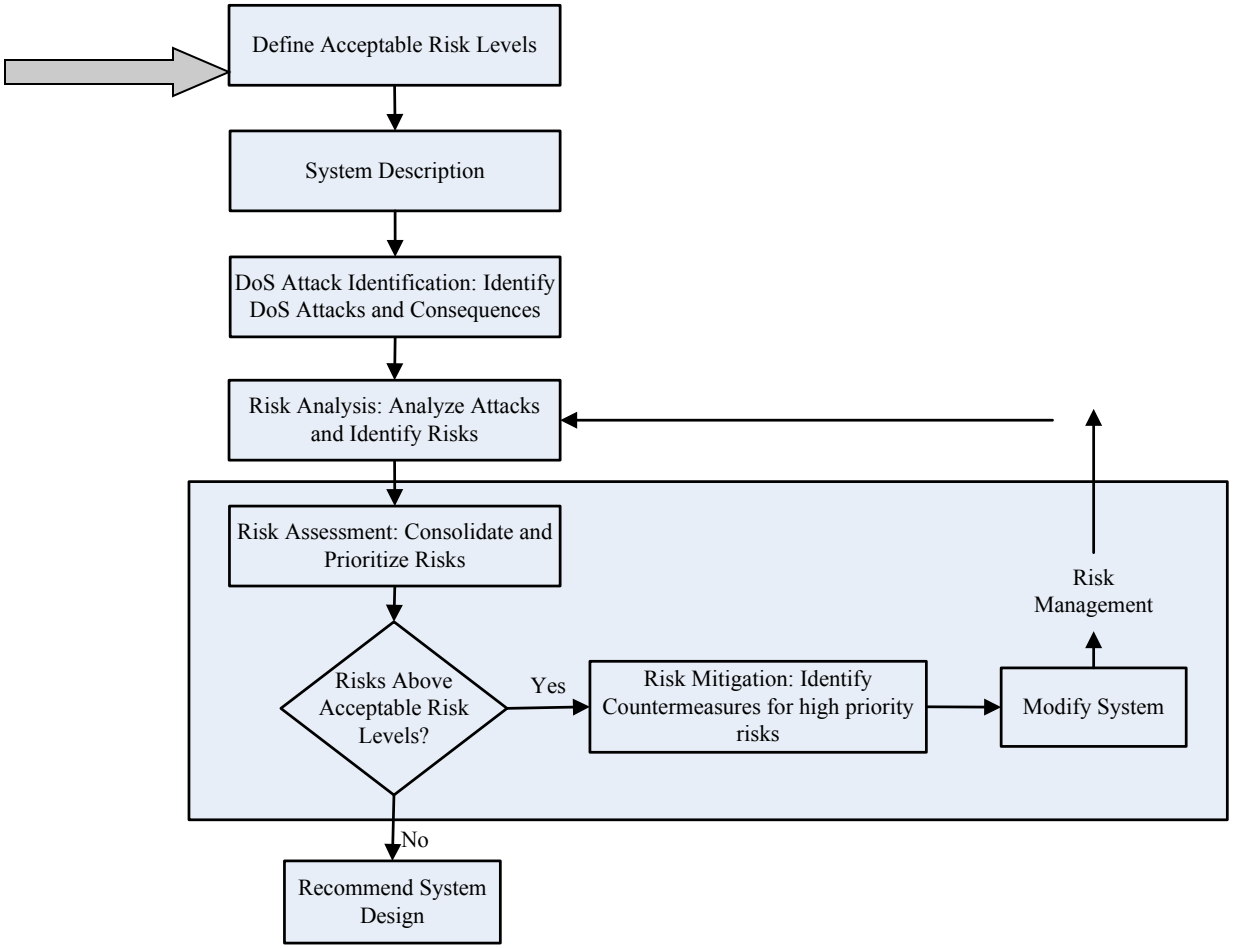
Attack Analysis: Risk Assessment (3/3)

3. Risk Level = Likelihood Rank X Impact Rank



Risk Case	Risk Mitigation Action
Minor	No Countermeasures Required
Major	Threat cannot be Ignored
Critical	Mandates High Priority Handling

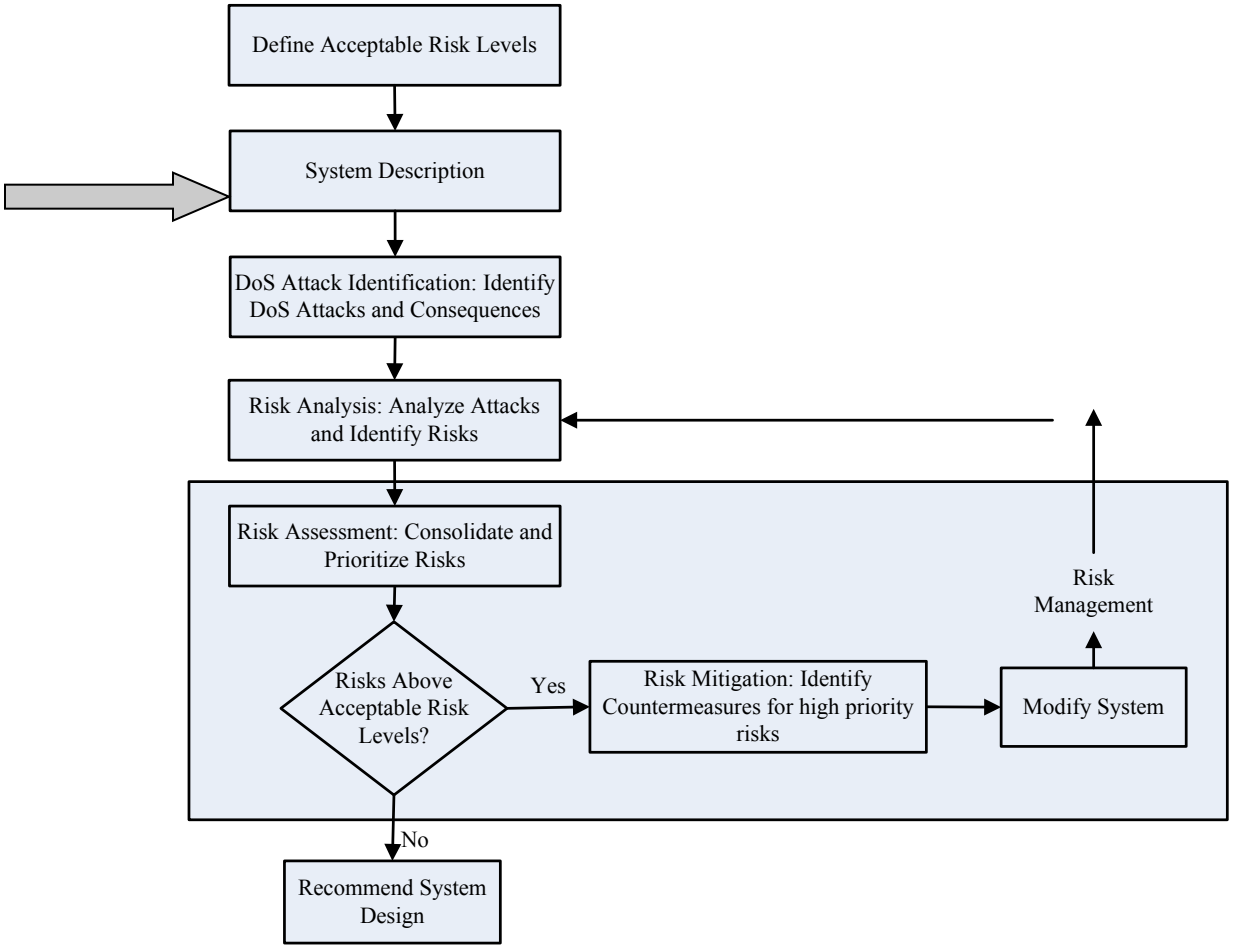
Research Methodology



Acceptable Risk Levels

- Every Critical or Major Threats should be countered in the CR System.
- Any Major Threats with high likelihood but low impact, or low likelihood but high impact need to be countered but are ultimately acceptable.
- Minor Threats can be ignored.

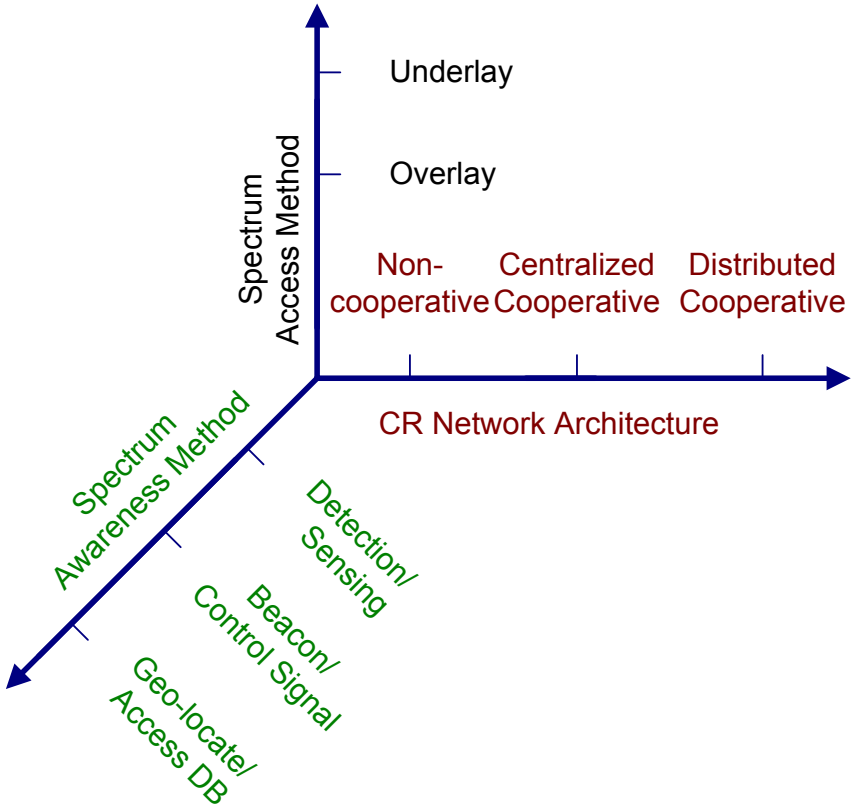
Research Outline



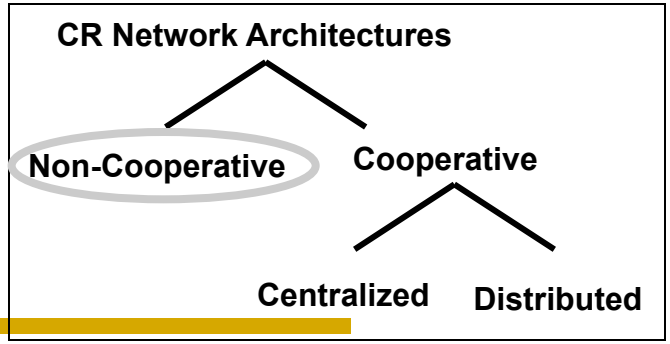
System Description

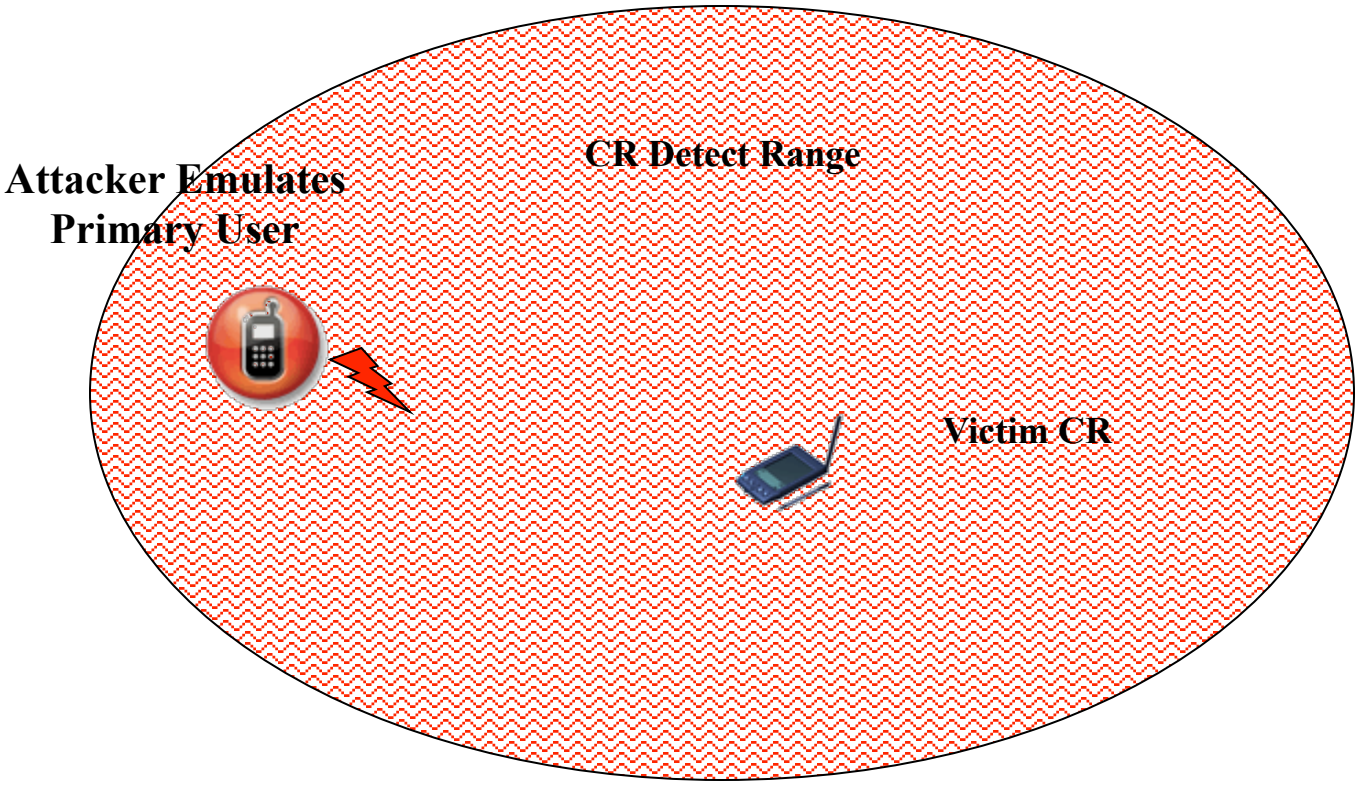
- Target System: Cognitive Radios
- Key Challenge: Multi-Dimensional CR Configurations

Multi-Dimensional CR Configurations



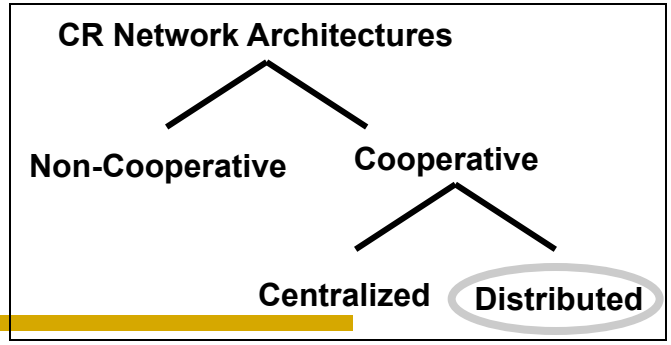
CR N/w Architectures – Non-cooperative

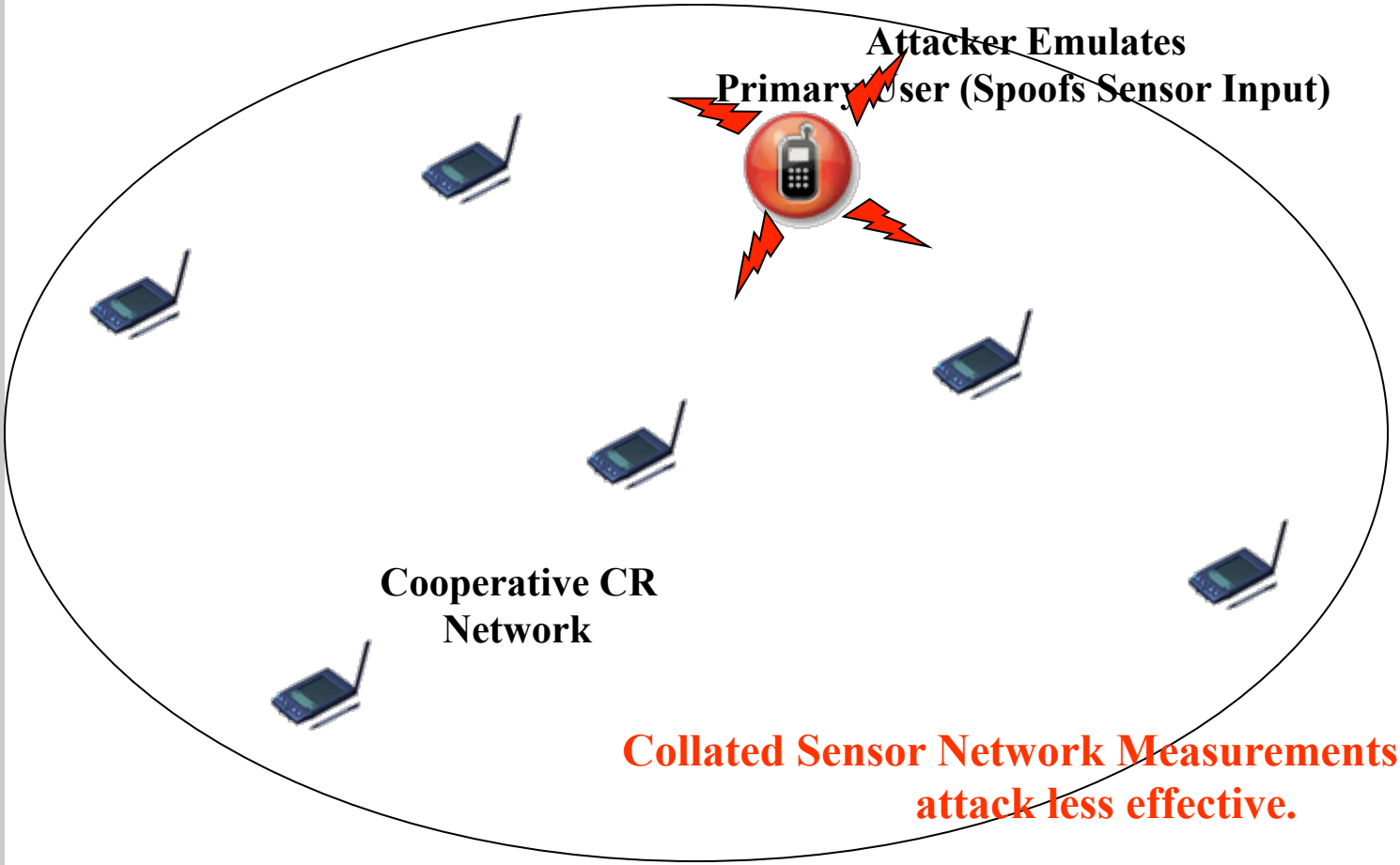




Attacker Successfully "Denies" Access

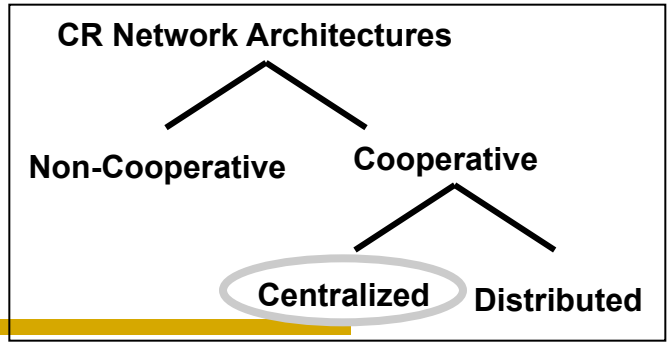
CR N/w Architectures – Distributed Cooperative

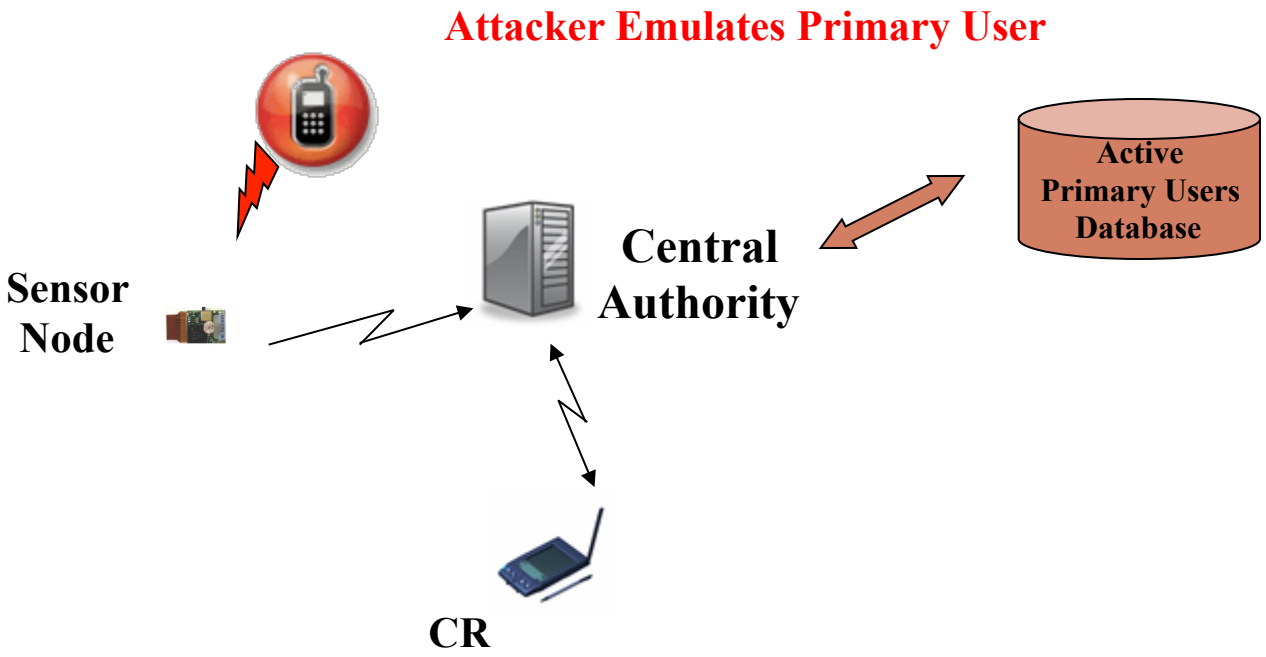




Collated Sensor Network Measurements make the attack less effective.

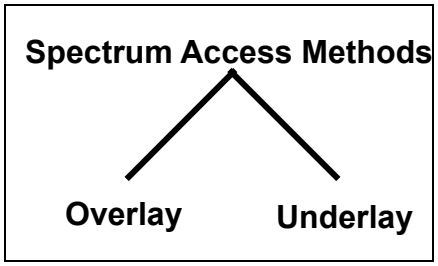
CR N/w Architectures – Centralized Cooperative

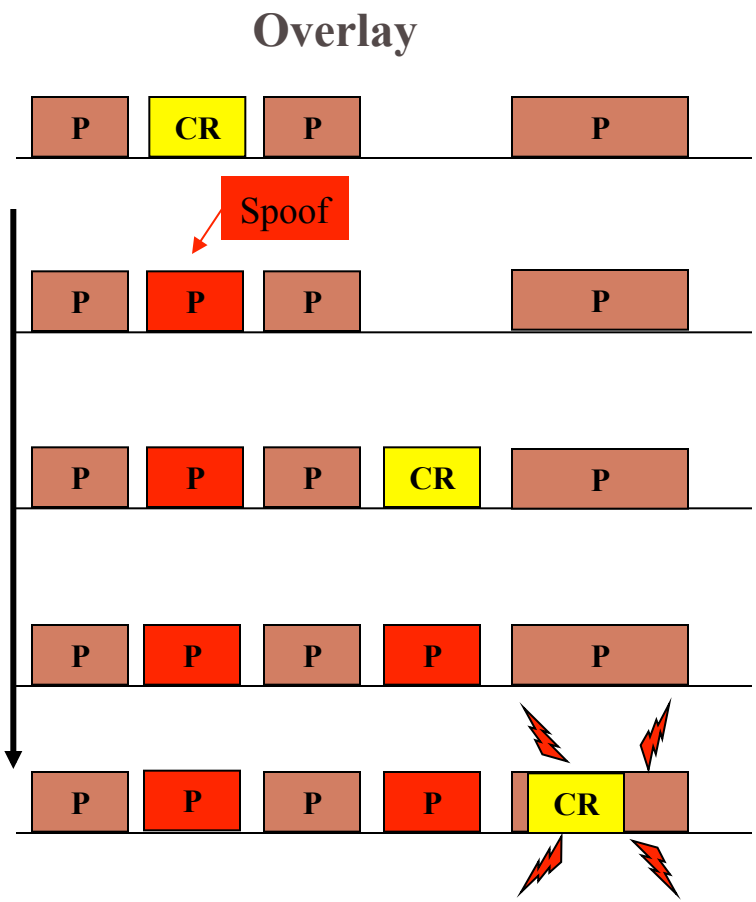


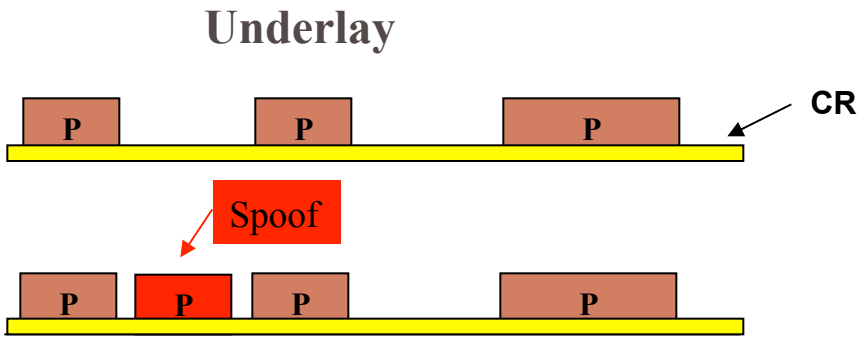


Attack is Ineffective due to Possible Verification of Collated Network Measurement against Active Primary User's DB

Spectrum Access Methods





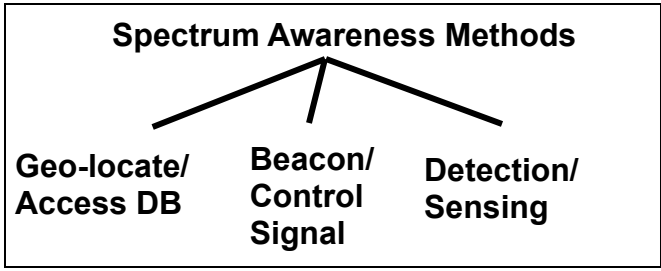


CR does not React to
Primary User Emulation

CR is Denied Access

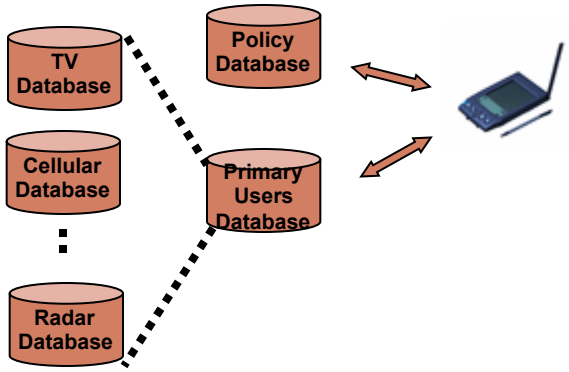
Or Induced to Interfere

Spectrum Awareness



Prone to Location/ DB Spoof, Jam, Replay

Geo-locate/ Access DB



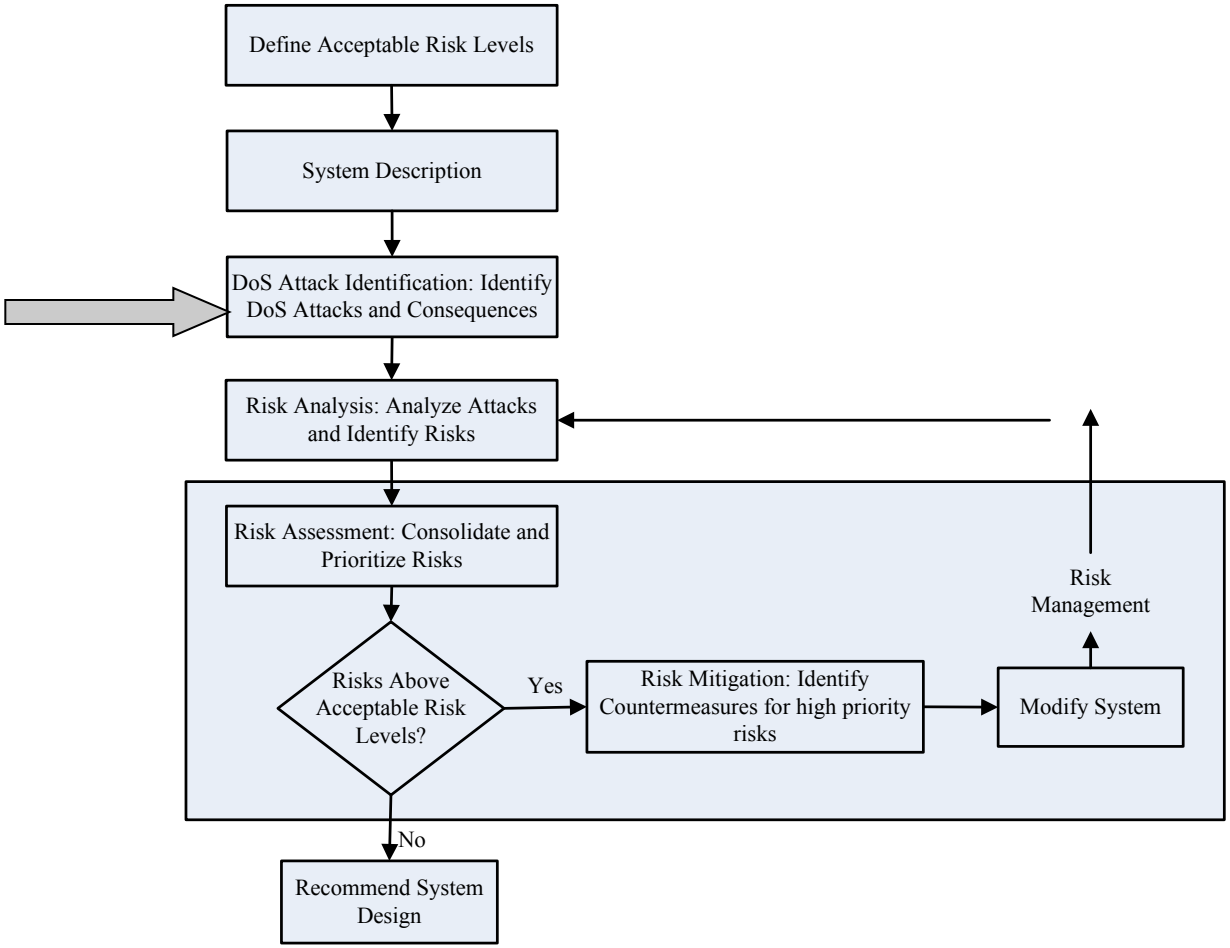
Prone to Sensing Spoof, Jam, Replay

Detection/ Sensing

Beacon/ Control Signal

Prone to Beacon/Control Signal Spoof, Jam, Relay

Research Outline



DoS Attack Identification

- Possible Attack Methods Considered
  - Constant or Direct Jamming
  - Intelligent Jamming
  - Intercept or Eavesdropping
  - Spoofing
  - Replay
  - Relay
  - Cryptanalysis

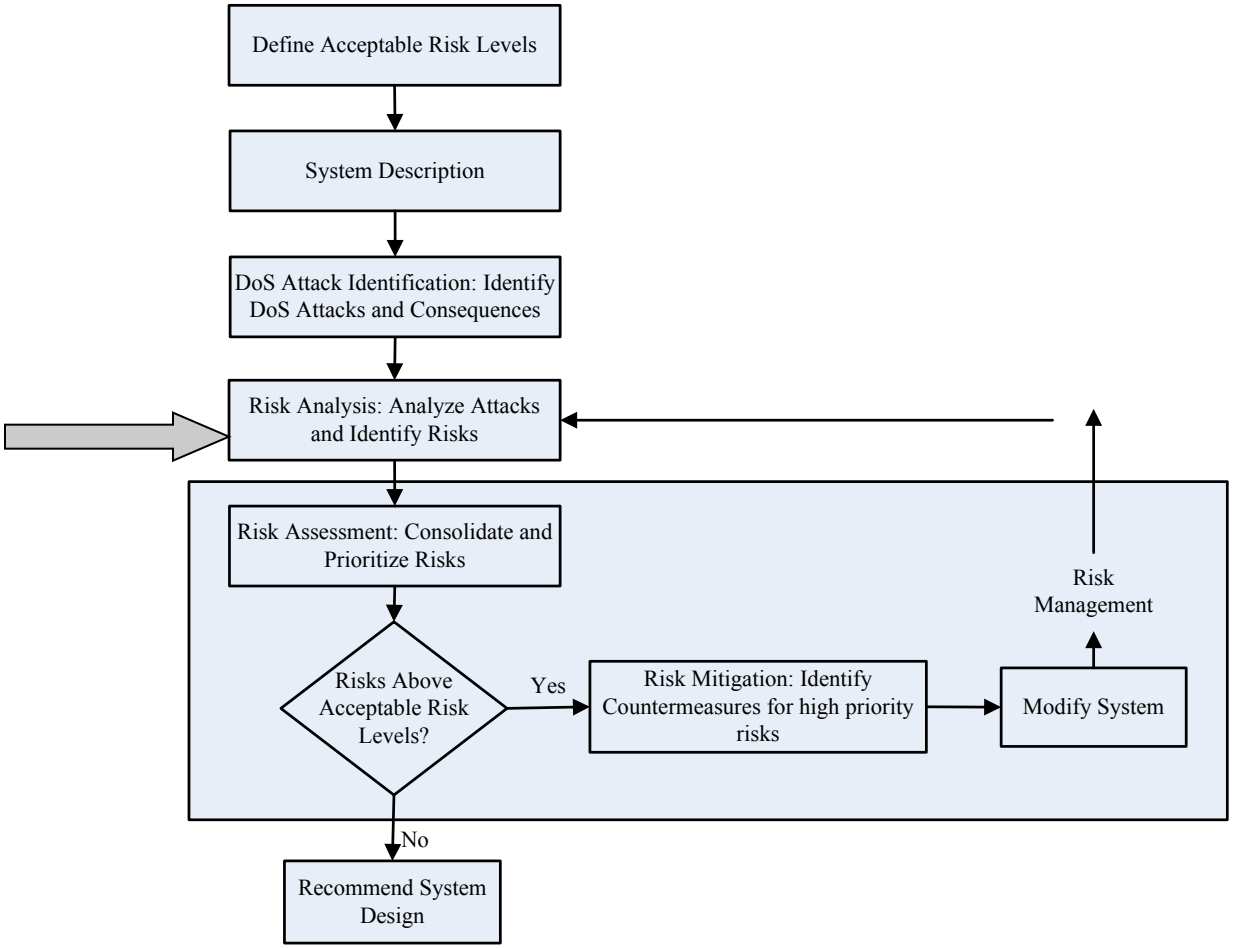
DoS Attacks Identified Against..

- Policy, Sensor, Geo-location and Other Networked Information exchanged
  - Between CR Elements in a Distributed CR.
  - Among CRs in a Distributed Cooperative Setup.
  - Between CRs and Central Entity in a Centralized Cooperative Setup.
  - From Central Entity to Non-cooperative CRs.

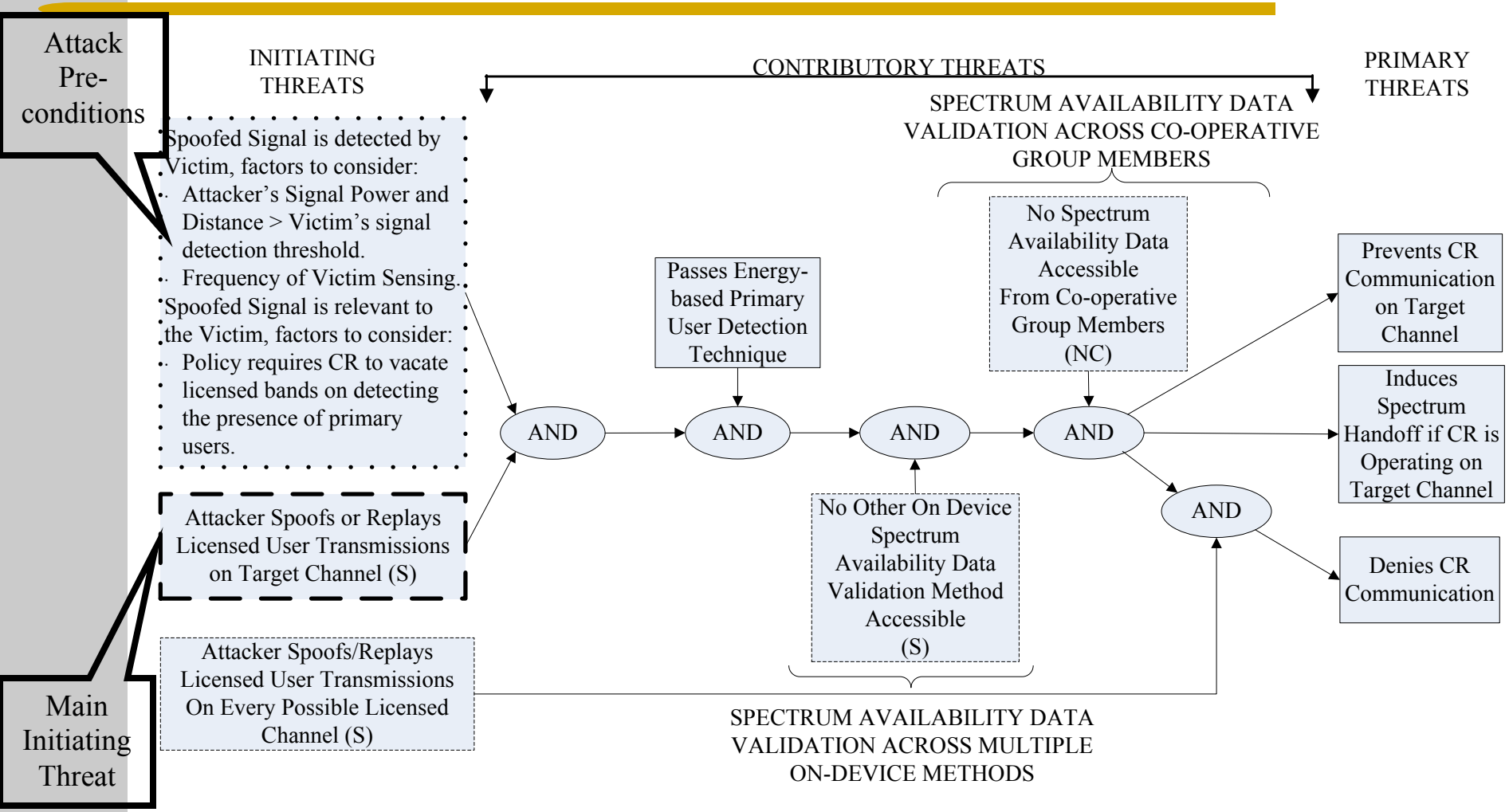
DoS Attacks Identified Against..

- Networked CR Network Entities such as
  - Elements in a Distributed CR.
  - Networked CRs in a Distributed Cooperative Setup.
  - Entities in a Centralized Cooperative Setup.
- Spectrum Information Sensed by CR
- CR Transmission/Reception

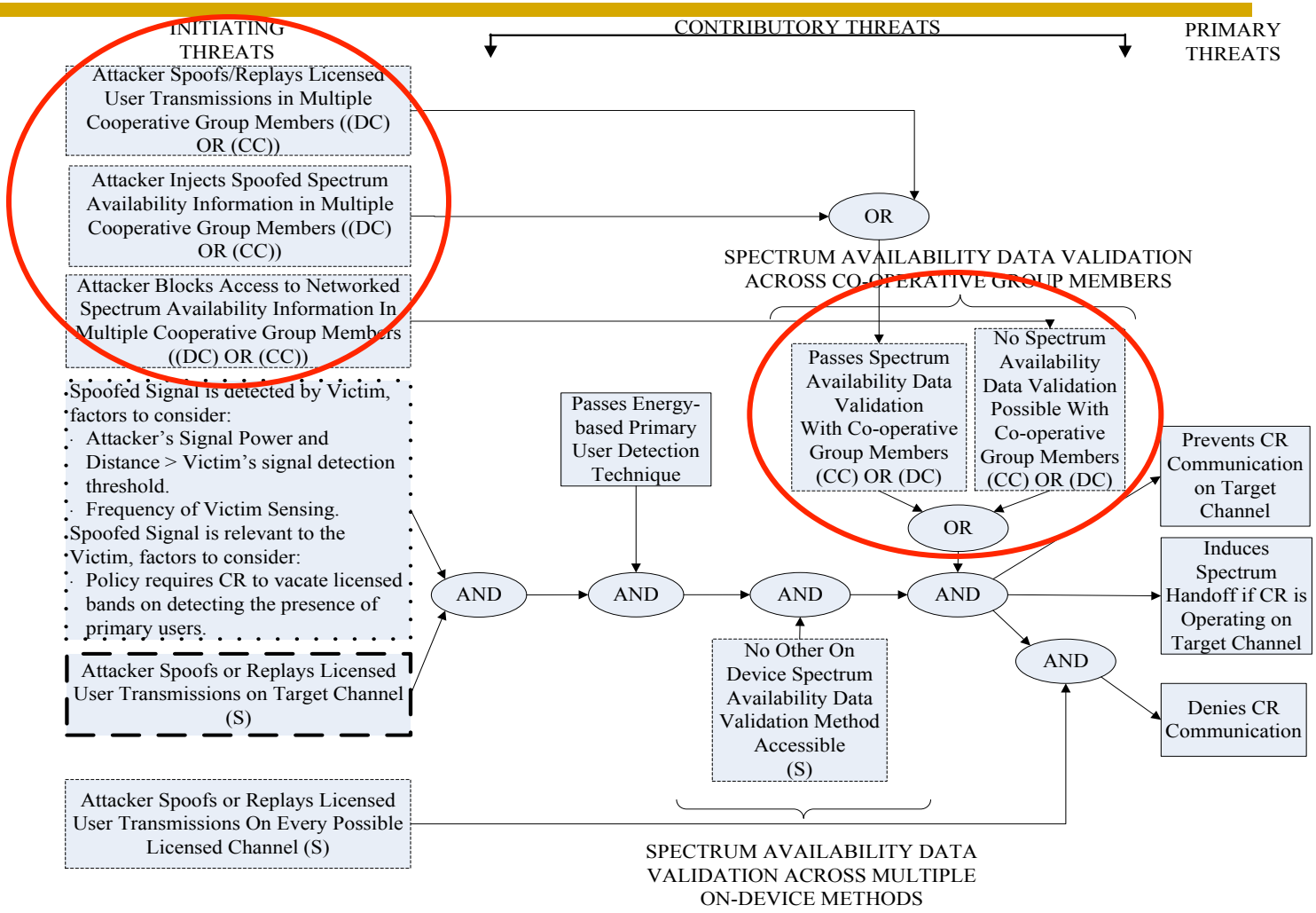
Research Outline



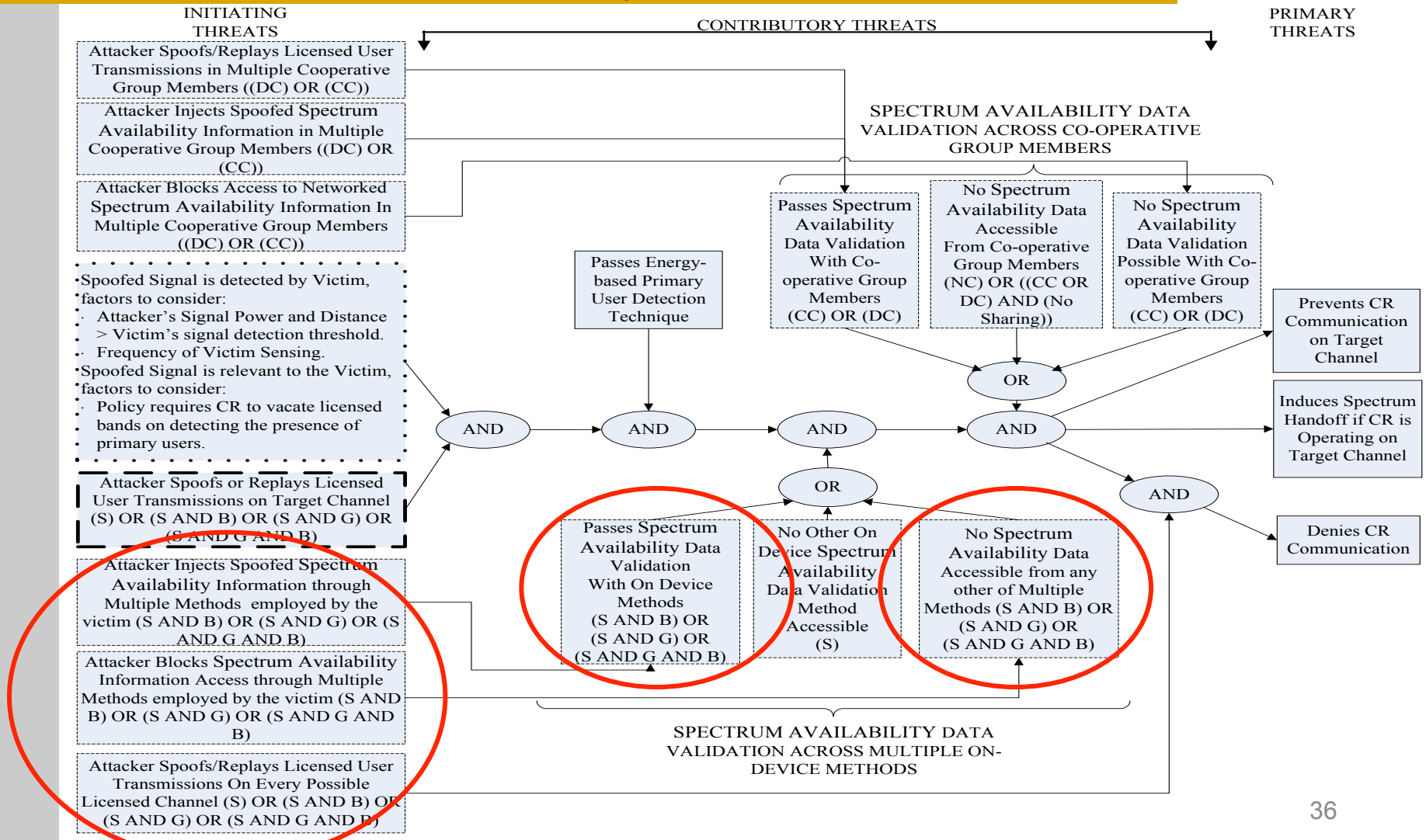
Example Attack Analysis: Primary User Emulation Attack in Non-Cooperative Architecture



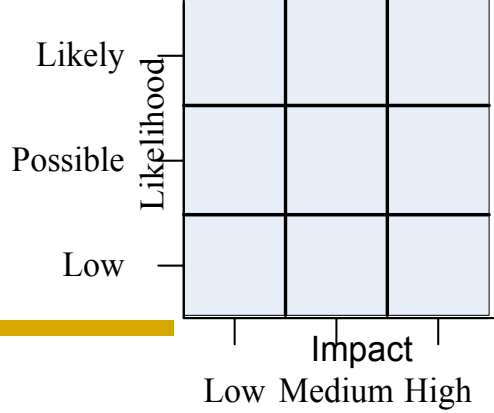
Example Attack Analysis: Primary User Emulation Attack in Cooperative Architectures



Example Attack Analysis: General Hammer Model for Primary User Emulation Attack



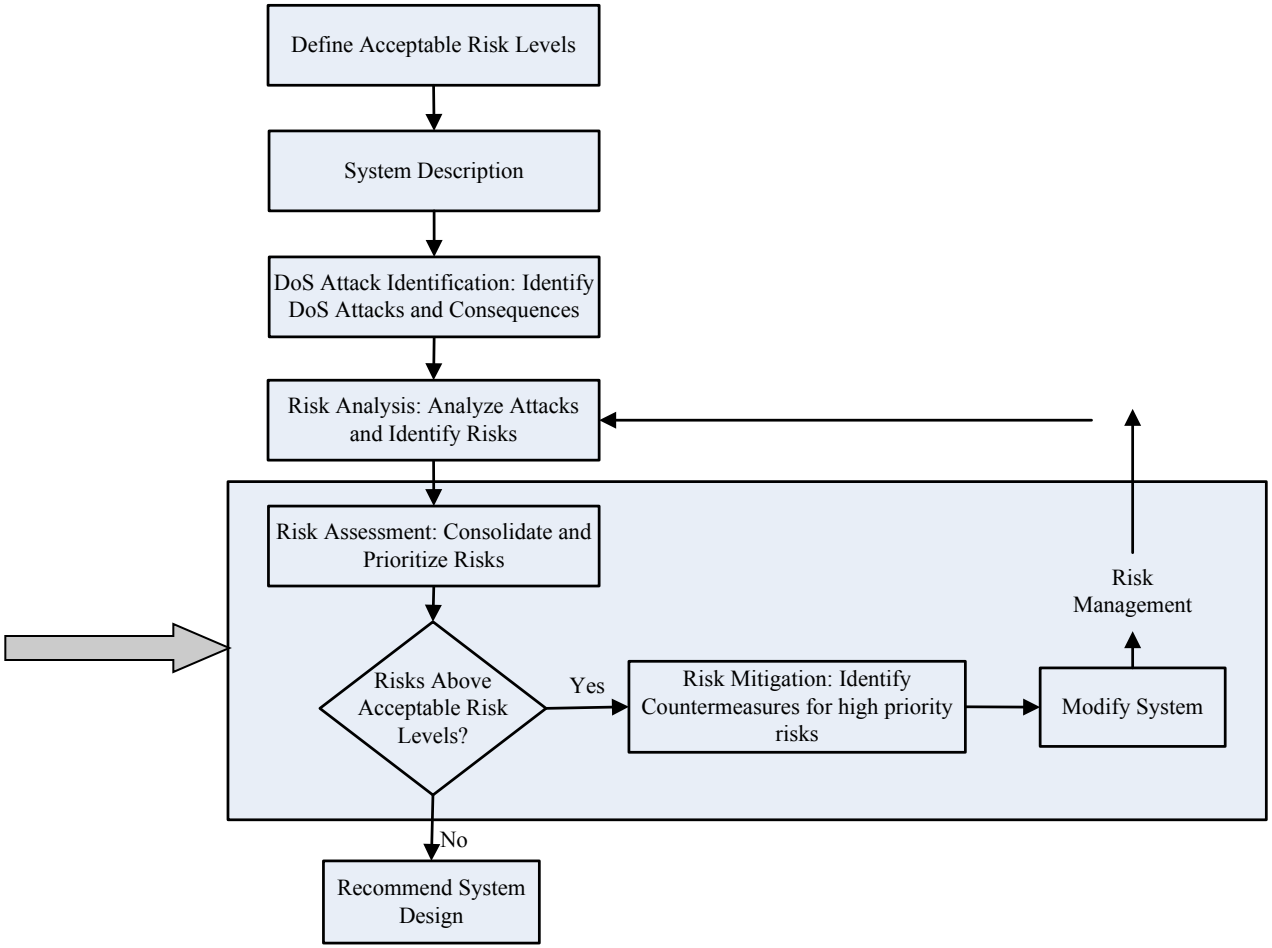
Example Risk Assessment



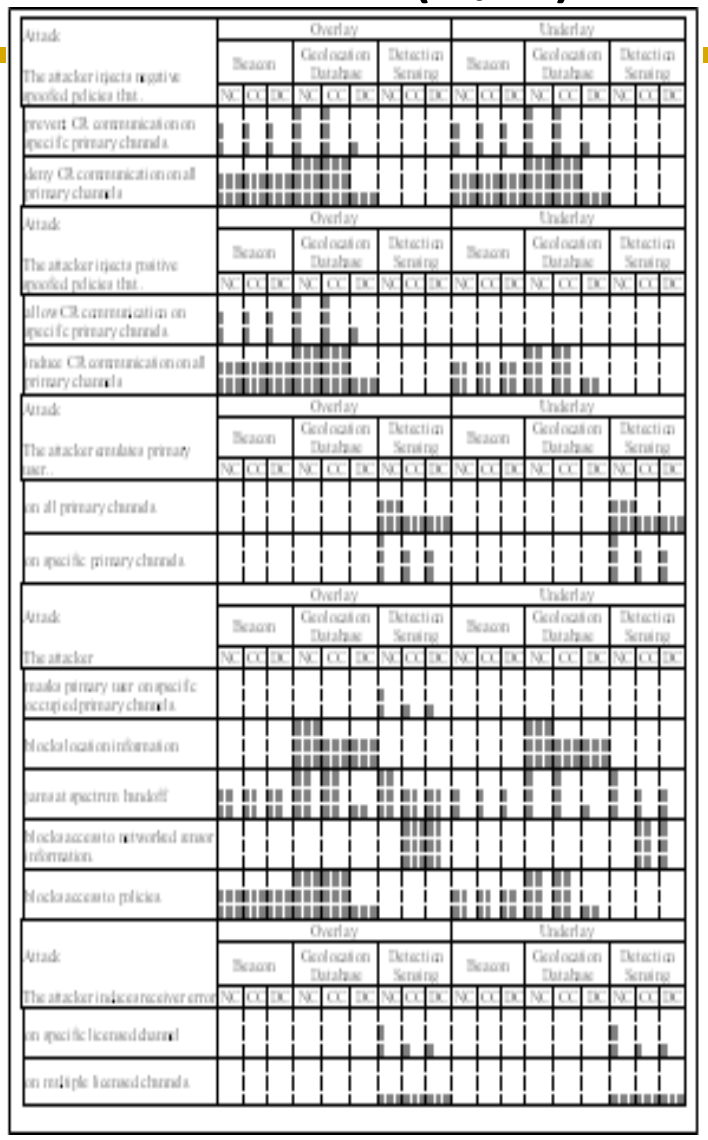
Spectrum Access Method: Overlay OR Underlay
Spectrum Awareness Method: Detection/Sensing

Attack.. The Attacker Emulates Primary User	Non-Cooperative	Centralized Cooperative	Distributed Cooperative
On all Licensed Channels	CRITICAL	MAJOR	MAJOR
On Specific Licensed Channel	MAJOR	MINOR	MINOR

Research Outline



Risk Management: Phase I Risk Assessment Results (1/2)



Risk Management: Phase I Risk Assessment Results (2/2)

Cumulative CRITICAL Risk Value

Cumulative MAJOR Risk Value

	Overlay			Underlay			Total Risk Value
	Beacon	Geo-locate Database	Detection Sensing	Beacon	Geo-locate Database	Detection Sensing	
Non-Cooperative	18, 4	42, 6	12, 6	6, 8	30, 6	6, 9	153
Centralized Cooperative	18, 4	39, 6	9, 10	6, 8	27, 6	6, 6	145
Distributed Cooperative	18, 4	6, 9	6, 10	6, 8	6, 3	0, 9	85
Total Risk Value	66	108	53	42	78	36	383
	227			156			

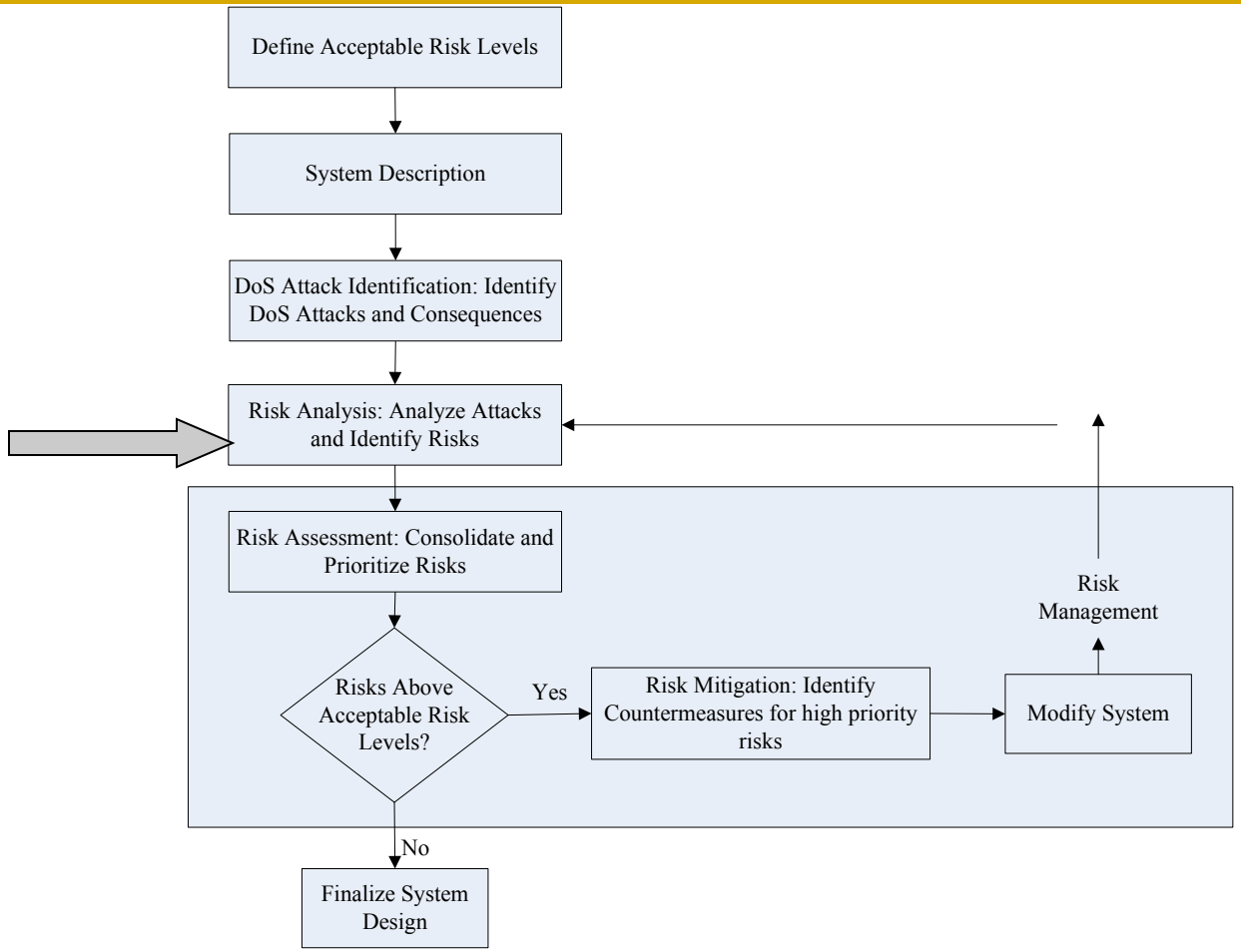
Total CRITICAL + MAJOR Risk Value

Risk Management: Next Steps

- Devise Countermeasure for Above Acceptable Risk Level Attacks. Example: Primary User Emulation Attack Mitigation – CR uses Feature based Primary User Detection Technique

- Modify CR System: Harden with Countermeasures

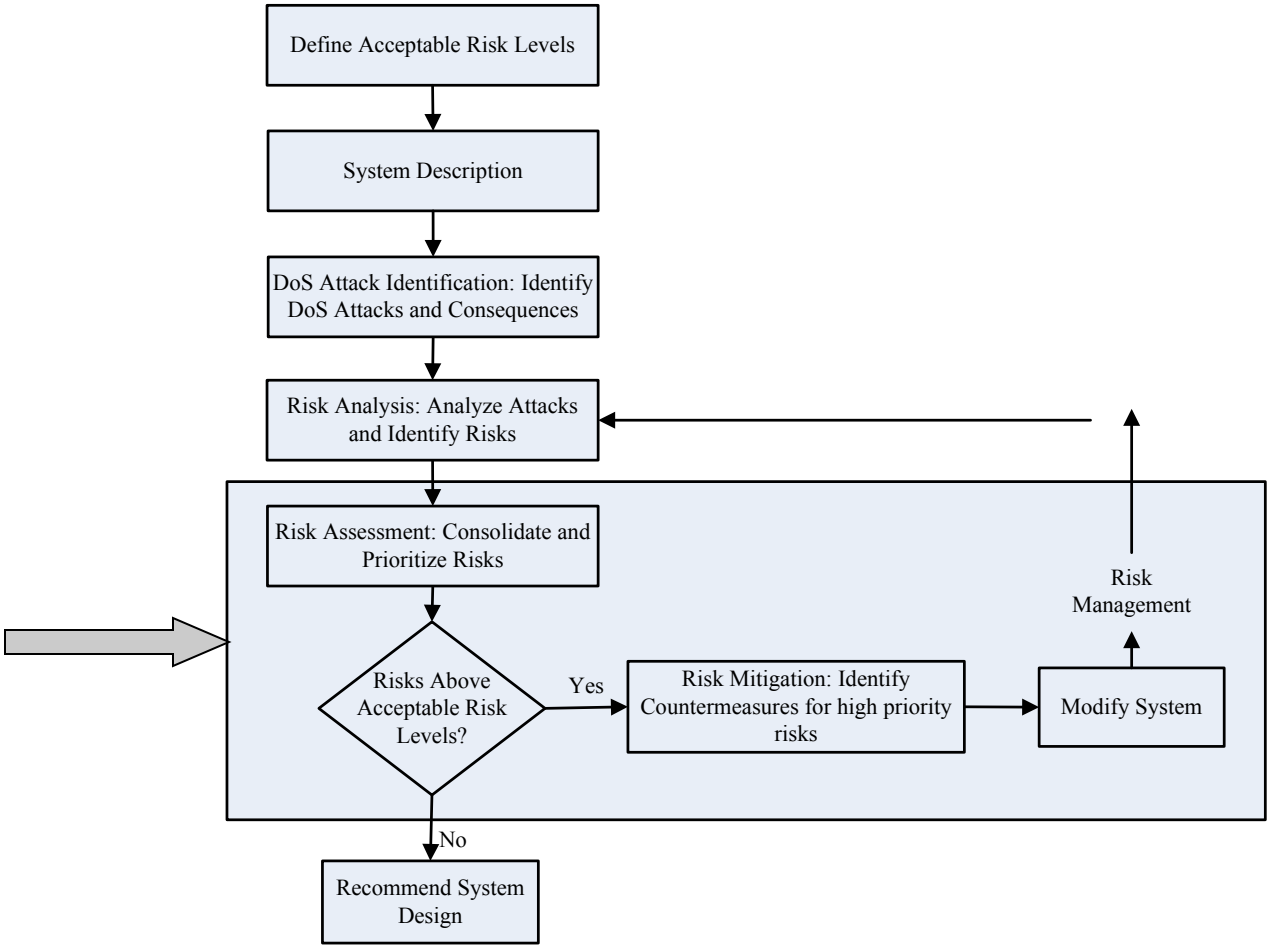
Research Outline



Phase II Risk Analysis

- Re-analyze High-Priority Attacks for Modified CR System
- Re-assess Risk Level based on Likelihood and Impact

Research Outline



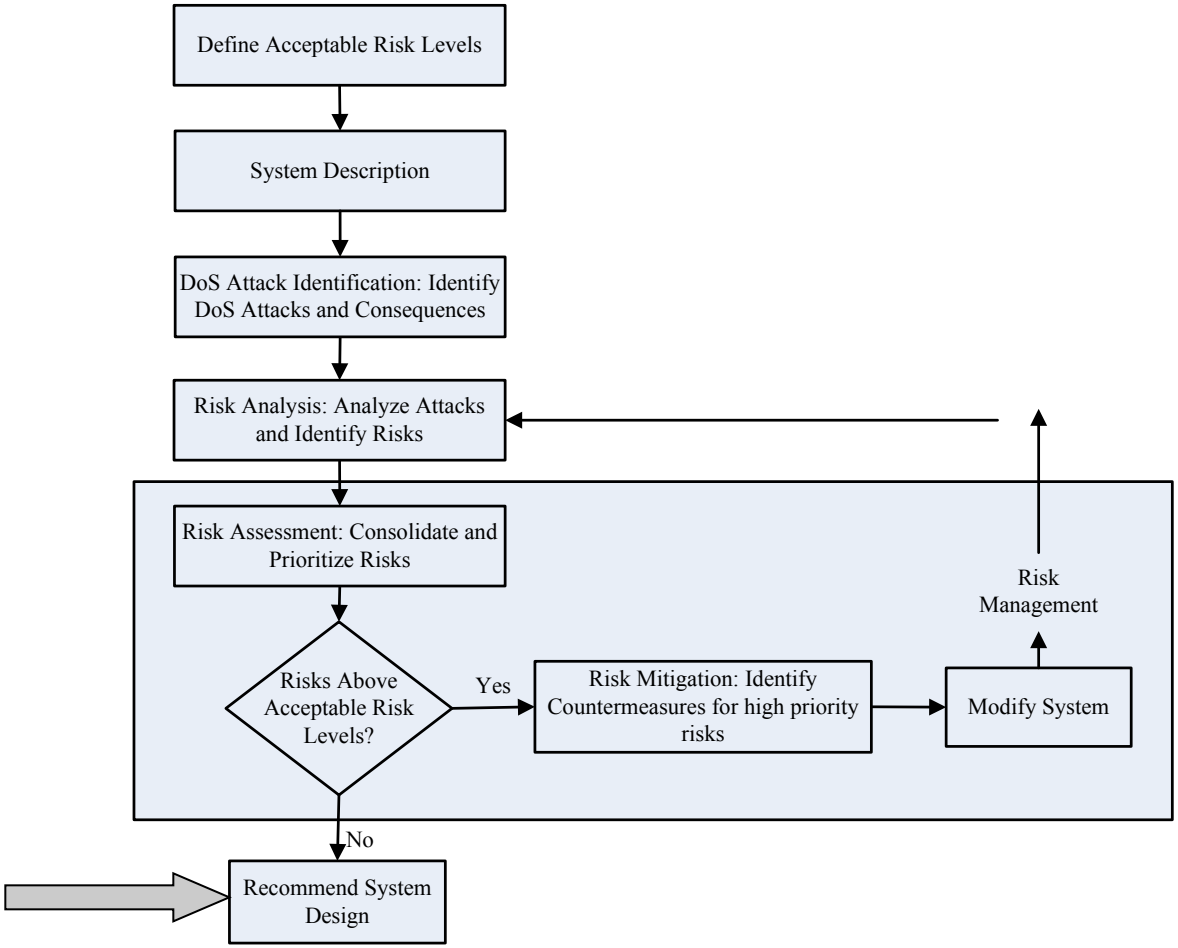
Risk Management: Phase II Risk Assessment Results

	Overlay			Underlay			Total Risk Value
	Beacon	Geo-locate Database	Detection Sensing	Beacon	Geo-locate Database	Detection Sensing	
Non-Cooperative	6, 6	0, 9	0, 6	0, 7	0, 3	0, 6	43
Centralized Cooperative	0, 9	0, 9	0, 9	0, 3	0, 3	0, 6	39
Distributed Cooperative	0, 9	0, 9	0, 6	0, 3	0, 3	0, 6	36
Total Risk Value	30	27	21	13	9	18	118
	78			40			

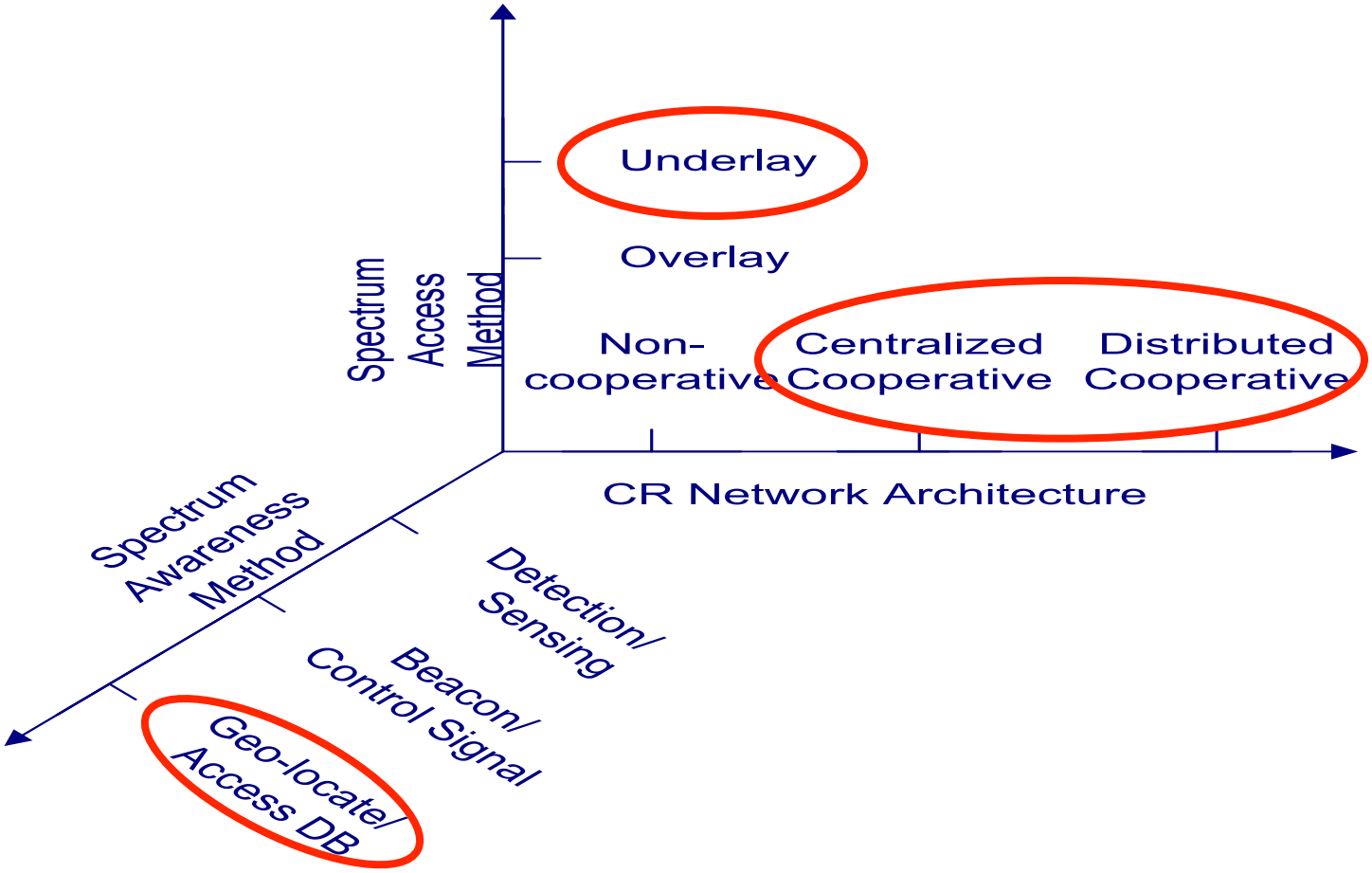
CR Configuration used in 802.22

Least Vulnerable CR Configurations

Research Outline



CR Design Recommendations



Conclusion

- CRs are susceptible to attacks.
- CRs open new avenues of attack.
- A Formal Risk Analysis and Assessment Process can help guide the least vulnerable CR Design Paradigm
- NOW is the best time to devise countermeasures to reduce CR-specific vulnerabilities.

References

- T. X Brown, A. Sethi, "Potential Cognitive Radio Denial-of-Service Vulnerabilities and Protection Countermeasures: a Multi-dimensional Analysis and Assessment," *Journal Mobile Networks and Applications*, v. 13, n. 5, October 2008, pp. 516-532, 17 p.
- A. Sethi, T. X Brown, "Hammer Model Threat Assessment of Cognitive Radio Denial of Service Attacks," *IEEE Dynamic Spectrum Access Networks* (DySpAN), Chicago, Oct. 14-17, 2008.
- T. X Brown, A. Sethi, "Potential Cognitive Radio Denial-of-Service Vulnerabilities And Protection Countermeasures: A Multi-dimensional Analysis/Assessment," *Proc. Second Int. Conf. on Cognitive Radio Oriented Wireless Networks and Communications* (CrownCom), Orlando, FL, Aug 1-3, 2007. 10pp.
- T. X Brown, A. Sethi, "Potential Cognitive Radio Denial-of-Service Vulnerabilities and Countermeasures," in *Proc. Int. Symposium on Advanced Radio Technologies* (ISART), Boulder, Feb. 2007.