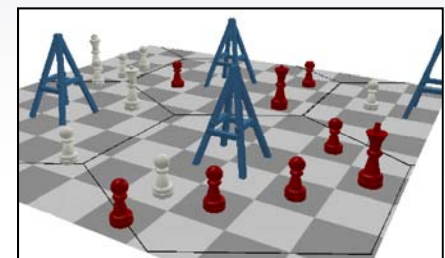
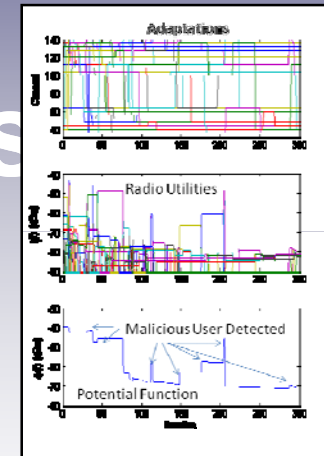


Practical Considerations for Cognitive Radio Networking Environments

James “Jody” Neel

james.neel@crtwireless.com

SDR ‘10



Material

- Interactions of CRs
- Impact of Hostile Users
- Security Issues

Issues Can Occur When Multiple Intelligences Interact

- Flash Crash of May 6, 2010
 - Not just a fat finger
 - Combination of bad economic news, big bet by Universa, and interactions of traders and computers

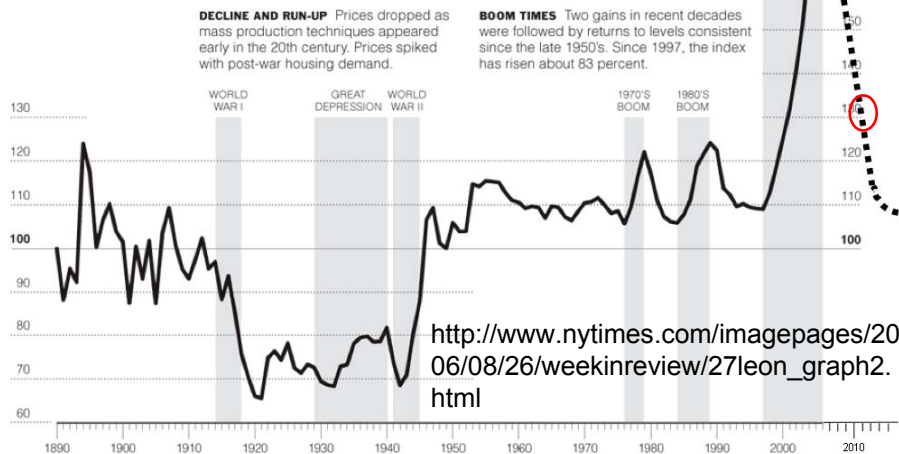


http://www.legitreviews.com/images/reviews/news/dow_drop.jpg

A History of Home Values

The Yale economist Robert J. Shiller created an index of American housing prices going back to 1890. It is based on sale prices of standard existing houses, not new construction, to track the value of housing as an investment over time. It presents housing values in consistent terms over 116 years, factoring out the effects of inflation.

The 1890 benchmark is 100 on the chart. If a standard house sold in 1890 for \$100,000 (inflation-adjusted to today's dollars), an equivalent standard house would have sold for \$66,000 in 1920 (66 on the index scale) and \$199,000 in 2006 (199 on the index scale, or 99 percent higher than 1890).



Source: "Irrational Exuberance" 2nd Edition, 2003, by Robert J. Shiller
Lynchburg, VA 24502

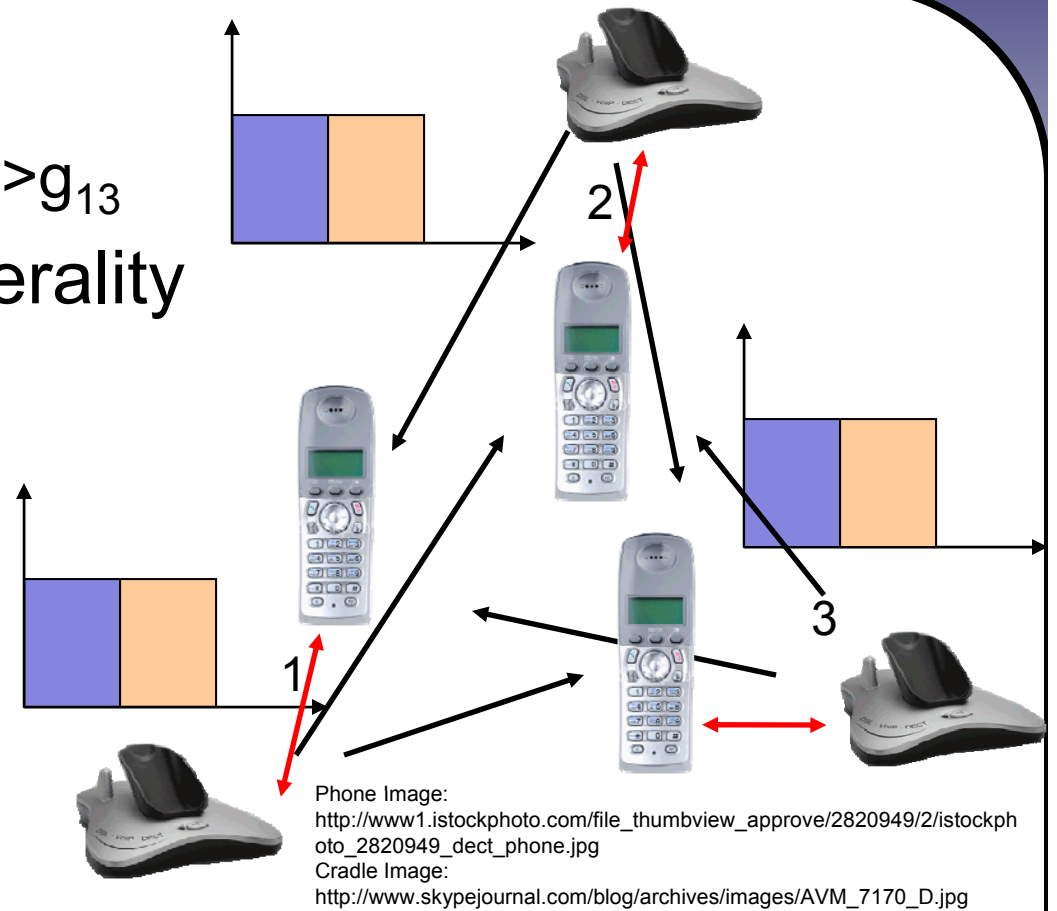
Bill Marsh/The New York Times

- Housing Bubble
 - Bounce up instead of down
 - Slower interactions lead to slower changes
 - Also indicative of the role beliefs play in instability

www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

In heavily loaded networks, a single vacation can spawn an infinite adaptation process

- Suppose
 - $g_{31} > g_{21}; g_{12} > g_{32}; g_{23} > g_{13}$
- Without loss of generality
 - $g_{31}, g_{12}, g_{23} = 1$
 - $g_{21}, g_{32}, g_{13} = 0.5$
- Infinite Loop!
 - 4,5,1,3,2,6,4,...



Interference Characterization

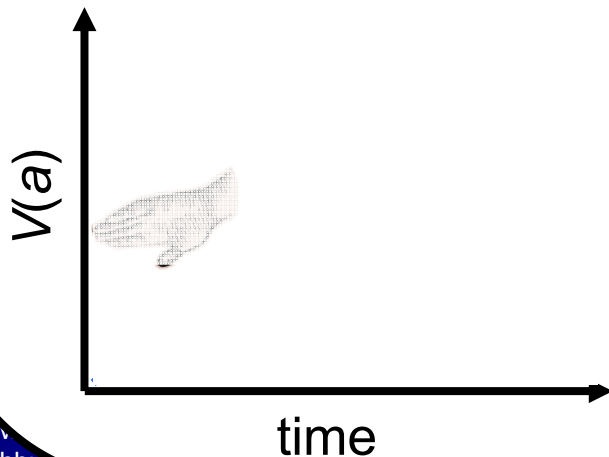
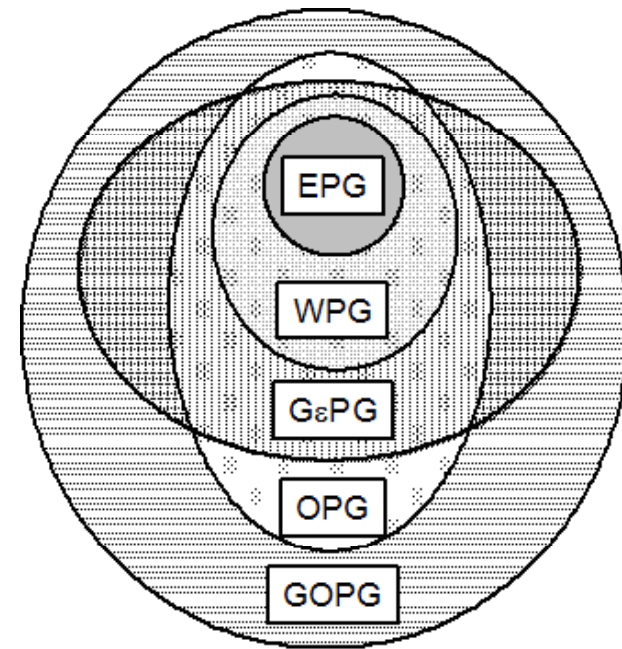
Chan.	(0,0,0)	(0,0,1)	(0,1,0)	(0,1,1)	(1,0,0)	(1,0,1)	(1,1,0)	(1,1,1)
Interf.	(1.5,1.5,1.5)	(0.5,1,0)	(1,0,0.5)	(0,0.5,1)	(0,0.5,1)	(1,0,0.5)	(0.5,1,0)	(1.5,1.5,1.5)
	0	1	2	3	4	5	6	7

Generalized Insights from the DECT Example

- If # links / clusters $>$ # channels, decentralized channel choices will have a non-zero looping probability
- As # links / clusters $\rightarrow \infty$, looping probability goes to 1
- Can be mitigated by increasing # of channels (DECT has 120) or reducing frequency of adaptations (DECT is every 30 minutes)
 - Both waste spectrum
 - And we're talking 100's of ms for vacation times
- “Centralized” solutions become distributed as networks scale
 - “Rippling” in Cisco WiFi Enterprise Networks
 - www.hubbert.org/labels/Ripple.html
- Also shows up in more recent proposals
 - Aug 2009 White Spaces paper from Microsoft
- Major reason most routing algorithms are not load sensitive

Potential games yield predictable interactions

- Existence of a function (called the potential function, V), that reflects the change in utility seen by a unilaterally deviating player.
- Cognitive radio interpretation:
 - Every time a cognitive radio unilaterally adapts in a way that furthers its own goal, some real-valued function increases.
- Our use:
 - Predictable, stable emergent behavior
 - Behavior inconsistent with the goals will immediately break the monotonicity



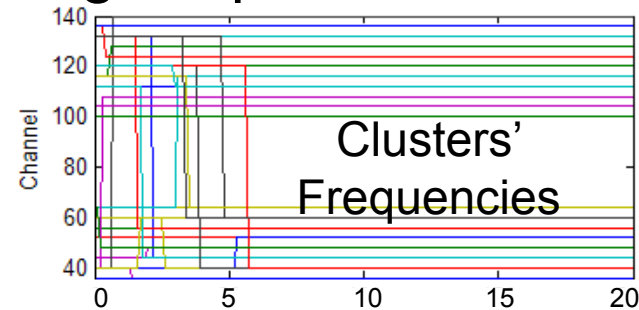
Potential Game	Relationship ($\forall i \in N, \forall a \in A$)
Exact (EPG)	$u_i(b_i, a_{-i}) - u_i(a_i, a_{-i}) = V(b_i, a_{-i}) - V(a_i, a_{-i})$
Weighted (WPG)	$u_i(b_i, a_{-i}) - u_i(a_i, a_{-i}) = \alpha_i [V(b_i, a_{-i}) - V(a_i, a_{-i})]$
Ordinal (OPG)	$u_i(b_i, a_{-i}) - u_i(a_i, a_{-i}) > 0 \Leftrightarrow V(b_i, a_{-i}) - V(a_i, a_{-i}) > 0$
Generalized Ordinal (GOPG)	$u_i(b_i, a_{-i}) - u_i(a_i, a_{-i}) > 0 \Rightarrow V(b_i, a_{-i}) - V(a_i, a_{-i}) > 0$
Generalized ε (GεPG)	$u_i(b_i, a_{-i}) > u_i(a_i, a_{-i}) + \varepsilon_1 \Rightarrow V(b_i, a_{-i}) > V(a_i, a_{-i}) + \varepsilon_2$

Example behavior

- For example, for a collection of 802.11 clusters independently choosing operating frequencies

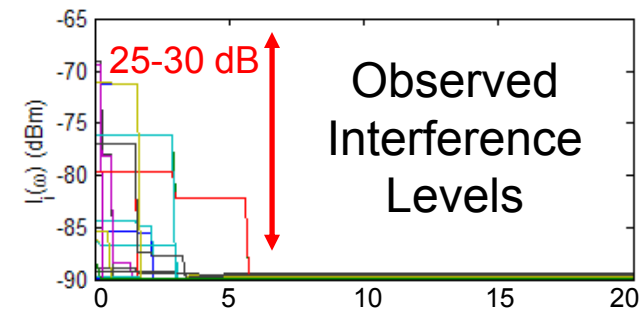
1. All self-interested adaptations

- Scalable resource utilization
- No synchronization required



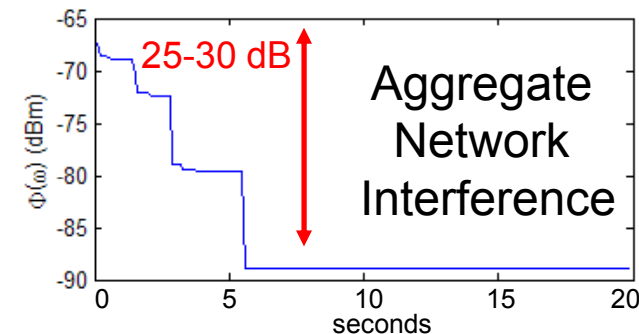
2. Based only on observations of own performance

- No information exchange overhead
- More responsive network



3. Decrease aggregate network interference

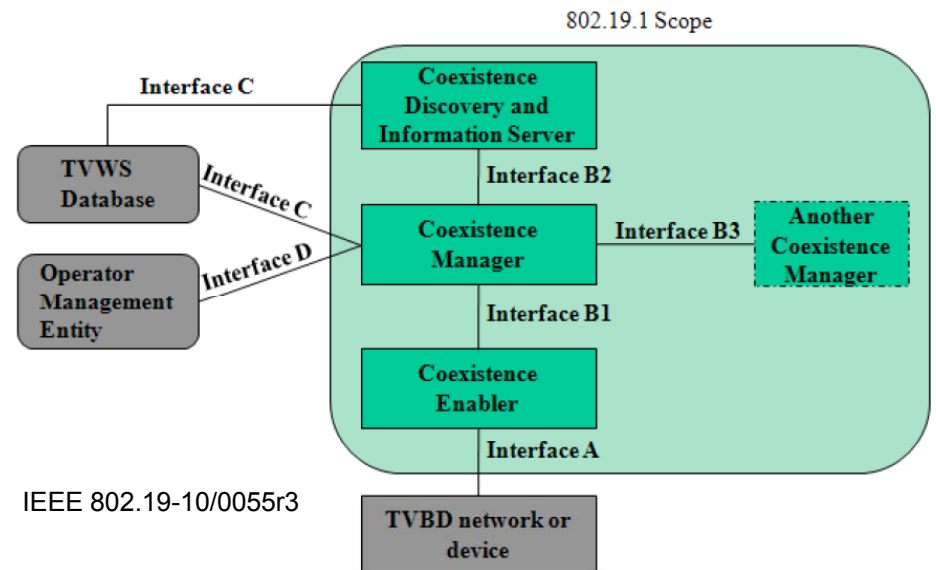
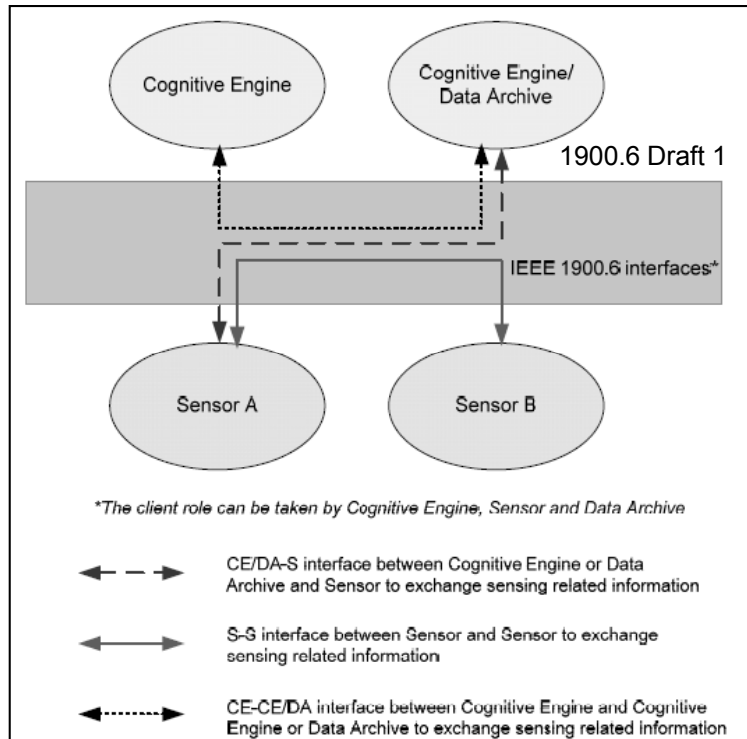
- Self-stable
- Converges to local-optima



No network is an island

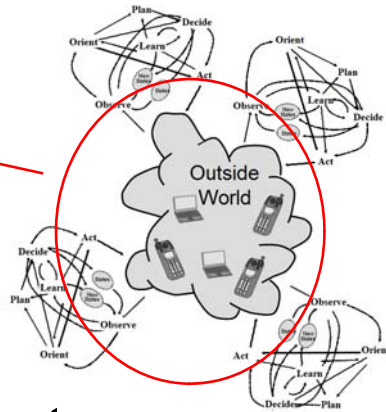
- Many TVWS standards
 - 802.22 (CR for rural)
 - 802.16h (CR WiMAX)
 - 802.11af (WhiteFi)
 - CogNeA

- Decisions impact one another
 - Etiquette
- Coordinate quiet periods
 - Common time base, scheduling
- Share information
 - Sensing
- Merging?

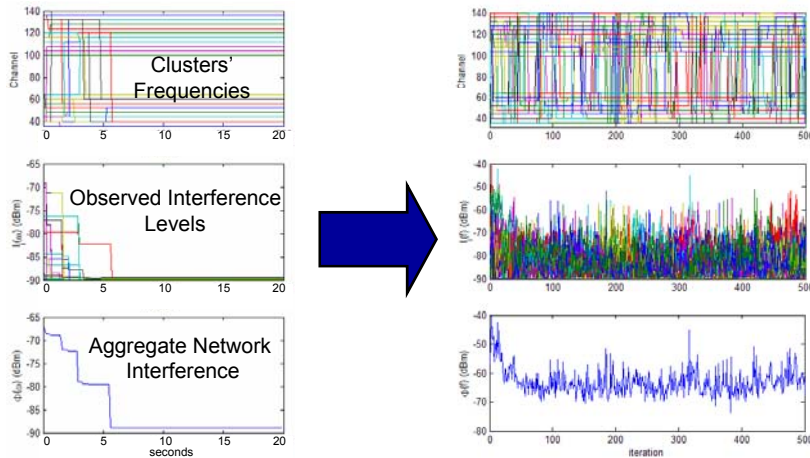


Hostile users can create problems from outside your network

What if the environment is "unstable"?



• Stability impact

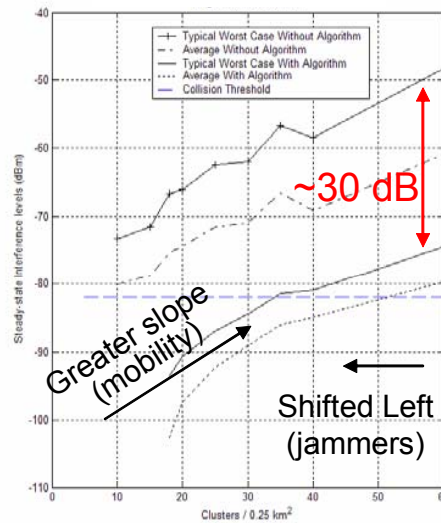


- Need to consider external actors
 - Detect unexpected behavior, adjust accordingly

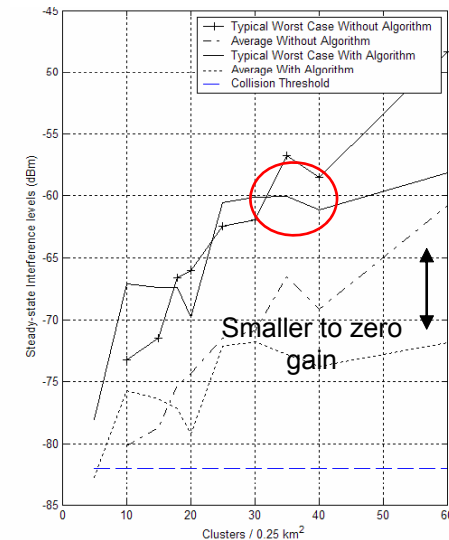
- Suppose another network is compromised in your area
- Their behavior influences your network's adaptations

• Performance Impact

Fixed Interferer (Mobile)



Adaptive Interferer (Mobile)

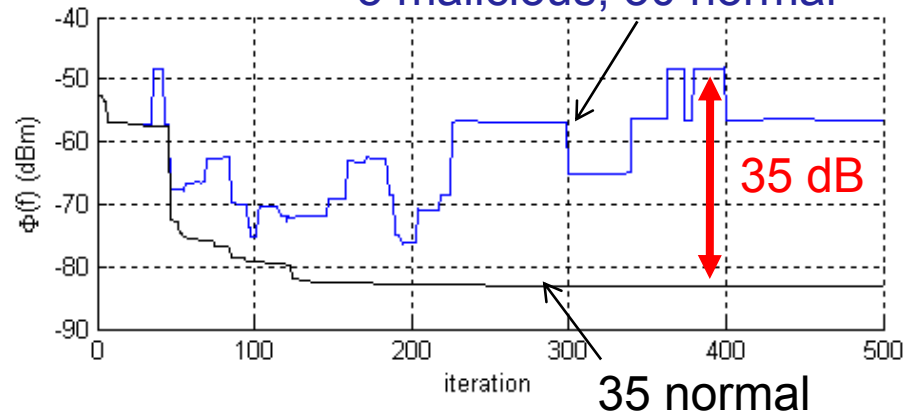


Hostile users can blend in

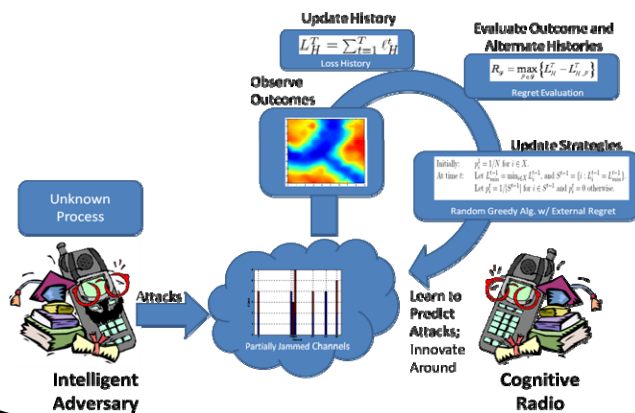
- Normal CR
 - Given available adaptations and knowledge about network state
 - Maximize system (own) performance
- Hostile CR
 - Given available adaptations and knowledge about network state
 - Minimize system performance

Average interference levels for nodes 6-35

5 malicious, 30 normal

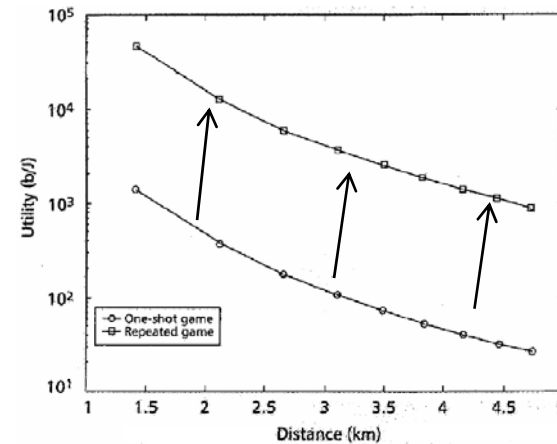


- Adapt at inopportune times
- Simply minimize performance
- Ensure marginally stable network goes unstable
- Plus learning exploits
 - And spoofing
 - And information corruption

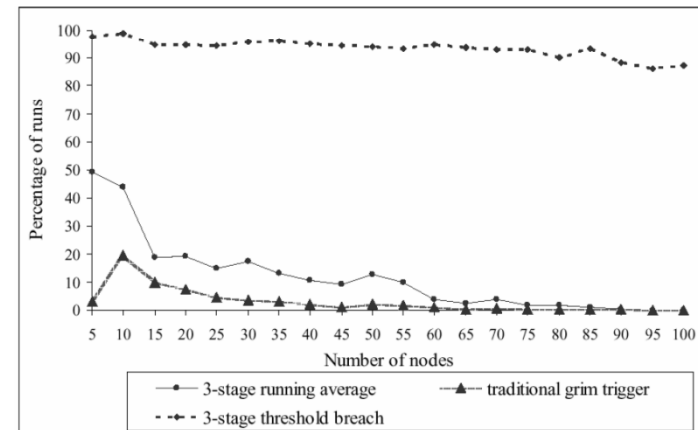


Malicious \neq Selfish

- Popular “solution” to mischievous nodes (selfish nodes that damage network) is to “punish” nodes
 - Also implies a way to “brainwash” learning nodes
- Imperfect information can obfuscate punishment from mischievous behavior and produce catastrophic cascades
 - Brittleness
- Even with perfect information, malicious node may be masochistic

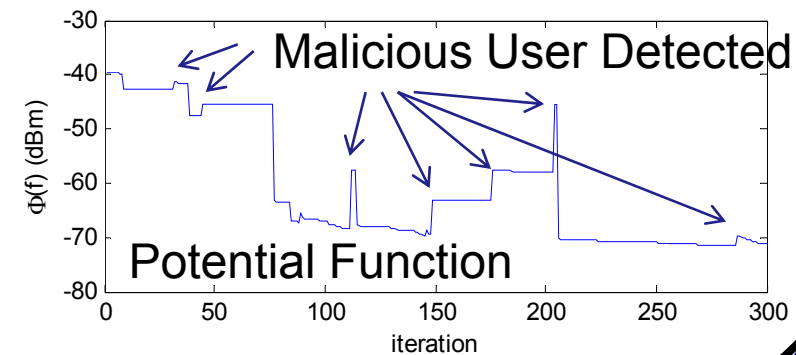
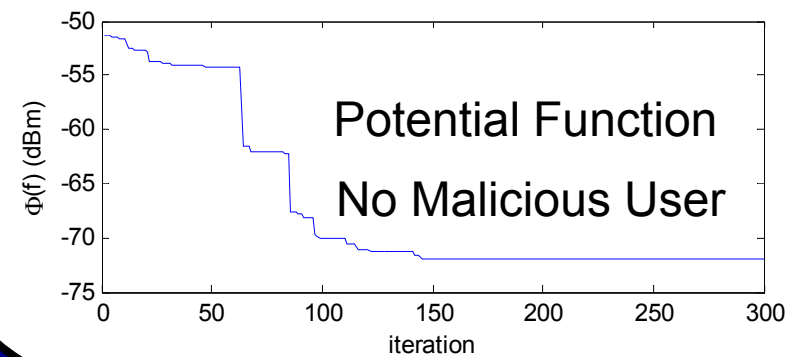
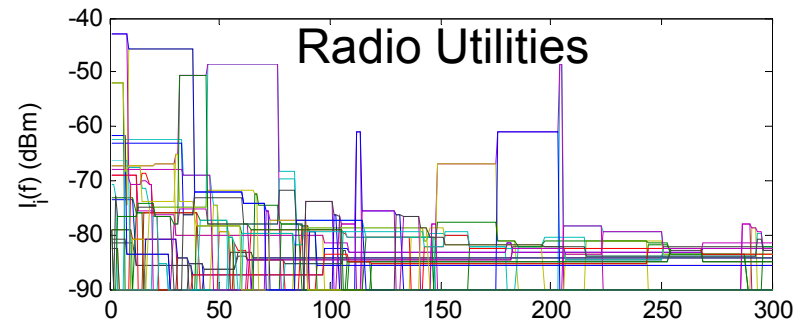
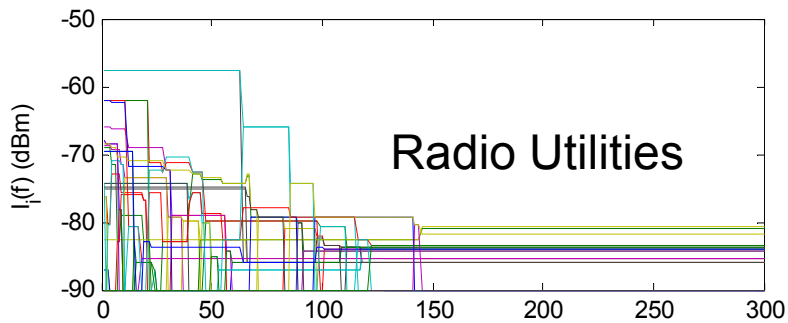
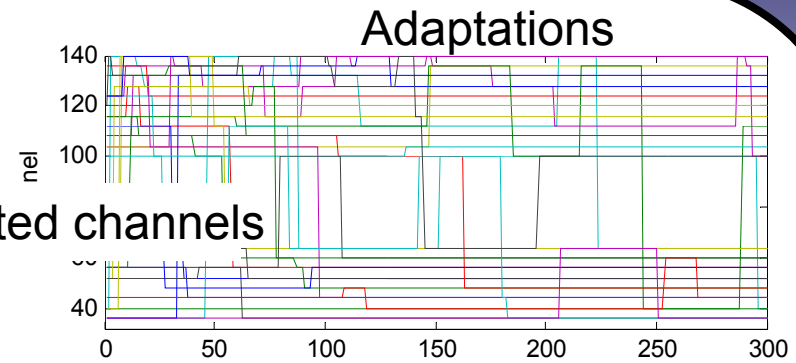
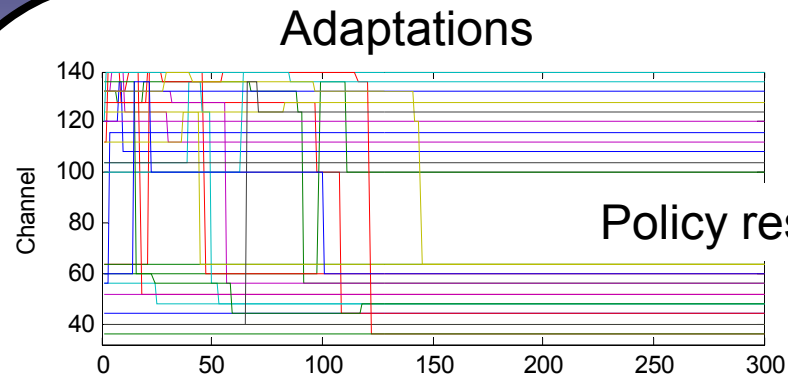


From Fig 6 in [MacKenzie_01]



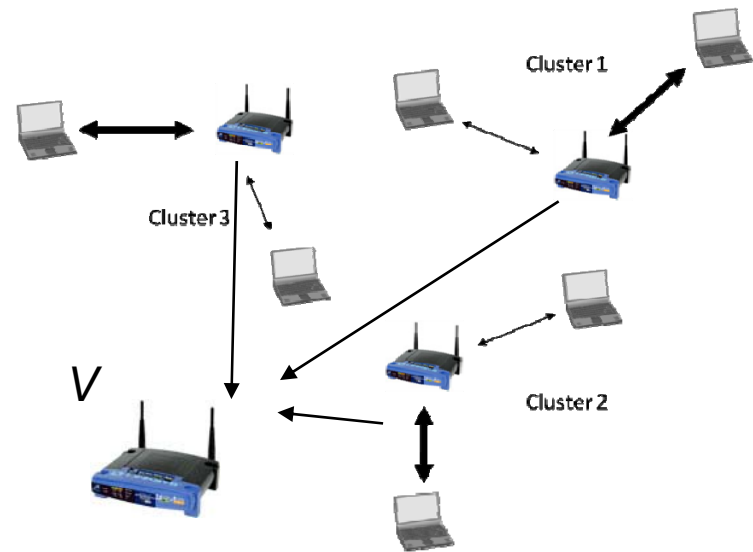
From [Srivastava_06]

Detecting aberrant behavior from predictable emergent properties



Implementation Discussion

- Implement as monitoring system that evaluates potential (emergent) function
 - Frequently sum of performance levels
 - Complexity is in the transmission / connectivity
 - No single node / cluster knows / can evaluate emergent function
- But a malicious CR will lie
 - E.g., Claim massive gains to offset others' losses
- With BSI, a malicious node can't tell a credible lie!
 - Other relationships exist
 - Need to be WPG / EPG for linear relationships



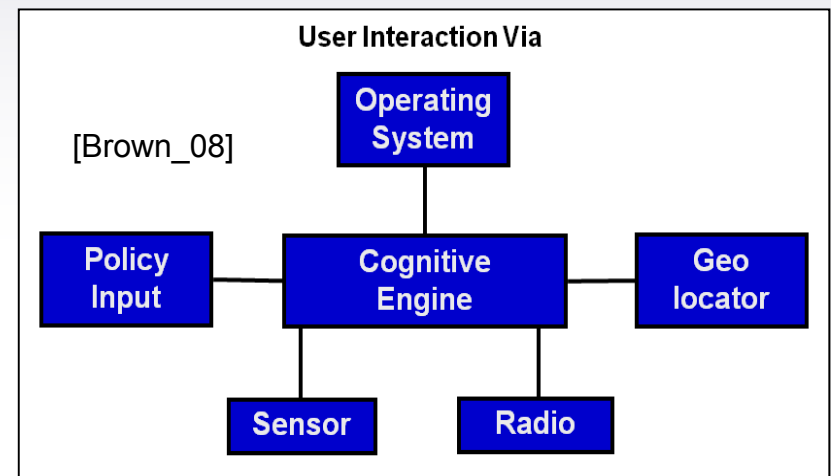
$$\frac{\partial u_i(\omega)}{\partial \omega_i} = \sum_{j \in N \setminus i} \frac{\partial u_j(\omega)}{\partial \omega_i} = \frac{\partial V(\omega)}{\partial \omega_i} / 2$$

Security Issues

- [Clancy_08]
 - Primary user emulation attacks
 - Belief manipulation attacks
 - A “cognitive radio virus”

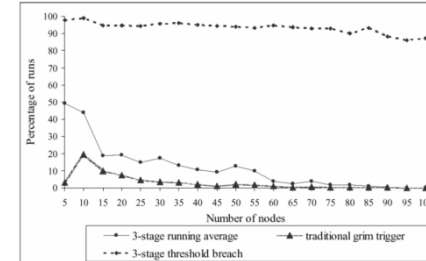
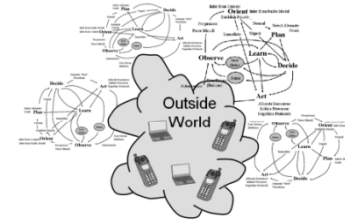
Attacker ...	Beacon	Geo-DB	Detect Sense
injects policies that prevent CR communication on specific primary channels.	■	■	
injects policies that deny CR communication on all primary channels.	■	■	■
injects policies that allow CR communication on specific primary channels.	■	■	
injects policies that induce CR communication on all primary channels.	■	■	
emulates primary user on all primary channels.			■
emulates primary user on specific primary channels.			■
masks primary user on specific occupied primary channels.			■
blocks location information		■	
jams at spectrum handoff.	■	■	■
blocks access to networked sensor information.		■	■
blocks access to policies.	■	■	
induces receiver errors on specific licensed channel			■
induces receiver errors on multiple licensed channels.			■

- Spectrum sensing data falsification [Chen_08a]
- Quiet period jamming [Bian_08]
- Replay sensing attacks [Bian_08]
- False coexistence information [Bian_08]
- Honeypot attacks [Newman_09]
- Chaff point attacks [Newman_09]



Questions you should ask before fielding your network

- Can you predict what will happen when the network scales and interactions occur?
- How might your measures be turned against you?
 - Sensing, learning, policy enforcement
 - Even when following the “rules”
- How do you accommodate CR networks other than your own?
 - Can be attacked from outside without jamming
- If there are vulnerabilities, how will you detect that they are being exploited?



Average Interference levels for nodes 6-35

5 malicious, 30 normal

