Issues in Fielding Large Scale Cognitive Radio Networks in Hostile Environments

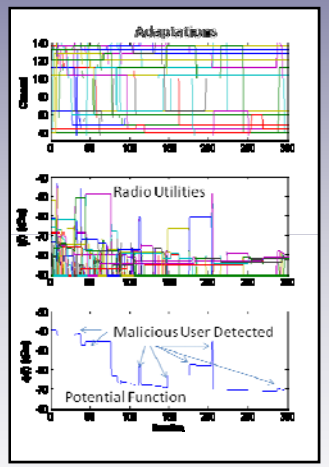
James “Jody” Neel

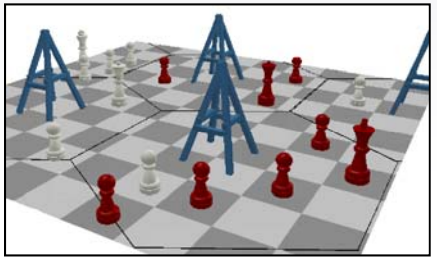
james.neel@crtwireless.com

June 7, 2010

International Software Radio Conference

crtwireless.com/files/CRT_SMI_2010.pdf





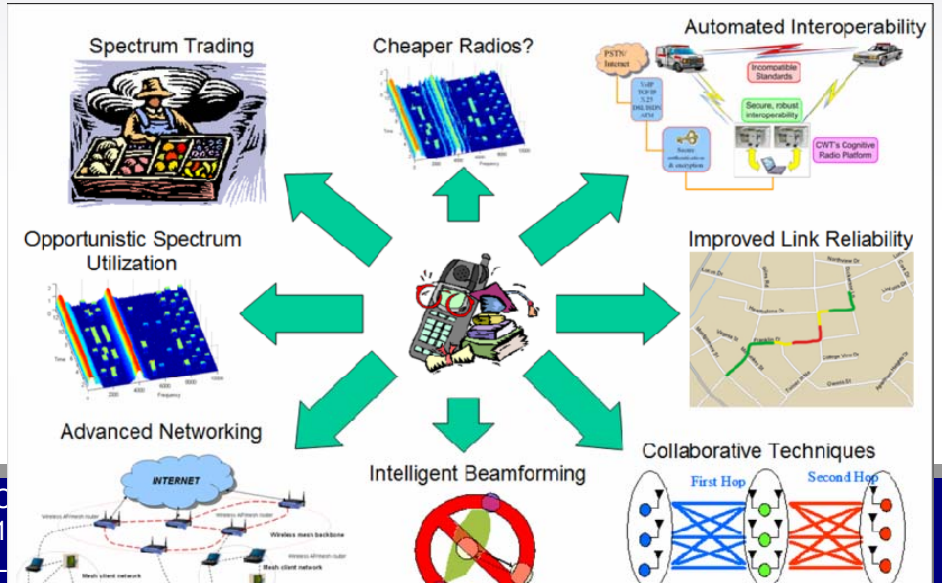
Cognitive Radio Technologies

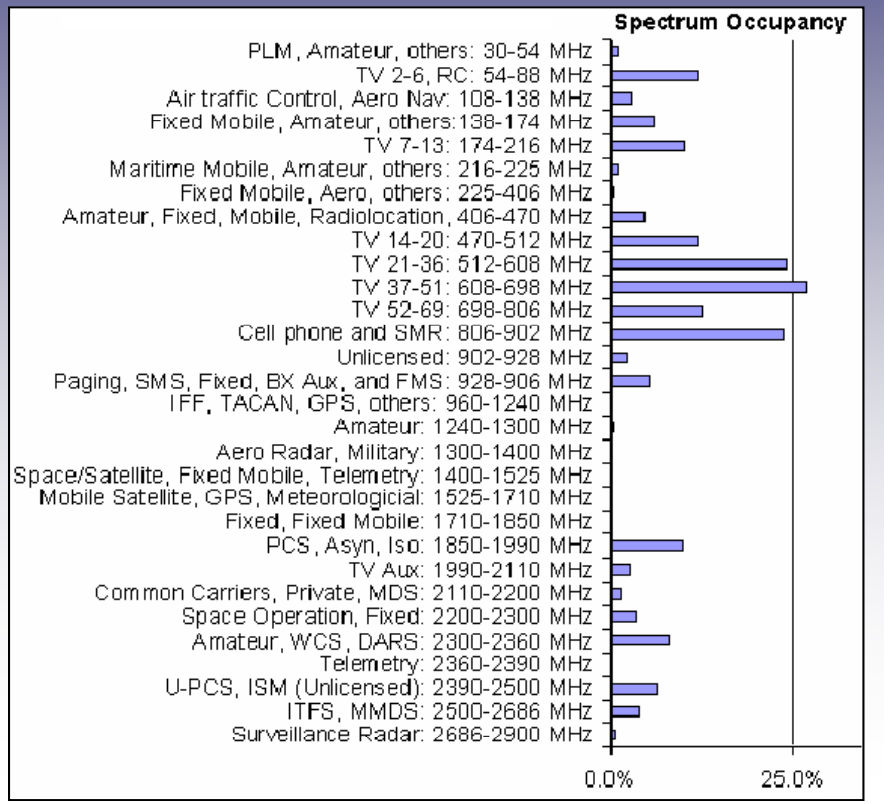
Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

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

Why Cognitive Radio?

- Spectrum is expensive
  - $19.12 billion from 700 MHz Auction
  - TV white spaces at over $100 billion
  - More access via DSA
- Reduce setup time and cost
  - Self organizing networks
  - Mitigate (WNAN)
- Link quality
- CRWG presenting results of survey of quantifiable benefits of document at ERRT in Mainz June 23

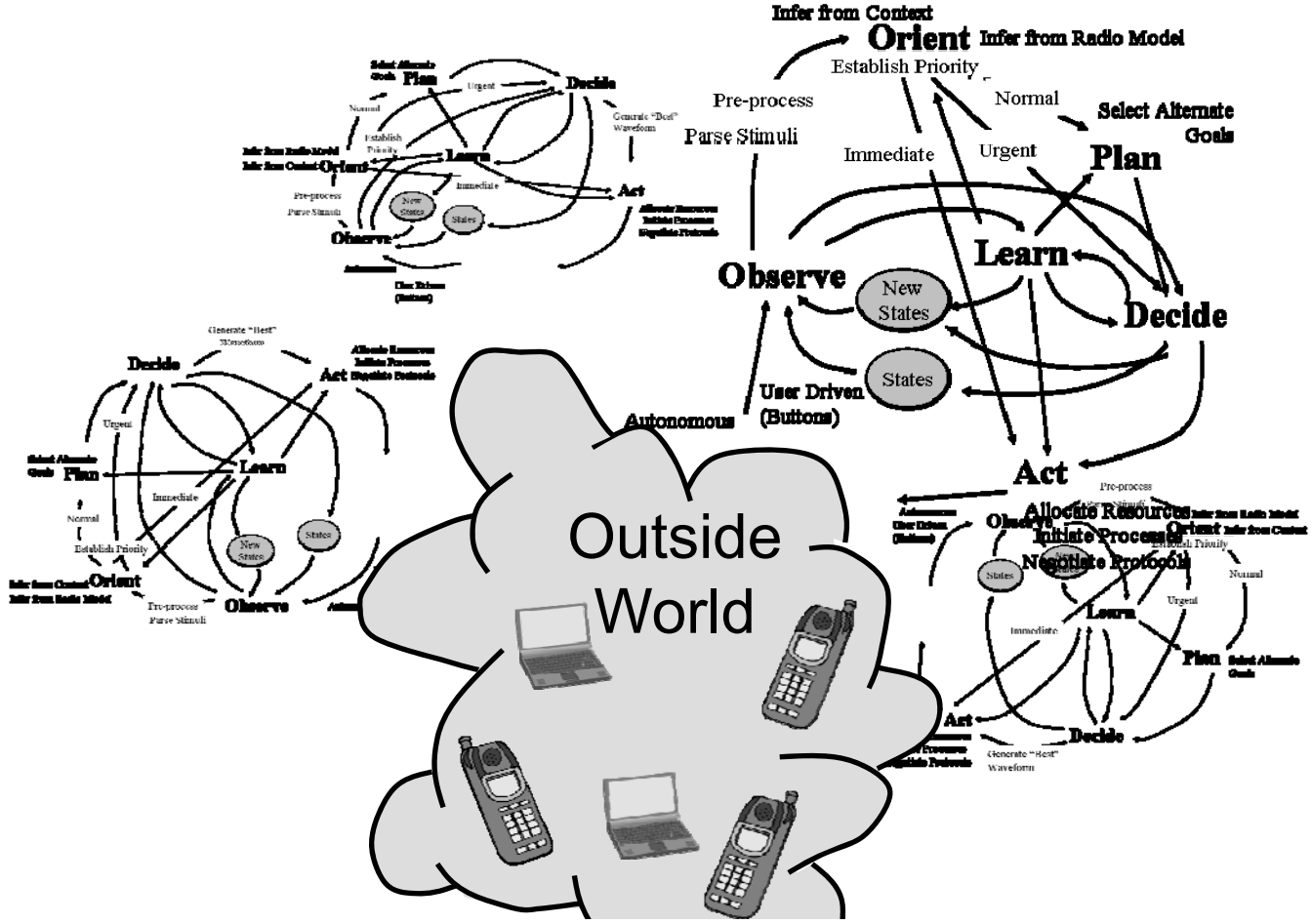




Modified from Figure 1 M. McHenry in "NSF Spectrum Occupancy Measurements Project Summary", Aug 15, 2005. Available online: http://www.sharedspectrum.com/?section=nsf_measurements

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

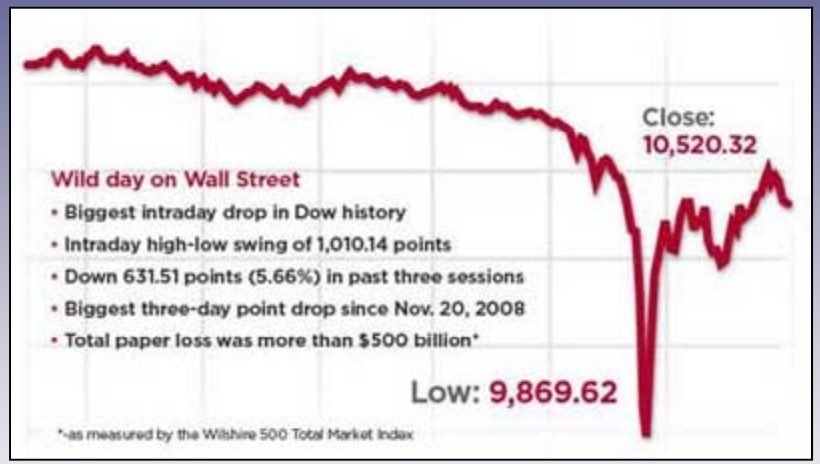
CRs don't just react, they interact



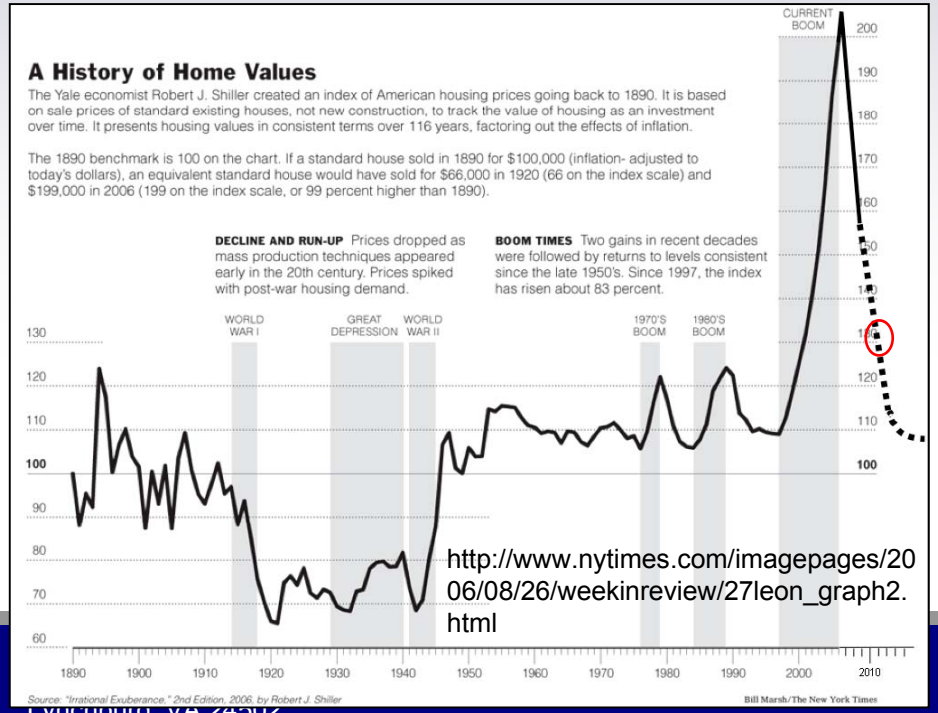
- Outside world is determined by the interaction of numerous cognitive radios
- What makes sense for a link, may not work for a net

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



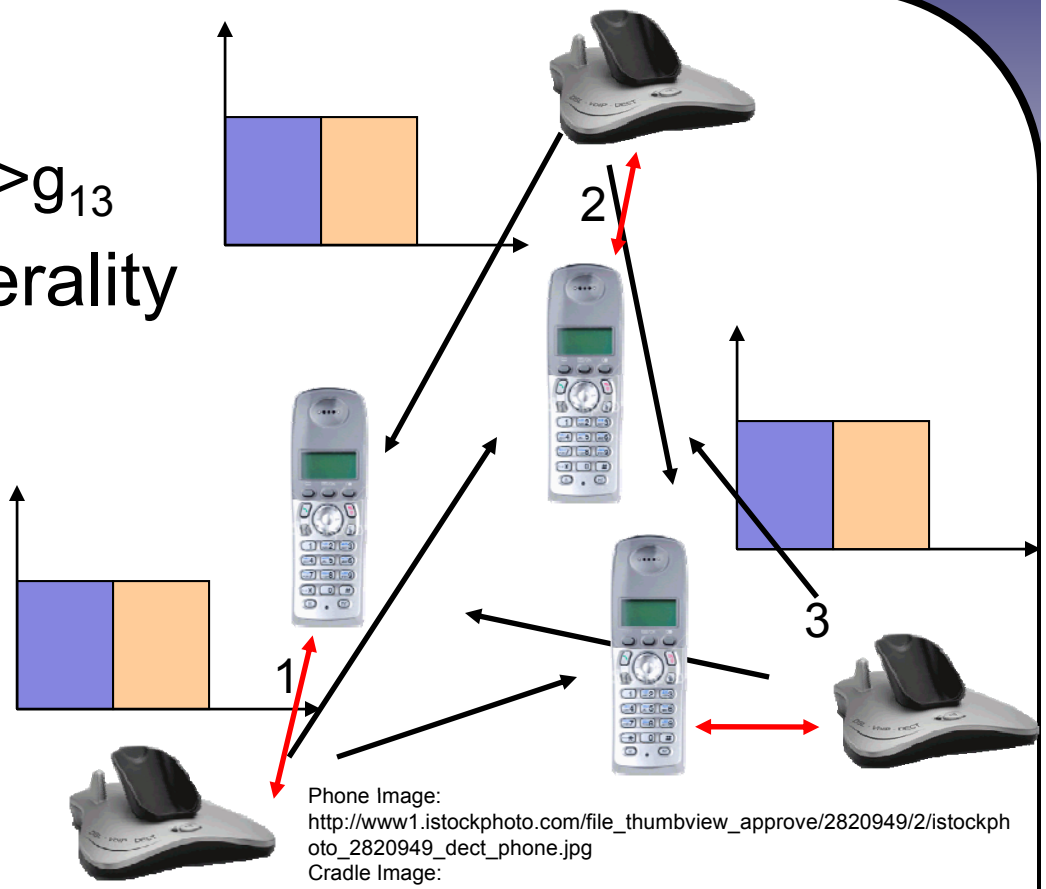
http://www.nytimes.com/imagepages/2006/08/26/weekinreview/27leon_graph2.html

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

Lynchburg, VA 24502
Web: 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,…



Phone Image:
http://www1.istockphoto.com/file_thumbview_approve/2820949/2/istockphoto_2820949_dect_phone.jpg
Cradle Image:
http://www.skypejournal.com/blog/archives/images/AVM_7170_D.jpg

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

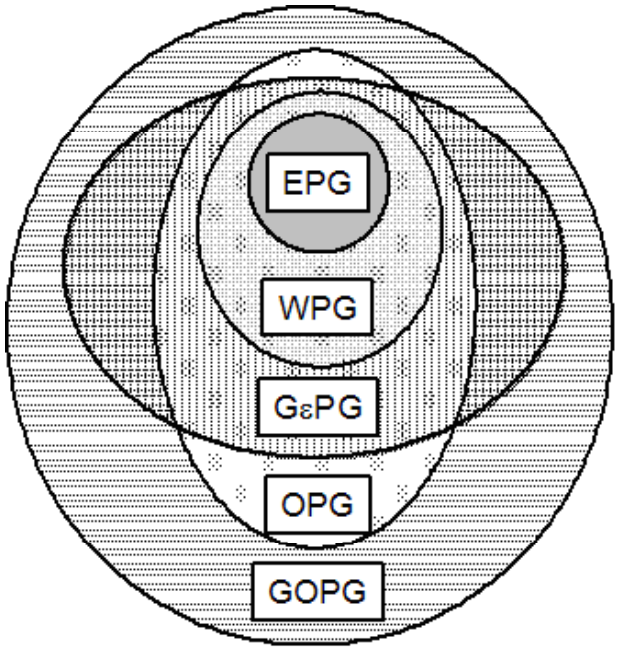
- If # links / clusters > # channels, decentralized channel choices will have a non-zero looping probability
- As # links / clusters $\rightarrow\infty$, looping probability goes to 1
- Can be mitigated by increasing # of channels (DECT has 120) or reducing frequency of adaptations (DECT is every 30 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

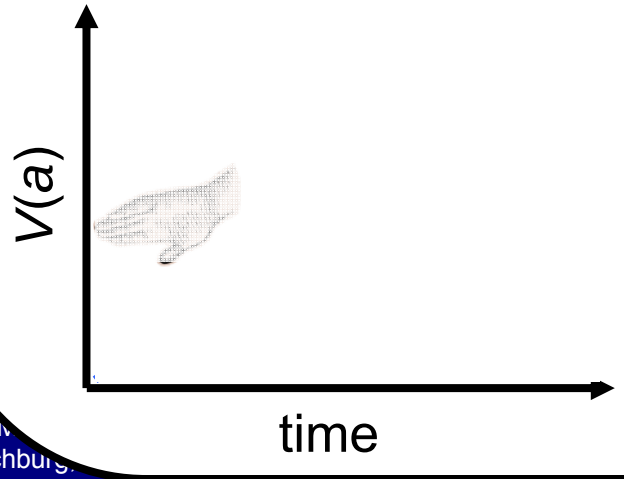
Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

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

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





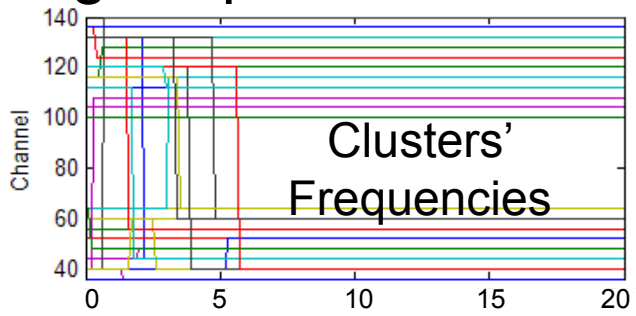
Potential Game	Relationship ($\forall i \in N, \forall a \in A$)
Exact (EPG)	$u_i(b_i,a_{-i})-u_i(a_i,a_{-i})=V(b_i,a_{-i})-V(a_i,a_{-i})$
Weighted (WPG)	$u_i(b_i,a_{-i})-u_i(a_i,a_{-i})=\ \alpha_i\left[V(b_i,a_{-i})-V(a_i,a_{-i})\right]$
Ordinal (OPG)	$u_i(b_i,a_{-i})-u_i(a_i,a_{-i})>0 \Leftrightarrow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

Co
147 M
Lynchbur
n
ess.com

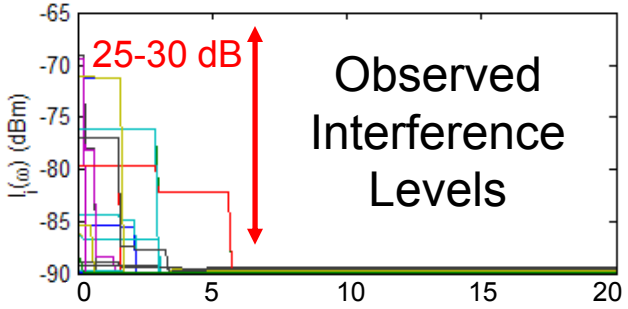
Example behavior

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

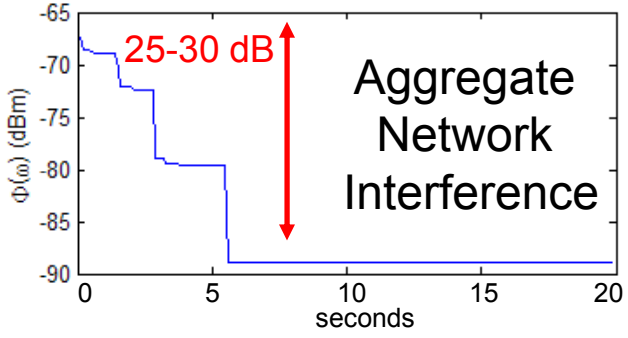
1. All self-interested adaptations
   - Scalable resource utilization
   - No synchronization required



2. Based only on observations of own performance
   - No information exchange overhead
   - More responsive network



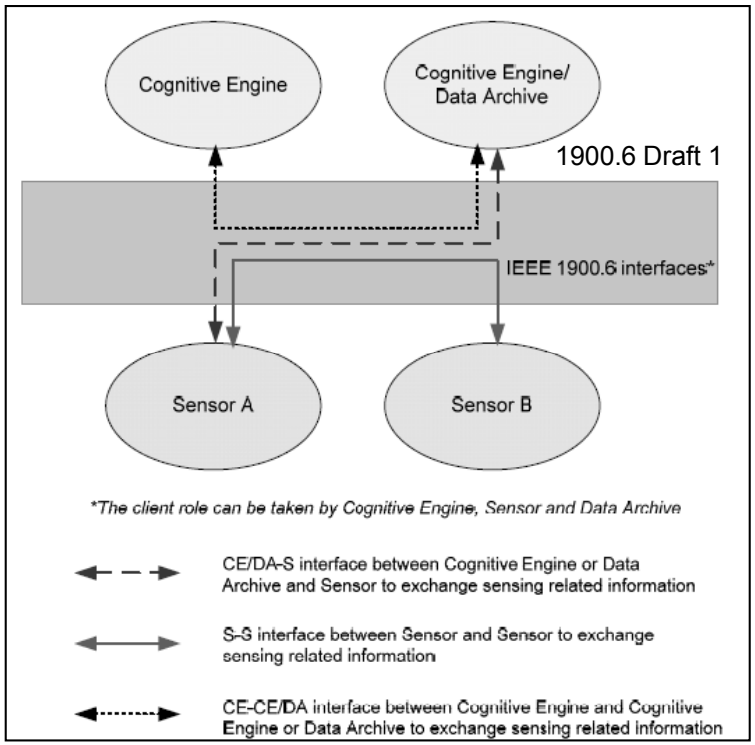
3. Decrease aggregate network interference
   - Self-stable
   - Converges to local-optima



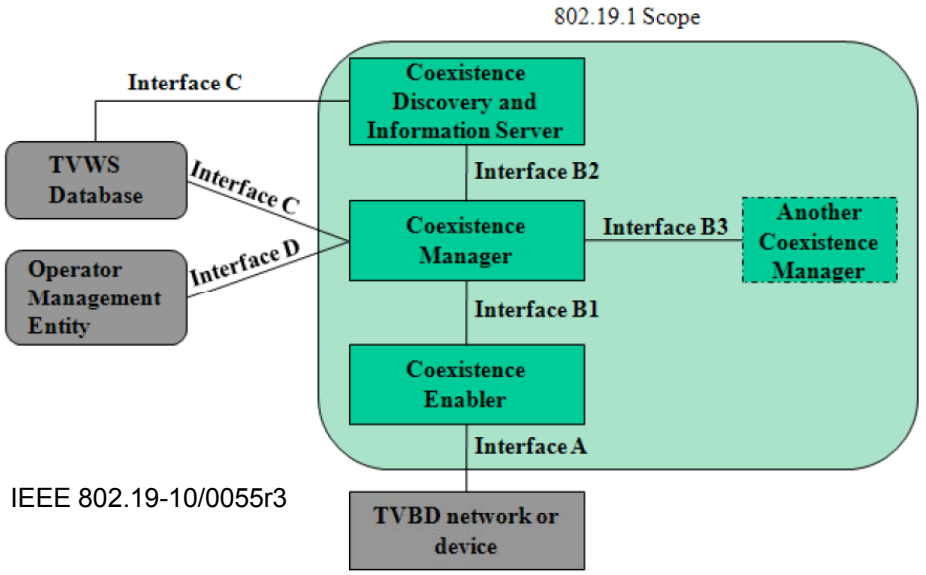
Cogn
147 Mill
Lynchburg, VA 24502
com
12
Email: info@cntwireless.com

No network is an island

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



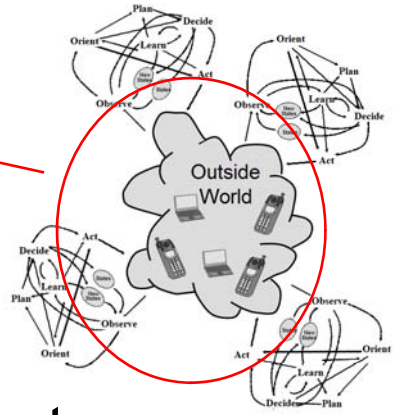
- Decisions impact one another
  - Etiquette
- Coordinate quiet periods
  - Common time base, scheduling
- Share information
  - Sensing
- Merging?



IEEE 802.19-10/0055r3

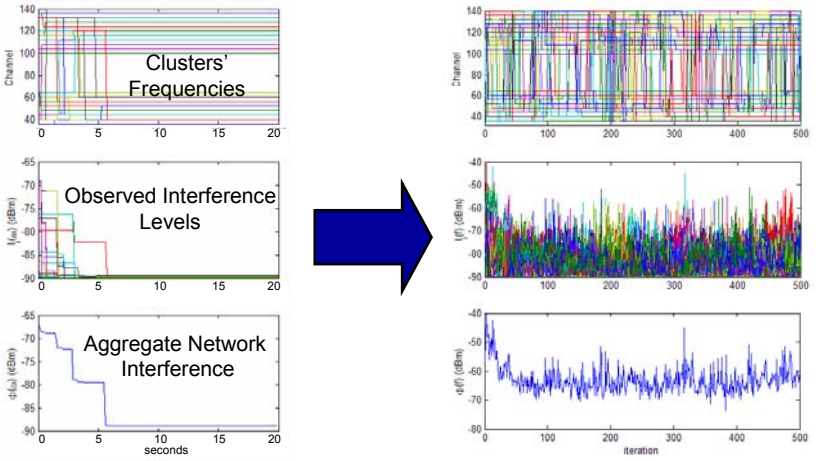
Hostile users can create problems from outside your network

What if the environment is “unstable”?



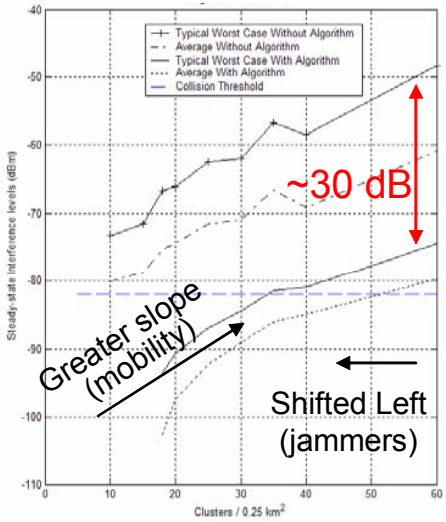
- Suppose another network is compromised in your area
- Their behavior influences your network’s adaptations

- Stability impact

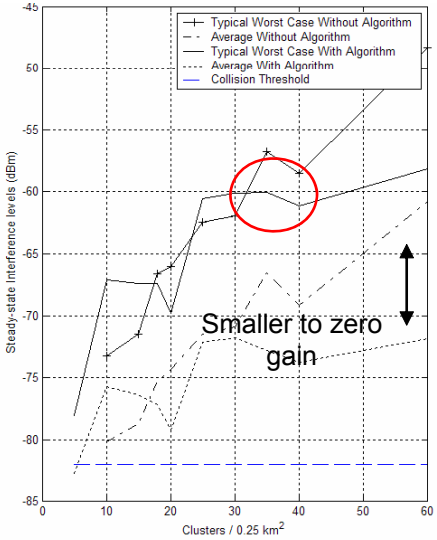


- Performance Impact

Fixed Interferer (Mobile)



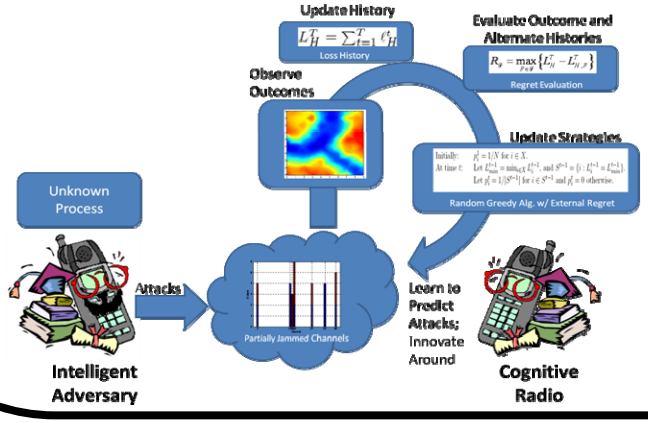
Adaptive Interferer (Mobile)



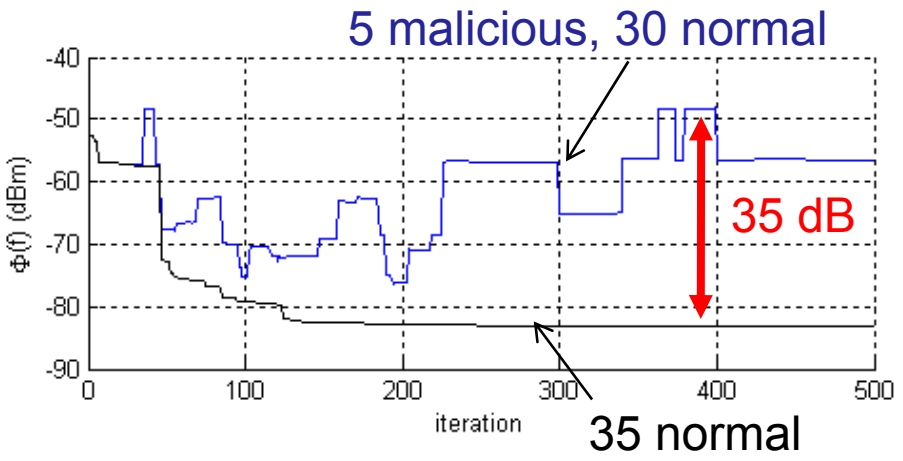
- Need to consider external actors
  - Detect unexpected behavior, adjust accordingly

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



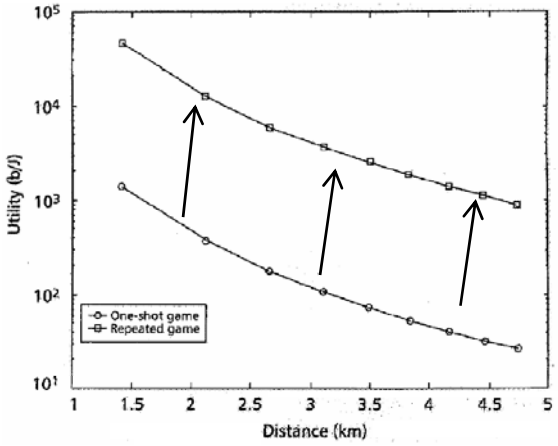
- Adapt at inopportune times
- Simply minimize performance
- Ensure marginally stable network goes unstable
- Plus learning exploits
  - And spoofing
    - And information corruption

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

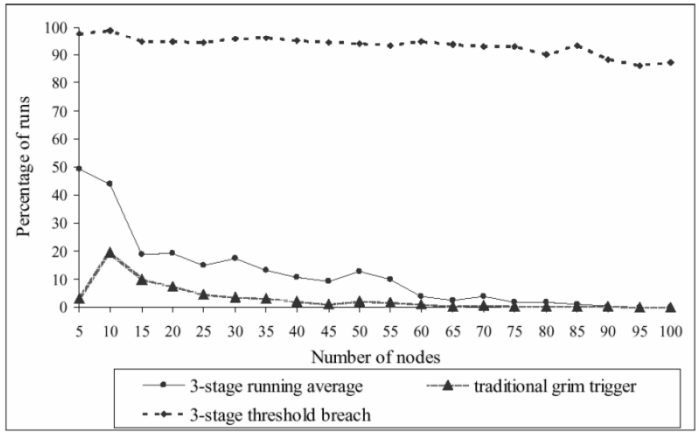
Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

Malicious != 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]

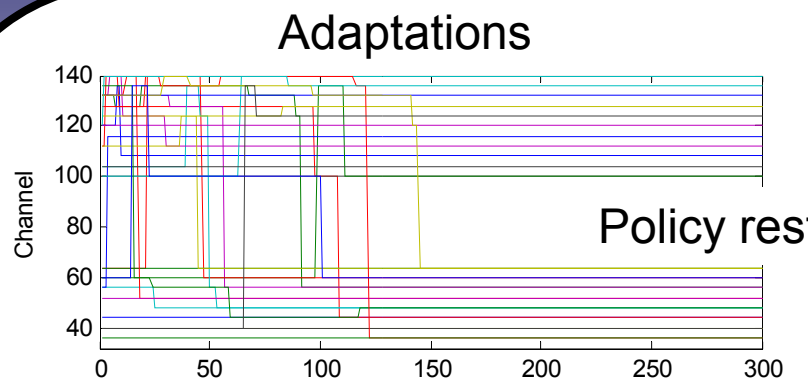


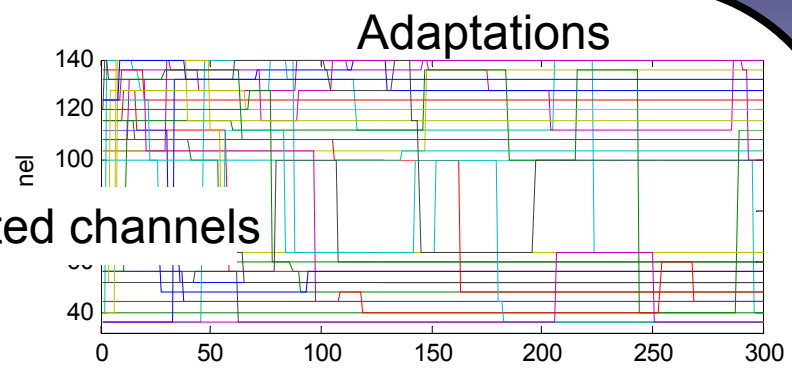
From [Srivastava_06]

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

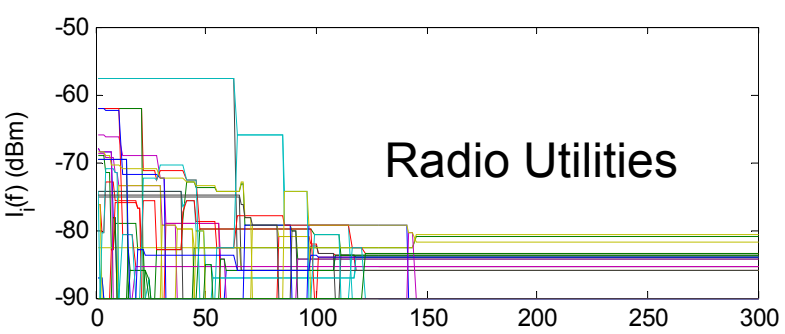
Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

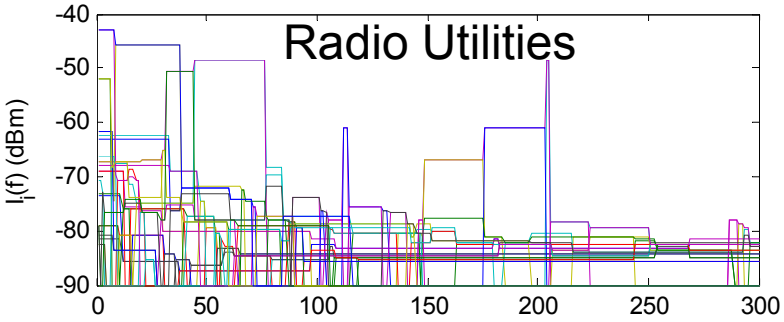
Detecting aberrant behavior from predictable emergent properties

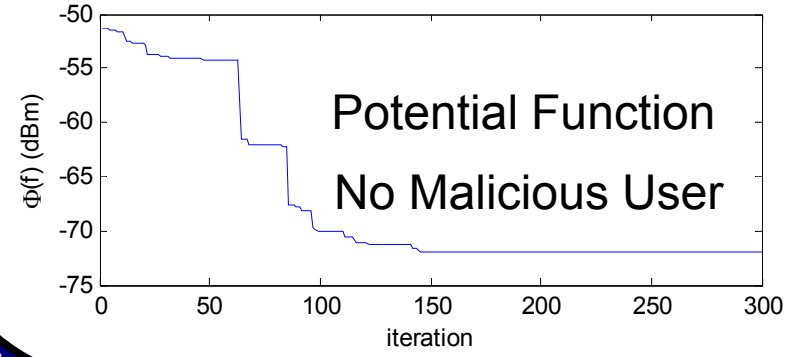


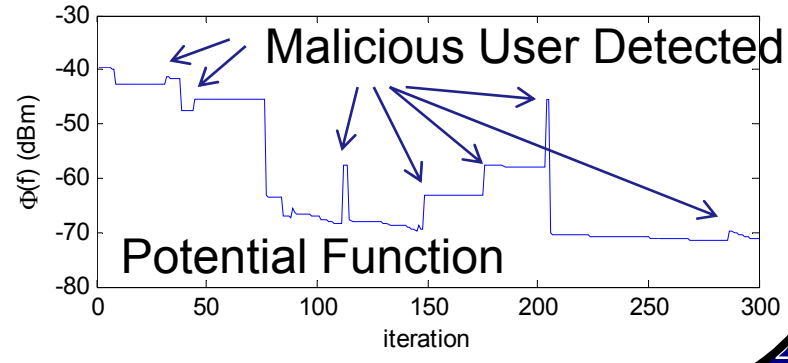


Policy restricted channels



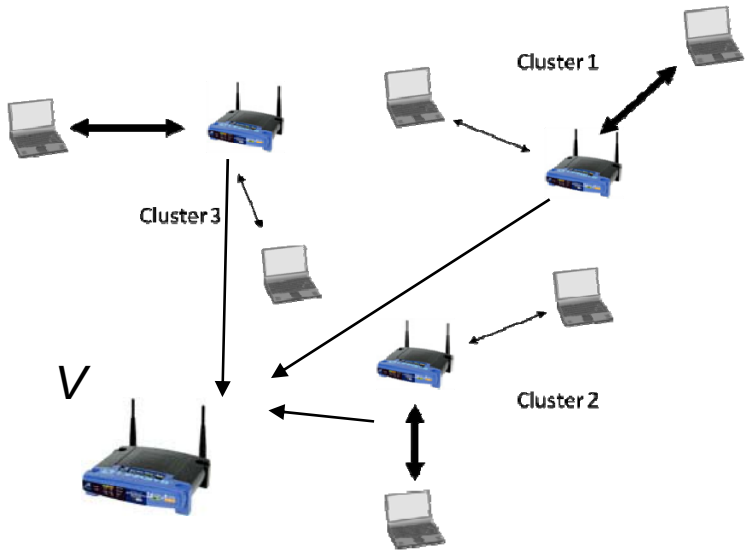






Implementation Discussion

- 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



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

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

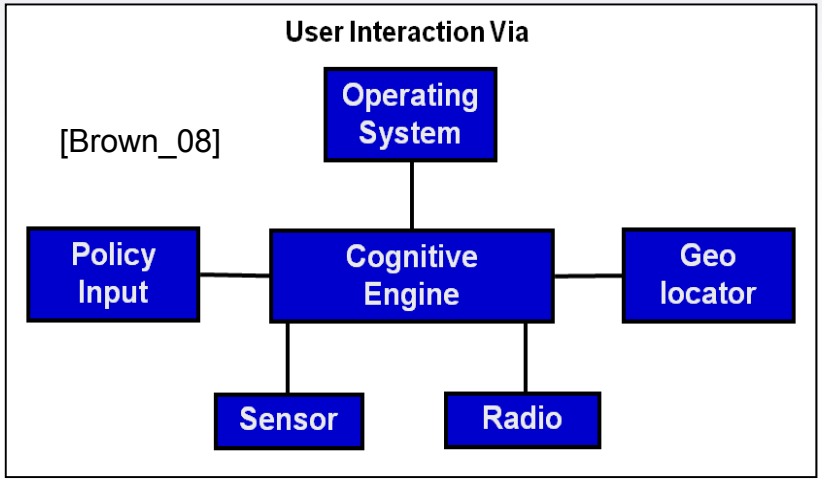
Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

Security Issues

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

Attacker …	Bea-con	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]

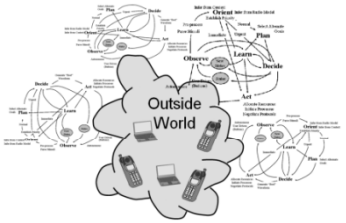


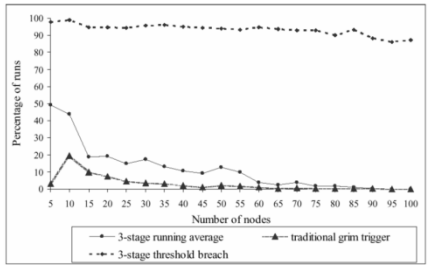
Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

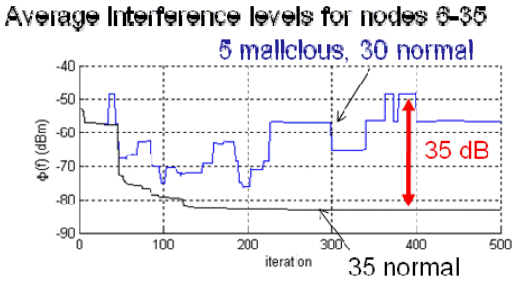
Web: www.crtwireless.com
Ph: (540) 230-6012
Email: info@crtwireless.com

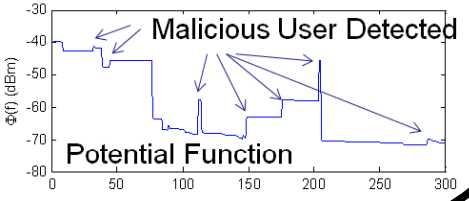
Questions you should address before fielding your network

- 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?









crtwireless.com/files/CRT_SMI_2010.pdf

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

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

Security References

- [Bian_08] K. Bian, J. Park, "Security Vulnerabilities in IEEE 802.22," *ACM International Conference on Wireless Internet*, Session: Cognitive Radio Networks, Article 9.
- [Bian_09] K. Bian, J. Park, R. Chen, "A quorum-based framework for establishing control channels for dynamic spectrum access networks," *International Conference on Mobile computing and networking,* Beijing, China, pp. 25-36, 2009.
- [Brown_08] T. Brown, "Threat Assessment to Primary and Secondary Users in a Centralized Cognitive Radio Network," *802.22-08/0217r0*, July 2008.
- [Chen_08a] R. Chen, J. Park, T. Hou, J. Reed, "Toward Secure Distributed Spectrum Sensing in Cognitive Radio Networks," *IEEE Communications Magazine*, April 2008, vol. 46, issue 4, pp. 50-55.
- [Chen_08b] R. Chen, J. Park, & J. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE Journal on Selected Areas in Communications*, vol. 26, no. 1, Jan. 2008.
- [Clancy_08], . Clancy, N. Goergen, "Security in Cognitive Radio Networks: Threats and Mitigation," *Int'l Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom)*, May 2008.
- [Google_10] R. Witt, M. Stull, "Proposal by Google Inc. to Provide a TV Band Device Database Management Solution," January 4, 2010. Available online: http://www.scribd.com/doc/24784912/01-04-10-Google-White-Spaces-Database-Proposal
- [Newman_09] T. Newman, T. Clancy, "Security Threats to Cognitive Radio Signal Classifiers," *Wireless @ Virginia Tech Symposium*, June 2009.
- [SDRF_ITU_08] SDRF-08-R-0010-V0.5.0, "Input to ITU-R WP5A on Cognitive Radio Systems," September 2, 2008.
- [Telcordia_10] J. Malyar, "Comments of Telcordia Technologies: Proposal Seeking to Be Designated as a TV Band Device Database Manager," January 4, 2010. Available online: http://fjallfoss.fcc.gov/ecfs/document/view?id=7020355227
- [Thomas_09] R. Thomas and B. Borghetti, "IA Implications for Software Defined Radio, Cognitive Radio and Networks," *IAnewsletter* Vol. 12 No 1 Spring 2009. Available online: http://iac.dtic.mil/iatac
- [Ward_08] R. Ward, "Innovation: Interference Heads Up," *GPS World*, June 1, 2008. Available online: http://www.gpsworld.com/gnss-system/receiver-design/innovation-interference-heads-up-4240
- [Zhang_08] Y. Zhan, G. Xu, X. Geng, "Security Threats in Cognitive Radio Networks," *High Performance Computing and Communications 2008*, pp. 1036-1041, September 25-27, 2008.

Cognitive Radio Technologies
147 Mill Ridge Rd, Ste 119
Lynchburg, VA 24502

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