White Space Security: Securing our Spectral Resources

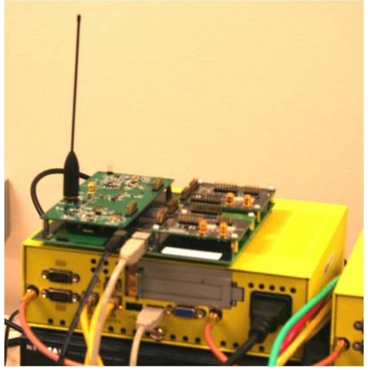
Wade Trappe

Setting the Stage

- Currently, 90% of licensed spectrum is unutilized
  - The FCC has opened up large chunks of spectrum in the 300MHz to 400MHz band for unlicensed use
  - National Broadband Plan: To open up 500 MHz in next 10 years
- Companies are testing products that will use unlicensed wireless spectrum (white spaces) that sit between broadcast TV channels.
  - Cognitive radio platforms and protocols will allow secondary users to opportunistically take advantage of spectrum opportunities for communication
- These new TVBD (TV Band Devices) must adhere to FCC Part 15 Rules:
  - No real limitations on type of applications being deployed
  - Minimal provisions by FCC to limit interference between TVBDs
  - Rules regarding TVBDs interference to Primary devices
    - *E.g. 40mWatt limitation if operating in bands adjacent to TV channels*
  - Officially, certain classes of TVBDs must utilize fixed outdoor antennas

Cognitive Radios are an emerging wireless technology supported by open-source-style of development

- Expose the lower-layers of the protocol stack to researchers, developers and the "public"
  - scan the available spectrum
  - select from a wide range of operating frequencies
  - adjust modulation waveforms
  - perform adaptive resource allocation



- Inexpensive and widely available cognitive radios:
  - USRP/GnuRadio – open source software support
  - Xilinx-based Rice platform
  - WINLAB WINC2R cognitive radio platform
  - JTRS Clusters (well, not necessarily widely available…)
- An ideal platform for *abuse* since the lowest layers of the wireless protocol stack are accessible to programmers.
  - Can be reprogrammed to violate or bypass locally fair spectrum policies

The CR platform is ripe for abuse, and could potentially cause more harm than benefit

There are many opportunities for exploitation:

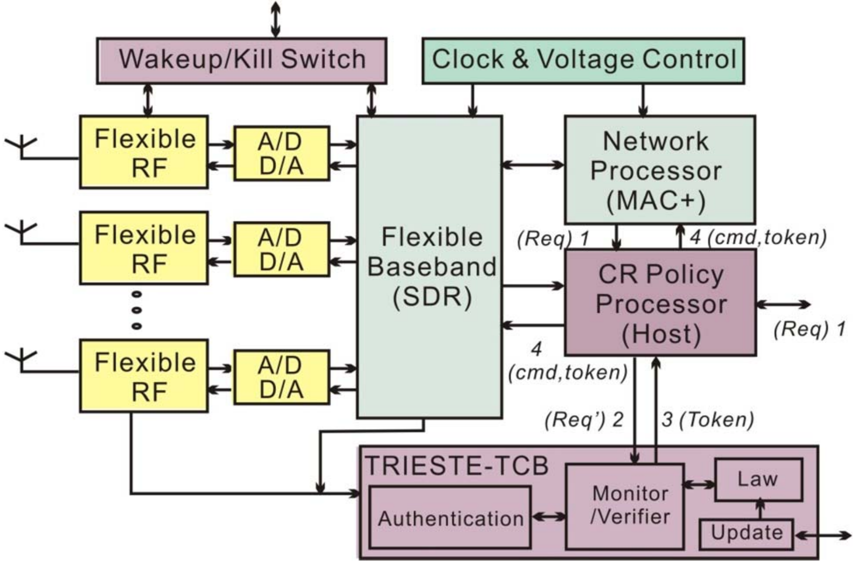
1. Poor programming:
   1. CR protocols will be complex, it will be easy to write buggy implementations of etiquettes that do not achieve their goal…
   2. Runaway software processes…
2. Greedy exploitation:
   1. Decrease back-off window in an 802.11 (or comparable) implementation
   2. Ignore fairness in spectrum etiquette (many co-existence protocols assume honest participants, or honest data)
3. Simply Ignoring Etiquette
   1. Primary user returns… so-what???
4. Economic/Game-theoretic Models
   1. Standard economic models for spectrum sharing seek to support cooperation– but cooperation does not ensure trusted operation!
   2. Security is an anti-social topic!
5. Plenty more…

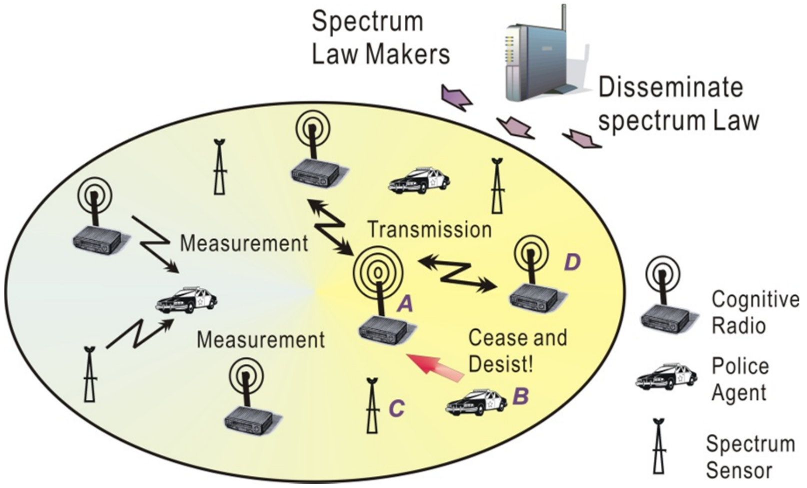
Stage is Set… Now the Rest of the Talk

- Overview of AUSTIN:
  - A framework for securing/regulating cognitive radio networks
- Anomaly Detection in DSA Networks:
  - Its not an easy matter to detect when devices are not following proper spectrum rules
- Interference Classification:
  - Are we jammers or just hidden terminals?

AUSTIN: An Initiative to Assure Software Radios have Trusted Interactions

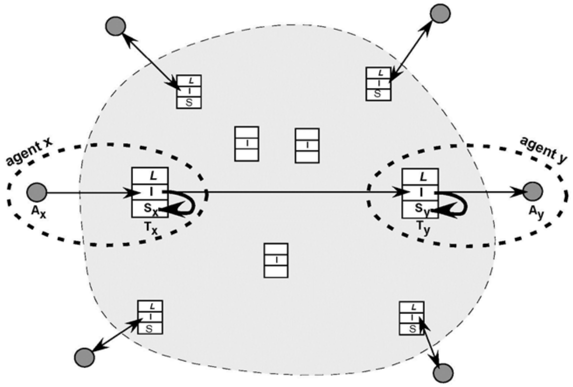
- Goal: to regulate the future radio environment, ensure trustworthy cognitive radio operation (Team: Rutgers, Virginia Tech, UMass)
- How — two complementary mechanisms
  - On-board enforcement – restrict any violation attempt from accessing the radio:
    - *Each CR runs its own suite of spectrum etiquette protocols*
    - *Onboard policy checking verifies actions occur according to “spectrum laws”*
  - An external monitoring infrastructure:
    - *Distributed Spectrum Authority (DSA) — police agent observes the radio environment*
    - *DSA will punish CRs if violations are detected via authenticated kill commands.*



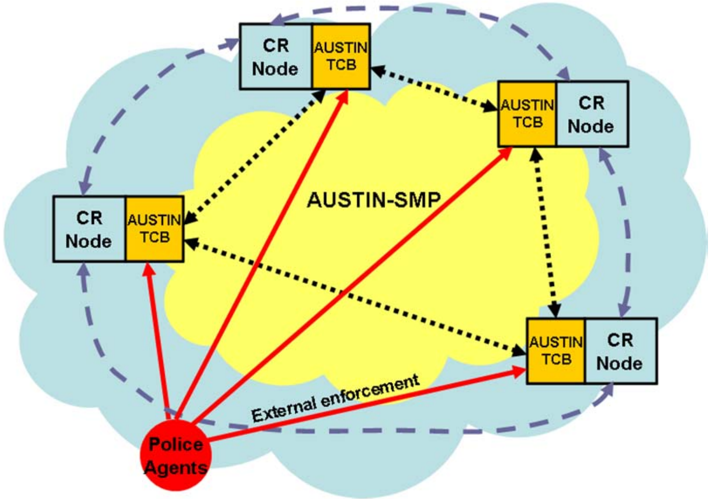


AUSTIN involves formalizing security languages for CR regulation and a security management plane

- AUSTIN will use *law-governed interaction* (*LGI*), which is more powerful than conventional access control in both expressive power and scalability.
  - LGI employs *locality*, which supports decentralization of access control, and scalability for stateful regulation
  - LGI can achieve global effects over a community because all members of that community are subject to the same law
- A broad and expressive regulatory language will be designed
  - XGPL is a starting point, but does not involve policy enforcement
  - AUSTIN-XGPL will use a concrete representation of past behaviors to allow a detailed evaluation for regulation.
  - AUSTIN-XGPL challenges:
    - *Make the language support variable degrees of interoperability between federations of CR devices.*
    - *Make the language powerful, yet simple enough to minimize the risk of a poorly-written/buggy law*
- AUSTIN Credo: Security must be “designed into” all future CR devices (e.g. an FCC-imposed requirement)
  - All CR devices will have a mandatory trusted computing component that includes a well-architected Security Management Plane (SMP)
  - RF units immediately partition incoming signals to extract SMP communications and relay these to a trusted module on the CR
  - AUSTIN-SMP will be driven by associated Security Management Agents (SMA)
  - Security Message Units (SMUs) will support multiple regulation services via a unified packet format.
  - AUSTIN-SMP provides an exciting approach to more provably secure protocols, as well as improved network manageability



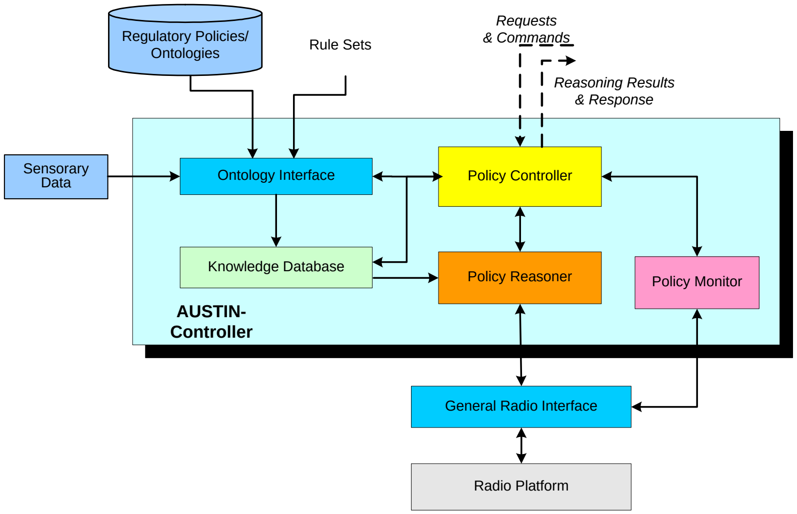
LGI-based Interaction



AUSTIN-SMP Architecture

Secure software and hardware methods prevent corruption of CR software, while the AUSTIN-Controller regulates actions

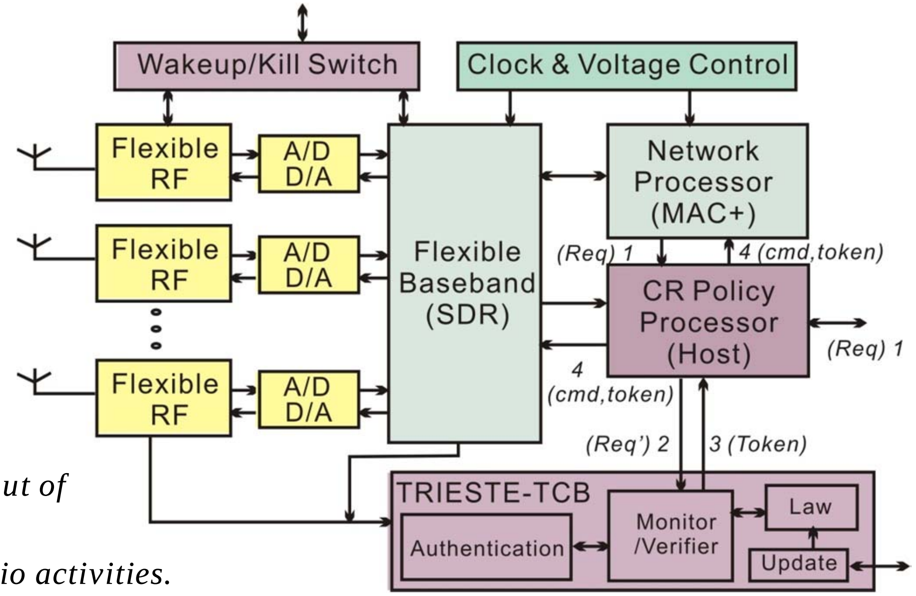
- Ensuring the security of radio software involves
  - Ensuring that the radio software components come from authorized entities
  - Assuring that the download and installation processes are secure
  - Thwarting the unauthorized modification of the software once it has been installed.
- Hardware security mechanisms should provide a root-of-trust and thus must be tamper-proof
  - Bitstream encryption prevents the configuration from being revealed outside the chip
  - Unlike ASICS, FPGAs reveal no design information when powered off, forcing the adversary to probe an active die.
  - AUSTIN will investigate the enforcement of basic operational policies using hardware-layer "interlocks" that cannot be overridden by software layers. Will require:
    - *Analyzing the interfaces and dependencies between hardware and software*
    - *Selecting the policies to be enforced with hardware*
    - *Formal state analysis of the hardware blocks responsible for policy enforcement*
    - *A mechanism for securely updating policy enforcement circuits.*



- The AUSTIN-Controller is a policy engine that receives requests from CR processes, and makes formal decisions on whether to allow requested actions to occur
- AUSTIN-Controller involves:
  - *Ontology Interface*
  - *Knowledge Database*
  - *Policy Reasoner*
  - *Policy Controller*
  - *Policy Monitor*

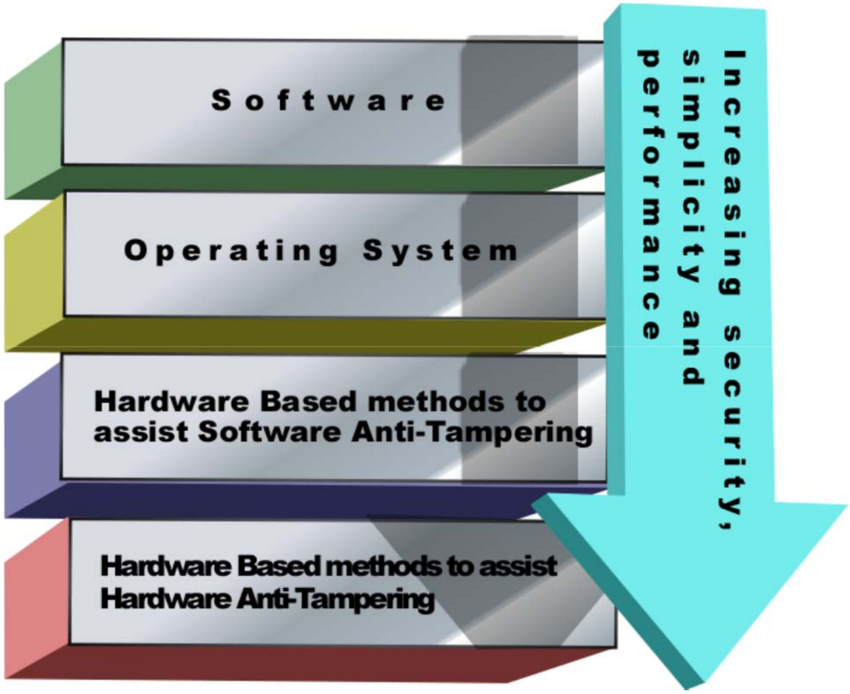
Challenge Topic: The AUSTIN-TCB needs to process and regulate activities internally quickly

- What is the AUSTIN-TCB (Trusted Computing Base)
  - A virtual block includes all the hardware and software that enforces universal laws and etiquette policies
  - A controlled gate that users have to go through to access radio
- Components:
  - ***CR processor*:** programmable by the User; performs request filtering based on user defined spectrum etiquette policies
  - ***Monitor/Verifier:*** a *Controller* which can interpret and enforce any well-formed *Law*. Verify user's radio access request, monitor the on-board radio activity.
  - ***Wake up/Kill Switch***:
    - *"wakeup": brings the baseband processor out of a deep (low power) sleep.*
    - *"kill": stops the corresponding ongoing radio activities.*
  - ***Update:*** allows the laws evolve over time, accepts a new law only if it is signed by the regulating authority,

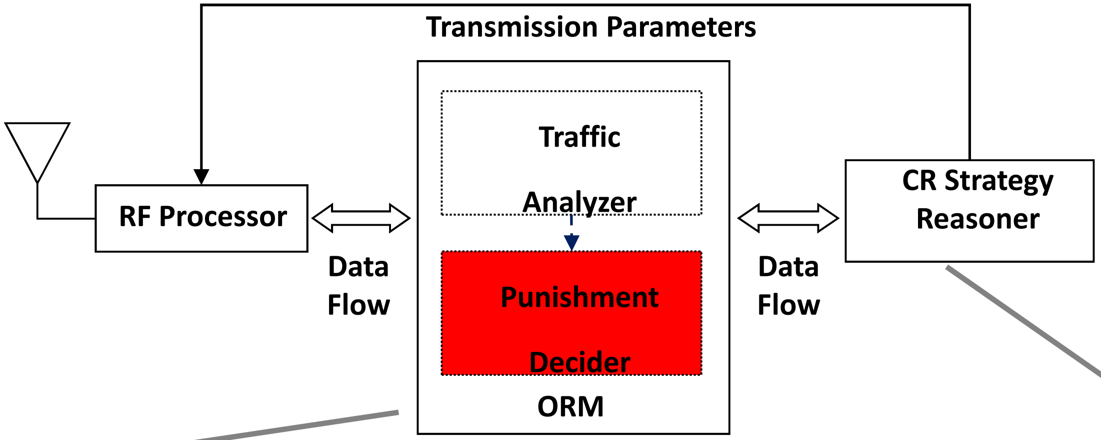


Challenge Topic: Hardware security is needed in order to provide a trusted base

- Must consider physical attacks on an embedded system such as a radio handset
  - Applications and OS ultimately have a hardware-based root of trust
  - Security assumptions made by software may not hold when the hardware can be probed
  - PC Trusted Platform Module (TPM) chips focus on software rather than hardware attacks
- Single-chip and system-in-package integration increases the difficulty of a physical attack
  - Also reduces size / cost / power, and fewer packages need to be tamper resistant
  - FPGAs can integrate a 500 MHz RISC processor core
  - Configuration files remain encrypted outside the FPGA die
  - Dynamic self-reconfiguration thwarts static die probes
- Direct hardware implementation of functions
  - Avoids memory sharing and trust in upper (OS and software) layers
  - Allows interlocks that cannot be overridden by software

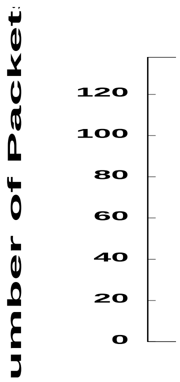


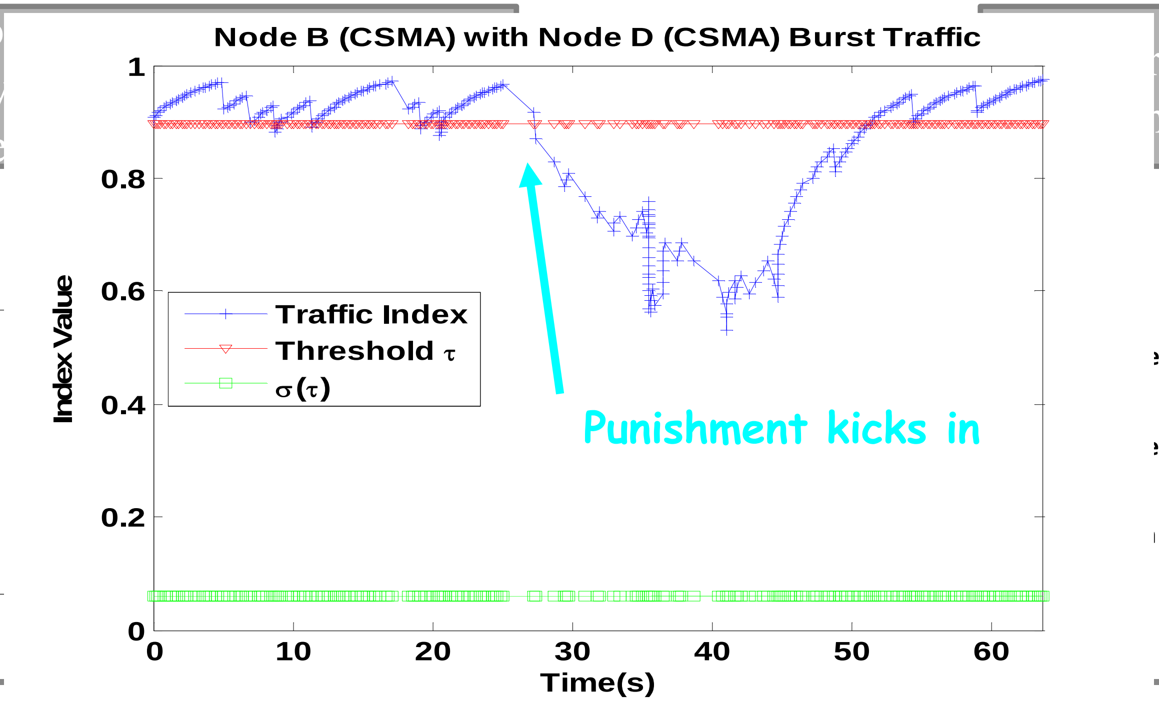
Challenge Topic: Implementing AUSTIN regulator on the USRP involves deciding analyzing MACs used and punishing

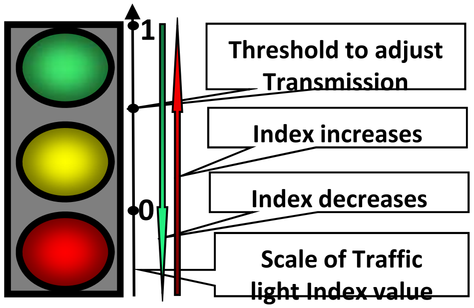


Onb
analy
whethe

ategy Reasoner chooses
nsmission parameters







RUTGERS

WINLAB

Anomaly Detection in DSA Networks

Case Study: Anomaly Detection in DSA Networks

- Openness of the Lower-layer Protocol in Cognitive Radio
  - A flexible solution to dynamic spectrum access (DSA)
  - Target for adversaries and susceptible to reckless users

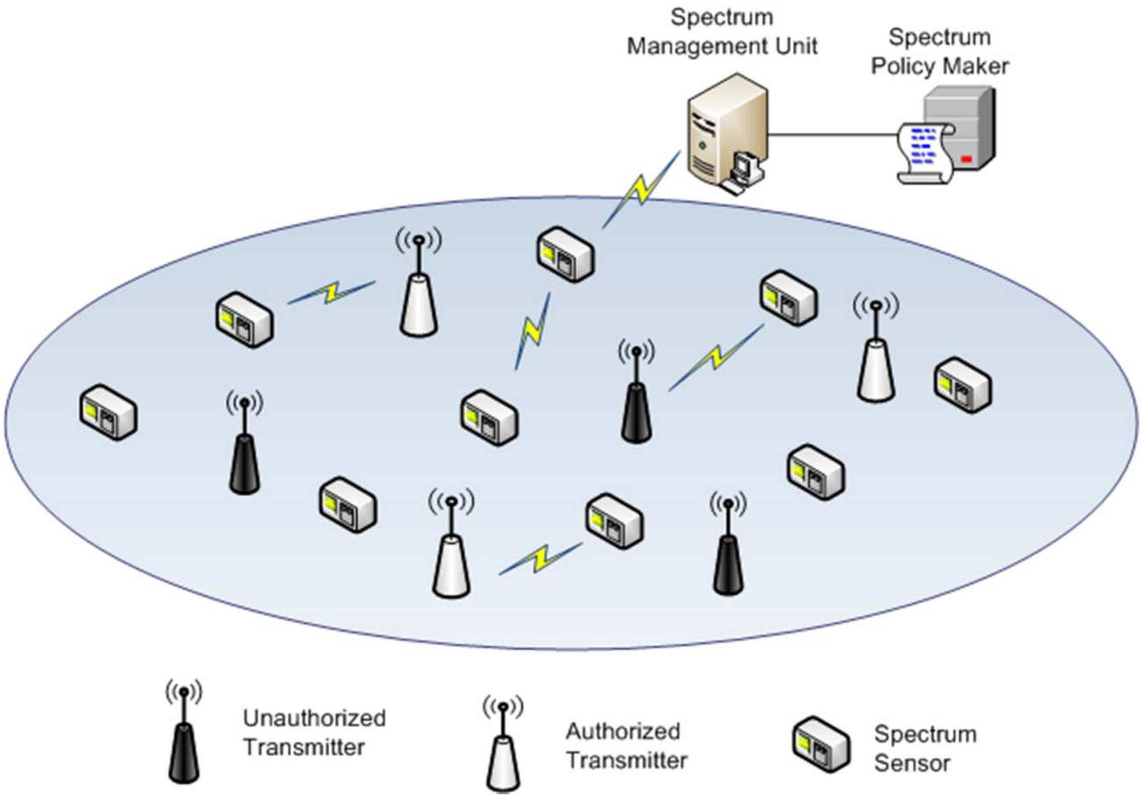
- Spectrum etiquette enforcement is critical to effectiveness and correctness of a DSA system
  - Detection
  - Localization
  - Elimination
- Network anomaly – unauthorized spectrum usage that can cause interference

Detection of Unauthorized Radios

- Distinguishing bad (unauthorized) transmissions from good (authorized) ones
  - **Challenge**: Conventional signal processing techniques are insufficient
    - ❑ *Heterogeneous communication modes*
    - ❑ *Spoofing attack by emulating primary users*
  - **Goal**: Effective detection mechanism relying on non-programmable features
    - ❑ *Propagation law – inherent property of channel*
    - ❑ *Signal strength based detection using energy detector*

DSA Network Structure

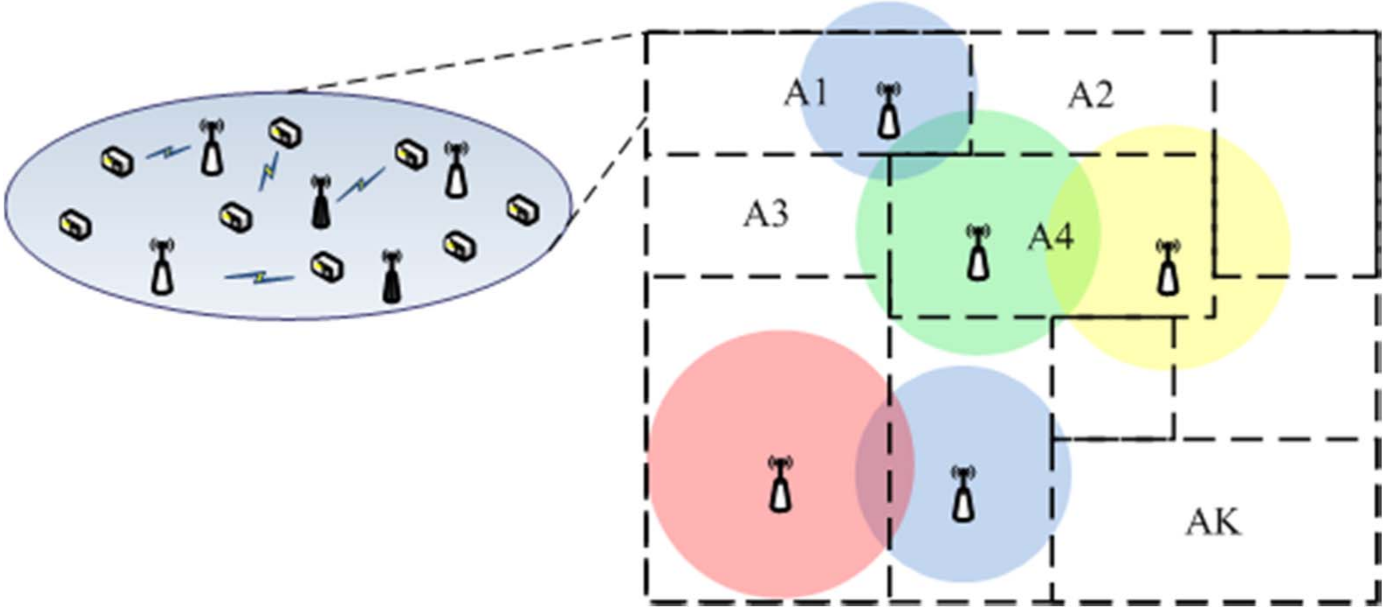
- Centralized Management
  - Making and distributing spectrum access policy
  - Collecting spatially distributed power measurements



DSA Network Structure (cont'd)

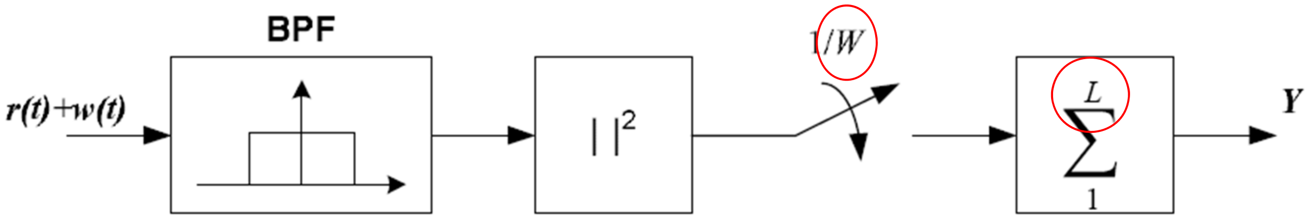
- **Zone-based** Network Structure
- Spectrum Dedicated to Authorized Users
  - Different spectrum bands in adjacent zones and in the same zone
- Spectrum Policy

  "User U_m is allowed to use frequency band W_i from time T_1 to T_2, as long as the power levels do not go above P dBm in zone A_k".



Energy Detection Model

- An energy detector



  - W: bandwidth of bandpass filter (BPF)
  - L: energy samples in each measurement

- Output at the *n*-th spectrum sensor:

$$y_n = \sum_{l=1}^{L} |r_n(l) + w_n(l)|^2$$

complex received si

complex Gaussian noise

  - Approx
    asymp
  - Energy measurements (in dB) across all sensors are jointly Gaussian distributed

Anomalous Detection Using Significance Testing

- Statistics of energy measurement are only given under the *normal condition*

$$H_0 : r(t) + w(t), \qquad \text{normal usage}$$

$$H_1 : r(t) + x(t) + w(t), \quad \text{anomalous usage}$$

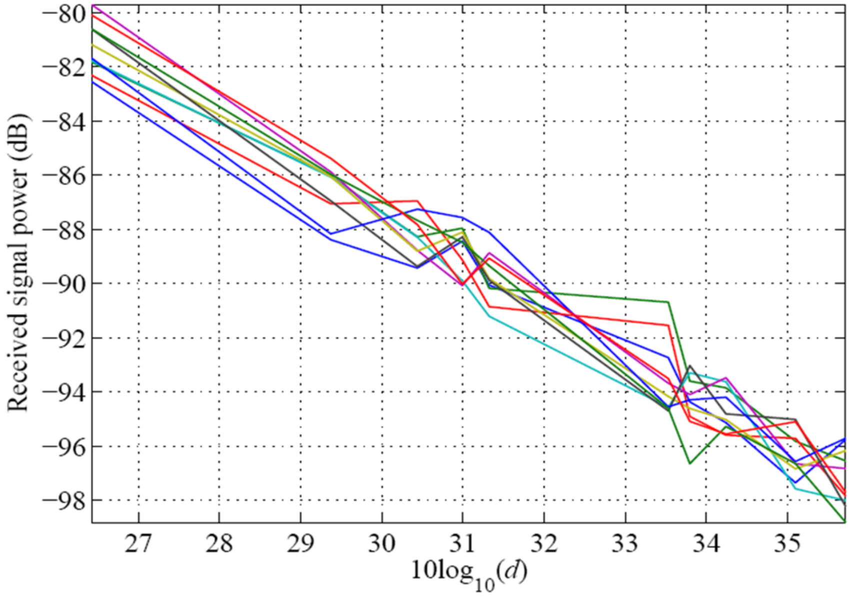
  - $r(t)$: authorized signal
  - $x(t)$: ***unknown*** unauthorized signal
  - $w(t)$: AWGN

- Significance Testing
  - Test statistic $\mathbf{T}$: a measure of observed data
  - Acceptance Region Ω: we accept the null hypothesis if $\mathbf{T} \in \Omega$
  - Significance level α : probability of false alarm

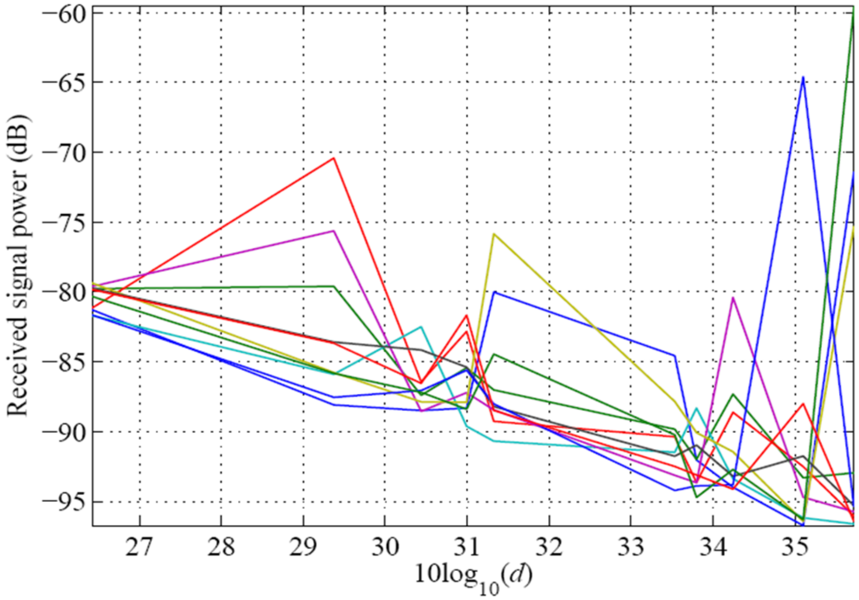
$$Prob(\mathbf{T} \notin \Omega | \mathcal{H}_0) \leq \alpha$$

When Authorized Transmitter is Mobile

- A channel is dedicated to a single authorized user
  - Distinguishing between single and multiple transmissions in the same channel
  - A decision statistic that captures the characteristics of the received power in the normal case
- Lognormal model: $Y_n = Y_0 - 10\gamma \log_{10}(d_n/d_0) + Y_{R,n}$



(a) $\mathcal{H}_0$



(b) $\mathcal{H}_1$

Linearity-Check-for-Mobile Transmitter (LCM)

- **Linear estimation** of the received energy $\mathbf{Y} = (Y_1, Y_2, \ldots, Y_N)^T$

$$\hat{\mathbf{Y}} = (\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T\mathbf{Y}, \qquad \mathbf{A} = \begin{bmatrix} 1 & -10\log_{10}(d_1/d_0) \\ \vdots & \vdots \\ 1 & -10\log_{10}(d_N/d_0) \end{bmatrix}$$

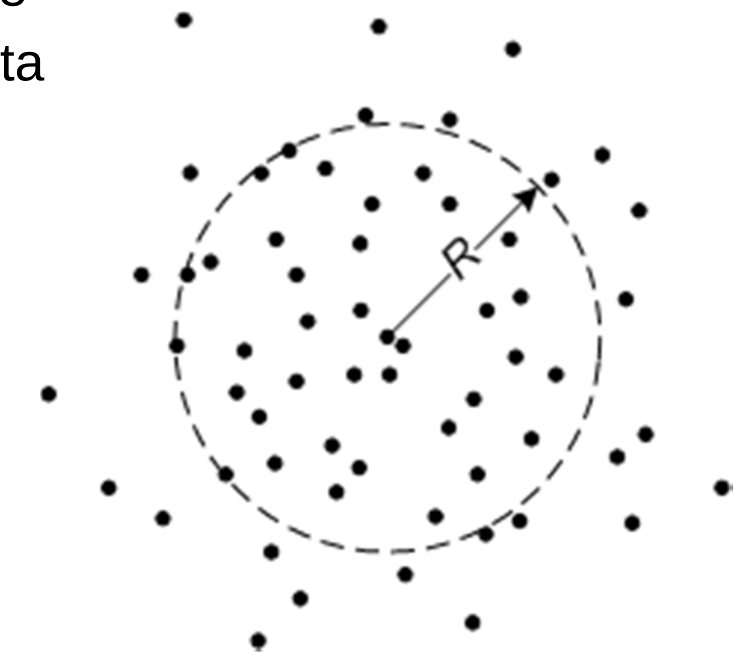
- Estimation error is **independent** of the transmission power

$$\hat{\mathbf{e}} = \mathbf{Y} - \hat{\mathbf{Y}} = (\mathbf{I} - \mathbf{A}(\mathbf{A}^T\mathbf{A})^{-1}\mathbf{A}^T)\mathbf{Y}_R$$

- Given the location of the authorized transmitter, the error is **Gaussian** distributed, $\hat{\mathbf{e}} \sim \mathcal{N}(0, \Sigma_e)$
- Acceptance region: $\Omega = \{\hat{\mathbf{e}} : \hat{\mathbf{e}}^T\mathbf{\Sigma}_e^{-1}\hat{\mathbf{e}} < T_{\hat{e}}\}$
- False alarm rate: $P_F = \dfrac{\Gamma((N-2)/2, T_e/2)}{\Gamma((N-2)/2)}$

One-class Support Vector Machine (SVM)

- If the location of the authorized transmitter is unknown, the distribution of the estimation error is ***unknown***
  - The transmitter location is estimated by localization methods
- We give ***empirical*** acceptance region using machine learning technique, One-class SVM [Scholkopf'01]
  - Minimizing the radius R of a hypersphere that encloses a subset of the training data
  - Given the training data are all from the normal case H_0, the fraction of the excluded data asymptotically equals the false alarm probability
  - In LCM, the input statistic is the error vector, $\hat{\mathrm{e}} = \mathbf{Y} - \hat{\mathbf{Y}}$

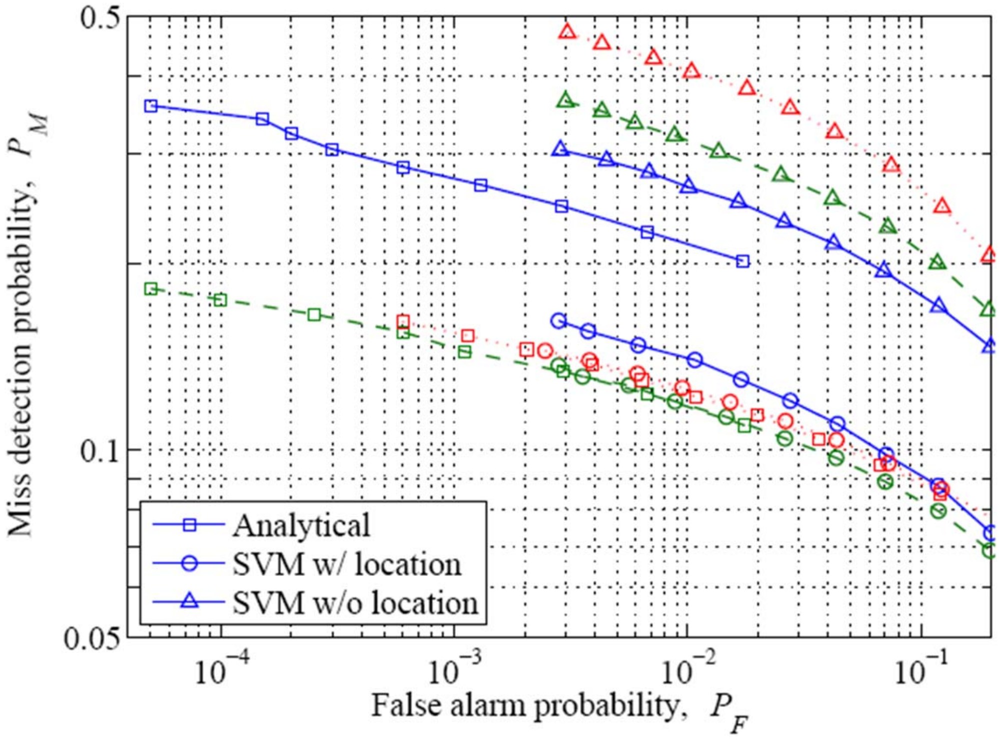


Signalprint-Check-for-Stationary-Transmitter (SCS)

- Y_n : *known* authorized signal energy
- $\tilde{Y}_n$: current measured energy
- Residue: $$\hat{e}_n = \tilde{Y}_n - Y - \hat{C}, \qquad \hat{C} = \frac{1}{N}\sum_{n=1}^{N}(\tilde{Y}_n - Y_n)$$
- The residue vector, $\hat{\mathbf{e}} = [\hat{e}_1, \ldots, \hat{e}_N]$, is a ***multivariate Gaussian***
- False alarm rate: $$P_F = \frac{\Gamma((N-1)/2, T_e/2)}{\Gamma((N-1)/2)}$$
- SVM based empirical solution uses the residue, $\hat{\mathbf{e}}$, as the input statistics.

Detection Performance -- LCM

- Complementary receiver operating curves, $P_F = [0.002, 0.2]$



- *N* = 50 sensors randomly distributed in a square area
- One authorized transmitter and one unauthorized transmitter are randomly located
- γ = 3.5; σ = 4 dB
- solid: SNR_{med} = 0 dB

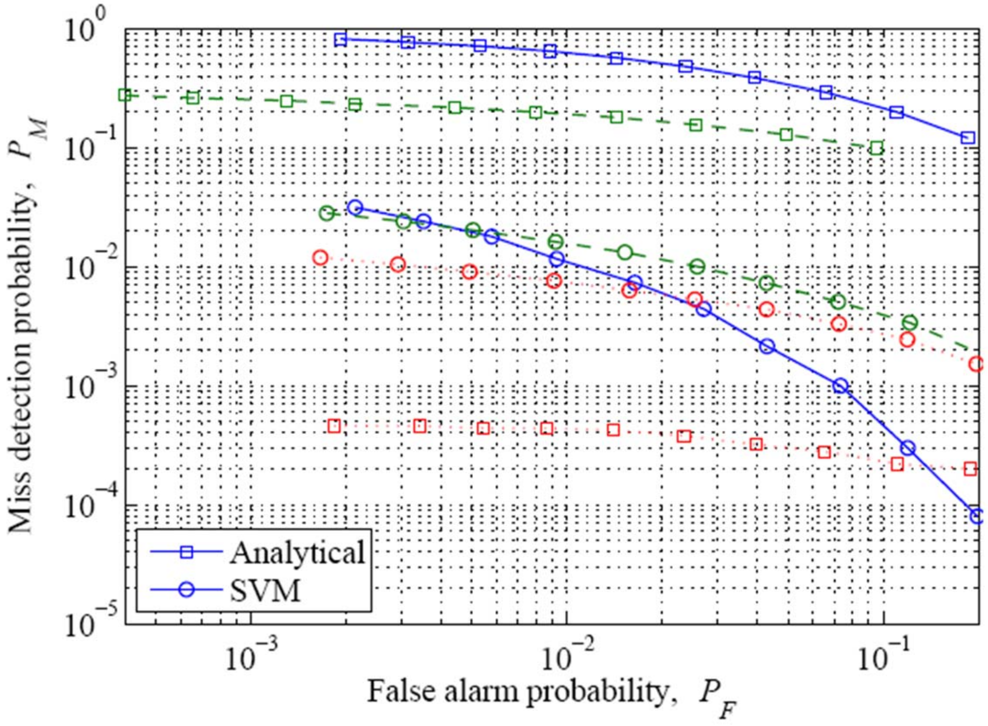
  dash: SNR_{med} = 10 dB

  dotted: SNR_{med} = 20 dB

- Analytical solution is accurate only for large SNR (SNR_{med} > 20 dB).
- Given the authorized Tx location, SVM and analytical solution have similar performance.
- Given authorized TX location, $P_D > 0.9$ for $P_F = 0.1$.

Detection Performance -- SCS

- Complementary receiver operating curves, $P_F = [0.002, 0.2]$



- N = 10 sensors randomly distributed in a square area
- γ = 3.5
- solid: SNR_{med} = -20 dB

  dash: SNR_{med} = 0 dB

  dotted: SNR_{med} = 20 dB

- Analytical solution is accurate for very high and very low SNR (i.e., $|SNR_{med}| > 20$ dB).
- SVM solution is more stable with respect to SNR
- Far superior to LCM thanks to the more stable metric – signalprints.

Summary

- For a single unauthorized transmitter and large SNR, both methods achieve $P_D > 0.9$ with $P_F = 0.1$.
- The detection probabilities are even higher when there are multiple unauthorized radios.
- SCS is far superior to LCM, thanks to the more reliable metric based on *signalprint*.
- Analytical solutions are accurate only when the asymptotic assumptions are met.
- LCM is significantly degraded by highly random channel fading (i.e., large σ) while SCS is independent of fading.
- SCS is sensitive to noise. Long measurement duration helps smooth the noise and improve its detection accuracy.

Interference Classification: Jamming or Hidden Terminal?

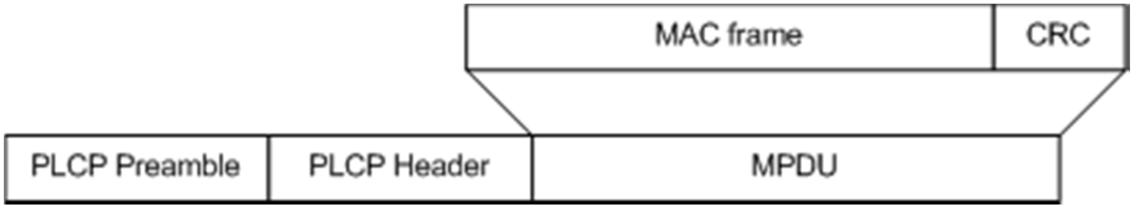
Interference Classification

- Consider a CSMA (e.g. 802.11) based MANET/Mesh

  - When a packet is received with errors, is it due to unintentional interference, malicious jamming, or just poor link quality with a low SNR?
  - When an expected ACK is missing, is the data packet lost at the receiver or the ACK is corrupted at the sender?

Terminology

- **Sender**: the node who is going to send a data packet and then to wait for an ACK.
- **Receiver**: the node who is going to receive a data packet and then to send an ACK.
- **Busy:** the channel is busy if a node detects any energy above the hardware set energy detection threshold. (CCA Mode 1).
- **Receive state**: a node enters the receive state after the PLCP header reception is successful.



Interference Classification Using ACK

- **Solution:** Classify interference scenarios based on the statistics of ACK reception at the sender
- **Rationale:**
  - **More robust:** the classification can be performed at the sender without cooperation from the receiver (except for sending an ACK for every received packet).
  - **More accurate:** Sender knows when an ACK should come, receiver does not know when a transmission should come
  - **Shorter packet:** an ACK packet is usually short (i.e., 14 Byte long in 802.11) and thus is less vulnerable to interference.
  - **Fixed size:** An ACK packet has a fixed length in most MAC protocols (except for piggybacked ACK) and thus its statistics are more stable compared to variable length packets.

Interference Models from Sender's Perspective

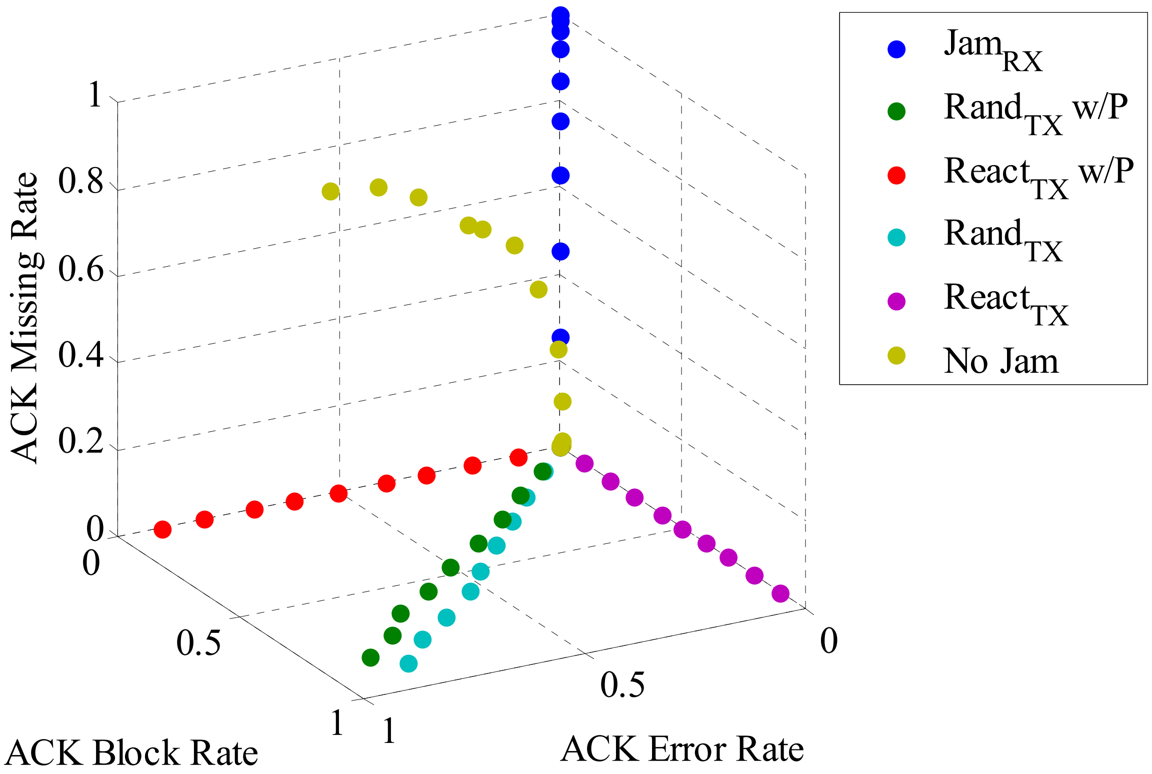
- Three basic jamming cases:
  - **Random Sender-Only Jamming:** random on-off jammer, only interfere with the ACK reception at the sender.
  - **Reactive Sender-Only Jamming:** protocol-aware ACK jammer.
  - **Receiver-Only Jamming:** any jammer that corrupts data packets at the receiver.
- **Combinations** of the three basic attacks
- **Interference-free**
  - Error occurs only when the link quality is poor, i.e., under the deep fading or large transmission distance
- **Unintentional interference**
  - Caused by non-malicious hidden terminals

Classification Metrics at Sender

- Three metrics correspond to distinct transmission anomalies.
  - **AER** (ACK Error Rate) $= N_e/(N_c + N_e)$
  - **ABR** (ACK Block Rate) $= N_{mh} / N_t$
  - **AMR** (ACK Missing Rate) $= N_{ml} / N_t$
  - N_t : the total number of transmitted packets
  - N_c : the number of correctly received ACKs
  - N_e : the number of error ACKs
  - N_{mh} : the number of missing ACKs when the channel is busy
  - N_{ml} : the number of missing ACKs when the channel is not busy
- **RSS** (Received signal strength): measured in the receive state

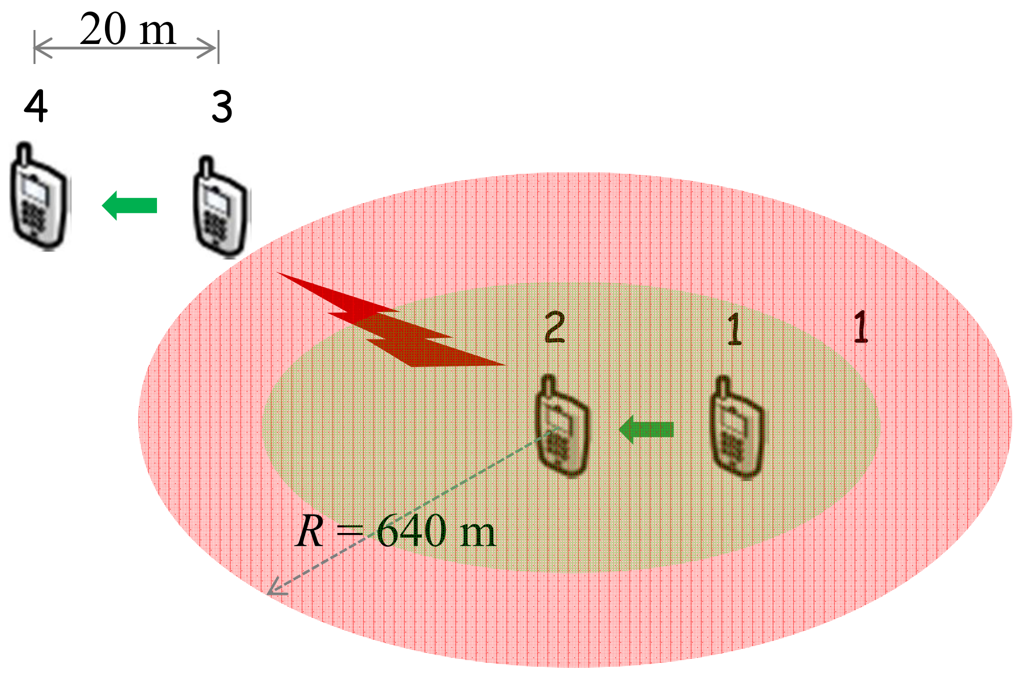
Differentiating Jamming Attacks at Sender

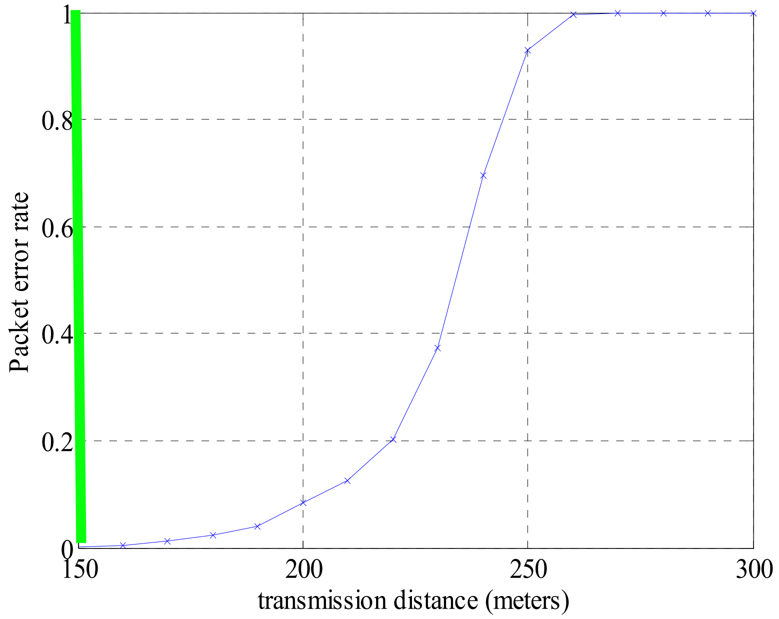
- Three basic scenarios
  - Reactive jammer corrupts ACK’s from RX→TX (React$_{TX}$)
  - Random jammer corrupts ACK’s from RX→TX (Rand$_{TX}$)
  - Any jammer corrupts Data from TX→RX (Jam$_{RX}$)



Challenge

- Normal Interference in Mobile Networks
  - Experiments in [XuK02] show RTS-CTS mechanism does not completely solve the *hidden terminal* problem, as a transmitter outside of the physical carrier sensing range can still cause interference.
  - It is equivalent to a low-power jamming attack.





AER-RSS Consistency Check

- Entire signal space consists of three regions
  - Interference-free: no hidden terminal
  - Normal interference: caused by legitimate hidden terminals
  - Intentional interference: malicious jamming
- Thresholds are empirically derived using a *support vector machine* technique, C-SVC.