Anomaly Detection in Dynamic Spectrum Access Networks

Song Liu, Yingying Chen, Wade Trappe, Larry J. Greenstein

Dec 10th, 2008
Outline

- Motivation
- Dynamic Spectrum Access Network Structure
- Anomalous Detection Using Significance Testing
- Detecting Unauthorized Signals with An Authorized Signal Present
- Summary
Motivation

- Openness of the Lower-layer Protocol in Cognitive Radio (CR)
  - 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
Detection of Unauthorized Radios

- Distinguishing bad (unauthorized) transmissions from good (authorized) ones

  - **Challenge**: Conventional signal processing techniques are insufficient
    - Heterogeneous communication modes
    - Primary User Emulation (PUE) attack [Chen’06]

  - **Goal**: Effective detection mechanism relying on non-programmable features
    - Propagation law
    - RSS based detection using energy detector
DSA Network Structure

- Centralized Management
  - Making and distributing spectrum access policy
  - Collecting spatially distributed power measurements
- **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 $A_k$.”
Anomalous Spectrum Usage

- The transmission power of an authorized user is above the specified power level. This will cause interference with users in neighboring zones;
  - Detecting Unauthorized Signals in Noise

- A transmitter is using a portion of the spectrum which is supposed to be idle. In this case, the transmitter is an unauthorized user;
  - Detecting Unauthorized Signals with an Authorized Signal Present

- A transmitter is using a portion of the spectrum that is granted to another authorized transmitter.
Anomalous Detection Using Significance Testing

- Statistics of RSS are only given under the normal condition
  \[ \mathcal{H}_0 : r(t) = s(t) + w(t), \quad \text{normal usage,} \]
  \[ \mathcal{H}_1 : r(t) = s(t) + x(t) + w(t), \quad \text{anomalous usage} \]

- \( s(t) \): authorized signal
- \( x(t) \): unauthorized signal
- \( w(t) \): AWGN

- Significance Testing
  - Test statistic \( T \): a measure of observed data
  - Acceptance Region \( \Omega \): we accept the null hypothesis if \( T \in \Omega \)
  - Significance level \( \alpha \): probability of false alarm

\[ \text{Prob}(T \notin \Omega | \mathcal{H}_0) \leq \alpha \]
Capturing the Characteristics of the Radiation Power in Normal Condition

- Propagation Law
  - The received power is roughly linear with the logarithmic distance between the transmitter and the receiver

\[ P_n = P_0 - 10\gamma \log_{10}(d_n/d_0) + S_n \text{ (dB)}, n = 1, \ldots, N \]

- Independent and identically-distributed shadow fading

\[ S \sim N(0, \sigma^2 I), \quad S = (S_1, S_2, \ldots, S_N)^T \]
Detecting Unauthorized Signals with An Authorized Signal Present

- 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

(a) $\mathcal{H}_0$

(b) $\mathcal{H}_1$
Linearity-Check-given-Location (LCL)

- **Linear estimation** of the received power $\mathbf{P} = (P_1, P_2, \ldots, P_N)^T$
  
  $$\hat{\mathbf{P}} = A(A^T A)^{-1} A^T \mathbf{P}, \quad A = \begin{bmatrix} 1 & \log_{10}(d_1/d_0) \\ \vdots & \vdots \\ 1 & \log_{10}(d_N/d_0) \end{bmatrix}$$

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

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

- Given the location of the authorized transmitter, the error is **Gaussian**

  $$\hat{\mathbf{e}} \sim \mathcal{N}(0, \Sigma_e)$$

- Acceptance region: $\Omega = \{\hat{\mathbf{e}} : \hat{\mathbf{e}}^T \Sigma_e^{-1} \hat{\mathbf{e}} < T_{\hat{\mathbf{e}}}\}$

- False alarm rate:
  $$Q_F = \frac{\Gamma(N/2, T_{\hat{\mathbf{e}}}/2)}{\Gamma(N/2)}$$
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
  - 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
Calibrating Power (CAL)

- The authorized transmitter periodically sends an "identity" signal.
- By normalizing the signal power, the unknown transmission power is removed.

\[ \tilde{P}_i = P_i - P_N \quad \text{(dB)}, \quad i = 1, \ldots, N - 1. \]

- The residue by subtracting the calibrating power from the measured power is also Gaussian.

\[ \hat{e}_c^c = \tilde{P}_i - \tilde{P}_i^c \]

- Acceptance region:
  \[ \Omega = \{ \hat{e}_c : (\hat{e}_c)^T (\Sigma_e^c)^{-1} (\hat{e}_c) < T_c \} \]

- False alarm rate:
  \[ Q_F = \frac{\Gamma((N - 1)/2, T_c/2)}{\Gamma((N - 1)/2)} \]
Detection Probability vs. Interference-to-Signal Ratio (ISR)

- $N = 100$ sensors randomly distributed in a square area
- One authorized transmitter and one unauthorized transmitter are randomly located
- $\gamma = 3.5; \sigma = 4$ dB
- solid: $Q_F = 0.1$
  - dash: $Q_F = 0.05$
  - dotted: $Q_F = 0.01$

- With additional information about the authorized signal (i.e., location or identity power), the LCL and CAL can achieve a detect rate above 0.9;

- SVM is applied without knowledge about the authorized signal, so it has its highest detection rate when ISR = 0 dB.
Detection Probability vs. the Number of Unauthorized Transmitter

- $N$ sensors randomly distributed in a square area
- One authorized transmitter and multiple unauthorized transmitter are randomly located
- $\gamma = 3.5; \sigma = 4$ dB
- Total interference vs. signal power ratio is 0 dB
- $Q_F = 0.1$
- solid: $N = 100$
dash: $N = 50$
dotted: $N = 20$

When the aggregate interference power from all unauthorized users is fixed, more unauthorized users lead to higher detection rate
Summary

- We presented a zone-based dynamic spectrum access network structure and a spectrum access policy such that authorized users will not interfere with each other.
- We proposed a policy enforcement mechanism to detect unauthorized radio sources via a sensor network. Without assuming signal structure, our method is based on spatially distributed measured power.
- We formulated the detection of anomalous spectrum usage as several statistical significance testing problems. When an authorize (primary) signal is present, we proposed three methods that make use propagation characteristics:
  - Linearity-Check-given-Location (LCL)
  - One-class Support Vector Machine (SVM)
  - Calibrating Power (CAL)
- Our approaches can effectively detect unauthorized spectrum usage with high detection rate and low false positive rate.
Thank You!

Special note from the innocent speaker:
Please direct your tough question to song@winlab.rutgers.edu.