An Energy-Detection-based Cooperative Spectrum Sensing Scheme for Minimizing the Effects of NPEE and RSPF

Oladiran Olaleye, Muhammad A Iqbal, Ahmed Aly, Dmitri Perkins, Magdy Bayoumi
The Center for Advanced Computer Studies
University of Louisiana at Lafayette, LA 70504, USA
{ogo8842, mxi1678, axa5234, perkins, mab}@cacs.louisiana.edu

ABSTRACT

For improved spectrum utilization, the key technique for acquiring spectrum situational awareness (SSA) — spectrum sensing — is greatly improved by cooperation among the active spectrum users, as network size increases. However, the many cooperative spectrum sensing (CSS) schemes that have been proposed are based on the assumptions of accurate noise power estimates, characterizable variation in noise level and absence of false or malicious users. As part of a series of SSA research projects, in this research work, we propose a novel scheme for minimizing the effects of noise power estimation error (NPEE) and received signal power falsification (RSPF) by energy-based reliability evaluation. The scheme adopts the Voting rule for fusing multiple spectrum sensing data. Based on simulation results, the proposed scheme yields significant improvement, 68.2—88.8%, over the conventional CSS schemes, when compared on the basis of the schemes' stability to uncertainties in noise and signal power.

CCS Concepts

•**Networks** → **Network performance analysis;**

Keywords

Cognitive Radio Networks, Cooperative Spectrum Sensing, Energy Detection, Received Signal Power, Spectrum Sensing Data Falsification Attacks, Noise Uncertainty, Noise Power Estimation, Reliability Evaluation.

1. INTRODUCTION

The current trend in demand and usage has exposed the vast underutilization of the available spectrum resources. As reported in a Federal communications commission (FCC) submission [1], for example, at least 80 percent of the spectrum below 3 GHz is unexploited the United States. As a result, methods and techniques have been proposed in literature, under the umbrella of cognitive radio networking, for improving spectrum utilization. To achieve that objective, assumptions about the state of the system are required, especially due to the heterogeneous and dynamic nature of future communication systems. One such assumption is the accuracy of noise power estimate, a highly variable parameter and one of the key metrics for achieving spectrum situational awareness (SSA) through spectrum sensing by energy detection. Although collaboration among multiple users helps to improve the performance of energy detection, the current cooperative spectrum sensing (CSS) schemes were formulated based on systematic and predictable noise component sources. Hence, in order to minimize the overall effects of noise for improved energy detection performance, a sensing scheme that considers the randomness and volatility of noise is required.

A number of techniques for minimizing the effects of noise power estimation error (NPEE) and received signal power falsification (RSPF) have been proposed. Some are based on individual secondary user (SU) properties such as signal-to-noise ratio (SNR), some are based on the interaction among SU's such as cluster index and consensus), while some are based on the detection threshold [2] [3]. Incorporating NPEE into threshold settings is one step to correctly adapt the process of energy detection to the random distribution of noise power. However, presetting the detection threshold to vary over a predetermined range, in order to conform to noise variation, would mean constraining the variation of noise between bounds, which are indeterminable to precision and irreproducible in variation. On the other hand, energy detection threshold can be modeled to adapt to the dynamics of noise power but the approach would also require making certain assumptions: identical distribution of noise samples, known noise average power fluctuation factor [2], and uniform SNR [3].

Hence, the novelty of this research work lies in the consideration of unsystematic and unpredictable inaccuracies in signal and noise power during spectrum sensing by energy detection. The rest of the paper is organized as follows: section II describes the system models, including the radio propagation, energy detection, noise and signal attack models; section III explains the proposed CSS scheme — energy-based reliability evaluation; the simulation experiments and results are discussed in section IV; while the conclusion and future works are stated in section V.

MSWiM '16, November 13-17, 2016, Malta, Malta

DOI: http://dx.doi.org/10.1145/2988287.2989169

2. SPECTRUM SENSING

2.1 System Model

Considering a n-secondary-user cognitive radio network (CRN), deployed in a region covered by a 50 dBm (100 Watt) EIRP primary user (PU) transmitter with a coverage radius R km. The secondary users (SU's) are assumed to be independent and stationary. A SU is r km away from the PU transmitter with received SNR γ. To detect the presence of a PU transmission, a SU: measures the power of the received signal $P_{\mathrm{S}}^{\mathrm{meas}}$; computes the estimated noise power $P_{\mathrm{N}}^{\mathrm{est}}$; then transmits the $P_{\mathrm{S}}^{\mathrm{meas}}$ and $P_{\mathrm{N}}^{\mathrm{est}}$ to the data fusion center (DFC) where the two energy parameters are corrected for error to obtain $P_{\mathrm{S}}^{\mathrm{corr}}$ and $P_{\mathrm{N}}^{\mathrm{corr}}$ respectively. At the DFC, the detection threshold λ is computed based on a pre-fixed probability of false alarm P_{FA} and $P_{\mathrm{N}}^{\mathrm{corr}}$, followed by a comparison with $P_{\mathrm{S}}^{\mathrm{corr}}$. If $P_{\mathrm{S}}^{\mathrm{corr}} > \lambda$ the DFC concludes for the SU, with a detection probability P_{D}, that there is a PU transmission in progress, else that the channel is free. The DFC then combines the probabilities by the Voting rule to obtain the fused probability of detection Q_{D} and false alarm Q_{FA}.

2.2 Radio Propagation Model

The simulation environment is developed using the irregular terrain model (ITM) [4], a radio propagation model developed by the Institute for Telecommunication Sciences, National Telecommunications and Information Administration, U.S. Department of Commerce. The PU transmits at 600 MHz from a height of 305 m with location and time reliability of 50% each while the receiver antenna height is 9 m, with 2 dBi antenna gain and horizontal polarization. The average terrain height is 90 m, the surface refractivity is 301 N-units and the ground dielectric constant and conductivity are 15 and 0.005 S/m respectively.

2.3 Energy Detection Model

Compared to other methods of detecting signals, such as the matched filter method and the cyclic feature detection method, the energy detection method requires no knowledge of the signal characteristics nor it's periodicity; it is simple and requires less computation but highly susceptible to variation in noise power. To characterize the impact of noise variation on energy detection, the detection process is modeled as a binary hypothesis testing problem:

$$\begin{cases} H_0 : x(k) &= n(k) \\ H_1 : x(k) &= h(k)s(k) + n(k), k = 1, 2, ..., M \end{cases} \quad (1)$$

Where $x(k)$ represents the received signal; $s(k)$, the transmitted signal; $h(k)$, the channel gain; $n(k)$, zero-mean additive white Gaussian noise with variance σ^2 ; M, the number of samples; and H_0 and H_1, the hypothesis of the absence and presence of PU signal respectively.

Assuming: $x(k)$ and $s(k)$ are independent; $h(k)$ is constant during the detection process; SU channels are independent; and the PU and SU's share the same spectrum allocation, the test statistics for the energy detection process, which is equivalent to an estimate of the received signal power, measured by applying a band-pass filter to the received signal in a particular frequency region in time domain [5], is given by:

$$x_{\mathrm{E}} = \frac{1}{M}\sum_{i=1}^{M} |x_i|^2, \quad M = 2tB \quad (2)$$

Where, x_i is the $i-th$ received signal sample i , t is the sensing time and B is the bandwidth.

Based on the Central Limit Theorem, when $M >> 1$, the test statistics can be approximated as a Gaussian random variable [5], giving:

$$P_{\mathrm{FA}} = Q\left(\sqrt{M}(\lambda - 1)\right) \quad (3)$$

$$P_{\mathrm{D}} = Q\left(\frac{\sqrt{M}(\lambda - (\gamma + 1))}{\sqrt{2}(\gamma + 1)}\right) \quad (4)$$

Where, λ is the energy detection threshold; $\gamma = P_{\mathrm{S}}^{\mathrm{meas}}/P_{\mathrm{N}}^{\mathrm{est}}$ and $Q(x)$ is the Marcum-Q function.

2.4 Noise and Attack Model

2.4.1 Noise

The estimation of noise power is based on ambient temperature, which is unstable in time domain. Hence, noise power estimates suffer from random error with severe impact on energy detection for CRN's. In this research work, the range of noise power estimates is modeled as an open set, with positive and negative deviations from an assumed average $P_{\mathrm{N}}^{\mathrm{avg}}$ thus,

$$P_{\mathrm{N},i}^{\mathrm{est}} - P_{\mathrm{N}}^{\mathrm{avg}} = \{\Delta_{\mathrm{N},1}^{-}, ..., 0, ..., \Delta_{\mathrm{N},N_{\mathrm{SU}}-1}^{+}, \Delta_{\mathrm{N},N_{\mathrm{SU}}}^{+}\} \quad (5)$$

$$P_{\mathrm{N}}^{\mathrm{avg}} = P_{\mathrm{TN}} + SG + NF \quad (6)$$

$$P_{\mathrm{TN}} = 10log_{10}(1000kTB) \quad (7)$$

Where $P_{\mathrm{N},i}^{\mathrm{est}}$ is the estimated noise power at the i-th SU; $\Delta_{\mathrm{N},i}^{+}$ and $\Delta_{\mathrm{N},i}^{-}$ are the positive and negative deviation, respectively, from the average noise power; $|\Delta_{\mathrm{N},i}^{+}|$ and $|\Delta_{\mathrm{N},i}^{-}|$ are not necessarily equal; N_{SU} is the total number of SU's present in the network; P_{TN} is the thermal noise in dBm; SG is the System Gain in dBm; NF is the noise figure in dBm; k is the Boltzmann constant (1.3807x10^{-23} joules/K); T is the Ambient Temperature in Kelvin; and B is the Bandwidth in Hz.

For a comprehensive analysis of the effects of NPEE and the proposed minimization approach, a spectrum of different combinations of NPEE's are considered: when all the SU's experience the same negative NPEE; when all the SU's experience the same positive NPEE; and random combinations of positive and negative NPEE.

2.4.2 Attack

As in the IEEE 802.22 standard [5], the DFC is aware of each SU's location and orientation and by the radio propagation model [4] and dynamic signal strength mapping, can predict the received signal power $P_{\mathrm{S}}^{\mathrm{pred}}$. While honest SU's report the actual $P_{\mathrm{S}}^{\mathrm{meas}}$ and $P_{\mathrm{N}}^{\mathrm{est}}$, malicious SU's may report any combination of false $P_{\mathrm{S}}^{\mathrm{meas}}$ and $P_{\mathrm{N}}^{\mathrm{est}}$. However, the main factors that determine the impact of spectrum sensing data falsification (SSDF) on the performance of energy detection include the number of honest SU's $N_{\mathrm{SU}}^{\mathrm{honest}}$, the number of malicious SU's $N_{\mathrm{SU}}^{\mathrm{malicious}}$, the magnitude of NPEE and

RSPF, and the distribution and cooperation among the malicious SU's in the network. The simple and self-correcting approach to minimizing the effects of malicious SU's would be by having a large ratio of honest SU's to malicious SU's. However, that approach is not always realizable since the number of malicious SU's in a network, at any time, is beyond the control of the DFC. Hence, for a complete investigation of the effects of malicious SU's and analysis of the minimization approach, the extremes of attack (from a large $N_{\mathrm{SU}}^{\mathrm{honest}}/N_{\mathrm{SU}}^{\mathrm{malicious}}$ ratio to the emulation of honest SU's) are considered. The range of possibilities includes: $N_{\mathrm{SU}}^{\mathrm{honest}} > N_{\mathrm{SU}}^{\mathrm{malicious}}$; $N_{\mathrm{SU}}^{\mathrm{honest}} < N_{\mathrm{SU}}^{\mathrm{malicious}}$; SU emulation; and positive, negative and random RSPF.

3. PROPOSED COOPERATIVE SPECTRUM SENSING SCHEME

The conventional method for fusing sensing data combines the raw computations from SU's without testing for authenticity. That approach is prone to error and susceptible to infiltration by faults from noise and signal data. Hence, to boost the dependability of the final decision made at the DFC, the SU sensing data must be corrected for faults. In our proposed scheme, we consider the range of possible governing factors that could affect a SU sensing data reliability (R_i): the SNR at the SU γ_i, the distance of the SU from the PU or incumbent device transmitter r_i, the intention of the SU (honest or malicious) I_i, measurement error $M_{\mathrm{err},i}$, device error $D_{\mathrm{err},i}$, computational error $C_{\mathrm{err},i}$ and environmental error $E_{\mathrm{err},i}$.

$$R_i = f(\gamma_i,\ r_i,\ I_i,\ M_{\mathrm{err},i},\ D_{\mathrm{err},i},\ C_{\mathrm{err},i},\ E_{\mathrm{err},i}) \qquad (8)$$

Where the impact of γ_i and r_i are dependent and those of I_i, $M_{\mathrm{err},i}$, $D_{\mathrm{err},i}$, $C_{\mathrm{err},i}$ and $E_{\mathrm{err},i}$ are cumulative.

Hence, in order to minimize the effects of NPEE and achieve a dependable probability of incumbent transmission detection, the proposed scheme, shown in Fig. 1, adopts an energy-based reliability evaluation approach.

3.1 Energy-based Reliability Evaluation

For the purpose of this work: the value of a parameter obtained by direct physical measurement (e.g. sampling and analysis) is referred to as a measured quantity; the value obtained indirectly by measuring a related parameter is referred to as an estimated quantity; while the value obtained from an existing mathematical model is referred to as a predicted quantity. In order to determine the true value of a parameter, its estimated and measured equivalents are weighted and adapted based on its predicted value and the observed absolute deviation; the observed quantity is corrected and adapted based on a more reliable equivalent.

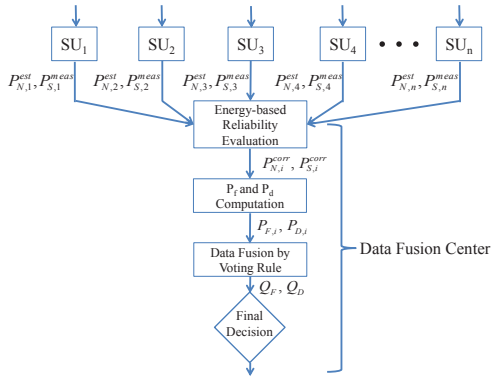


Figure 1: The proposed cooperative spectrum sensing scheme. It is based on the use of estimation, prediction and measurement for minimizing the impacts of NPEE and RSPF on signal detection.

Let P_{corr} be the corrected value of a parameter P; P_{meas}, the measured value of P; P_{pred}, the predicted value of P; P_{est}, the estimated value of P; r_{meas}, the weighted reliability of P_{meas}; r_{pred}, the weighted reliability of P_{pred}; and r_{est}, the weighted reliability of P_{est}. Hence,

$$P_{\mathrm{corr}} = r_{\mathrm{meas}} P_{\mathrm{meas}} + r_{\mathrm{pred}} P_{\mathrm{pred}} + r_{\mathrm{est}} P_{\mathrm{est}} \qquad (9)$$

Where r_{meas}, r_{pred} and r_{est} are adapted to the variation of P_{meas}, P_{pred} and P_{est} respectively.

3.1.1 *Detection and minimization of noise power estimation error*

Based on the assumption that all the SU's in the network are honest ($N_{\mathrm{SU}}^{\mathrm{malicious}} = 0$), the corrected noise power is calculated from (9) thus,

$$P_{\mathrm{N}}^{\mathrm{corr}} = r_{\mathrm{N}}^{\mathrm{est}} P_{\mathrm{N}}^{\mathrm{est}} + r_{\mathrm{NS}}^{\mathrm{meas}} P_{\mathrm{N+S}}^{\mathrm{meas}} - r_{\mathrm{S}}^{\mathrm{pred}} P_{\mathrm{S}}^{\mathrm{pred}} \qquad (10)$$

Where $r_{\mathrm{N}}^{\mathrm{est}}$ is the weighted reliability of noise power based on the measured ambient temperature; and $P_{\mathrm{N}}^{\mathrm{est}}$ is the estimated noise power based on ambient temperature; $r_{\mathrm{NS}}^{\mathrm{meas}}$ is the weighted reliability of the measured signal plus noise power; $P_{\mathrm{N+S}}^{\mathrm{meas}}$ is the measured signal plus noise power; $r_{\mathrm{S}}^{\mathrm{pred}}$ is the weighted reliability of the predicted signal power based on the pathloss model; and $P_{\mathrm{S}}^{\mathrm{pred}}$ is the predicted signal power based on the pathloss model.

If the estimated noise power is equal to the expected value, that is, the NPEE $\Delta_{\mathrm{N}} = 0$, then

$$\begin{cases} P_{\mathrm{N}}^{\mathrm{est}} &= P_{\mathrm{N+S}}^{\mathrm{meas}} + P_{\mathrm{S}}^{\mathrm{pred}} \\ r_{\mathrm{N}}^{\mathrm{est}} &= r_{\mathrm{NS}}^{\mathrm{meas}} = r_{\mathrm{S}}^{\mathrm{pred}} = 0.5 \end{cases} \qquad (11)$$

Otherwise,

$$\begin{cases} r_{\mathrm{N}}^{\mathrm{est}} &= 0.5 - 0.5 * \frac{|P_{\mathrm{N}}^{\mathrm{est}} - P_{\mathrm{N+S}}^{\mathrm{meas}} + P_{\mathrm{S}}^{\mathrm{pred}}|}{P_{\mathrm{N+S}}^{\mathrm{meas}} - P_{\mathrm{S}}^{\mathrm{pred}}} \\ r_{\mathrm{NS}}^{\mathrm{meas}} &= r_{\mathrm{S}}^{\mathrm{pred}} = 1.0 - r_{\mathrm{N}}^{\mathrm{est}} \end{cases} \qquad (12)$$

Where,

$$r_{\mathrm{N}}^{\mathrm{est}} = \begin{cases} 0.0 < r_{\mathrm{N}}^{\mathrm{est}} \leq 0.5 \\ 0.0 \quad otherwise \end{cases}$$

3.1.2 *Detection and minimization of received signal power falsification*

Based on the assumption of accurate noise estimate ($\Delta_{\mathrm{N}} = 0$), the corrected signal power is calculated from (9) thus,

$$P_{\mathrm{S}}^{\mathrm{corr}} = r_{\mathrm{NS}}^{\mathrm{meas}} P_{\mathrm{N+S}}^{\mathrm{meas}} - r_{\mathrm{N}}^{\mathrm{est}} P_{\mathrm{N}}^{\mathrm{est}} + r_{\mathrm{S}}^{\mathrm{pred}} P_{\mathrm{S}}^{\mathrm{pred}} \qquad (13)$$

If the reported measured signal power is equal to the predicted signal power, that is, the RSPF $\Delta_{\mathrm{S}} = 0$, then

$$\begin{cases} P_{\mathrm{N+S}}^{\mathrm{meas}} &- P_{\mathrm{N}}^{\mathrm{est}} = P_{\mathrm{S}}^{\mathrm{pred}} \\ r_{\mathrm{NS}}^{\mathrm{meas}} &= r_{\mathrm{N}}^{\mathrm{est}} = r_{\mathrm{S}}^{\mathrm{pred}} = 0.5 \end{cases} \qquad (14)$$

Otherwise,

$$\begin{cases} r_{\mathrm{NS}}^{\mathrm{meas}} &= r_{\mathrm{N}}^{\mathrm{est}} = 0.5 - 0.5 * \frac{|P_{\mathrm{N+S}}^{\mathrm{meas}} - P_{\mathrm{N}}^{\mathrm{est}} - P_{\mathrm{S}}^{\mathrm{pred}}|}{P_{\mathrm{S}}^{\mathrm{pred}}} \\ r_{\mathrm{S}}^{\mathrm{pred}} &= 1.0 - r_{\mathrm{NS}}^{\mathrm{meas}} \end{cases} \qquad (15)$$

Where,

$$r_{\mathrm{NS}}^{\mathrm{meas}} = r_{\mathrm{N}}^{\mathrm{est}} = \begin{cases} 0.0 < r_{\mathrm{NS}}^{\mathrm{meas}} \leq 0.5 \\ 0.0 \qquad otherwise \end{cases}$$

3.2 Data fusion by voting rule

Having corrected the energy parameters, the probabilities of false alarm and detection is computed from (3) and (4), and then combined based on Voting rule — a preferable weighted-data fusion method [5]. Thus,

$$Q_{\mathrm{D}} = \sum_{k \geq (\tau * N)}^{N} \left(\frac{N!}{k!(N-k)!} (P_{\mathrm{D},i})^k (1 - P_{\mathrm{D},i})^{N-k} \right) \quad (16)$$

Where N is the number of SU's being considered; τ is the voting threshold for k successes and was set at 0.5 for the simulation experiment; while $P_{\mathrm{D},i}$ is the detection probability for the i-th SU. The global decision is made based on Q_{D} and Q_{FA}, which is also calculated from (16) by replacing $P_{\mathrm{D},i}$ with $P_{\mathrm{FA},i}$.

4. SIMULATION RESULTS AND ANALYSIS

Different combinations of NPEE and RSPF were simulated in MATLAB in order to characterize the effects of uncertainties on the performance of energy detection for spectrum sensing and also demonstrate the efficiency of the proposed approach. For the simulation, $P_{\mathrm{N}}^{\mathrm{avg}}$ is set at -65 dBm while the channel bandwidth B is 6 MHz (for minimal multipath fading [5]).

As shown in Fig. 2(a), negative NPEE increases the probability of detection for a fixed probability of false alarm and vice versa. The figure also reveals the sensitivity of the detection probability to a unit magnitude decibel error as seen in the rapid spread of the receiver operating characteristics curves (ROC) curves from the average noise power. At $Q_{\mathrm{F}} = 0.1037$, the actual probability of detection is 0.5052 but when the magnitude of NPEE is varied between $-3 \leq \Delta_{\mathrm{N}}(dBm) \leq 3$, the detection probability fluctuates between $0.7922 \leq Q_{\mathrm{D}} \leq 0.3473$ respectively. With the proposed scheme, however, the fluctuation is reduced to $0.5512 \leq Q_{\mathrm{D}} \leq 0.5044$ (Fig. 2(b)), an equivalent of 88.8% improvement based on stability to NPEE. To demonstrate the efficacy of the scheme in a more practical scenario, NPEE's at the different SU's is made to vary randomly between $-5 \leq \Delta_{\mathrm{N}}(dBm) \leq 5$ (Fig. 2(c)). The results obtained are similar to those of equal NPEE.

Fig. 3(a) and 3(b) show the performance of the proposed scheme over the conventional method when all the SU's in the network had equal magnitude of RSPF while in Fig. 4, the simulation is carried out with different combinations of the honest and malicious users: 100 percent honest users; 50 and 100 percent malicious users all with -2 dBm RSPF; and 50 and 100 percent malicious users with the malicious users emulating the absence of PU transmission. The figures reveal the upshot of error in P_{S} by replicating the effect of the RSPF from a single SU as a cumulative effect from all the SU's in the network. As expected, positive RSPF results in increased probability of detection, and vice versa, while an increase in the number of malicious users (from 0 to 5 to 10 in the 10-user network) results in a pronounced corresponding effect in the detection probability. Based on the simulation parameters, with an even number of honest and malicious users in the network and $\Delta_{\mathrm{S}} = -2dBm$ (Fig. 4(a)), at $Q_{\mathrm{F}} = 0.1037$, the actual probability of detection is 0.5052 (as in the previous cases) but when the number of malicious users increases to 5 and 10, the detection probability are 0.5052 and 0.3871 correspondingly, while the proposed scheme (Fig. 4(b)) reduces the instability to 0.5052 and 0.4676 respectively — approximately 68.2% improvement based on stability to RSPF. On the other hand, when all the SU's in the network have equal RSPF (Fig. 3(a) and 3(b)), the improvement is similar to that in Fig. 2(a) and 2(b). For the cases where individual malicious users have random RSPF, Fig. 3(c) illustrates the efficiency of the proposed scheme in minimizing the impact of RSPF. From the plots (Fig. 3(c)), the scheme also proves to be better than the conventional method in stabilizing the detection probability with the potential to completely detect and eliminate all RSPF, provided $P_{\mathrm{S}}^{\mathrm{pred}}$ is accurate.

5. CONCLUSIONS

In this paper, we have presented a novel cooperative spectrum sensing scheme, based on radio propagation models, measured signal power and estimated noise power, for minimizing the effects of NPEE and RSPF. NPEE and RSPF were detected and corrected based on reliability metrics obtained by comparing the measured signal power and the estimated noise power to the predicted received signal power. Simulation results revealed the behavior of the ROC curve in different cases and combinations of NPEE and RSPF. The performance of the proposed scheme over the conventional method varies between 68.2 and 88.8% when compared using the resulting ROC curves. While the scheme relies on the accuracy of the predicted received signal power, we have designed and initiated our next research plan with the main focus of improving the prediction accuracy using machine learning techniques.

6. ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation (NSF) under NSF Career Grant No. 1454835.

7. REFERENCES

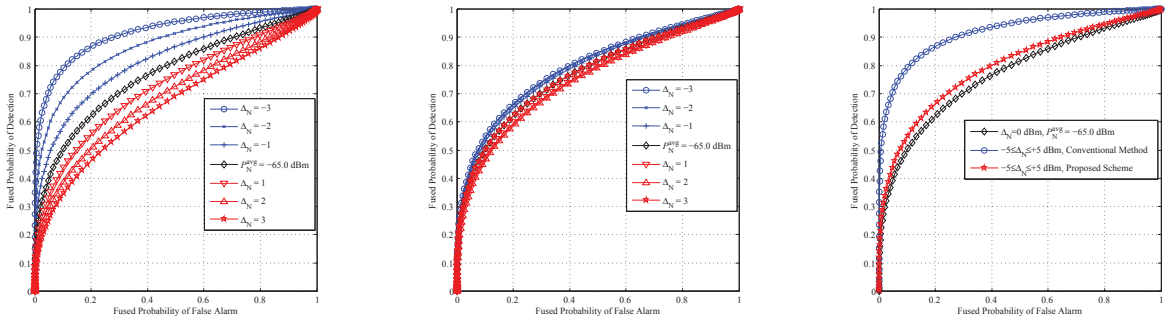
[1] M. Calabrese, "The End of Spectrum Scarcity: Building on the TV Bands Database to Access Unused Public Airwaves," New America Foundation's Wireless Future Program, Working Paper #25, June 2009.

[2] G. Yu, C. Long, M. Xiang and W. Xi, "A Novel Energy Detection Scheme Based on Dynamic Threshold in Cognitive Radio Systems," Journal of Computational Information Systems, Vol. 8, pp. 2245-2252, Mar. 2012.

[3] A. Gorcin, K. A.Qaraqe, H. Celebi, and H. Arslan, "An adaptive threshold method for spectrum sensing in multichannel cognitive radio networks," Telecommunications (ICT), 2010 IEEE 17th International Conference on, vol., no., pp. 425, 429, 4-7 April 2010.

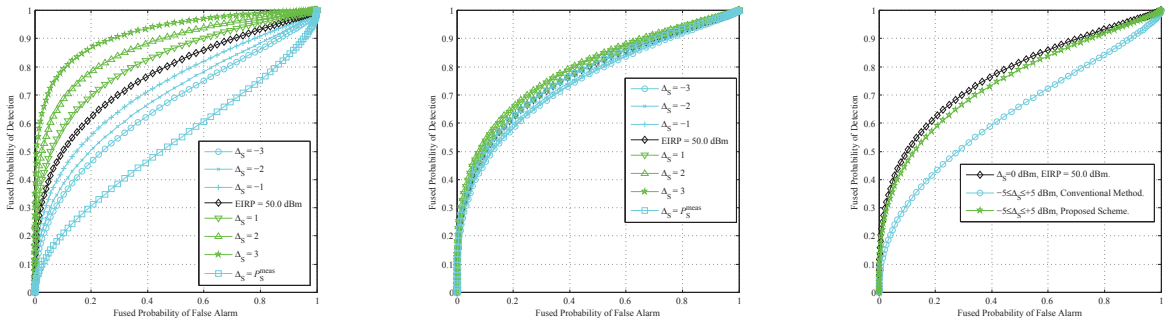
[4] G. Hufford, "The ITS Irregular Terrain Model Algorithm, Version 1.2.2, The Algorithm," http://www.its.bldrdoc.gov/resources/radio-propagation-software/itm/itm.aspx, 2016.

[5] "IEEE standard for information technology-telecommunications and information



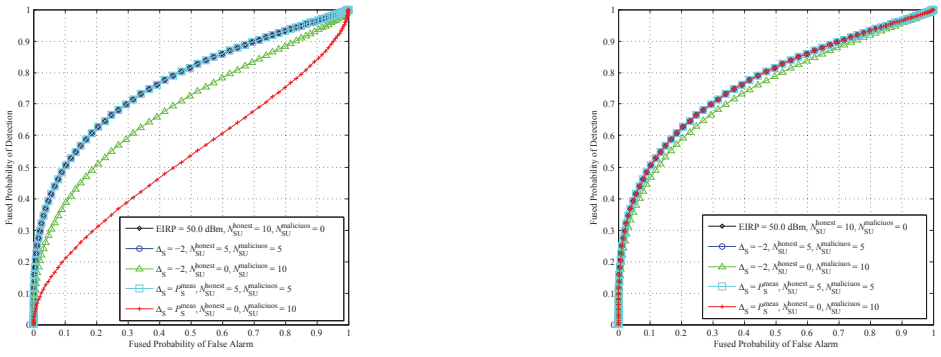
(a) (b) (c)

Figure 2: ROC curves comparing the proposed scheme to the conventional method based on the performance in minimizing the effects of positive and negative uncertainties in noise power estimates for a 10-SU cognitive radio network. (a) and (b) simulates the scenario with equal NPEE at each SU while (c) simulates constrained but random NPEE.



(a) (b) (c)

Figure 3: ROC curves comparing the proposed scheme to the conventional method based on the performance in minimizing the effects of positive and negative deviations from the actual received signal power for a 10-SU cognitive radio network. (a) and (b) assumed each SU's received signal power had equal magnitude of deviation while (c) assumed random deviations. The emulation of SU for the absence of PU transmission was simulated with $\Delta_S = P_S^{meas}$.



(a) (b)

Figure 4: ROC curves comparing the proposed scheme, in (b), to the conventional method, in (a), based on the performance in minimizing the effects of a slight and total deviation from the actual received signal power, for a 10-SU cognitive radio network with different combinations of honest and malicious users: 100% honest SU's, 50% honest SU's; and 100% malicious SU's respectively.

exchange between systems wireless regional area networks (wran)-specific requirements part 22: Cognitive wireless ran medium access control (mac) and physical layer (phy) specifications: Policies and procedures for operation in the TV bands," IEEE Std 802.22-2011, pp. 1-680, 1 2011.