This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the ICC 2008 proceedings.

Secure Cooperative Sensing Techniques for Cognitive Radio Systems

Praveen Kaligineedi, Majid Khabbazian and Vijay K. Bhargava
Department of Electrical and Computer Engineering
University of British Columbia
Vancouver, BC
Email: {praveenk, majidk, vijayb}@ece.ubc.ca

***Abstract*— The most important task for a Cognitive Radio (CR) system is to identify the primary licensed users over a wide range of spectrum. Cooperation among spectrum sensing devices has been shown to offer various benefits including decrease in sensitivity requirements of the individual sensing devices. However, it has been shown in the literature that the performance of cooperative sensing schemes can be severely degraded due to presence of malicious users sending false sensing data. In this paper, we present techniques to identify such malicious users and mitigate their harmful effect on the performance of the cooperative sensing system.**

I. Introduction

Radio spectrum is one of the most scarce and valuable resource for wireless communications. Given this fact, new insights into the use of spectrum have challenged the traditional approaches to spectrum management. Actual measurements have shown that most of the allocated spectrum is largely under-utilized and similar views about the under-utilization of the allocated spectrum have been reported by Spectrum-Policy Task Force appointed by Federal Communications Commission (FCC) [1]. Spectrum efficiency can be increased significantly by giving opportunistic access of these frequency bands to a group of potential users for whom the band has not been licensed. Cognitive Radio (CR) [2] has been proposed as a way to improve spectrum efficiency by exploiting the unused spectrum in dynamically changing environments. The CR design is, therefore, an innovative radio design philosophy which involves smartly sensing the swaths of spectrum and then determining the transmission characteristics (e.g., symbol rate, power, bandwidth, latency) of a group of potential users based on the primary users behavior.

The most important challenge for a cognitive radio system is to identify the presence of primary users over wide range of spectrum. This process is very difficult as we need to identify various primary users employing different modulation schemes, data rates and transmission powers in presence of variable propagation losses, interference generated by other secondary users and thermal noise. This is especially true in the case of broadcast TV channels, where the receivers are passive, and as such it is not possible to detect the presence of a nearby receiver. For example, if the channel between the primary transmitter and the sensing device is under a deep fade, it is possible that the sensing device may not detect the primary signal. As a result, the cognitive radio might transmit signal in the corresponding primary user band causing interference to the nearby primary receiver. This is called the hidden terminal problem. To overcome this problem, the sensitivity of the cognitive radio sensing device has to be at least 20-30dB more than that of the primary receiver. Moreover, the sensing process must be very quick in order to scan the entire wide-band without significant delay. Traditionally, there are two techniques which are used for spectrum sensing, viz., energy detection and cyclostationary feature detection. The energy detector fails to detect the signal whose power is below the noise floor and hence, cannot achieve high sensitivity requirements of CR devices. The cyclostationary feature detector takes advantage of the fact that most of the signals encountered in wireless communications are cyclostationary whereas the noise is stationary. However, not all signals exhibit same level of cyclostationarity. The problem is even more complicated due to presence of secondary user interference.

The burden on signal processing techniques can be alleviated to a large extent by using cooperative diversity between cognitive radio spectrum sensors. Few cognitive radio spectrum sensors under independent fades can help in reducing individual sensitivity requirements and essentially help in overcoming the hidden terminal problem by countering the shadowing and multi-path effects. Several cooperative sensing schemes have been proposed in the literature [3], [4], [5]. However, it was shown in [3] that presence of few malfunctioning sensing devices could adversely effect the performance of cooperative sensing system. In this paper, we investigate techniques to identify the sensors which provide false sensing information and nullify their effect on the cooperative spectrum sensing system.

The rest of this paper is organized as follows. In Section II, we define the system model. In Section III, we present the average combination scheme which is used to combine sensing data from various sensing devices in this paper. In Section IV, we propose techniques to identify and tackle malicious users for the average combination scheme. Simulation results are presented in Section V. Finally, conclusions are drawn in Section VI.

II. System Model

We consider a group of U cognitive users in the presence of a primary transmitter. We assume a log-normal shadowing

for the channel between primary transmitter and CR. The shadowing components of the channels between primary user and various cognitive users are assumed to be independent of each other. The area of coverage of the cognitive radio system is assumed to be small enough so that the variations in path loss can be neglected. All of the sensing devices use energy detectors. We assume that the sensing devices can distinguish the signal of a primary user from a secondary user's signal. The sensing devices send their sensing data to an access point through control channels. We assume perfect channel conditions for the control channels. Based on the detection statistics from the sensing devices and its own measurements the access point makes a decision regarding the presence of the primary user.

III. Average Combination Scheme

Let $e[u;k]$ for $u = 1, 2, ..., U$ represent the outputs of energy detectors at various nodes at time instant k. Let hypothesis H_1 denote presence of a signal and hypothesis H_0 denote absence of the signal. Then, the outputs of the energy detectors in decibels (dB) are given by

$$e[u;k] = \begin{cases} 10\log_{10}\left(\sum_{l=T_k}^{T_k+T-1} |h[u;l]s[l] + z[u;l]|^2\right) & ; H_1 \\ 10\log_{10}\left(\sum_{l=T_k}^{T_k+T-1} |z[u;l]|^2\right) & ; H_0 \end{cases} \quad (1)$$

where T denotes the length of the sensing interval. T_k represents the time instant at which the k^{th} sensing interval starts. $h[u;l]$ represents the channel gain between the primary transmitter and the u^{th} cognitive user. We assume that the log-normal shadowing component remains constant during the sensing interval. $s[l]$ represents the primary user transmitted signal and $z[u;l]$ represents the zero mean additive white Gaussian noise with variance σ_z^2.

The optimum detection scheme based on the energy detector outputs is given by [6]

$$\frac{p(e[1,k], e[2,k], ..., e[U,k]/H_1)p(H_1)}{p(e[1,k], e[2,k], ..., e[U,k]/H_0)p(H_0)} \underset{H_0}{\overset{H_1}{\gtrless}} e_T \quad (2)$$

The threshold e_T can be determined using the cost functions in case of Bayesian formulation and required probability of false alarm or probability of detection in case of Neyman-Pearson formulation.

However, the optimum detection scheme could be quite cumbersome when individual signal-to-noise ratios (SNRs) are not known. In this paper, we consider the detection scheme based on average combining due to its simplicity. In the average combination scheme, the mean of the energy received in dB by all the nodes is evaluated at the access point and passed through a threshold detector.

The average combination based detection scheme is as follows

$$(1/U)\sum_{u=1}^{U} e[u;k] \underset{H_0}{\overset{H_1}{\gtrless}} e_T \quad (3)$$

In this paper, we consider Neyman-Pearson formulation. The threshold e_T is determined so that the probability of false alarm is fixed at a certain value P_f. This threshold is obtained empirically through Monte Carlo simulations. Note, that for high SNR, the $e[u;k]$ are approximately Gaussian distributed at a given time instant k since the channel coefficient is lognormal distributed.

IV. Methods to detect malicious users

Presence of malicious nodes can have significant effect on the performance of the cooperative sensing system [3]. A node might be malicious due to device malfunctioning or due to selfish reasons. For example, a node might detect that there is no signal present. However, it might inform the access point that a signal is present, so that if the access point makes a wrong decision that there is a primary signal present, the malicious node can selfishly transmit its own signal on the free channel.

We consider different kinds of malicious nodes. We first consider simple malicious nodes such as an 'Always Yes' node or an 'Always No' node. An 'Always Yes' node gives a value above the threshold (i.e., it declares that a primary user is present) all the time. An always 'No' node gives a value below the threshold (i.e., it declares that a primary user is absent) all the time. 'Always Yes' users increase the probability of false alarm P_f and 'Always No' users decrease the probability of detection P_d. Also, there might be malicious nodes which produce extreme false values once in a while, significantly affecting the performance of the sensing system during those particular sensing intervals, and give correct values rest of the time. The malicious node detection schemes that we propose in this section can identify any malicious node whose energy value differs in distribution from the underlying distribution of the energy values of the legitimate nodes.

A. Pre-filtering of the Sensing Data

Pre-filtering of the sensing data is essential in identifying and removing the malicious nodes which significantly affect the final decision at the access point by giving extreme false values. We apply an outlier detection method to detect such malicious nodes. An outlier is an observation which is numerically distant from the rest of the data. There are several well studied methods to determine such outliers [7]. We implement a simple method commonly used to identify extreme outliers [7].

We evaluate upper bound $e_u[k]$ and lower bound $e_l[k]$ for values $e[u;k]$ as follows

$$\begin{aligned} e_u[k] &= e_3[k] + 3e_{iqr}[k] \\ e_l[k] &= e_1[k] - 3e_{iqr}[k] \end{aligned} \quad (4)$$

where $e_1[k]$ and $e_3[k]$ represent the first and third quartile of the values $e[u;k]$ and $e_{iqr}[k] = e_3[k] - e_1[k]$ represents the interquartile range. If a particular value of $e[u;k]$ does not lie in the interval $[e_l[k], e_u[k]]$, then it is considered as an outlier and its value is ignored in making the final decision. This outlier detection technique avoids calculation of the mean and the standard deviation of the sensing data which might be affected by the presence of malicious nodes producing

extreme values. Let $S_k \subseteq \{1, 2, ..., U\}$ represent the set of users whose energy values lie in the range $[e_l[k], e_u[k]]$. Also, let the number of users in the set S_k be represented by $U_S[k]$.

B. Trust Factors

We assign a trust factor $\lambda[u;k]$ for each user $u \in \{1, 2, ..., U\}$ such that

$$\sum_{u=1}^{U} \lambda[u;k] = 1 \tag{5}$$

The trust factor gives a measure of reliability of a particular user. Trust factors are used as the weighing factors while calculating the mean of the energy values obtained from various users. The final decision is made using the trust factors as follows

$$\sum_{u=1}^{U} \lambda[u;k] e[u;k] \underset{H_0}{\overset{H_1}{\gtrless}} e_T \tag{6}$$

The trust factor of a user is calculated based on the past and present sensing data sent by the user as well as the sensing data sent by other users. $\lambda[u;k] = 0$ for the set of users not lying in S_k, as we do not consider their energy values in making the final decision. In the rest of this section, we will discuss methods to calculate the trust factors of the users.

1) Evaluation of Trust Factors: At the beginning, the trust factor of $1/U_S[k]$ is assigned to all the users lying in S_k. At each sensing iteration k, based on the energy statistics $e[u;k]$, an instant trust penalty $d[u;k]$ is assigned to each user in U. These instant trust penalties are used to evaluate the trust factors $\lambda[u;k]$ and make the final decision.

The instant trust penalties are evaluated as follows

$$d[u;k] = \frac{|e[u;k] - \mu[k]|}{\sigma[k]} \tag{7}$$

where $\mu[k]$ and $\sigma[k]$ are the sample mean and variances of the energies $e[u;k]$ of the users lying in the set S_k. These trust penalties are then summed over certain time period L to obtain $D[u;k]$.

$$D[u;k] = \sum_{k'=k-L+1}^{k} d[u;k'] \tag{8}$$

Observing values of $D[u;k]$ would give a clear idea of which sensing nodes are deviating from the underlying distribution of $e[u;k]$. Intuitively, one would expect that $D[u;k]$ for a malicious node would be different from the rest.

There are different ways in which un-normalized trust factors $\lambda'[u;k]$ can be obtained from $D[u;k]$. One approach is to identify the mild outliers [7] among $D[u;k]$ by defining upper and lower bounds on $D[u;k]$ as follows

$$\begin{aligned} D_u[k] &= D_3[k] + 1.5 D_{iqr}[k] \\ D_l[k] &= D_1[k] - 1.5 D_{iqr}[k] \end{aligned} \tag{9}$$

where $D_1[k]$ and $D_3[k]$ represent the first and third quartile of the values $D[u;k]$ and $D_{iqr}[k] = D_3[k] - D_1[k]$ represents the interquartile range. We completely trust all the values which lie between $D_u[k]$ and $D_l[k]$ and assign equal trust factors to all of them. In this case, un-normalized trust factors $\lambda'[u;k]$ are obtained as follows

$$\lambda'[u;k] = \begin{cases} 1 & : \quad D[u;k] \in [D_l[k], D_u[k]], u \in S_k \\ 0 & : \quad \text{Otherwise} \end{cases} \tag{10}$$

Another possible approach is to assign trust factors such that they are exponentially decreasing according to their distance from the median $m_D[k]$ of the values $D[u;k]$. In this case, un-normalized trust factors $\lambda'[u;k]$ are obtained as follows

$$\lambda'[u;k] = \begin{cases} e^{-|m_D[k] - D[u;k]|} & : \quad u \in S_k \\ 0 & : \quad \text{Otherwise} \end{cases} \tag{11}$$

If the sensing data of one of the users (u_t) can be completely trusted, (for example, that of the access point assuming that its sensing device is not malfunctioning), then one can use $D[u_t;k]$ instead of the median $m_D[k]$ in the above equation to obtain un-normalized trust factors. The normalized trust factors are finally obtained from un-normalized trust factors as follows

$$\lambda[u;k] = \frac{\lambda'[u;k]}{\sum_{u'=1}^{U} \lambda'[u';k]} \tag{12}$$

Intuitively, the proposed schemes should be able to identify all the malicious nodes which produce values that differ in distribution from rest of the values. Thus, an 'Always Yes' and 'Always No' nodes must be easily identified using these schemes. Smaller values of L could be used to identify nodes which behave maliciously over short periods of time and larger values of L would help identify nodes which regularly send false values over larger time periods. In complex scenarios containing different kinds of malicious users, multiple values of L could be used to identify the malicious nodes. In such cases, we can evaluate trust factors using two or more different values of L and then combine them to obtain a final trust factor for each user. Also, pre-filtering the data as shown in Section IV-A helps in nullifying the effect of malicious nodes which produce extreme false values once in a while and produce true values rest of the time.

C. Quantization

Since control channels have limited bandwidth, the energy values need to be quantized before they are sent to the access point. The optimal quantization schemes for distributed detection have been extensively studied [6]. However, finding the optimal threshold values is, in general, a non-linear optimization problem and is highly complex.

In this section, we consider suboptimal quantization of the energy values $e[u;k]$. Let b represent the number of quantization bits. We approximate the energy value of each user $e[u;k]$ under Hypothesis H_1 with a Gaussian distribution with mean and variance obtained numerically using Monte-Carlo simulations. We then implement the Lloyd-Max quantizer for this Gaussian distribution designed to minimize the mean square error [8], [9]. At the access point, the mean of the quantized energy values $\{e_q[u;k]\}_{u=1}^{U}$ is compared to a

threshold, which is determined so that the probability of false alarm is fixed at P_f.

For the case in which very few quantization bits are available, we do not apply the pre-filtering to eliminate extreme values, since the outlier detection scheme is not very effective for the data sets with low cardinality. The rest of the detection procedure remains the same as in case of un-quantized energy values. We take weighted average of the the quantized energy values and compare it to the threshold. The instant trust penalties are evaluated as in (7), but using the quantized energy values. We study the effect of quantization over our malicious node detection schemes through simulations.

V. Simulation Results

We consider a $U = 50$ user system. Mean received SNR of the cognitive radio users is -10dB. The mean and standard deviation of lognormal shadowing component is 0dB and 4dB respectively. In the energy detectors, length of the sensing time interval T is chosen to be 50. The time period L over which instant trust penalties are added to obtain $D[u;k]$ is 50 for all the sensing systems presented in this section. In all the malicious node detection schemes used in the simulations, unnormalized trust factors $\lambda'[u;k]$ are obtained by eliminating the mild outliers in $D[u;k]$ and completely trusting the rest of the users in the set S_k as suggested in Section IV-B.

In Fig. 1, we consider a cooperative sensing system in which 10% of the users are 'Always Yes' users, each giving a value twice the threshold on a linear scale (i.e, a value 3dB higher than the threshold in dB). We present the probability of detection P_d and probability of false alarm P_f for the case in which no malicious node detection scheme is used and for the case in which the malicious node detection scheme is used. From Fig. 1, we can see that using the malicious node detection scheme, we can easily identify 'Always Yes' users and bring the probability of false alarm of the system close to that of a cooperative sensing system without a malicious node. At the same time, the probability of detection of the system remains close to that of a cooperative sensing system without a malicious node. In most of our simulations, the malicious nodes were identified in less than 10 iterations. In Fig. 2, we consider a system in which 10% of the users are 'Always No' users giving a value half the threshold on a linear scale. From Fig. 2, we can see that our malicious node identification scheme successfully identifies the 'Always No' nodes and nullifies their effect on the final decision. In Fig. 3, we observe the probability of false alarm as we vary the percentage of 'Always Yes' users in the system. The threshold e_T is fixed such that probability of false alarm is 0.01 when no malicious node is present. From the figure, its easy to see that the malicious node identification scheme works quite well for up to 20% malicious nodes, keeping the probability of false alarm close to 0.01. Also, the effect on probability of detection, which is not presented in this paper, is marginal (less than 2%). In Fig. 4, we consider a system in which 10% of the users produce extreme false values (6dB higher than the threshold) once in 10 sensing intervals and study their impact on the system performance. We also show the effect of our malicious node identification schemes on the system. The simulation results indicate that our scheme can detect and eliminate the effect of such malicious nodes. In Fig. 5, we consider quantized energy values. We fix threshold such that probability of false alarm is 0.01. We consider cases with quantization bits $b = 1, 2, 3$. We see that our detection scheme still successfully identifies "Always Yes" users in all cases for up to 20% malicious nodes.

It should be noted that the simulation results presented in this section do not consider very complex malicious users. In general, the proposed malicious node detection schemes can identify any malicious node whose distribution differs from the underlying distribution of the legitimate nodes.

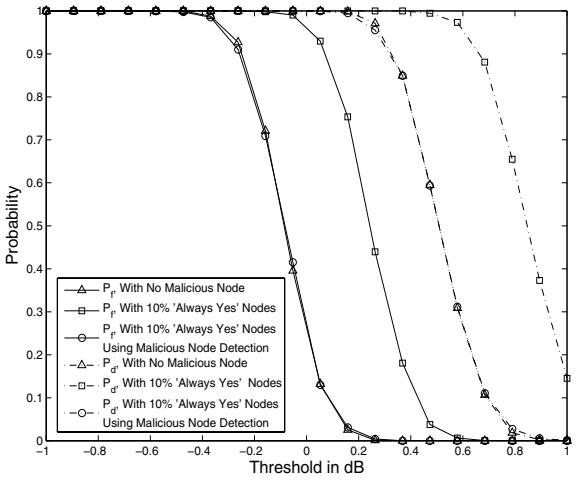

Fig. 1. Performance of malicious node detection scheme for a system containing 10% 'Always Yes' nodes

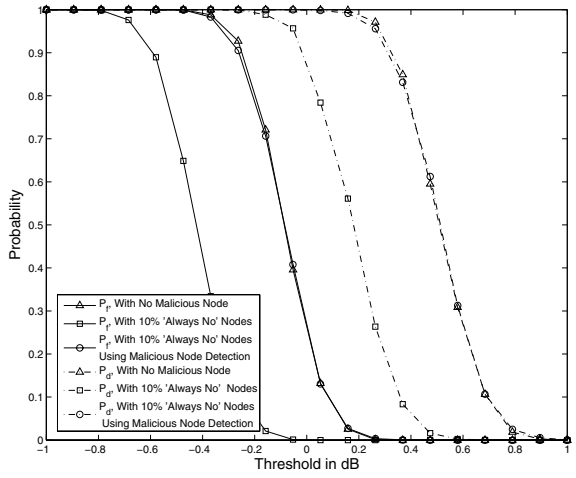

Fig. 2. Performance of malicious node detection scheme for a system containing 10% 'Always No' nodes

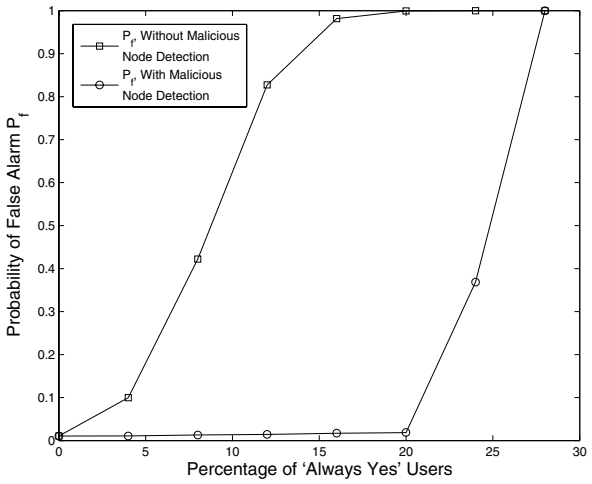

Fig. 3. Probability of false alarm P_f of the system vs. Percentage of 'Always Yes' nodes

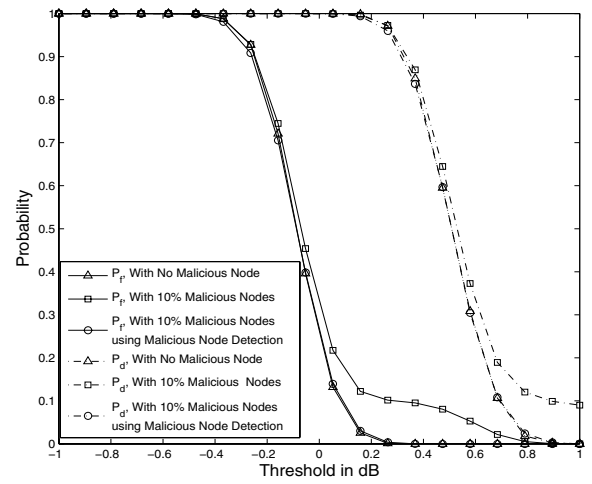

Fig. 4. Performance of malicious node detection scheme for system containing 10% malicious nodes which produce false extreme values once in 10 sensing iterations

VI. Conclusion

In this paper, we have devised schemes to identify and nullify the effect of malicious nodes for the case where energy detectors are used by the sensing devices. We employed a simple and fast average combination scheme to simplify the decision process at the access point. Using simulations, we verified that the proposed schemes can identify 'Always Yes' users, 'Always No' users and malicious nodes producing extreme values. We have also studied the performance of our schemes when quantization is applied to energy values before transmission. In future work, we will develop malicious node detection algorithms for the case of sensing devices using cyclostationary detectors and will consider more complex scenarios.

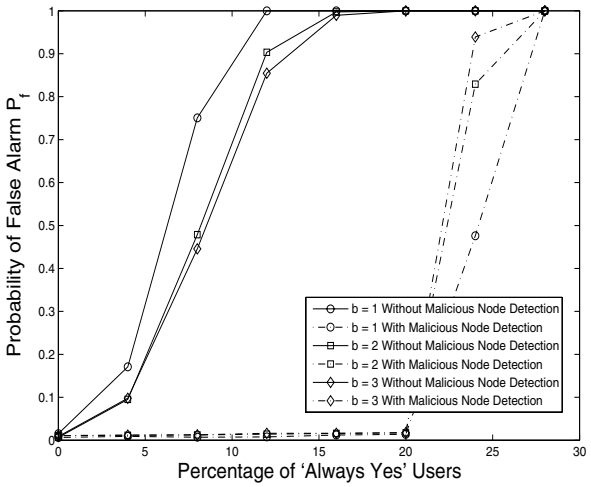

Fig. 5. Probability of false alarm P_f of the system vs. Percentage of 'Always Yes' nodes for quantized energy values with number of quantization bits $b = 1, 2, 3$

References

[1] Spectrum policy task force report. Technical Report 02-135, Federal Communications Commission, Nov 2002.

[2] J. Mitola, "*Software Radio Architecture*," John Wiley & Sons, 2000.

[3] S. M. Mishra, A. Sahai and R. W. Brodersen, "Cooperative sensing among cognitive radios," *IEEE International Conference on Communications ICC'06* , vol. 4, pp. 1658-1663, June 2006.

[4] A. Ghasemi and E. S. Sousa,"Collaborative Spectrum Sensing for Opportunistic Access in Fading Environments," *IEEE Conference on Dynamic Spectrum Access Networks (DYSPAN'05)*, pp. 131-136, Nov. 2005.

[5] G. Ganesan and Y. Li, "Cooperative spectrum sensing in cognitive radio networks," *IEEE Conference on Dynamic Spectrum Access Networks (DYSPAN'05)*, pp. 137-143, Nov. 2005.

[6] P. K. Varshney, *Distributed Detection and Data fusion* New York: Springer-Verlag, 1996.

[7] V. Barnett and T. Lewis, "*Outliers in Statistical Data*," Wiley Publisher, 1994

[8] S. P. Lloyd, "Least squares quantization in PCM," *IEEE Trans. Inform. Theory*, vol. IT-28, pp. 129-137, Mar. 1982.

[9] J. Max, "Quantizing for minimum distortion," IRE Trans. Inform. Theory, vol. IT-6, pp. 7-12, Mar. 1960.