Adaptive Learning of Byzantines’ Behavior in Cooperative Spectrum Sensing

Aditya Vempaty, Keshav Agrawal
Department of Electrical Engineering
Indian Institute of Technology Kanpur, UP 208016 INDIA
{vaditya,kesh}@iitk.ac.in

Hao Chen
Department of Electrical and Computer Engineering
Boise State University
Boise, ID, 83725
haochen@boisestate.edu

Pramod K. Varshney
Department of Electrical Engineering and Computer Science
Syracuse University
Syracuse, NY 13244 USA
varshney@syr.edu

Abstract—This paper considers the problem of Byzantine attacks on cooperative spectrum sensing in cognitive radio networks. Our major contribution is a technique to learn about the potential malicious behavior of cognitive radios (CRs) over time which identifies the Byzantines and then estimates their probabilities of false alarm ($P_{fa}$) and detection ($P_D$). We show that for a given set of data over time, the Byzantines can be identified for any $\alpha$ (percentage of Byzantines). It has also been shown that these estimates of $P_{fa}$ and $P_D$ of the Byzantines are asymptotically unbiased and converge to their true values at the rate of $O(T^{-1/2})$. We then use these probabilities to adaptively design the fusion rule. We calculate the Probability of error ($Q_e$) and compare it with the minimum possible probability of error.

Index Terms—Cognitive Radio Networks, Spectrum Sensing, Byzantine Attacks

I. INTRODUCTION

In order to address the issue of spectrum scarcity and to increase the efficiency of the spectrum usage, the idea of cognitive radios (CR) has recently been proposed. In CR networks, the secondary users sense the presence of a primary user without interfering in the primary user’s communication. This process is called spectrum sensing which allows a secondary user to operate when the primary is not present thereby increasing the efficiency of spectrum usage. Cooperative sensing has shown very good results [1]. In such sensing, each CR (secondary user) sends its decision regarding the presence of the primary to the fusion center (FC) which makes the final decision using a fusion rule. In the binary decision case, each local CR makes and sends a binary decision (0/1) on whether the Primary User is present (‘1’) or absent (‘0’). The different fusion rules possible could be Chair-Varshney Rule [2], K out of N rule [3][4] etc.

In this paper, we consider the problem of spectrum sensing operating in an adversarial environment. Some CRs in the network may be controlled by the adversary or they become malicious and try to gain an advantage in using the network. They try to manipulate the final decision taken at the FC via their own actions in terms of what they transmit to the FC. One particular kind of attack of interest is a Byzantine attack, wherein the ‘malicious’ CRs may send wrong decisions using a predetermined strategy. This can be done either by changing their local thresholds or by simply swapping the result in a probabilistic manner. In other words, they operate at different values of probability of false alarm and probability of detection, rather than operating at the ones as defined by the FC.

To encounter the Byzantine attacks, the FC would like to adaptively learn the behavior of the CRs and use this information to make the final decision. Similar work of finding the ‘best’ CRs has been presented in [5] to reduce the energy consumption in the perfect secured scenario where there are no Byzantine CRs. But when the Byzantines are present, the scenario would be different as the main objective here would be to secure the network rather than reducing the energy to be used.

Learning the Byzantines’ behavior, in particular, learning the probabilities of false alarm and detection of the Byzantines would help in finding the weights of the Chair-Varshney rule. Such adaptive learning of probabilities has been considered in [6] and [7]. For this, we need to first identify the Byzantines in the CRN. In our earlier work in this area of identifying the Byzantines [8], we had assumed that the CR is honest if its local decision is the same as the global decision which is normally the case when the honest CRs are in majority. But if that is not the case, then this algorithm identifies the honest CRs as the Byzantines and removes them and thereby makes the network a ‘Byzantine network’. In this paper, we propose a learning based framework to detect and identify Byzantines more reliably. Further, instead of just removing the Byzantine CRs from the fusion process, we propose to learn the Byzantine patterns to incorporate Byzantine CR decisions at the FC to improve detection performance. In Section II, we describe the system model used and the assumptions made. In Section III, we propose the Byzantine detection scheme. In Section IV, we formulate and then solve the problem of
estimating the probabilities of detection and false alarm of the Byzantines. In Section [VI] we prove the convergence of these estimates and in Section [VII] we calculate the probability of error using the Chair-Varshney fusion rule. We present some simulations and results in Section [VII] and then conclude the paper with some possible future work in Section [VIII].

II. SYSTEM MODEL

The cognitive radio network model used in this paper is discussed here. Let the number of CRs in the network be ‘N’ out of which M = αN are malicious ones. The CRs have been distributed over the region of interest (ROI) to detect the presence of a primary user. Each CR decides either on hypothesis $H_1$ (primary user present) or hypothesis $H_0$ (primary absent). Each CR makes this decision $v_i(1/0)$ solely based on its observation and sends a signal $u_i(1/0)$ to the fusion center. For honest CRs, $u_i=v_i$, but for malicious nodes, they need not be the same.

Each CR makes a decision using an energy detection scheme as discussed in our earlier work [2]. Under $H_0$, the power received, $P_r = W$ where $W$ is Gaussian distributed as $N(\mu_0, \sigma_0)$. Given the transmitted power ($P_t$) of the primary,

$$P_r = P_t - PL(d)$$

where $PL(d)$ is the path loss. This is calculated by subjecting the links between primary and secondary users to an i.i.d (independent and identically distributed) shadowing path loss,

$$PL(d) = PL(d) + X_\sigma$$

and

$$PL(d) = 27.77 + 46.05\log(f_c) - 4.78(\log(f_c)^2 - 13.82\log(h_t) - (1.1\log(f_c) - 0.7)h_r + (44.9 - 6.55\log(h_t))\log(d)$$

assuming a rural environment where $f_c$ is the carrier frequency, $h_t$ is the transmitter antenna height, $h_r$ is the receiver antenna height, $d$ is the distance between primary and secondary users and $X_\sigma$ is a zero mean Gaussian random variable with variance $\sigma$.

In the above discussed case, the probability of false alarm ($P_{fa}$) can be expressed as

$$P_{fa} = Q\left(\frac{\eta - \mu_0}{\sigma_0}\right)$$

and the probability of detection ($P_D$) can be expressed as

$$P_D = Q\left(\frac{\eta - \mu_1}{\sigma}\right)$$

where $\eta$ is the threshold used for binary hypothesis testing, $\mu_1 = P_t - PL(d)$ and $Q(z) = \frac{1}{\sqrt{2\pi}} \int_{-}\infty^{z} e^{-\frac{x^2}{2}} dx$.

All the Byzantines have the same $P_{fa}$ and $P_D$ and all the honest CRs use the same threshold for their local decisions and therefore have the same $P_{fa}^H$ and $P_D^H$. We assume that the fusion center knows the prior probability of hypothesis $H_1$ ($P_1$). It also has the complete information of the honest CRs’ behavior and the probabilities. Other assumptions used are that $P_1 \neq 0, 1, 0.5$, which is a reasonable assumption as in spectrum sensing, the probability of the primary present is approximately 0.2-0.3. It has also been assumed that $P_{fa} \neq P_D$ for the honest CRs which is reasonable as the fusion CR would not select such a pair of probabilities.

III. BYZANTINE IDENTIFICATION

For the identification of the Byzantines, we use a relatively simple approach. It uses the idea of comparing the observed behavior of the CR with the expected behavior of an honest CR and declares it honest if it matches. At the fusion center, the expected behavior of an honest CR is known through the joint probability of two CR observations. These values are estimated for every CR over time by averaging the number of times a decision is made over a time interval of T instants. These probabilities can be updated after every time instant using the relation

$$\gamma_i^{T+1} = \hat{P}(u_i = 1) = \frac{T\eta_i^T + u_i^{T+1}}{T+1}$$

$$\delta_{ij}^{T+1} = \hat{P}(u_i = 1, u_j = 1) = \frac{T\delta_{ij}^T + u_{ij}^{T+1}}{T+1}$$

$$\rho_{ij}^{T+1} = \hat{P}(u_i = 0, u_j = 0) = \frac{T\rho_{ij}^T + (u_{ij}^{T+1} - 1)(u_{ij}^{T+1} - 1)}{T+1}$$

For an honest CR,

$$\gamma_H = P(u_i = 1|i = Honest) = P_1P_D^H + (1 - P_1)P_{fa}^H$$

$$\delta_H = P(u_i = 1, u_j = 1|i = j = Honest) = P_1P_D^H P_{fa}^H$$

$$\rho_H = P(u_i = 0, u_j = 0|i = j = Honest) = P_1(1 - P_D^H)(1 - P_{fa}^H) + (1 - P_1)(1 - P_{fa}^H)(1 - P_D^H)$$

under the assumption that the decisions are conditionally independent.

Now, for every CR, the joint probabilities ($\delta_{ij}, \rho_{ij}$) with every other CR (‘N – 1’) values per CR are calculated and their deviation from ($\delta_H, \rho_H$) is calculated. The test statistics $\Lambda_i^T$ for the ith CR after time T is

$$\Lambda_i^T = |\gamma_i^T - \gamma_H| + \min_{1 \leq j \neq i \leq N} |\delta_{ij}^T - \delta_H| + \min_{1 \leq j \neq i \leq N} |\rho_{ij}^T - \rho_H|.$$
i.e., the sum of deviations between \( \gamma_H \) and \( \gamma_H^T \), minimum of the ‘-1’ deviations between \( \delta_H \) and \( \delta_{ij} \) and between \( \rho_H \) and \( \rho_{ij} \).

The fusion center declares a CR as a Byzantine if \( \Lambda_H^T \) is greater than a particular threshold \( \lambda \) which will be determined in the following subsection [II-A]. After identifying the Byzantines, the fraction of Byzantines \( \alpha_T \) can be estimated as \( \alpha_T = \frac{M_T}{N} \), where \( M_T \) is the number of Byzantines identified after time \( T \).

A. Problem formulation

A CR is said to be Byzantine if its operating point is in the lower half of the ROC (\( P_{fa} \leq P_D \)) as shown in Figure 1. We define the threshold \( \lambda \) to be the minimum of the sum of deviations between \( \gamma_H \) and \( \gamma_B \), \( \delta_B \) and \( \rho_H \) and \( \rho_B \) under the condition when the Byzantines’ operating point is in the region as described above. Here \( \gamma_B = P(u_i = 1|i = Byzantine) = P_1 P_D^B + (1 - P_1)P_{fa}^B \) and

\[
\delta_B = P(u_i = 1, u_j = 1|i = j = Byzantine) = P_1 P_D^B P_D^B + (1 - P_1)P_{fa}^B P_{fa}^B
\]

and

\[
\rho_B = P(u_i = 0, u_j = 0|i = j = Byzantine) = P_1(1 - P_D^B)(1 - P_D^B) + (1 - P_1)(1 - P_{fa}^B)(1 - P_{fa}^B)
\]

This problem can be formulated as

\[
\lambda = \min_{(P_{fa}^B, P_D^B) \in R} (|\gamma_H - \gamma_B| + |\delta_B - \delta_B| + |\rho_H - \rho_B|)
\]

where \( R \) is the region as shown in Figure 1.

IV. Estimation of Probabilities

A. Problem formulation

For learning the behavior of the Byzantines, the fusion center would like to know \( P_{fa}^B \) and \( P_D^B \) or in other words would like to locate the Byzantines’ operating point. For this purpose, we use the values of \( \gamma_B \) of the CRs identified as Byzantines. For a Byzantine, the probability of decision being equal to ‘1’ (\( P(u_i = 1) \)) is \( \gamma_B \).

So, the problem can now be stated as

\[
(P_{fa}^B, P_D^B) = \arg\min_{(P_{fa}^B, P_D^B) \in R} \sum_{i \in B^T} (\hat{\gamma}_i - \gamma_B)^2
\]

where \( B^T \) is the set consisting of the CRs detected as Byzantines after the \( T^{th} \) time instant.

The above problem can be easily simplified to the form

\[
(P_{fa}^B, P_D^B) = \arg\min_{(P_{fa}^B, P_D^B) \in R} (P_1 P_D^B + (1 - P_1)P_{fa}^B - \bar{\gamma})^2
\]

where

\[
\bar{\gamma} = \frac{\sum_{i \in B^T} \gamma_i}{M_T}
\]

is the mean of the observed Byzantine probabilities. Obviously, the solution to this problem consists of all the points in \( R \) lying on the line

\[
P_1 P_D^B + (1 - P_1)P_{fa}^B = \bar{\gamma}
\]

Now to find the exact value of the operating point, the attack strategy of the Byzantines has to be known. This attack strategy can be inferred from the joint probabilities. The joint probability of an honest CR deciding on ‘1’ and a Byzantine CR deciding on ‘1’ (\( \delta_{BH} \)) is given by

\[
\delta_{BH} = P(u_i = 1, u_j = 1|i = Honest, j = Byz)
\]

\[
= P_1 P_D^H P_D^B + (1 - P_1)P_{fa}^H P_{fa}^B
\]

Now taking the joint probabilities of one detected Byzantine and one honest CR, we can find \( \delta_{ij} \) for all possible combinations of Byzantines and honest CRs. The problem can now be restated as

\[
(P_{fa}^B, P_D^B) = \arg\min_{(P_{fa}^B, P_D^B) \in R} \sum_{i \in B^T, j \in H^T} (\hat{\delta}_{ij} - \delta_{BH})^2
\]

whose solution satisfies

\[
P_1 P_D^H P_D^B + (1 - P_1)P_{fa}^H P_{fa}^B = \bar{\delta}
\]

Similarly, the above can also be performed for a joint probability of an honest CR and a Byzantine CR deciding ‘0’.

\[
\rho_{BH} = P(u_i = 0, u_j = 0|i = Honest, j = Byz)
\]

\[
= P_1(1 - P_D^H)(1 - P_D^B) + (1 - P_1)(1 - P_{fa}^H)(1 - P_{fa}^B)
\]

\[
(P_{fa}^B, P_D^B) = \arg\min_{(P_{fa}^B, P_D^B) \in R} \sum_{i \in B^T, j \in H^T} (\hat{\rho}_{ij} - \rho_{BH})^2
\]

whose solution satisfies

\[
P_1(1 - P_D^H)(1 - P_D^B) + (1 - P_1)(1 - P_{fa}^H)(1 - P_{fa}^B) = \bar{\rho}
\]

where

\[
\bar{\rho} = \frac{\sum_{i \in B^T, j \in H^T} \hat{\rho}_{ij}}{M_T(N - M_T)}
\]

B. Solution

Now from equations \[18\], \[21\] and \[25\], the exact operating point can be estimated. It can be mathematically expressed by taking any two equations at a time depending on the operating point of the honest CR (OPH). If the OPH is such that \( P_D^H + P_{fa}^H > 1 \), then Equations \[18\] and \[21\] can be taken to get

\[
\hat{P}_{fa}^B = \left[ \frac{\bar{\gamma} P_D^H - \bar{\delta}}{(1 - P_1)(P_D^H - P_{fa}^H)} \right]^{-1}
\]
\[ p_{fa}^B = \left[ \frac{\hat{\gamma} P_{fa}^H - \delta}{P_{fa}^H - P_B^H} \right]^+ \]  

where \([.]^+\) denotes the projection operator onto the unit interval, that is \([z]^+ = \min(\max(z, 0), 1)\).

But, if the OPH is such that \(P_{fa}^H + P_B^H < 1\), Equations Equations (18) and (25) can be solved similarly. It is important here to understand that these three equations intersect at a common point. But only two equations have been considered at a time to get an analytical expression for the estimates in order to prove convergence. The condition of \(P_{fa}^H + P_B^H < 1\) implies that there are more number of zero decisions expected from the CRs and thereby the joint probabilities of the CRs deciding a zero would give more information and thereby Equations (18) and (25) are preferred. Similarly \(P_{fa}^H + P_B^H > 1\) implies that there are more number of one decisions expected and thereby we use the joint probabilities of CRs deciding on one.

V. CONVERGENCE OF THE ESTIMATES

The convergence of the probabilities can be proved as follows:

Due to law of large numbers

\[ \lim_{T \to \infty} \gamma_i^T = \gamma_B \]  

for \(i \in B^T\) and

\[ \lim_{T \to \infty} \delta_i^T = \delta_{BH} \]  

for \(i \in B^T\) and \(j \in H^T\) implying that

\[ \lim_{T \to \infty} \hat{\gamma}_i^T = \gamma_B \]  

and

\[ \lim_{T \to \infty} \hat{\delta}_i^T = \delta_{BH} \]  

As the denominators of \(\hat{P}_{fa}^B\) and \(\hat{P}_{fa}^H\) are bounded and as the projection operator \([.]^+\) is a Lipschitz continuous mapping, \(P_{fa}^B\) and \(P_{fa}^H\) are also Lipschitz continuous functions of \(\gamma_i^T\) and \(\delta_j^T\). This implies that

\[ \lim_{T \to \infty} \hat{P}_{fa}^B = P_{fa}^B, \quad \lim_{T \to \infty} \hat{P}_{fa}^H = P_{fa}^H \]  

(Note that index ‘\(T\)’ has been removed from the notations for simplicity).

Since \(\hat{P}_{fa}^B\) and \(\hat{P}_{fa}^H\) are bounded due to the projection operator, the almost sure convergence given in (33) implies \(L^1\) convergence. This implies the asymptotic unbiasedness of the estimators:

\[ \lim_{T \to \infty} E(\hat{P}_{fa}^B) = P_{fa}^B, \quad \lim_{T \to \infty} E(\hat{P}_{fa}^H) = P_{fa}^H \]  

Similarly, the rate of convergence can be shown as \(T^{-1/2}\) using a similar approach as in [7].

VI. ADAPTIVE FUSION AND PROBABILITY OF ERROR

The final decision can be made by using the Chair-Varshney rule [2] using the estimated probabilities for finding the optimum weights given by:

\[ a_0 = \log \left( \frac{P_1}{P_0} \right) \]  

\[ a_i = \begin{cases} \log \left( \frac{P_{fa}}{P_B} \right), & v_i = 1 \\ \log \left( \frac{1-P_{fa}}{1-P_B} \right), & v_i = 0 \end{cases} \]  

where \(P_D = P_{fa}^H\) for honest CRs and \(P_D = P_B^H\) for Byzantine CRs.

Similarly \(P_{fa} = P_{fa}^H\) for honest CRs and \(P_{fa} = P_B^H\) for Byzantine CRs and the rule being

\[ a_0 + \sum_i a_i \geq 0 \]  

The probability of error for this rule can be calculated at every time instant as

\[ Q_e = P_1(1 - Q_D) + (1 - P_1)Q_{fa} \]  

where \(Q_D\) and \(Q_{fa}\) are the overall probability of detection and overall probability of false alarm respectively. If

\[ f(v; w, p) = \binom{w}{v} p^v (1-p)^{w-v} \]  

is the probability of getting exactly \(v\) successes in \(w\) trials, then \(Q_D\) and \(Q_{fa}\) are given by

\[ Q_D = P(u_0 = 1|H_1) = \sum_{m=1}^{N-M} \sum_{n=A}^{B} f(N-M; m, P_{fa}^H) f(M; n, P_{fa}^B) \]  

where \(u_0\) is the final decision taken, \(A = 0\) and \(B = \min(\text{ceil}((\beta-pm)/q), M)\) if \(q < 0\) and \(A = \max(0, \text{ceil}((\beta-pm)/q))\) and \(B = M\) if \(q > 0\), and

\[ Q_{fa} = P(u_0 = 1|H_0) = \sum_{m=1}^{N-M} \sum_{n=A}^{B} f(N-M; m, P_{fa}^H) f(M; n, P_{fa}^B) \]  

\[ p = \log \left( \frac{P_{fa}^H}{P_B^H} \right) - \log \left( \frac{1-P_{fa}^H}{1-P_B^H} \right) \]  

\[ q = \log \left( \frac{P_{fa}^B}{P_B^H} \right) - \log \left( \frac{1-P_{fa}^B}{1-P_B^H} \right) \]  

\[ r = \log \left( \frac{1-P_{fa}^H}{1-P_B^H} \right) \]  

\[ s = \log \left( \frac{1-P_{fa}^B}{1-P_B^H} \right) \]
Byzantine identification scheme, we performed seen in Figures 5 and 6. To evaluate the performance of this
\[ \alpha \in \text{majority}, \quad i.e. \] fusion rule is correct which is true when the honest CRs are
have assumed that the final decision after the ‘K out of N’
values of the original operating point to see its effect. The
operating point. We also were able to learn their behavior with time
of the Byzantines are in majority unlike [8]. The Byzantine’s
exactly detected without any mismatches when \( T \) is between
and thereby make the network a Byzantine network. In our
 Rawat et al [8] in their technique to find the Byzantines
have assumed that the final decision after the ‘K out of N’
fusion rule is correct which is true when the honest CRs are
in majority, i.e. \( \alpha \leq 0.5 \). If the Byzantines are in majority,
this algorithm would detect the honest CRs as Byzantines
and thereby make the network a Byzantine network. In our
algorithm, honest CRs need not to be in majority and even
though it takes more time, it can be used to detect the
Byzantines for any \( \alpha \). This is due to the fact that our Byzantine
detection algorithm is based on the probabilities rather than on
‘K out of N’ fusion rule.

VII. SIMULATION RESULTS

In this section, some simulation results are presented. We
assumed that the primary is transmitting at the UHF frequency
of 617MHz with effective transmitter antenna height \( h_t = 100 \text{m} \) and the effective isotropic radiated power (EIRP) is
assumed to be 35dBm. All CRs are assumed to be equipped
with a simple energy detector and effective receiver antenna
height \( h_r = 1 \text{m} \). The minimum power for a signal to be
detected is assumed to be -94dbm. We use the noise power
equal to -106dBm and in the log-normal shadowing path loss
model as well as noise we use standard deviation, \( \sigma = \sigma_0 =
3 \). We consider a large rural environment where the distance
between primary and secondary users is assumed to be equal
to 13Km. A threshold of \( \eta=2 \) has been used.

The simulation has been done for \( N=20 \) CRs and data
generated using \( P_e=0.3 \), \( P_f^H=0.9 \), \( P_f^U=0.01 \) and with different
values of \( \alpha \), \( P_f^H \) and \( P_f^U \). The process of detecting the
Byzantines and estimating the probabilities was done and
results can be seen in Figures 3 and 7.

As can be seen from the Figure 2, the Byzantines can be
easily detected without any mismatches when \( T \) is between
100 and 150. Also within this time, the estimated \( \alpha \) also
reaches the true value as can be seen from Figure 3. It can
also be observed that this algorithm works even when the
Byzantines are in majority unlike [8]. The Byzantine’s
operating point can be seen in Figure 3, with the point of
intersection of the 3 lines in the ROC being the Byzantine’s
operating point.

To observe the convergence of the estimated probabilities
to the actual values and the convergence overall probability of
error (\( Q_e \)) to the minimum possible, simulation was carried
out for a relatively high value of \( T \), \( T=5000 \) and different
values of the original operating point to see its effect. The
value of \( \alpha \) has been kept the same though. The results can be
seen in Figures 5 and 6. To evaluate the performance of this
Byzantine identification scheme, we performed 100 Monte-
Carlo simulation runs and the probability of an honest being
detected as a Byzantine and probability of Byzantine being
detected as honest has been plotted with time. These probabilities
for Byzantine identification can be treated analogous to the
probability of false alarm and misdetection of the Byzantine
identification respectively. The plots can be seen in Figure
7. The figure shows these probabilities reach zero when \( T \)
is around 100-150.

Rawat et al [8] in their technique to find the Byzantines
have assumed that the final decision after the ‘K out of N’
fusion rule is correct which is true when the honest CRs are
in majority, i.e. \( \alpha \leq 0.5 \). If the Byzantines are in majority,
this algorithm would detect the honest CRs as Byzantines
and thereby make the network a Byzantine network. In our
algorithm, honest CRs need not to be in majority and even
though it takes more time, it can be used to detect the
Byzantines for any \( \alpha \). This is due to the fact that our Byzantine

VIII. CONCLUSION

In this paper, we have proposed a scheme for identifying
the Byzantines for spectrum sensing in a cognitive radio
network. We also were able to learn their behavior with time
by estimating their probabilities which converge to their true
values in rms error sense at a rate \( O(T^{-1/2}) \). Although this
scheme takes more (around 100-150) time instants in the
simulation example presented as compared to the scheme
proposed in [8], it works under any scenario, even when the
Byzantines are in majority. In the future, we would like
to extend this scheme for detecting the Byzantines in user
localization problems.

REFERENCES

[1] David Maldonado, Bin Le, Akilah Hugine, Thomas W. Rondeau, Charles
W. Bostian “Cognitive Radio Applications to Dynamic Spectrum Allocation: A Discussion and an Illustrative Example”, Proc. IEEE DySPAN
[7] Ghasem Mirjailily, Zhi-Quan Luo, Timothy N. Davidson and Elio Bosse,
“Blind Adaptive Decision Fusion for Distributed Detection”, IEEE Trans-
actions on Aerospace and Electronic Systems Vol. 39, No. 1 January 2003
[8] Ankit Singh Rawat, Priyank Anand, Hao Chen and Pramod K. Varshney,
“Countering Byzantine Attacks in Cognitive Radio Networks”, Proc. of ICASSP 2010
[9] Priyank Anand, Ankit Singh Rawat, Hao Chen and Pramod K. Varshney,

Fig. 1. Different regions of possible operating point of Byzantines
Fig. 2. Mismatches with Time $P_H^D=0.9, P_H^{fa}=0.1, N=20, P_B^D=0.3, P_B^{fa}=0.7$

Fig. 3. Estimated $\alpha$ with Time $P_H^D=0.9, P_H^{fa}=0.1, N=20, P_B^D=0.3, P_B^{fa}=0.7$

Fig. 4. Final ROC $P_H^D=0.9, P_H^{fa}=0.1, \alpha=0.3, N=20, P_B^D=0.3, P_B^{fa}=0.7$

Fig. 5. Estimated probabilities $N=20, \alpha=0.3$

Fig. 6. $Q_e$ $N=20, \alpha=0.3$

Fig. 7. Probability of misdetection and false alarm of the proposed scheme