RANDOM DISTRIBUTED DETECTION WITH AN APPLICATION TO COGNITIVE RADIO BYZANTINE ATTACK

Uri Rogers, Jun Guo, Xia Li, and Hao Chen

Department of Electrical and Computer Engineering, Boise State University, Boise, ID 83725 USA

ABSTRACT

In this paper, a distributed detection model is introduced for m-ary hypotheses testing where the local sensors quantize their decisions to messages with alphabet size of D and the number of local sensors is random following a Poisson distribution. This model can be applied to a wide variety of distributed detection problems including homogenous and heterogeneous networks, robust detection under security attacks, and sensor failure mode analysis. As an illustrative example, the proposed model is applied to a Cognitive Radio network where the performance and strategies regarding Byzantine attacks are investigated under a game theoretical setting. Performance tradeoff between the detection efficiency and robustness of the sensor network is evaluated under the independent Byzantine attack model, where the malicious nodes attack based solely on their own observations. It is shown that, when the system is designed for maximum efficiency versus optimal robustness, then the malicious users may completely blind the fusion center, with less than one half of the total number of sensors.

***Index Terms*—Distributed Detection, Random Sensor Model, Byzantine Attacks, Cognitive Radio, Spectrum Sensing**

I. INTRODUCTION

Sensors are subject to power failure, drift, poor communication links, and other challenges that impact the active number of sensors performing distributed data collection and inference. As a result, the number of resource constrained wireless sensors within any distributed detection (DD) system is often a random variable. Contrast this with most DD analysis where the network is considered rather static and homogeneous, and the number of active sensor is often considered to be fixed and known [1], [2]. Even within the dynamic environment of collaborative spectrum sensing (SS) for wireless sensor networks (WSN) or Cognitive Radio networks (CRNs) under Byzantine security attacks, the sensor count is often assumed deterministic and known (see [3], [4] and references therein). Notable exceptions to this claim appear in [5] and references therein.

To investigate the random active sensor problem, this paper introduces a new method based on a statistical model for the number of active sensors with multiple levels of local decisions that can be used to effectively study DD problems of interest. This includes collaborative sensing in CRNs, security attacks in WSNs, performance analysis of heterogeneous WSNs, etc. It also provides a method to study the impact of sensor failure modes on network detection performance. Generally, the model allows for m-ary hypotheses testing where the local sensors quantize their decisions to D messages and the number of local sensors is random following a homogeneous spatial Poisson process.

Using the model developed in Section II this paper will study Byzantine attacks in CRNs in Section III. There we analyze the case, where in an attempt to garner an advantage in spectrum access, the malicious Cognitive Radios (CRs) apply a random attack strategy in an attempt to mask their presence to the Fusion Center (FC) while deteriorating the CRN SS performance. In doing so, this work essentially extends [6] and [7] by incorporating randomized attacks with FC detection sensitivity considerations.

Throughout, we use the following notation. Upper case letters represent a random variable and lower case a realization of a random variable (e.g. $X = x$). The operation $E[\cdot]$ is the probability expectation operator. $\mathcal{I}(p||q)$ denotes the Kullback-Leibler divergence (KLD) between two probability mass functions p and q and it is assumed $0 \log({}^{0}/_{q_k}) = 0, \ \forall q_k$.

II. RANDOM DISTRIBUTED DETECTION MODEL

Consider a general distributed target detection problem in a sensor network consisting of a random N number of sensors, and a single FC. There are m hypotheses about the target, $H_0, \ldots, H_{m-1}$. Each sensor's local observation X_j is conditionally independent given a respective hypothesis with a conditional distribution $\Pr(\boldsymbol{X}_j|H_k)$. The sensor generates an output $U_j = \gamma_j(X_j)$, where $\gamma_j : X_j \to \{0, \ldots, D-1\}$ with D the size of the sensor message set. Each of the messages $u_1, \ldots, u_N$ is transmitted to the FC, which applies a decision rule $\gamma_0 : \{0, \ldots, D-1\}^N \to \{0, \ldots, m-1\}$. The preceding formulation is similar to [8], but assumes a random number of sensors.

II-A. Proposed Model

Let the local observation under hypothesis H_k be $x_j = h_k(\boldsymbol{r}_j, w_j)$, which is a deterministic function of the random vector parameter $\boldsymbol{R}_j = \boldsymbol{r}_j$ under H_k and independent identically distributed (i.i.d.) noise, w_j. Also, assume the location of the target and all the sensors to be randomly distributed across the area of interest (AOI) as described in [9]. Clearly, when the target is mobile and the sensor network is resource constrained (bandwidth and power) it is not feasible to know $\boldsymbol{r}_j$ exactly. Hence, $\Pr(\boldsymbol{X}_j|H_k)$ is unknown and the optimal statistical test can not be applied for γ_0 or any γ_j. However, it may be possible to estimate via training or by statistical calculation an average $\boldsymbol{r}_j$, say $\bar{\boldsymbol{r}}$ ([9] and cellular area reliability in [10] or the appendix of [11]). With this formulation, each sensors observation is conditionally independent and identically distributed (i.i.d.) in an average sense.

When the DD performance is evaluated under the Bayesian framework, the performance of the DD system is often measured by the overall probability of error, $\Pr(U_0 \neq H_k)$ in the m-ary hypotheses testing problems [12]. With a-priori known probabilities $\Pr(H_k)$, $k = 0, \ldots, m-1$, then the minimum probability of error fusion rule γ_0 is the maximum a posteriori (MAP) rule

$$\gamma_0 : \text{Select } H_k \ : \ k = \arg \max_{k=0,\ldots,m-1} \Pr(H_k) \cdot \Pr(\boldsymbol{a}|H_k), \quad (1)$$

978-1-4799-2893-4/14/$31.00 ©2014 IEEE

where $\boldsymbol{a} = [A_0,\, A_1, \cdots, A_{D-1}]$, $A_d = \sum_{j=1}^{N} (u_j = d)$, and $d = 0, 1, \ldots, D-1$.

Let $\phi_{k,d} = \Pr(u_j = d \,|\, H_k, \bar{\boldsymbol{r}})$ be the conditional probability of making decision d at sensor j when the underlying hypothesis is H_k. Given the conditionally i.i.d. in an average sense assumption, it can be shown that $\phi_{k,d}$ is equal across all sensors and uniquely determined by $\bar{\gamma}$ and $h_k(\bar{\boldsymbol{r}}, w_j)$ for a given H_k. For any given realization of the random variable $N = n$, then A_d given H_k follows a binomial distribution with parameters n, and $\phi_{k,d}$ (i.e. $(A_d \,|\, H_k,\, N = n) \;\sim\; \text{Binomial}(n, \phi_{k,d})$). Consistent with [5], [13], we model N as a homogeneous spatial Poisson process with parameter λ across the AOI. That is, $A_d \,|H_k \sim \text{Poisson}(\lambda\phi_{k,d})$ such that

$$\Pr(A_d|H_k) = \frac{(\lambda\phi_{k,d})^{A_d}\, e^{-\lambda\phi_{k,d}}}{A_d!} \tag{2}$$

by section 4.4 of [14].

Employing the proposed Poisson model can greatly reduce the complexity in analyzing complicated distributed inference systems, for example, a simple linear optimal fusion rule at the FC as described in the following Lemma 1. A similar linear form can be obtained for the binary hypotheses testing case under the Neyman-Pearson framework.

Lemma 1. *With the known a-priori probability* $\Pr(H_k)$*, the m-ary MAP detector of* (1) *is equivalent to*

$$\arg \max_{k=0,\ldots,m-1} \left[\log \Pr(H_k) + \sum_{d=0}^{D-1} \left(A_d \log(\lambda\phi_{k,d}) - \lambda\phi_{k,d} \right) \right],$$

where the number of sensors $N \sim$ *Poisson*(λ)*, and* A_d *and* $\phi_{k,d}$ *are as previously defined.*

Proof: Substitute (2) into $\Pr(\boldsymbol{a}\,|H_k) = \prod_{d=0}^{D-1} \Pr(A_d\,|H_k)$ and apply to (1). Then take the logarithm and cancel common terms. ■

II-B. WSNs with On-Off-Keying Transmission Scheme

Even though (1) has a closed form solution, calculation of the general m-ary probability of error is often complicated. However, there are special cases of interest to DD that do offer tractable solutions. One application is for WSNs under very stringent resource constraint where the sensors employ an on-off-keying (OOK) transmission scheme such that they only transmit when needed, e.g., when their decision is 1. In this case, the only information available at the FC is the observed active sensor count A_1 with $m = D = 2$. This OOK scheme purposefully trades off detection accuracy for a reduction in both transmission power consumption and spectrum usage/interference. Both of which are of importance in CRNs and in general WSNs.

Under the OOK transmission scheme and assuming that the communication link is virtually error free for this ultra low communication scheme, the optimal fusion rule determined in Lemma 1 can be reduced to

$$A_1 \underset{H_0}{\overset{H_1}{\gtrless}} \eta_0, \tag{3}$$

where η_0 is the fusion rule threshold.

III. BYZANTINE ATTACK IN A CRN OF RANDOM SIZE

The remainder of this paper will explore this latter special case of OOK transmission scheme and analyze the collaborate SS performance in CRNs. Specifically, we consider a CRN using parallel collaborative SS to determine if the primary user (PU) is present, say H_1, versus the primary absent, say H_0. When the local observations are conditionally independent, the CRs make their own independent inference regarding H_0 versus H_1 and transmit only $u_j = 1$ when deciding H_1 and make no transmission when deciding H_0 to minimize spectrum interference (i.e. $m = 2$, $D = 2$, with an OOK transmission scheme)

Under the relatively common path loss model [7], the observed signal to noise ratio (SNR) at local sensor j is $h_1(\bar{\boldsymbol{r}}, w_j)\,[\text{dB}] = P_0[\text{dB}] - PL(\bar{r})\,[\text{dB}] + W[\text{dB}]$ and $h_0(\boldsymbol{r}_j, w_j) = W[\text{dB}]$, under H_1 and H_0, respectively, where P_0 is the PU transmission power, $PL(\bar{r})$ the average path loss, $W[\text{dB}]$ a Gaussian noise $W[\text{dB}] \sim \mathcal{N}(0, \sigma^2)$ (i.e. log-normal), and $\bar{\boldsymbol{r}}$ as described in II-A. As a result, the local sensor performance is given by

$$\phi_{0,1} = \bar{p}_{fa} = Q\left(\frac{\eta}{\sigma}\right), \tag{4}$$

$$\phi_{1,1} = \bar{p}_d = Q\left(\frac{\eta - (P_0 - PL(\bar{r}))}{\sigma}\right) \tag{5}$$

based on the local likelihood ratio test (LRT) with an identical threshold η $\forall j$ and $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty \exp\left(-\frac{1}{2}\tau^2\right) d\tau$ is the Gaussian complementary cumulative distribution function.

For CR applications, it is critical for the secondary users to maintain a very low level of spectrum interference against the primary. That is, the probability of spectrum collision has to be held below some constraint β. Putting things into a Neyman-Pearson framework, this is equivalent to requiring the CRN probability of miss, $P_M \leq \beta$ or the detection probability $P_D = 1 - P_M > \beta$, at the fusion center. Similarly, the CRN system level false alarm probability notation is P_{FA}.

As spectrum is highly desirable, in certain cases one or some users may want to gain an unfair advantage over the other users in obtaining access to the spectrum when it is available. In such cases, a Byzantine attack can be made by internal members of the CRN having full knowledge of the collaborative sensing scheme including the local CR sensing rules, FC algorithm, and their respective thresholds [4]. Within a CRN, the goal of the Byzantines is to provide false information to the FC, attempting to make the FC decide the primary is present, when it is in fact absent. With this attack strategy, the Byzantines increase their chances of using the spectrum, relative to the honest CRs in the network.

The security problem we investigate here, at first glance, is very similar to the ones studied in [6], [7]. There are, however, substantial differences in the problem setups such as the network structure and the security problem constraints. The first difference is that we are interested in a CRN with a random number of CRs, which can be described by the proposed Poisson model in Section II. That is, the CRN consists of $\mathcal{C}$ classes of CRs having labels $C_i,\ i = 1, 2, \ldots, \mathcal{C}$ where class C_i has $N_i \sim \text{Poisson}(\lambda_i)$ total CRs. Here, all CRs sharing a common decision rule and subsequent communication strategy are grouped into the same class. This formulation allows some CRs to move between classes by selecting different strategies, as would be the case if Byzantine attackers were attempting to thwart FC Byzantine detection strategies (see [7], [15]). Let $CR_{i,j}$ represent the jth CR in the ith class, where $j =$

$0, 1, \ldots, N_i$. Then the local decision by $CR_{i,j}$ is $u_{i,j} = k$, when the local inference is H_k, $k = 0, 1$. Second, the security problems considered in [6], [7] are mostly 1-shot detection problems, i.e., the malicious users' only goal is to cause the maximum performance degradation in the detection performance for a single round. In practical applications, the malicious user's can be identified based on the CRs historical decisions when spectrum sensing is carried out for many rounds. Upon identification, the suspicious user's decisions can then be removed from the FC decision making and defeat the Byzantine attack. Therefore, in order to perform a lasting attack, it is pivotal that the behavior of the Byzantine CRs is not too different from the honest CRs as they attempt to mask their identities. In short, we focus on an independent Byzantine attack (IBA), where the attackers operate solely on their own decision, and study performance degradation and masking sensitivity when the CRN has reached quasi-equilibrium / steady state. The settings for our security problem is presented as follows.

- The FC has the full knowledge of the CR Byzantine probability, δ, and from its perspective, the decision rules and the performance of the average Byzantine and honest CR.
- Based on the full knowledge of both the malicious and honest CR decision performance, the FC can adjust its decision rule to ensure a CRN probability of miss, $P_M \leq \beta$, where $\beta \in (0, 1)$ defines the maximum acceptable probability of spectrum collision with the primary. Under this and the previous assumption, it is known that the asymptotic detection performance can be measured by the KLD .
- The IBA CRs know the honest CR decision rule, and can select their local decision rules. The number of different decision rules available is finite, constrained by $\mathcal{C}$, the total number of classes available.
- The average IBA CR inference performance is within a certain range of the honest CRs, (e.g. limiting FC sensitivity to IBA presence), to reduce their chance of being identified by the FC. In this paper, we evaluate the sensitivity by the KLD.
- The communication of $u_{i,j}$, when received by the FC, is received error free and only $u_{i,j} = 1$ is transmitted (OOK).

As the communication to the FC by $CR_{i,j}$ is $u_{i,j}$, we define the average local detection probability as $\bar{p}_{d_i} = E_{C_i}\left[\Pr\left\{u_{i,j} = 1 | H_1\right\}\right]$ and false alarm probability as $\bar{p}_{fa_i} = E_{C_i}\left[\Pr\left\{u_{i,j} = 1 | H_0\right\}\right]$, where the expectation is taken across class i. Notice that we have added the subscript i relative to (4) and (5). Throughout, we define C_1 as the honest class and assume that the Byzantines can select any $(\bar{p}_{fa_i}, \bar{p}_{d_i})$ pair on the interior of the upper receiver operating characteristic (ROC) curve defined by $(\bar{p}_{fa_1}, \bar{p}_{d_1})$ obtained by adjusting the threshold η_1 for C_1, and the lower or reciprocal ROC defined by $(1 - \bar{p}_{fa_1}, 1 - \bar{p}_{d_1})$. Both the upper and reciprocal ROC curves define a closed set and appear in Fig. 1. In this manner, the Byzantines are able to select any achievable operating point on this interior that optimizes their attack strategy.

Clearly, under Byzantine attack the FC is unaware of $\mathcal{C}$, $\bar{p}_{d_i}$, and $\bar{p}_{fa_i}$ for some i and cannot apply the optimal Chair-Varshney fusion rule even in equilibrium. Therefore, the FC has to treat the local decision $u_{i,j}$ equally and the optimal fusion rule reduces to a simple counting rule such that

$$\gamma_0 : \sum_{i,j} u_{i,j} = \sum_{i=1}^{\mathcal{C}} A_{i,1} \underset{H_0}{\overset{H_1}{\gtrless}} \eta_0, \tag{6}$$

where $A_{i,1} = \sum_{j=1}^{N_i} (u_{i,j} = 1) \ \forall j \in C_i$.

III-A. Byzantine Attacks: A Performance Analysis

We now analyze the performance of the Byzantine attack from both the viewpoint of the attackers and the FC. Let $\delta \in [0, 1]$ be the probability that a CR in the CRN is a Byzantine attacker. Specifically, if $\lambda = \sum_{i=1}^{\mathcal{C}} \lambda_i$ is the mean number of CRs in the CRN, then

$$\lambda_B = \delta\lambda = \sum_{i \in \mathscr{C}_B} \lambda_i, \tag{7}$$

where λ_B is the mean number of Byzantine CRs, $\mathscr{C}_B$ is an index set for all Byzantine classes $(\mathscr{C}_B = \{i : \forall CR_{i,j} \in C_i,\ P(u_{i,j} = u_{1,j}) \neq 1 \ \forall j\})$, and each λ_i can be chosen arbitrarily subject to (7).

In order to maximize their access to the shared spectrum, the Byzantine attackers desire the FC to infer that the primary is present when in fact they are absent. Define $b_d = E_{\mathscr{C}_B}[\bar{p}_{d_i}]$ as the average quasi-equilibrium detection probability across the Byzantine classes and similarly $b_{fa} = E_{\mathscr{C}_B}[\bar{p}_{fa_i}]$. Then the KLD between the honest and average Byzantine CR is $\mathcal{I}_{fa}(\bar{p}_{fa_1} || b_{fa}) = \bar{p}_{fa_1} \log \frac{\bar{p}_{fa_1}}{b_{fa}} + (1 - \bar{p}_{fa_1}) \log \frac{(1-\bar{p}_{fa_1})}{(1-b_{fa})}$ and similarly for $\mathcal{I}_d(\bar{p}_{d_1} || b_d)$. Thus our sensitivity masking constraint in terms of these KLDs is defined as $\mathcal{I}_{fa} + \mathcal{I}_d \leq \rho$ for an appropriate $\rho > 0$. To maximize their attacking performance, the Byzantine attackers then have the following optimization problem to solve

$$\begin{aligned} &\text{maximize: } P_{FA} \\ &\text{subject to: } \sum_{i \in \mathscr{C}_B} \lambda_i \leq \lambda_B;\ \mathcal{I}_{fa} + \mathcal{I}_d \leq \rho \end{aligned} \tag{8}$$

using the tuple $(\mathcal{C}, \lambda_i, \bar{p}_{fa_i}, \bar{p}_{d_i})$ for all $i \in \mathscr{C}_B$. When the Byzantines achieve $P_{FA} = P_D$ for (8), we will call this fusion center blinding (FCB), as the fusion center cannot make a more informative decision than a random guess.

Next, to shed light on this security problem and illustrate the tradeoff between the performance and robustness, we evaluate the Byzantine attack security problem for a CRN with $\lambda = 50$, $SNR = -2.2$dB corresponding to an honest CR operating point of $(\bar{p}_{fa_1}, \bar{p}_{d_1}) = (0.3, 0.6)$, a Byzantine probability $\delta = 0.45$, and a sensitivity masking threshold $\rho = 0.4$.

Notice that the pairs $(\bar{p}_{fa_1}, \bar{p}_{d_1})$ and (b_{fa}, b_d) define an equivalent $\mathcal{C} = 2$ CRN and that formulation is sufficient to study the performance degradation and sensitivity masking problems from the viewpoint of the FC. Using this sufficient model, the optimization problem in (8) can be depicted graphically. As described previously, Fig. 1 shows the ROC curves obtained by adjusting the threshold η_1 for the honest class. The interior of the upper and reciprocal ROC curves bound the possible values allowed for (b_{fa}, b_d), which in general requires a class decision rule that uses randomization between different LRTs in order to be achieved. The "Honest" label in Fig. 1 highlights the quasi-equilibrium operating point for the honest CRs. Fig. 1 also depicts the constraint $\mathcal{I}_{fa} + \mathcal{I}_d \leq \rho$ and the optimal average attack at the point labeled (b_{fa}, b_d).

While solving (8) is possible for the Byzantines, it is not so straightforward for the FC to analyze in order to understand its sensitivity to an IBA. Certainly, the FC can calculate $P_{FA} = \Pr\left(\sum_{i,j} u_{i,j} > \eta_0 | H_0\right)$ and $P_M = 1 - \Pr\left(\sum_{i,j} u_{i,j} > \eta_0 | H_1\right)$ with the Poisson complementary cumulative distribution function

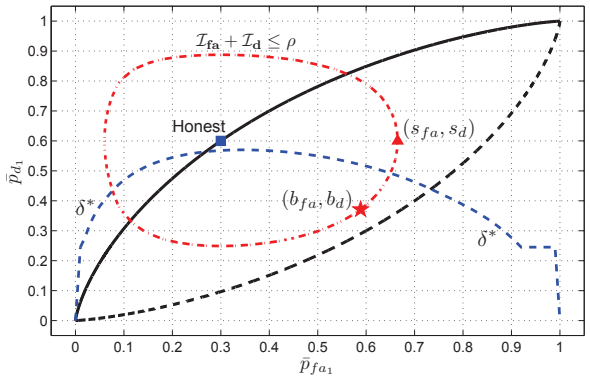

Fig. 1. Local CR ROC Operating Model: $\rho = 0.4$, $\lambda = 50$, $\delta = 0.45$, $(\bar{p}_{fa_1}, \bar{p}_{d_1}) = (0.3, 0.6)$, $(b_{fa}, b_d) = (0.58, 0.36)$, $(s_{fa}, s_d) = (0.67, 0.60)$

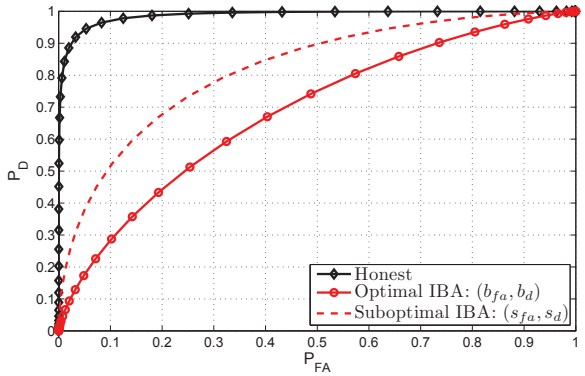

Fig. 2. CRN Byzantine Attack Sensitivity: $\lambda = 50$, $\delta = 0.45$, $(\bar{p}_{fa_1}, \bar{p}_{d_1}) = (0.3, 0.6)$, $(b_{fa}, b_d) = (0.58, 0.36)$, $(s_{fa}, s_d) = (0.67, 0.60)$

(CCDF) and determine sensitivity directly. However, the Poisson CCDF does not have a closed form solution and it is difficult to form equations that offer deeper insight into the problem. An alternative approach is to use the KLD to evaluate the error exponent similar to [6], [7].

Given the constraint such that $P_M \leq \beta$, the exponential rate for P_{FA} with conditionally i.i.d. observations is [7]

$$\lim_{N\to\infty} \frac{\log P_{FA}}{N} = -\mathcal{I}\left(\Pr\left(\sum_{i,j} u_{i,j}|H_1\right) || \Pr\left(\sum_{i,j} u_{i,j}|H_0\right)\right),$$

based on the fusion rule in (6). Thus for N large $P_{FA} \approx 2^{-N\mathcal{I}\left(\Pr\left(\sum_{i,j} u_{i,j}|H_1\right)|| \Pr\left(\sum_{i,j} u_{i,j}|H_0\right)\right)}$, which can be asymptotically maximized by minimizing the KLD. Notice that $\Pr\left(\sum_{i,j} u_{i,j}|H_1\right) \sim$ Poisson $\left(\sum_i \lambda_i \bar{p}_{d_i}\right)$ and similarly under H_0. Let $\lambda_d = \sum_i \lambda_i \bar{p}_{d_i}$ and let $\lambda_f = \sum_i \lambda_i \bar{p}_{fa_i}$. For two Poisson distributions with parameters λ_d and λ_f, the KLD $\mathcal{I}(\lambda_d || \lambda_f)$ between these two distributions is

$$\mathcal{I}(\lambda_d || \lambda_f) = \log e \left(\lambda_d (\log \lambda_d - \log \lambda_f) - (\lambda_d - \lambda_f)\right). \quad (9)$$

Since $\mathcal{I}(\lambda_d || \lambda_f)$ is convex in the pair (λ_d, λ_f) [16], the maximization problem of (8) can be formed as the following convex minimization problem when the solution is on the ROC interior

$$\begin{aligned} &\text{minimize: } \mathcal{I}(\lambda_d || \lambda_f) \quad (10)\\ &\text{subject to: } P_M \leq \beta;\ \sum_{i\in\mathscr{C}_B} \lambda_i \leq \lambda_B;\ \lambda_f \leq \lambda_d;\ \mathcal{I}_{fa} + \mathcal{I}_d \leq \rho, \end{aligned}$$

that is straightforward to solve [17]. Notice that the FC suffers FCB in (10) when $\log \frac{\lambda_d}{\lambda_f} = 1 - \frac{\lambda_f}{\lambda_d}$, with $\lambda_f = \lambda_d$ a solution. Expanding $\lambda_f = \lambda_d$ using $\lambda_1 = (1-\delta)\lambda$ via (7) results in

$$\Sigma_{i=2}^{\mathcal{C}} \lambda_i (\bar{p}_{fa_i} - \bar{p}_{d_i}) = (1-\delta)\lambda (\bar{p}_{d_1} - \bar{p}_{fa_1}), \quad (11)$$

representing a general FCB equation with C_1 the honest class.

As the FC desires to understand its sensitivity to a worst case IBA attack under quasi-equilibrium it is sufficient to use the equivalent (b_{fa}, b_d) and $\mathcal{C} = 2$ model to find a relationship between FCB and δ, which we will define as δ^*. Simplifying (11) and solving

$$\delta^* = \frac{(\bar{p}_{d_1} - \bar{p}_{fa_1})}{(\bar{p}_{d_1} - \bar{p}_{fa_1}) + (b_{fa} - b_d)} \quad (12)$$

so that if $\delta \geq \delta^*$, FCB at the FC is possible. Note that (12) based on a random number of CRs in the CRN is similar to the minimal KLD version derived in [7] for a fixed number of sensors.

We now plot δ^* versus $\bar{p}_{fa_1}$ in Fig. 1 for the associate $(\bar{p}_{fa_1}, \bar{p}_{d_1})$ and (b_{fa}, b_d) parameters defined. The required δ^* changes as a function of $\bar{p}_{fa_1}$ and provides a robust method that the FC can employ to avoid FCB. When the DD system is designed to be less aware of the IBA and operating in a non-robust region, then there are $\delta = \delta^* \leq \frac{1}{2}$ that achieve IBA FCB, which differs relative to [7] since our model allows the Byzantines to pick freely from the set of all possible ROC bounded operating points.

In general, the IBA tries to minimize δ^*, while the FC attempts to maximize it by adjusting $(\bar{p}_{fa_1}, \bar{p}_{d_1})$ and its threshold η_0 to meet $P_M \leq \beta$. This essentially defines the game played between the FC and the IBA attackers. Finally, the optimal attack location, (b_{fa}, b_d), in Fig. 1 was determined by solving (10) using CVX, a package for specifying and solving convex programs [18], [19].

Intuitively, it would seem optimal to select the local Byzantine operating point to be the maximum false alarm rate, say s_{fa} where the s stand for suboptimal, given the $\mathcal{I}_{fa} + \mathcal{I}_d \leq \rho$ constraint. This point is labeled as (s_{fa}, s_d) in Fig. 1. However, (12) implies that the optimal attack occurs when $(b_{fa} - b_d)$ is maximized, which certainly does not occur at (s_{fa}, s_d).

We close with a plot of system level ROC curves generated using P_D versus P_{FA} calculated using the Poisson CCDF function for the IBA described in Fig. 1. These results appear in Fig. 2. The first ROC is the case where all CRs are honest and is the "best achievable" bound. The second curve is an optimal IBA with $\delta = 0.45$. Since $\delta < \delta^*$ (see Fig. 1), FCB is not achieved as expected. The final ROC curve is for the (s_{fa}, s_d) operating point, which is clearly inferior to the optimal (b_{fa}, b_d) strategy.

IV. CONCLUSION

A new distributed detection model was introduced for distributed m-ary hypotheses testing where the local sensors quantize their decisions to D messages and the number of local sensors is random. The model was applied to a CRN and provided a tool to analyze Byzantine attacks, where the attackers randomly changed their strategy using a defined number of classes, under a game theoretical settings. Both the optimal FC and Byzantine strategies were determined as well as the associated tradeoffs between the detection performance and system security against the attacks.

V. REFERENCES

[1] P. K. Varshney, *Distributed Detection and Data Fusion*. Springer, 1997.

[2] S. Kar and J. Moura, "Consensus + innovations distributed inference over networks: cooperation and sensing in networked systems," *Signal Processing Magazine, IEEE*, vol. 30, no. 3, pp. 99–109, May 2013.

[3] E. Axell, G. Leus, E. G. Larsson, and H. V. Poor, "Spectrum sensing for cognitive radio: State-of-the-art and recent advances," *Signal Processing Magazine, IEEE*, vol. 29, no. 3, pp. 101–116, 2012.

[4] A. Vempaty, L. Tong, and P. Varshney, "Distributed inference with byzantine data: State-of-the-art review on data falsification attacks," *Signal Processing Magazine, IEEE*, vol. 30, no. 5, pp. 65–75, 2013.

[5] R. Niu and P. Varshney, "Performance analysis of distributed detection in a random sensor field," *Signal Processing, IEEE Transactions on*, vol. 56, no. 1, pp. 339–349, 2008.

[6] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of byzantine attacks," *Signal Processing, IEEE Transactions on*, vol. 57, no. 1, pp. 16–29, 2009.

[7] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative spectrum sensing in the presence of byzantine attacks in cognitive radio networks," *Signal Processing, IEEE Transactions on*, vol. 59, no. 2, pp. 774–786, 2011.

[8] J. N. Tsitsiklis, "Decentralized detection by a large number of sensors," *Mathematics of Control, Signals, and Systems (MCSS)*, vol. 1, no. 2, pp. 167–182, 1988.

[9] R. Niu and P. Varshney, "Distributed detection and fusion in a large wireless sensor network of random size," *EURASIP Journal on Wireless Communications and Networking*, vol. 2005, no. 4, pp. 462–472, 2005.

[10] D. Reudink, *Microwave Mobile Communications*, W. Jakes, Ed. Wiley-IEEE Press, 1994.

[11] P. Bernardin, M. Yee, and T. Ellis, "Cell radius inaccuracy: a new measure of coverage reliability," *Vehicular Technology, IEEE Transactions on*, vol. 47, no. 4, pp. 1215–1226, 1998.

[12] H. Van Trees, *Detection, Eestimation, and Modulation Theory: Detection, Estimation, and Linear Modulation Theory*. Wiley, 1968.

[13] Y. Sung, L. Tong, and A. Swami, "Asymptotic locally optimal detector for large-scale sensor networks under the poisson regime," *Signal Processing, IEEE Transactions on*, vol. 53, no. 6, pp. 2005–2017, 2005.

[14] G. Casella and R. L. Berger, *Statistical Inference*. Duxbury Press, 2001.

[15] P. Kaligineedi, M. Khabbazian, and V. Bhargava, "Malicious user detection in a cognitive radio cooperative sensing system," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 8, pp. 2488–2497, 2010.

[16] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. John Wiley and Sons, Inc., 1991.

[17] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge Univ Pr, 2004.

[18] M. Grant and S. Boyd, "CVX: Matlab software for disciplined convex programming, version 2.0 beta," http://cvxr.com/cvx, Sep. 2013.

[19] ——, "Graph implementations for nonsmooth convex programs," in *Recent Advances in Learning and Control*, ser. Lecture Notes in Control and Information Sciences, V. Blondel, S. Boyd, and H. Kimura, Eds. Springer-Verlag Limited, 2008, pp. 95–110, http://stanford.edu/ boyd/graph_dcp.html.