On the Effects of Colluded Statistical Attacks in Cooperative Spectrum Sensing

Chung-Kai Yu, Mihir Laghate, Ali H. Sayed, and Danijela Cabric

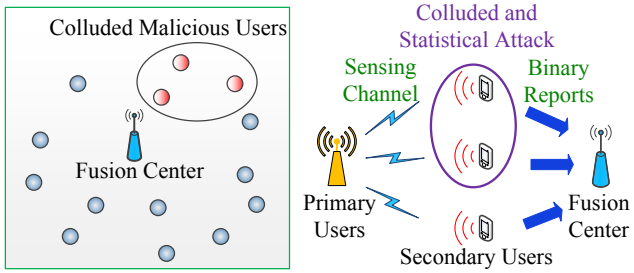
Department of Electrical Engineering
University of California, Los Angeles

***Abstract*—Cooperative spectrum sensing is vulnerable to attacks from malicious nodes, especially when collusion occurs. In this paper, we analyze the effect of colluded statistical attacks and show that collusion could cause performance degradation in terms of both false-alarm and detection probabilities, which is not possible via independent attacks. Closed-form expressions for system performance under the majority fusion rule are provided for a generalized form of colluded attacks. Then, for specific scenarios of collusion and mimicry attacks, we study the conditions under which the probabilities of false alarm and detection are both degraded.**

I. Introduction

Cooperative spectrum sensing has been shown to significantly alleviate hidden terminal and non-ideal channel problems, such as fading and shadowing, by exploiting the diversity of secondary users (SUs) [1]. However, cooperative sensing is vulnerable to attacks when malicious users report false sensing results to achieve their own goals. For example, false reporting that a spectrum is occupied allows malicious SUs to obtain more opportunities to use the spectrum. Previous work in [2] and [3] studied the case of statistically independent attacks and used belief-propagation to counteract the attacks. These investigations considered two types of attacks with different goals, type-1 and type-0, and showed that attackers can either increase the probability of false alarm or decrease the probability of detection, but not both simultaneously. Naturally, more harmful effects are expected when malicious users collude. In this work, we examine some ways by which malicious users can collude and we assess the degradation that their coordinated action can cause. Two types of colluded statistical attacks are considered: intentional collusion and mimicry attacks. For intentional collusion, malicious users share their sensing results, based on which their reports are falsified to attack the system. For mimicry attacks, some selfish users avoid spending power on sensing and instead generate their reports by referring to the reports from other sensors. One of the main results in this paper is that in both types of attacks, malicious users can achieve an operating condition under which they can simultaneously degrade the probabilities of false alarm and detection and more so than in the case of independent attacks.

The work of C.-K. Yu and A. H. Sayed is supported in part by NSF grant CCF-1011918. The work of M. Laghate and D. Cabric is supported in part by the Office of the Director of National Intelligence (ODNI), Intelligence Advanced Research Projects Activity (IARPA), via US Navy (USN) SPAWAR Systems Center Pacific (SSCPac). The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of ODNI, IARPA, USN, SSCPac, or the U.S. Government. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright annotation thereon.
Emails: {ckyuna,mvlaghate,sayed,danijela}@ee.ucla.edu



(a) Spatial illustration (b) Sensing process

Fig. 1: Malicious users collude to attack the system.

In the system model, a centralized cooperative spectrum sensing implementation is considered, in which a data fusion center collects binary-valued sensing reports from the SUs, as illustrated in Fig. 1. If malicious SUs share their sensing results to modify their reports to the fusion center, then some of the sensing reports arriving at the fusion center will contain statistically correlated information. In our examination of the problem, we introduce a set of correlation coefficients to model the colluded sensing. This set is then used to characterize the probability distribution of the SU sensing reports and to assess the degraded performance of the cooperative sensing system.

II. System Model

Consider a cognitive network with N secondary users, also called nodes. We denote the spectrum status by means of a binary variable $\boldsymbol{j} \in \{0, 1\}$, where $\boldsymbol{j} = 0$ means that the spectrum is not occupied and $\boldsymbol{j} = 1$ means that the primary signal is present.[1] Each node k receives signals $\boldsymbol{z}_k(t)$ at each discrete time instant t such that

$$\boldsymbol{z}_k(t) = \boldsymbol{j} \cdot \boldsymbol{h}(t)\boldsymbol{s}(t) + \boldsymbol{n}_k(t) \tag{1}$$

where $\boldsymbol{n}_k(t)$ is noise, $\boldsymbol{s}(t)$ is the primary signal, and $\boldsymbol{h}(t)$ is the channel gain summarizing the fading and path-loss effects.

[1] We will use boldface letters for random variables.

In this paper, we assume the nodes use a collection of data, $\{\boldsymbol{z}_k(t)\}_{t=1}^{T}$, to detect $\boldsymbol{j}$ by means of energy detection as follows. Let the local decision of node k be $\boldsymbol{u}_k$, where $\boldsymbol{u}_k = 1$ refers to the decision that the spectrum is occupied and $\boldsymbol{u}_k = 0$ refers to the noise only case. Each node k determines $\boldsymbol{u}_k$ based on a threshold η [4], [5] such that

$$\boldsymbol{u}_k = \begin{cases} 0, & \text{if } \sum_{t=1}^{T} |\boldsymbol{z}_k(t)|^2 \le \eta \\ 1, & \text{otherwise} \end{cases} \tag{2}$$

We assume the local decisions $\{\boldsymbol{u}_k\}$ are spatially independent among all nodes.

After sensing the spectrum, nodes report the sensing results to the fusion center for evaluation. We denote the sensing reports by the binary variables $\boldsymbol{y}_k \in \{1, 0\}$. We assume there exist some malicious nodes that alter the sensing results with some non-zero probability, i.e., for which $P\{\boldsymbol{y}_k = \boldsymbol{u}_k\} < 1$. Furthermore, the malicious nodes could collude with each other to achieve a more harmful attack. In this case, the sensing reports become correlated. Generally, we can represent the colluded statistical attack by a finite set of correlation coefficients[2] defined as follows:

$$C_y = \left\{ \mathbb{E}_j \left[\prod_{k\in\mathcal{I}} \boldsymbol{y}_k \right] : \mathcal{I} \subseteq \mathcal{N}, \mathcal{I} \neq \varnothing, j = 0, 1 \right\} \tag{3}$$

where $\mathcal{N} \triangleq \{1, ..., N\}$ and $\mathbb{E}_j[\cdot] \triangleq \mathbb{E}[\,\cdot\,|\boldsymbol{j} = j]$. For convenience, we define $\mathbb{E}_j\left[\prod_{k\in\mathcal{I}} \boldsymbol{y}_k\right] = 1$ if $\mathcal{I}$ is an empty set. From the property $\boldsymbol{y}_k \in \{0, 1\}$, we have

$$\mathbb{E}_j \left[\prod_{k\in\mathcal{I}} \boldsymbol{y}_k \right] = P_j(\boldsymbol{y}_{k_1} = 1, ..., \boldsymbol{y}_{k_n} = 1) \tag{4}$$

where $\mathcal{I} = \{k_1, k_2, ..., k_n\} \subseteq \mathcal{N}$ and $P_j(\cdot) \triangleq P(\,\cdot\,|\boldsymbol{j} = j)$ for $j = 0, 1$. The joint probability density function of $(\boldsymbol{y}_{k_1}, \boldsymbol{y}_{k_2}, ..., \boldsymbol{y}_{k_n})$ is known to be [6]:

$$P_j(\boldsymbol{y}_{k_1}, \boldsymbol{y}_{k_2}, ..., \boldsymbol{y}_{k_n}) = \sum_{\mathcal{S}\subseteq\mathcal{B}_0} (-1)^{|\mathcal{S}|} \mathbb{E}_j \left[\prod_{k\in\mathcal{B}_1\cup\mathcal{S}} \boldsymbol{y}_k \right] \tag{5}$$

where $\mathcal{B}_0 = \{k_i : \boldsymbol{y}_{k_i} = 0, 1 \le i \le n\}$ is the set of nodes that report 0 and $\mathcal{B}_1 = \{k_i : \boldsymbol{y}_{k_i} = 1, 1 \le i \le n\}$ is the set of nodes that report 1. The notation $\sum_{\mathcal{X}\subseteq\mathcal{Y}}$ means sum over all subsets $\mathcal{X}$ of the set $\mathcal{Y}$.

It is noted that the sensing reports $\{\boldsymbol{y}_{k_i}\}_{k_i\in I}$ will be mutually independent when $P_j(\boldsymbol{y}_{k_1}, \boldsymbol{y}_{k_2}, ..., \boldsymbol{y}_{k_n}) = \prod_{k\in\mathcal{I}} P_j(\boldsymbol{y}_k)$ for both $j = 0$ and 1. A necessary and sufficient condition for this to hold is provided in [6]:

$$\mathbb{E}_j \left[\prod_{k\in\mathcal{I}} \boldsymbol{y}_k \right] = \prod_{k\in\mathcal{I}} \mathbb{E}_j[\boldsymbol{y}_k] \tag{6}$$

which can be derived from (5).

[2]The correlation coefficients defined in this paper are the expectation of products of random variables, which are different from the conventional definition used in probability theory.

III. Detection Performance for Majority Rule

To characterize system performance, we consider the majority rule because of its simplicity and robustness when most nodes are honest [7]. Therefore, the fusion center adopts the following decision rule to detect the spectrum status:

$$\hat{h}_{\text{maj}} = \begin{cases} 1, & \text{if } \sum_{k=1}^{N} \boldsymbol{y}_k > N/2 \\ 0, & \text{if } \sum_{k=1}^{N} \boldsymbol{y}_k < N/2 \\ 1 \text{ or } 0 \text{ w.p. } 1/2, & \text{if } \sum_{k=1}^{N} \boldsymbol{y}_k = N/2 \end{cases} \tag{7}$$

The false-alarm and detection probabilities are defined as

$$P_{\text{fa}} \triangleq P_0(\hat{h}_{\text{maj}} = 1), \quad P_{\text{d}} \triangleq P_1(\hat{h}_{\text{maj}} = 1) \tag{8}$$

These probabilities can be expressed in terms of the correlation coefficients C_y as follows.

Lemma 1. *For an odd $N = 2w - 1$ where w is a positive integer, the false-alarm and detection probabilities of (8) are given by:*

$$P_{\text{fa}}^{\text{odd}} = \sum_{p=w}^{N} \left(\sum_{\mathcal{S}_p\subseteq\mathcal{N}} \mathbb{E}_0 \left[\prod_{k\in\mathcal{S}_p} \boldsymbol{y}_k \right] \sum_{i=0}^{p-w} (-1)^i \binom{p}{i} \right) \tag{9}$$

$$P_{\text{d}}^{\text{odd}} = \sum_{p=w}^{N} \left(\sum_{\mathcal{S}_p\subseteq\mathcal{N}} \mathbb{E}_1 \left[\prod_{k\in\mathcal{S}_p} \boldsymbol{y}_k \right] \sum_{i=0}^{p-w} (-1)^i \binom{p}{i} \right) \tag{10}$$

where $|\mathcal{S}_p| = p \ge 0$. On the other hand, for an even $N = 2w$, the false-alarm and detection probabilities of (8) are given by:

$$P_{\text{fa}}^{\text{even}} = \sum_{p=w}^{N-1} \left(\sum_{\mathcal{S}_p\subseteq\mathcal{N}} \mathbb{E}_0 \left[\prod_{k\in\mathcal{S}_p} \boldsymbol{y}_k \right] \left[\sum_{i=0}^{p-w} (-1)^i \binom{p}{i} - \frac{(-1)^{p-w}}{2} \binom{p}{w} \right] \right) \tag{11}$$

$$P_{\text{d}}^{\text{even}} = \sum_{p=w}^{N-1} \left(\sum_{\mathcal{S}_p\subseteq\mathcal{N}} \mathbb{E}_1 \left[\prod_{k\in\mathcal{S}_p} \boldsymbol{y}_k \right] \left[\sum_{i=0}^{p-w} (-1)^i \binom{p}{i} - \frac{(-1)^{p-w}}{2} \binom{p}{w} \right] \right) \tag{12}$$

Proof: Using (5) and denoting by $\mathcal{B}_1(p)$ as the set with p nodes reporting 1, we can write $P_{\text{fa}}^{\text{odd}}$ as

$$\begin{aligned} P_{\text{fa}}^{\text{odd}} &= \sum_{p=w}^{N} \sum_{\mathcal{B}_1(p)\subseteq\mathcal{N}} \sum_{\mathcal{S}\subseteq\mathcal{B}_0} (-1)^{|\mathcal{S}|} \mathbb{E}_0 \left[\prod_{k\in\mathcal{B}_1(p)\cup\mathcal{S}} \boldsymbol{y}_k \right] \\ &= \sum_{p=w}^{N} \sum_{\mathcal{B}_1(p)\subseteq\mathcal{N}} \mathbb{E}_0 \left[\prod_{k\in\mathcal{B}_1(p)} \boldsymbol{y}_k \right] \sum_{i=0}^{p-w} (-1)^i \binom{p}{i} \end{aligned} \tag{13}$$

The second equality comes from collecting all common terms with $\mathbb{E}_0[\prod_{k\in\mathcal{B}_1(p)} \boldsymbol{y}_k]$, and summing their respective coefficients. The same argument applies to $P_{\text{d}}^{\text{odd}}$ except for changing $\mathbb{E}_0$ into $\mathbb{E}_1$.

When N is even, we need to subtract the probability that half of the nodes report one and the other half report zero. Therefore, starting from the definition (5), we can collect all

common terms with $\mathbb{E}_0[\prod_{k\in\mathcal{B}_1(p)} \boldsymbol{y}_k]$ and sum the coefficients:

$$\begin{aligned}
P_{\text{fa}}^{\text{even}} &= \sum_{p=w}^{N} \sum_{\mathcal{B}_1(p)\subseteq\mathcal{N}} \sum_{\mathcal{S}\subseteq\mathcal{B}_0} (-1)^{|\mathcal{S}|}\mathbb{E}_0\left[\prod_{k\in\mathcal{B}_1(p)\cup\mathcal{S}} \boldsymbol{y}_k\right] \\
&\quad - \frac{1}{2}\sum_{\mathcal{B}_1(w)\subseteq\mathcal{N}} \sum_{\mathcal{S}\subseteq\mathcal{B}_0} (-1)^{|\mathcal{S}|}\mathbb{E}_0\left[\prod_{k\in\mathcal{B}_1(w)\cup\mathcal{S}} \boldsymbol{y}_k\right] \\
&= \sum_{p=w}^{N} \sum_{\mathcal{B}_1(p)\subseteq\mathcal{N}} \mathbb{E}_0\left[\prod_{k\in\mathcal{B}_1(p)} \boldsymbol{y}_k\right] \sum_{i=0}^{p-w}(-1)^i\binom{p}{i} \\
&\quad - \frac{1}{2}\sum_{\mathcal{B}_1(w)\subseteq\mathcal{N}} \mathbb{E}_0\left[\prod_{k\in\mathcal{B}_1(p)} \boldsymbol{y}_k\right] \\
&= \sum_{p=w}^{N-1} \sum_{\mathcal{S}_p\subseteq\mathcal{N}} \mathbb{E}_0\left[\prod_{k\in\mathcal{S}_p} \boldsymbol{y}_k\right]\left[\sum_{i=0}^{p-w}(-1)^i\binom{p}{i} - \frac{(-1)^{p-w}}{2}\binom{p}{w}\right]
\end{aligned}$$

Changing $\mathbb{E}_0$ into $\mathbb{E}_1$, we can similarly obtain $P_{\text{d}}^{\text{even}}$. ∎

We remark that Lemma 1 holds for correlated local decisions $\{\boldsymbol{u}_k\}$ since the proof only depends on C_y.

IV. Attacks through Collusion and Mimicry

In this section, we consider two kinds of malicious behavior with correlated sensing reports that degrade the system performance: intentionally colluded attacks and mimicry attacks.

A. Case Study: Two Correlated Nodes

Let us begin our exploration by assuming there is a pair of colluded nodes, say, nodes 1 and 2. The other nodes are assumed to sense and report independently. That is, we have $\mathbb{E}_j[\boldsymbol{y}_1\boldsymbol{y}_2] \neq \mathbb{E}_j[\boldsymbol{y}_1]\mathbb{E}_j[\boldsymbol{y}_2]$ and $\mathbb{E}_j[\prod_{k\in\mathcal{I}} \boldsymbol{y}_k] = \prod_{k\in\mathcal{I}} \mathbb{E}_j[\boldsymbol{y}_k]$ for any subset $\mathcal{I} \subseteq \{3, ..., N\}$.

For an even $N = 2w$, the false-alarm probability $P_{\text{fa}}^{\text{even}}$ can then be computed as

$$\begin{aligned}
P_{\text{fa}}^{\text{even}} &= \frac{1}{2}P_0\left\{\sum_{k=1}^{N} \boldsymbol{y}_k = w\right\} + P_0\left\{\sum_{k=1}^{N} \boldsymbol{y}_k > w\right\} \\
&= \frac{1}{2}\left[\sum_{l=0}^{2} P_0\{\boldsymbol{y}_1 + \boldsymbol{y}_2 = l\}P_0\left\{\sum_{k=3}^{N} \boldsymbol{y}_k = w - l\right\}\right] \\
&\quad + \sum_{i=w+1}^{N}\sum_{l=0}^{2}\left[P_0\{\boldsymbol{y}_1 + \boldsymbol{y}_2 = l\}P_0\left\{\sum_{k=3}^{N} \boldsymbol{y}_k = i - l\right\}\right] \\
&= \sum_{l=0}^{2} P_0\{\boldsymbol{y}_1 + \boldsymbol{y}_2 = l\}\left[\frac{1}{2}P_0\left\{\sum_{k=3}^{N} \boldsymbol{y}_k = w - l\right\}\right. \\
&\qquad \left. + \sum_{i=w+1}^{N} P_0\left\{\sum_{k=3}^{N} \boldsymbol{y}_k = i - l\right\}\right] \quad (14)
\end{aligned}$$

For comparison purposes, we consider another situation where all sensing reports (including those by nodes 1 and 2) are independent. We denote the independent sensing reports of nodes 1 and 2 in this case by $\boldsymbol{y}_1^{\text{ind}}$ and $\boldsymbol{y}_2^{\text{ind}}$, respectively. Suppose we constrain the probabilities that nodes 1 and 2 attack the system in both cases in order to compare them under similar conditions:

$$r_1 = P(\boldsymbol{y}_1 = 1|\boldsymbol{u}_1 = 0) = P(\boldsymbol{y}_1^{\text{ind}} = 1|\boldsymbol{u}_1 = 0) \quad (15)$$

$$r_2 = P(\boldsymbol{y}_2 = 1|\boldsymbol{u}_2 = 0) = P(\boldsymbol{y}_2^{\text{ind}} = 1|\boldsymbol{u}_2 = 0) \quad (16)$$

We illustrate the analysis for the case of even N and then list the result for odd N as well.

The false-alarm probability with $\boldsymbol{y}_1^{\text{ind}}$ and $\boldsymbol{y}_2^{\text{ind}}$ is denoted by $P_{\text{fa}}^{\text{ind}}$. Using (14), the difference between independent and colluded attacks is

$$\begin{aligned}
&\triangle P_{\text{fa}}^{\text{even}} \triangleq P_{\text{fa}}^{\text{even}} - P_{\text{fa}}^{\text{ind}} \\
&= \sum_{l=0}^{2}\left(\left[P_0\{\boldsymbol{y}_1 + \boldsymbol{y}_2 = l\} - P_0\{\boldsymbol{y}_1^{\text{ind}} + \boldsymbol{y}_2^{\text{ind}} = l\}\right]\right. \\
&\qquad \left.\cdot\left[\frac{1}{2}P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w - l\Big\} + \sum_{j=w+1}^{N} P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = j - l\Big\}\right]\right) \quad (17)
\end{aligned}$$

We denote

$$\Delta\mathbb{E}_j[\boldsymbol{y}_k] \triangleq \mathbb{E}_j[\boldsymbol{y}_k] - \mathbb{E}_j[\boldsymbol{y}_k^{\text{ind}}] \quad (18)$$

$$\Delta\mathbb{E}_j[\boldsymbol{y}_1\boldsymbol{y}_2] \triangleq \mathbb{E}_j[\boldsymbol{y}_1\boldsymbol{y}_2] - \mathbb{E}_j[\boldsymbol{y}_1^{\text{ind}}]\mathbb{E}_j[\boldsymbol{y}_2^{\text{ind}}] \quad (19)$$

for $j = 0$ and 1. From (5), we know that

$$\begin{aligned}
&P_0(\boldsymbol{y}_1 + \boldsymbol{y}_2 = 0) - P_0(\boldsymbol{y}_1^{\text{ind}} + \boldsymbol{y}_2^{\text{ind}} = 0) \\
&\quad = -(\Delta\mathbb{E}_0[\boldsymbol{y}_1] + \Delta\mathbb{E}_0[\boldsymbol{y}_2]) + \Delta\mathbb{E}_j[\boldsymbol{y}_1\boldsymbol{y}_2] \quad (20) \\
&P_0(\boldsymbol{y}_1 + \boldsymbol{y}_2 = 1) - P_0(\boldsymbol{y}_1^{\text{ind}} + \boldsymbol{y}_2^{\text{ind}} = 1) \\
&\quad = \Delta\mathbb{E}_0[\boldsymbol{y}_1] + \Delta\mathbb{E}_0[\boldsymbol{y}_2] - 2\Delta\mathbb{E}_j[\boldsymbol{y}_1\boldsymbol{y}_2] \quad (21) \\
&P_0(\boldsymbol{y}_1 + \boldsymbol{y}_2 = 2) - P_0(\boldsymbol{y}_1^{\text{ind}} + \boldsymbol{y}_2^{\text{ind}} = 2) = \Delta\mathbb{E}_j[\boldsymbol{y}_1\boldsymbol{y}_2] \quad (22)
\end{aligned}$$

Then, $\triangle P_{\text{fa}}^{\text{even}}$ becomes

$$\begin{aligned}
\triangle P_{\text{fa}}^{\text{even}} &= \frac{1}{2}\Delta\mathbb{E}_0[\boldsymbol{y}_1\boldsymbol{y}_2]\Big[P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w - 2\Big\} - P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w\Big\}\Big] \\
&\quad + \frac{1}{2}\left(\Delta\mathbb{E}_0[\boldsymbol{y}_1] + \Delta\mathbb{E}_0[\boldsymbol{y}_2]\right) \\
&\qquad \cdot\left[P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w - 1\Big\} + P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w\Big\}\right] \quad (23)
\end{aligned}$$

To simplify the analysis of (23), we assume that each independent node's report has the same mean distribution, i.e., $\mu_0 \triangleq \mathbb{E}_0[\boldsymbol{y}_k]$ for $k = 3$ to N. This is satisfied if each independent node has the same attack probability $P\{\boldsymbol{y}_k \neq \boldsymbol{u}_k\}$. In this situation, we have

$$\begin{aligned}
&P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w - 2\Big\} - P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w\Big\} \\
&\qquad = \binom{N-2}{w}\mu_0^{w-2}(1-\mu_0)^{w-2}(1-2\mu_0) \quad (24) \\
&P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w - 1\Big\} + P_0\Big\{\sum_{k=3}^{N} \boldsymbol{y}_k = w\Big\} \\
&\qquad = \binom{N-2}{w-1}\mu_0^{w-1}(1-\mu_0)^{w-2}\left(1 - \frac{\mu_0}{w}\right) \quad (25)
\end{aligned}$$

Therefore, $\triangle P_{\text{fa}}^{\text{even}}$ can be rewritten as

$$\begin{aligned}
\triangle P_{\text{fa}}^{\text{even}} &= \frac{1}{2w}\binom{N-2}{w-1}\mu_0^{w-2}(1-\mu_0)^{w-2} \\
&\quad \cdot\left[\left(\Delta\mathbb{E}_0[\boldsymbol{y}_1] + \Delta\mathbb{E}_0[\boldsymbol{y}_2]\right)\mu_0(w-\mu_0)\right. \\
&\qquad \left. + \Delta\mathbb{E}_0[\boldsymbol{y}_1\boldsymbol{y}_2](1-2\mu_0)(w-1)\right] \quad (26)
\end{aligned}$$

TABLE I: Parameters for intentionally colluded attacks by two nodes.

$(\boldsymbol{u}_1, \boldsymbol{u}_2)$	(0,0)	(0,1)	(1,0)	(1,1)
$P(\boldsymbol{y}_1 = 0 \mid \boldsymbol{u}_1, \boldsymbol{u}_2)$	$1-\alpha_1$	$1 - \frac{r_1 P(\boldsymbol{u}_1=0) - \alpha_1 P(\boldsymbol{u}_1=0, \boldsymbol{u}_2=0)}{P(\boldsymbol{u}_1=0, \boldsymbol{u}_2=1)}$	0	0
$P(\boldsymbol{y}_2 = 0 \mid \boldsymbol{u}_1, \boldsymbol{u}_2)$	$1-\alpha_2$	0	$1 - \frac{r_2 P(\boldsymbol{u}_1=0) - \alpha_2 P(\boldsymbol{u}_1=0, \boldsymbol{u}_2=0)}{P(\boldsymbol{u}_1=1, \boldsymbol{u}_2=0)}$	0
$P(\boldsymbol{y}_1 = 1 \mid \boldsymbol{u}_1, \boldsymbol{u}_2)$	α_1	$\beta_1 = \frac{r_1 P(\boldsymbol{u}_1=0) - \alpha_1 P(\boldsymbol{u}_1=0, \boldsymbol{u}_2=0)}{P(\boldsymbol{u}_1=0, \boldsymbol{u}_2=1)}$	1	1
$P(\boldsymbol{y}_2 = 1 \mid \boldsymbol{u}_1, \boldsymbol{u}_2)$	α_2	1	$\beta_2 = \frac{r_2 P(\boldsymbol{u}_1=0) - \alpha_2 P(\boldsymbol{u}_1=0, \boldsymbol{u}_2=0)}{P(\boldsymbol{u}_1=1, \boldsymbol{u}_2=0)}$	1

Similarly, $\triangle P_{\mathrm{d}}^{\mathrm{even}} \triangleq P_{\mathrm{d}}^{\mathrm{even}} - P_{\mathrm{d}}^{\mathrm{ind}}$ can be obtained as

$$\begin{aligned}\triangle P_{\mathrm{d}}^{\mathrm{even}} = \frac{1}{2w}\binom{2w-2}{w-1}\mu_1^{w-2}(1-\mu_1)^{w-2} \\ \cdot \left[\left(\Delta\mathbb{E}_1[\boldsymbol{y}_1] + \Delta\mathbb{E}_1[\boldsymbol{y}_2]\right)\mu_1(w-\mu_1)\right. \\ \left. +\Delta\mathbb{E}_1[\boldsymbol{y}_1\boldsymbol{y}_2](1-2\mu_1)(w-1)\right] \end{aligned} \quad (27)$$

where $\mu_1 \triangleq \mathbb{E}_1[\boldsymbol{y}_k]$ for $3 \le k \le N$. For odd N, we get:

$$\begin{aligned}\triangle P_{\mathrm{fa}}^{\mathrm{odd}} = \binom{N-2}{w-1}\mu_0^{w-2}(1-\mu_0)^{w-1}\Big\{ \left(\Delta\mathbb{E}_0[\boldsymbol{y}_1] + \Delta\mathbb{E}_0[\boldsymbol{y}_2]\right)(1-\mu_0) \\ + \Delta\mathbb{E}_0[\boldsymbol{y}_1\boldsymbol{y}_2]\Big[\frac{(1-\mu_0)}{w} - (1-2\mu_0)\Big]\Big\}\end{aligned}$$

$$\begin{aligned}\triangle P_{\mathrm{d}}^{\mathrm{odd}} = \binom{N-2}{w-1}\mu_1^{w-2}(1-\mu_1)^{w-1}\Big\{ \Big(\Delta\mathbb{E}_1[\boldsymbol{y}_1] + \Delta\mathbb{E}_1[\boldsymbol{y}_2]\Big)(1-\mu_1) \\ + \Delta\mathbb{E}_1[\boldsymbol{y}_1\boldsymbol{y}_2]\Big[\frac{(1-\mu_1)}{w} - (1-2\mu_1)\Big]\Big\}\end{aligned}$$

B. Intentionally Colluded Attacks

Based on the above model, we now describe a collusion strategy in which malicious users share their raw local decisions $\{\boldsymbol{u}_k\}$ to generate correlated sensing reports. Nodes are classified into honest users, type-1 attackers, and type-0 attackers, where a variable r_k is used to describe the reporting behavior of node k. If node k is honest, we have $\boldsymbol{u}_k = \boldsymbol{y}_k$ and $r_k = 0$. For a type-1 attacker, the malicious node k alters the sensing reports as follows:

$$P(\boldsymbol{y}_k = 1 \mid \boldsymbol{u}_k = 0) = r_k, \;\; P(\boldsymbol{y}_k = 1 \mid \boldsymbol{u}_k = 1) = 1 \quad (28)$$

For a type-0 attacker, the attack probabilities become

$$P(\boldsymbol{y}_k = 0 \mid \boldsymbol{u}_k = 1) = r_k, \;\; P(\boldsymbol{y}_k = 0 \mid \boldsymbol{u}_k = 0) = 1 \quad (29)$$

Let us consider the collusion of two type-1 nodes 1 and 2. The results for type-0 attackers can be obtained similarly. The behavior of the type-1 attackers can be described by two probabilities:

$$\alpha_1 \triangleq P(\boldsymbol{y}_1 = 1 \mid \boldsymbol{u}_1 = 0, \boldsymbol{u}_2 = 0), \alpha_2 \triangleq P(\boldsymbol{y}_2 = 1 \mid \boldsymbol{u}_1 = 0, \boldsymbol{u}_2 = 0)$$

For convenience, we define

$$\beta_1 \triangleq P(\boldsymbol{y}_1 = 1 \mid \boldsymbol{u}_1 = 0, \boldsymbol{u}_2 = 1) \quad (30)$$

$$\beta_2 \triangleq P(\boldsymbol{y}_2 = 1 \mid \boldsymbol{u}_1 = 1, \boldsymbol{u}_2 = 0) \quad (31)$$

The conditional distribution of $\boldsymbol{y}_1$ and $\boldsymbol{y}_2$ is listed in Table I. In the following lemma, we describe the conditions under which collusion increases $P_{\mathrm{fa}}^{\mathrm{even}}$ and reduces $P_{\mathrm{d}}^{\mathrm{even}}$ simultaneously. Note that, as shown in [2], this is not possible if all attackers behave independently.

Lemma 2. *For the system described above, assume that nodes have sensing statistics $\mathbb{E}_j[\boldsymbol{u}_k] = \epsilon_j$ for all $k \in \mathcal{N}$ and $\mathbb{E}_j[\boldsymbol{y}_k] = \mu_j$ for all $k \in \mathcal{N}\backslash\{1,2\}$. Then, the following conditions ensure that collusion simultaneously increases the false alarm probability and decreases the detection probability of the system, i.e., $\triangle P_{\mathrm{fa}}^{\mathrm{even}} > 0$ and $\triangle P_{\mathrm{d}}^{\mathrm{even}} < 0$:*

$$\mu_0 < 1/2, \qquad \mu_1 > 1/2, \qquad \alpha_1 + \alpha_2 > r_1 + r_2, \quad (32)$$

$$(\alpha_1 - z)(\alpha_2 - z) > (r_1 - z)(r_2 - z) \quad (33)$$

where $z = \max\{z_0, z_1\}$ and

$$\begin{aligned} z_0 &= \frac{1-\mathbb{E}[\boldsymbol{u}_1]}{\mathbb{E}[\boldsymbol{u}_1]} \cdot \frac{\epsilon_0}{1-\epsilon_0} \\ &\quad - \frac{1}{2} \cdot \frac{\mu_0}{1-2\mu_0} \cdot \frac{w-\mu_0}{w-1} \cdot \frac{\epsilon_1 - \epsilon_0}{P(\boldsymbol{u}_1 = 0, \boldsymbol{u}_2 = 1)} \cdot \frac{1-\epsilon_0}{1-\epsilon_1} \\ z_1 &= \frac{1-\mathbb{E}[\boldsymbol{u}_1]}{\mathbb{E}[\boldsymbol{u}_1]} \cdot \frac{\epsilon_1}{1-\epsilon_1} \\ &\quad - \frac{1}{2} \cdot \frac{\mu_1}{2\mu_1 - 1} \cdot \frac{w-\mu_1}{w-1} \cdot \frac{\epsilon_1 - \epsilon_0}{P(\boldsymbol{u}_1 = 0, \boldsymbol{u}_2 = 1)} \cdot \frac{1-\epsilon_1}{1-\epsilon_0} \end{aligned}$$

Proof: Using (26) and (32), we have $\triangle P_{\mathrm{fa}}^{\mathrm{even}} > 0$ if

$$\frac{\Delta\mathbb{E}_0[\boldsymbol{y}_1\boldsymbol{y}_2]}{\Delta\mathbb{E}_0[\boldsymbol{y}_1] + \Delta\mathbb{E}_0[\boldsymbol{y}_2]} > -\frac{\mu_0(w-\mu_0)}{(1-2\mu_0)(w-1)}$$

Using Table I, we can evaluate the terms on the LHS:

$$\begin{aligned}\Delta\mathbb{E}_0[\boldsymbol{y}_1\boldsymbol{y}_2] &= (\alpha_1\alpha_2 - r_1 r_2)(1-\epsilon_0)^2 \\ &\quad + (r_1 + r_2 - \alpha_1 - \alpha_2)\frac{1-\mathbb{E}[\boldsymbol{u}_1]}{\mathbb{E}[\boldsymbol{u}_1]}\epsilon_0(1-\epsilon_0) \end{aligned} \quad (34)$$

$$\begin{aligned}&\Delta\mathbb{E}_0[\boldsymbol{y}_1] + \Delta\mathbb{E}_0[\boldsymbol{y}_2] \\ &\quad = \frac{(1-\epsilon_0)(1-\epsilon_1)(\epsilon_1 - \epsilon_0)}{\epsilon_0(1-\epsilon_0) + \epsilon_1(1-\epsilon_1)}(\alpha_1 + \alpha_2 - r_1 - r_2) \end{aligned} \quad (35)$$

Substituting (34) and (35) into the above inequality and rearranging terms gives:

$$\frac{\alpha_1\alpha_2 - r_1 r_2}{\alpha_1 + \alpha_2 - r_1 - r_2} > z_0 \quad (36)$$

Similarly, using (27) gives

$$\triangle P_{\mathrm{d}}^{\mathrm{even}} < 0 \text{ if } \frac{\alpha_1\alpha_2 - r_1 r_2}{\alpha_1 + \alpha_2 - r_1 - r_2} > z_1 \quad (37)$$

Combining (36) and (37), and defining $z = \max\{z_0, z_1\}$, we arrive at the required condition (33). ∎

C. Mimicry Attacks

In mimicry attacks, a malicious node does not sense the spectrum on its own, e.g., to save power. Instead, it spies on the sensing reports of other node(s), and generates its own report by randomizing the report of the victim. In the computer security literature, this behavior is associated with malicious users pretending to be normal users [8], [9].

Assume that node 1 is an attacker spying on node 2. The malicious node 1 randomizes its report in a manner similar to the type-1 attack defined by (28). We define the conditional probability of the sensing report $\boldsymbol{y}_1$ as

$$m_1 \triangleq P(\boldsymbol{y}_1 = 1|\boldsymbol{y}_2 = 0),\ P(\boldsymbol{y}_1 = 1|\boldsymbol{y}_2 = 1) = 1 \qquad (38)$$

The following lemma provides the conditions under which the mimicry attacks cause more harm to the system than in the case of independent attacks.

Lemma 3. *For the system described above, consider* $\mathbb{E}_j[\boldsymbol{y}_k] = \mu_j$ *for all* $k \in \mathcal{N}\backslash\{1\}$. *The false-alarm probability increases and the detection probability decreases simultaneously if*

$$m_1 < \frac{(2\mu_1 - 1)(w-1)}{w - \mu_1},\quad \mu_0 < 1/2,\quad \mu_1 > 1/2 \qquad (39)$$

Proof: We can express $\mathbb{E}_0[\boldsymbol{y}_1] = m_1(1 - \mathbb{E}_0[\boldsymbol{y}_2]) + \mathbb{E}_0[\boldsymbol{y}_2]$ and $\mathbb{E}_0[\boldsymbol{y}_1\boldsymbol{y}_2] = \mathbb{E}_0[\boldsymbol{y}_2]$. Then, $\Delta\mathbb{E}_0[\boldsymbol{y}_1\boldsymbol{y}_2] = \mathbb{E}_0[\boldsymbol{y}_2](1 - \mathbb{E}_0[\boldsymbol{y}_2])$, $\Delta\mathbb{E}_0[\boldsymbol{y}_1] = m_1(1 - \mathbb{E}_0[\boldsymbol{y}_2])$ and $\Delta\mathbb{E}_0[\boldsymbol{y}_2] = 0$. Expression (26) then gives the linear dependence of $\triangle P_{\text{fa}}^{\text{even}}$ on m_1:

$$\triangle P_{\text{fa}}^{\text{even}} = \binom{N-2}{w-1}\frac{[\mu_0(1-\mu_0)]^{w-1}}{2w}\left[(1-2\mu_0)(w-1) + m_1(w-\mu_0)\right]$$

Since $\mu_0 < 1/2$, $(1-2\mu_0)(w-1) + m_1(w-\mu_0) > 0$ for all m_1. Therefore $\triangle P_{\text{fa}}^{\text{even}} > 0$ always.

Similar computation on (27) gives the relation

$$\triangle P_{\text{d}}^{\text{even}} = \binom{N-2}{w-1}\frac{[\mu_1(1-\mu_1)]^{w-1}}{2w}\left[(1-2\mu_1)(w-1) + m_1(w-\mu_1)\right]$$

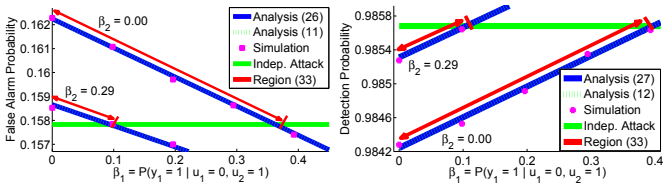
and, hence,

$$m_1 < \frac{(2\mu_1 - 1)(w-1)}{w - \mu_1} \ \Rightarrow\ \triangle P_{\text{d}}^{\text{even}} < 0 \qquad \blacksquare$$

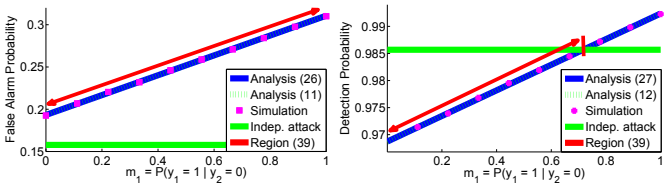
V. Simulation Results

In simulations, we consider a network with $N = 6$ nodes where nodes 1 and 2 are correlated and the remaining nodes behave independently. For intentional collusion of type-1 malicious users 1 and 2, the false-alarm and detection probabilities are simulated and compared to the theoretical expressions from Lemma 1 and the specific expressions for two nodes in (26) and (27). In Fig. 2(a), we simulate different β_1 and β_2 to verify conditions (32) and (33).

The effects of mimicry attacks are shown in Fig. 2(b) for the attacker (node 1) performing type-1 attacks with different parameter m_1. In this case, compared to independent attacks, we observe that $P_{\text{fa}}^{\text{even}}$ is always larger, and $P_{\text{d}}^{\text{even}}$ is lower when the mimic attack probability is below a certain threshold, around $m_1 = 0.65$ in this simulation. The red arrow indicates the region for conditions (39) to be satisfied.



(a) Intentional Collusion: $N = 6$, $r_k = 0.2$, $\mathbb{E}_0[\boldsymbol{u}_k] = 0.12$, $\mathbb{E}_1[\boldsymbol{u}_k] = 0.85$



(b) Mimicry Attack: $N = 6$, $r_k = 0.2$, $\mathbb{E}_0[\boldsymbol{u}_k] = 0.12$, $\mathbb{E}_1[\boldsymbol{u}_k] = 0.85$

Fig. 2: Simulation of the probabilities of false alarm and detection under various conditions.

Therefore, in both attack models, we showed that although the attackers are all type-1, there exist feasible regions, denoted with red arrows in Fig.2, for intentional collusion and mimicry attacks to degrade the performance of both false-alarm and detection probabilities. It follows that the effects of colluded attacks can be more serious than independent attacks.

VI. Conclusions

We provided closed form expressions for the performance evaluation of majority rule fusion using correlated sensing reports. We formulated and discussed two kinds of malicious behavior and showed that these perform worse than independent attacks. These results serve as motivation for designing fusion schemes, as our future work, to take into account correlations among sensing reports and counteract the effects of collusion.

References

[1] S. Mishra, A. Sahai, and R. Brodersen, "Cooperative sensing among cognitive radios," in *Proc. IEEE ICC*, vol. 4, Istanbul, Turkey, Jun. 2006, pp. 1658–1663.

[2] F. Penna, S. Yifan, L. Dolecek, and D. Cabric, "Joint spectrum sensing and detection of malicious nodes via belief propagation," in *Proc. IEEE GLOBECOM*, Houston, Texas, USA, Dec. 2011, pp. 1–5.

[3] ——, "Detecting and counteracting statistical attacks in cooperative spectrum sensing," *IEEE Trans. Signal Process.*, vol. 60, no. 4, pp. 1806–1822, Apr. 2012.

[4] Z. Quan, S. Cui, and A. H. Sayed, "Optimal linear cooperation for spectrum sensing in cognitive radio networks," *IEEE J. Sel. Topics in Signal Process.*, vol. 2, no. 1, pp. 28–40, Feb. 2008.

[5] P. Sofotasios, E. Rebeiz, L. Zhang, T. Tsiftsis, D. Cabric, and S. Freear, "Energy detection-based spectrum sensing over generalized and extreme fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 3, pp. 1031–1040, Feb. 2012.

[6] E. Drakopoulos and C.-C. Lee, "Optimum multisensor fusion of correlated local decisions," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 27, no. 4, pp. 593–606, Jul. 1991.

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

[8] D. Wagner and P. Soto, "Mimicry attacks on host-based intrusion detection systems," in *Proc. 9th ACM conference on Computer and communications security,* Washington, DC, USA, May 2002, pp. 255–264.

[9] H. Feng, O. Kolesnikov, P. Fogla, W. Lee, and W. Gong, "Anomaly detection using call stack information," in *Proc. IEEE Symposium on Security and Privacy*, Oakland, California, USA, May 2003, pp. 62–75.