Online Malicious Behavior Detection in Collaborative Spectrum Sensing: A Change Detection Approach

Junnan YAO, Qihui WU, Shuo FENG, Jinlong WANG

Institute of Communications Engineering, PLA University of Science and Technology,
Biaoying #2, Street Yudao, District Baixia, 210007, Nanjing, P.R. China

15053337jn@gmail.com, wqhqhw@163.com, fengshuo1010@gmail.com, wjl543@sina.com

Abstract. *Intelligent attackers in a collaborative spectrum sensing system could act as honest users to conceal themselves and start malicious behavior abruptly since an unpredictable time slot. Affected by honest behavior before attacking time, traditional malicious behavior detection (MBD) algorithms are not agile enough to identify the abrupt change of behavior. To alleviate this challenge, in this paper, we propose the Rao test-based malicious behavior detection (RT-MBD) algorithm, which could detect the malicious behavior with unknown parameter and unknown starting time. The proposed RT-MBD is not affected by honest behavior before attacking time and has a shorter detection delay with constraint of a certain false alarm rate than conventional algorithms. Performance of RT-MBD is validated by both mathematical proof and numerical experiments.*

Keywords

Malicious behavior, change-point detection, Rao test statistic, collaborative spectrum sensing.

1. Introduction

Spectrum sensing [1] is a fundamental technology of cognitive radio networks (CRNs) [2], which guides the cognitive radios (CRs) to access to the licensed spectrum bands properly. In the CRNs, cognitive radios are allowed to access to the licensed spectrum bands only when primary users are absent. Because of the uncertainty of the wireless environment such as shadowing and fading, sensing results from a single CR may be unreliable [3]. Therefore, collaborative spectrum sensing (CSS) [4], [5] is proposed to conquer the unfavorable wireless channel effects. In a typical CSS system, at each sensing slot, all the CRs perform local spectrum sensing procedure individually and send the sensing results to the fusion center (FC), where a global decision is derived according to a certain fusion rule [6]. CSS improves sensing performance by exploiting spatial diversity gain [7] when all the CRs behave honestly. In contrast, when some CRs turn to malicious behavior, the performance of CSS degrades fiercely. In this paper, the term *behavior* specifies how a CR deals with its sensing results. For honest users, the sensing results are reported to the FC directly, while the malicious users may falsify their sensing results to mislead the FC.

Security issues in CSS system, which deal with malicious behavior, have attracted considerable attention of research community. In [8], an attacker detection approach bases on data mining is proposed. It calculates Hamming distance between each pair of two CRs and declares the presence of attackers when the distance deviates from a normal level. A method to learn the malicious behavior of attackers is provided in [9]. The behavior is measured by probability of sensing reports from CRs. In [10], the dissimilarity of local sensing reports among CRs is applied as behavior metric. All these studies base on the same assumption that behavior of a CR is fixed and unchangeable. However, In practical scenarios, after intruding into the CRN, attackers may not take malicious behavior immediately. It is reasonable that the attackers act as honest users (to lurk in the CRN and to avoid being detected) and turn to malicious behavior at an unknown time. In this circumstance, the behavior metric applied in [8]-[10] cannot converge to the true value regarding to malicious behavior after change-point (start of malicious behavior), because honest reports before attacking are included in calculation of malicious behavior. Although a forgetting mechanism is adopted to eliminate the impact of historical behavior in our previous work [11], the decay factor cannot be derived analytically, and the algorithm cannot be optimized when the attacking time is unknown.

To alleviate this challenge, in this paper, we investigate online malicious behavior detection schemes that applies change-point detection theory, and two scenarios are considered. In the first scenario, parameters of malicious behavior are assumed to be known to the FC. We utilize the repeated sequential probability ratio test (RSPRT) [12] as a malicious behavior detection algorithm to identify the change of behavior. The RSPRT-MBD achieve a minimum average detection delay subjects to a given false alarm level. In the second scenario, which is more practical, the behavior parameter is unknown. We use the generalized likelihood ratio test (GLRT) [13], a traditional change-point detection algorithm, as a MBD approach. Furthermore, to

reduce computational complexity of GLRT-MBD, we substitute the GLRT statistic by the Rao test statistic [14] and propose a Rao test-based malicious behavior detection (RT-MBD) algorithm. The proposed algorithm achieves less detection delay than GLRT-MBD does with constraint of the same false alarm rate .

The remainder of this paper is organized as follows. CSS system model and malicious behavior in CSS system is introduced in Section 2. In Section 3, online malicious behavior detection algorithms for two scenarios are proposed. In Section 4, the performance bounds of proposed MBD algorithms are analyzed. The simulation results is presented in Section 5, and the paper is concluded in Section 6.

2. System Model

In this section, CSS system of cognitive radio networks is introduced. After that, we investigate the behavior of CRs in the CSS system.

2.1 CSS System Model

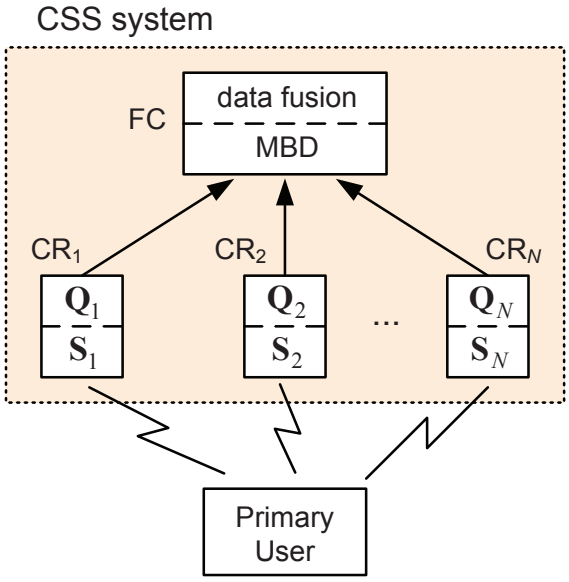

Fig. 1. Collaborative spectrum sensing system model.

As shown in Fig. 1, cognitive radios (CRs) coexist with a primary user (PU). Both the PU and CRs are assumed to use time slotted system with perfect time-synchronization [15]. The PU has a priority to utilize the licensed spectrum band, while the CRs are allowed to access the band only when the PU is idle. Let P_0 be the prior probability that PU is absent and P_1 be the prior probability that the PU is present. In addition, the prior probability of PU's status is assumed to be known, because it could be learned from historical information. At the beginning of each time slot, there is a short period of time for CRs to detect the status of the PU in the licensed band. Without lost of generality, we assume that all the CRs adopt energy-detection scheme [16] to detect the PU, and they achieve the same sensing performance [17]. The sensing performance of CRs could be depicted by sensing matrix

$$\mathbf{S} = \begin{pmatrix} 1-P_{fa} & P_{fa} \\ P_{md} & 1-P_{md} \end{pmatrix} \tag{1}$$

where $P_{fa} = \Pr(u=1|\mathcal{H}_0)$ is false alarm probability of the CR, and $P_{md} = \Pr(u=0|\mathcal{H}_1)$ is missed detection probability of the CR. $\mathcal{H}_0$ is the hypothesis that PU is absent, and $\mathcal{H}_1$ is that of PU is present.

After local sensing phase, the CRs report their sensing results $\mathbf{u} = (u^{(1)}, u^{(2)}, \cdots, u^{(N)})$ to the FC for data fusion, where $u^{(i)} = \{0,1\}$, $i \in \{1,2,\cdots,N\}$, denotes the i^{th} CR's sensing result. The distance between PU and CR is usually much larger than that between CR and FC, then reporting channels could be assumed error-free [4] and local results are perfectly received by FC. Moreover, it is reasonable to assume that $\mathbf{S}$ is known to the FC, because sensing performance of CRs could be adjusted by the FC.

2.2 Malicious Behavior in CSS System

In a CSS system, security threats are generally raised by two kinds of malicious users, i.e., intruded attackers and compromised CRs [18]. Both the two types could falsify their local sensing reports and mislead the FC. When the FC executes malicious behavior detection (MBD), all the CRs are regarded as potential malicious users.

We use the behavior matrix [10] to describe the behavior (the way a CR deal with its sensing results) of the checked CR. Take the i^{th} CR as an example, the behavior matrix of it could be denoted by

$$\mathbf{Q}^{(i)} = \begin{pmatrix} 1-q_{01}^{(i)} & q_{01}^{(i)} \\ q_{10}^{(i)} & 1-q_{10}^{(i)} \end{pmatrix} \tag{2}$$

where $q_{jk}^{(i)} = \Pr(v^{(i)} = k | u^{(i)} = j)$, $j,k \in \{0,1\}$, is the conditional probability, and it indicates the probability that the i^{th} CR reports k to the FC while its sensing result is j. For convenient analysis, we omit the superscript "i" of the checked CR in the remainder of this paper and denote the behavior parameter by $\boldsymbol{\theta} = (q_{01}, q_{10})^T$. Clearly, for malicious behavior, $0 < q_{01}, q_{10} \leq 1$, and for honest behavior, $q_{01} = q_{10} = 0$. Intuitively, that matrix of honest behavior could be written as

$$\mathbf{Q}^{\text{H}} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{3}$$

In most existing works, behavior matrix of the checked CR is time-invariant. In view of the FC, all the CRs act following their unchangeable behavior parameters. However, in practical scenarios, a malicious user can disguise itself by acting as an honest one and turns to malicious behavior abruptly since an unknown time slot. An adequate MBD algorithm has to be sensitive to the abrupt behavior change and raise an alarm after it happens.

Because the exact status of PU is unknown at FC, the only clue to detect malicious behavior is sensing reports of

CRs. Suppose that the FC starts MBD at time slot 1, and the behavior of the checked CR changes since time slot t_c (including time slot t_c), then the probability mass function of sensing report v_t, $t = 1,2,\cdots$, could be presented as

$$v_t \sim \begin{cases} f(v_t;\boldsymbol{\theta}_{\mathrm{H}}) & 1 \le t < t_c \\ f(v_t;\boldsymbol{\theta}_{\mathrm{M}}) & t \ge t_c \end{cases} \tag{4}$$

where $\boldsymbol{\theta}_{\mathrm{H}}$ is the parameter of honest behavior of the CR before the change, and $\boldsymbol{\theta}_{\mathrm{M}}$ is behavior parameter after malicious behavior occurs. In this paper, the process that a CR's behavior changes from honest behavior to malicious behavior is assumed could be finished at once (without delay).

3. Malicious Behavior Detection

In this section, we provide malicious behavior detection (MBD) algorithms for two cases. In the first case, parameter of malicious behavior is known to the FC, and repeated sequential probability ratio test (RSPRT) algorithm is adopted to solve the problem. In the other case, which is more practical, the parameter of malicious behavior unknown. We propose a Rao test-based malicious behavior detection (RT-MBD) algorithm.

3.1 Detection of Known Malicious Behavior

Notice that the sensing reports have only two possible values, and it follows Bernoulli distribution

$$f(v_t;\boldsymbol{\theta}) = p^{v_t}(1-p)^{1-v_t} \tag{5}$$

where $v_t \in \{0,1\}$, $t \ge 1$, and $p = \Pr(v_t = 1;\boldsymbol{\theta})$. For malicious behavior, parameter $\boldsymbol{\theta}_{\mathrm{M}} = (q_{01}, q_{10})^T$, and we have

$$\begin{aligned} p_{\mathrm{M}} &= \Pr(v_t = 1;\boldsymbol{\theta}_{\mathrm{M}}) \\ &= ((1-P_{fa})\,q_{01} + P_{fa}(1-q_{10}))\,P_0 \\ &\quad + (1-P_{md}(1-q_{01}) - (1-P_{md})\,q_{10})\,P_1 \end{aligned} \tag{6}$$

where $0 < q_{01}, q_{10} \le 1$. Similarly, for honest behavior, $\boldsymbol{\theta}_{\mathrm{H}} = (0,0)^T$, and we have

$$\begin{aligned} p_{\mathrm{H}} &= \Pr(v_t = 1;\boldsymbol{\theta}_{\mathrm{H}}) \\ &= P_{fa}P_0 + (1-P_{md})\,P_1. \end{aligned} \tag{7}$$

Based on analysis above, the log-likelihood ratio (LLR) between probabilities of sensing report v_t comes from malicious behavior and that comes from honest behavior could be calculated and denoted as follows,

$$s_t = \ln \frac{f(v_t;\boldsymbol{\theta}_{\mathrm{M}})}{f(v_t;\boldsymbol{\theta}_{\mathrm{H}})}. \tag{8}$$

If $s_t > 0$, it has larger probability that v_t is generated by malicious behavior. In contrast, if $s_t < 0$, it has larger probability that v_t comes from honest behavior.

The detection algorithm will stop when the statistic exceeds a predetermined threshold. The stopping time (alarming time) could be presented as

$$t_a = \min\{t : g_t > \eta\} \tag{9}$$

where

$$g_t = \max_j \sum_{i=j}^{t} s_i \tag{10}$$

is the statistic of the algorithm, and it is the largest sum of the LLR over time slots i to t. η is the predetermined threshold. Expressions of (9) and (10) formulate the cumulative sum-type algorithm, and it could be implemented by repeated sequential probability ratio test (RSPRT) [12] of two hypotheses,

$$g_{\mathrm{RSPRT}}(t) = \begin{cases} g_{\mathrm{RSPRT}}(t-1) + s_t & g_{\mathrm{RSPRT}}(t) > 0 \\ 0 & g_{\mathrm{RSPRT}}(t) \le 0 \end{cases} \tag{11}$$

where $g_{\mathrm{RSPRT}}(0) = 0$. The statistic $g_{\mathrm{RSPRT}}(t)$ could also be presented in recursive form,

$$g_{\mathrm{RSPRT}}(t) = (g_{\mathrm{RSPRT}}(t-1) + s_t)^+ \tag{12}$$

where $(x)^+ = \sup(x,0)$.

If $t_a \ge t_c$, we define *detection delay* by $t_d = t_a - t_c$. On the other hand, when $t_a < t_c$, a *false alarm* comes up.

3.2 Detection of Unknown Malicious Behavior

In a practical system, not only the behavior change time is unpredictable, but also the parameter of malicious behavior is unknown. The statistic g_t of the detection algorithm cannot be calculated directly. Conventional approach to solve hypothesis test with unknown parameter in change-point detection theory is to substitute the statistic g_t by $\hat{g}_t$, which is the most possible value of g_t and is calculated based on maximum likelihood estimation (MLE) of the unknown parameter. This is the generalized likelihood ratio test (GLRT) [13]. Based on GLRT, the GLRT-MBD could be derived as follows.

When parameter of malicious behavior is unknown, we cannot derive $f(v_t;\boldsymbol{\theta}_{\mathrm{M}})$ directly, and the log-likelihood ratio s_t is also unknown. The standard statistical approach is using the MLE of $\hat{t}_c$ and $\hat{\boldsymbol{\theta}}_{\mathrm{M}}$,

$$\left(\hat{t}_c, \hat{\boldsymbol{\theta}}_{\mathrm{M}}\right) = \arg \max_{1 \le t_c \le t_a} \sup_{\boldsymbol{\theta}_{\mathrm{M}}} \sum_{i=t_c}^{t_a} \ln \frac{f(v_i;\boldsymbol{\theta}_{\mathrm{M}})}{f(v_i;\boldsymbol{\theta}_{\mathrm{H}})}. \tag{13}$$

The statistic of GLRT-MBD at time slot t is denoted by

$$g_{\mathrm{GLRT}}(t) = \max_{1 \le j \le t} \ln T_{\mathrm{GLRT}}(j,t) \tag{14}$$

where

$$T_{\mathrm{GLRT}}(j,t) = \sup_{\boldsymbol{\theta}_{\mathrm{M}}} \frac{f(\mathbf{x};\boldsymbol{\theta}_{\mathrm{M}})}{f(\mathbf{x};\boldsymbol{\theta}_{\mathrm{H}})} = \sup_{\boldsymbol{\theta}_{\mathrm{M}}} \prod_{i=j}^{t} \frac{f(v_i;\boldsymbol{\theta}_{\mathrm{M}})}{f(v_i;\boldsymbol{\theta}_{\mathrm{H}})} \tag{15}$$

is the statistic of GLRT[1], and $\mathbf{x} = (v_j, v_{j+1}, \cdots, v_t)^T$ is the vector of sensing reports from time slot j to t. Applying $g_{\mathrm{GLRT}}(j,t)$ in (9), the GLRT-MBD is derived.

[1] Notice that the statistic of GLRT and statistic of GLRT-MBD are different. The relation of the two kinds of statistics is revealed in (14).

We notice that statistic of GLRT is maximum value of likelihood ratio and should be computed for each $i = j, j+1, \cdots, t$ respectively. The GLRT-MBD is computationally complex and sometime unavailable. If $T_{\mathrm{GLRT}}(j,t)$ is substituted, the GLRT-MBD could be simplified. In the following of this subsection, we substitute the GLRT statistic by Rao test (RT) [14] statistic, which is calculated without MLE of behavior parameter, and propose the RT-MBD algorithm.

According to (6) and (7), we find the probability that the checked CR reports a certain value (i.e., 0 and 1) is a function of the behavior parameter $\boldsymbol{\theta}$. Then we substitute behavior parameter $\boldsymbol{\theta}$ by parameter p and derive the RT statistic as follows

$$T_{\mathrm{RT}}(j,t) = \left.\frac{\partial f(\mathbf{x};p)}{\partial p}\right|_{p=p_{\mathrm{H}}}^{T} \mathbf{I}^{-1}(p_{\mathrm{H}}) \left.\frac{\partial f(\mathbf{x};p)}{\partial p}\right|_{p=p_{\mathrm{H}}} \tag{16}$$

where $\mathbf{x} = (v_j, v_{j+1}, \cdots, v_t)^T$, and p_{H} is value of p under hypothesis that the observed sensing reports come from honest behavior. $\mathbf{I}(\cdot)$ is the Fisher information matrix [19]. Because there is only one unknown parameter in (16), then we have

$$\begin{aligned}\mathbf{I}(p_{\mathrm{H}}) &= -\mathbf{E}\left(\frac{\partial^2}{\partial p^2}\ln f(\mathbf{x};p)\right)\Big|_{p=p_{\mathrm{H}}} \\ &= \frac{W}{(1-p_{\mathrm{H}})\,p_{\mathrm{H}}}\end{aligned} \tag{17}$$

where $W = t - j + 1$ is the length of sensing reports $\mathbf{x}$. The RT statistic could be further simplified as follows,

$$T_{\mathrm{RT}}(j,t) = \frac{\left(\mathbf{x}^T\mathbf{x} - W p_{\mathrm{H}}\right)^2}{W p_{\mathrm{H}}(1-p_{\mathrm{H}})}. \tag{18}$$

Comparing with the GLRT statistic $T_{\mathrm{GLRT}}(j,t)$ in (15), $T_{\mathrm{RT}}(j,t)$ need not MLE of any parameters and is computationally convenient. Moreover, $T_{\mathrm{RT}}(j,t)$ has the same asymptotic ($W \to \infty$) probability mass function as $2\ln T_{\mathrm{GLRT}}(\mathbf{x})$, that is

$$T_{\mathrm{RT}}(j,t) \sim 2\ln T_{\mathrm{GLRT}}(j,t) \sim \begin{cases} \chi_1^2 & \mathcal{H}_{\mathrm{H}} \\ \chi_1'^2(\lambda) & \mathcal{H}_{\mathrm{M}} \end{cases} \tag{19}$$

where $\mathcal{H}_{\mathrm{H}}$ denotes the observed sensing reports come from honest behavior, $\mathcal{H}_{\mathrm{M}}$ indicates that come from malicious behavior, χ_r^2 denotes a chi-squared probability mass function (pmf) with r degrees of freedom, and $\chi_r'^2(\lambda)$ denotes a non-central chi-squared pmf with r degrees of freedom and non-centrality parameter $\lambda = \frac{W(p_{\mathrm{M}}-p_{\mathrm{H}})^2}{(1-p_{\mathrm{H}})p_{\mathrm{H}}}$. The statistic of RT-MBD could be denoted by

$$g_{\mathrm{RT}}(t) = \max_{1\le j\le t} T_{\mathrm{RT}}(j,t). \tag{20}$$

Therefore, proposed Rao test-based malicious behavior detection algorithm is summarized as follows,

Algorithm 1: RT-MBD

Check the behavior of a given CR via its current and historical sensing reports:

1: **do** (before the algorithm is terminated)
2: Receive sensing report of the checked CR at time slot t, i.e., v_t.
3: **for** $j = 1, 2, \cdots, t$
4: Derive the historical sensing reports vector, i.e., $\mathbf{x}_j = (v_j, v_{j+1}, \cdots, v_t)^T$.
5: Calculate $T_{\mathrm{RT}}(j,t)$ according to (18).
6: **end for**
7: **if** $g_{\mathrm{RT}}(t) = \max\{T_{\mathrm{RT}}(j,t)\} > \eta$, $j = 1, 2, \cdots, t$
8: Declare that the checked CR has been a malicious user and starting time of malicious behavior is $\hat{t}_c = j$. End the algorithm.
9: **end if**
10: Wait for the sensing report of the next time slot.
11: **end do**

4. Performance Analysis

In this section, we introduce the performance index of malicious behavior detection (MBD), i.e., average run length (ARL) function. Then we provide properties and performance bounds of investigated MBD algorithms.

4.1 The ARL Function

The goal of malicious behavior detection is to raise an alarm as quickly as possible after malicious action starts with constraint of a certain level of false alarm. To evaluate performance of detection algorithm, we introduce the average run length (ARL) function [13], which is denoted as follows,

$$L_z(\boldsymbol{\theta}) = \begin{cases} \bar{T}_0 & \boldsymbol{\theta} = \boldsymbol{\theta}_{\mathrm{H}} \\ \bar{T}_1^* & \boldsymbol{\theta} = \boldsymbol{\theta}_{\mathrm{M}} \end{cases} \tag{21}$$

where the subscript "z" of ARL function $L_z(\cdot)$ means the statistic of detection algorithm starts from z, i.e., $g(0) = z$. Specifically, the ARL functions could be denoted by the worst mean detection delay

$$L_z(\boldsymbol{\theta}_{\mathrm{M}}) = \bar{T}_1^* = \sup_{t_c\ge 1} \operatorname{ess\,sup} \mathbf{E}_{\boldsymbol{\theta}_{\mathrm{M}}}(t_d | t_a \ge t_c, \mathbf{y}) \tag{22}$$

where the notation "esssup" indicates essential supremum, $\mathbf{y} = (v_1, v_2, \cdots, v_{t_c-1})^T$ is the vector of sensing reports of checked CR from the first sensing slot to sensing slot t_c (not including the time slot t_c), and the mean time between false alarm

$$L_z(\boldsymbol{\theta}_{\mathrm{H}}) = \bar{T}_0 = \mathbf{E}_{\boldsymbol{\theta}_{\mathrm{H}}}(t_a). \tag{23}$$

4.2 Performance of RSPRT-MBD

In this subsection, we investigate detection performance of optimal algorithm, i.e., RSPRT-MBD, which could be applied in circumstance that behavior parameter $\boldsymbol{\theta}_{\mathrm{M}}$ is known. Let $0 < \alpha < 1$ be the predetermined false alarm rate, then $\beta = \alpha^{-1} > 1$ is the mean time between false alarms. We

have the lower bound for mean time between the false alarms [20]

$$\bar{T}_0 \geq e^{\eta} = \beta, \tag{24}$$

and the upper bound for the worst mean delay

$$\bar{T}_1^* \leq \bar{L}_0(\boldsymbol{\theta}_M) = (\eta + \beta(\boldsymbol{\theta}_M))/\mathbf{E}_{\boldsymbol{\theta}_M} s_t \tag{25}$$

where $\beta(\boldsymbol{\theta}_M) = \sup_{\lambda>0} \mathbf{E}_{\boldsymbol{\theta}_M}(s_t - \lambda | s_t \geq \lambda > 0)$. When the threshold $\eta \to \infty$, the asymptomatic upper bound of $\bar{T}_1^*$ could be denoted by

$$\bar{T}_1^* \leq \eta / \mathbf{E}_{\boldsymbol{\theta}_M} s_t. \tag{26}$$

Furthermore, we have

$$\bar{T}_1^* \sim \ln\beta / \mathbf{K}\left(f_{\boldsymbol{\theta}_M}, f_{\boldsymbol{\theta}_H}\right), \quad \beta \to \infty \tag{27}$$

where

$$\mathbf{K}\left(f_{\boldsymbol{\theta}_M}, f_{\boldsymbol{\theta}_H}\right) = \mathbf{E}_{\boldsymbol{\theta}_M} s_t \tag{28}$$

is Kullback information between $f(v_t;\boldsymbol{\theta}_M)$ and $f(v_t;\boldsymbol{\theta}_H)$. The conclusion above shows optimality of the RSPRT-MBD from an asymptotic point of view. More precisely, RSPRT-MBD is optimal, with respect to the worst mean delay, when the mean time between false alarms goes to infinity. This asymptotic point of view is convenient in practice because a low false alarm rate is always desirable. The performance bounds are significant in design of malicious behavior detection algorithm. When the threshold is determined to achieve a specific false alarm rate according to (24), the bound of detection delay is derived by (25).

Although in many practical scenarios the RSPRT-MBD is unavailable (because of the unknown malicious behavior $\boldsymbol{\theta}_M$), the performance bounds of it are also useful to compare different algorithms respects to its asymptotic optimal property. The difference between RSPRT-MBD and other MBD algorithms is how much prior information of malicious behavior they have. The uncertainty of parameter generates the performance gap between detection algorithms. When $\hat{\boldsymbol{\theta}}_M$ is substituted by its true value, GLRT-MBD achieves the same performance as RSPRT-MBD does.

4.3 Performance of RT-MBD

In this subsection, we derive performance of RT-MBD via analyzing performance of GLRT-MBD. Substituting parameter p by $r = \ln\frac{p}{1-p}$, the pmf of sensing report v_t (provided in (5)) could be written in exponential form as

$$f(v_t;r) = e^{v_t r - d(r)} \tag{29}$$

where $d(r) = \ln(1+e^r)$.

Given unknown parameter $r_M \in [r_0, r_1]$, when the threshold η is set to be

$$\eta = -\ln \frac{\alpha}{3\ln\alpha^{-1}\left(1 + 1/\mathbf{K}(f_{r_0}, f_{r_H})\right)^2} \tag{30}$$

where $r_H = \ln\frac{p_H}{1-p_H}$, f_{r_0} is the pmf of v_t when $r = r_0$, and f_{r_H} is that of v_t when $r = r_H$. Then the lower bound of mean time between false alarms of GLRT-MBD could be given by [21]

$$\bar{T}_0 \geq \alpha^{-1} = \beta \tag{31}$$

and the upper bound of worst mean delay could be presented as [21]

$$\begin{aligned}\bar{T}_1^* \leq & \frac{\ln\bar{T}_0 + \ln\ln\bar{T}_0}{\mathbf{K}(f_{r_M}, f_{r_H})} + \frac{r_M^2 \ddot{d}(r_M)}{\mathbf{K}^2(f_{r_M}, f_{r_H})} \\ & + \frac{2\ln\left(3^{1/2}\left(1 + 1/\mathbf{K}(f_{r_0}, f_{r_H})\right)\right)}{\mathbf{K}(f_{r_M}, f_{r_H})} + 1\end{aligned} \tag{32}$$

where $\ddot{d}(r_M) = \frac{\partial^2}{\partial r_M^2} d(r_M)$.

Now we discuss the performance RT-MBD and GLRT-MBD by comparing them with the optimal algorithm, i.e., RSPRT-MBD. When the checked CR acts as honest user, we have $\mathbf{K}\left(f_{\boldsymbol{\theta}_M}, f_{\boldsymbol{\theta}_H}\right) = 0$. In this circumstance, because parameter $\hat{\boldsymbol{\theta}}_M$ maximizes $g_{GLRT}(t)$, the expectation of statistic $g_{GLRT}(t)$ has a large deviation from that of $g_{RSPRT}(t)$. On the contrary, $g_{RT}(t)$ is calculated based on sensing reports wihtout procedure of maximization, and its expectation has small deviation from that of $g_{RSPRT}(t)$. Consequently, $g_{RT}(t)$ has a lower probability of exceeding a given threshold than $g_{GLRT}(t)$ does, and mean time between false alarms of RT-MBD is larger than thant of GLRT-MBD under the same threshold. In the other hand, the difference between the two statistics is not significant when $\mathbf{K}\left(f_{\boldsymbol{\theta}_M}, f_{\boldsymbol{\theta}_H}\right) > 0$. It means the mean time of detection delay of RT-MBD is close to that of GLRT-MBD. Based on these analyses, the performance bounds of RT-MBD can be derived via performance bounds of GLRT-MBD. Specifically, the lower bound of $\bar{T}_0$ of GLRT-MBD could be used as a loose lower bound of mean time between false alarms of RT-BMD, and the mean times of delay of the two algorithms share the same upper bound which is given by (32). When $\beta \to \infty$, we have

$$\bar{T}_1^* \sim \frac{\ln\beta + \ln\ln\beta}{\mathbf{K}(f_{r_M}, f_{r_H})} + C \tag{33}$$

where $C = \frac{2\ln\left(3^{1/2}\left(1+1/\mathbf{K}\left(f_{r_0}, f_{r_H}\right)\right)\right)}{\mathbf{K}\left(f_{r_M}, f_{r_H}\right)} + 1$. As a result, RT-MBD achieves better performance (a shorter mean time of detection delay with constraint of the same false alarm rate) than GLRT-MBD. The performance of the two algorithms is further discussed by numerical experiments in the following section.

5. Simulation Results

In this section, we evaluate the performance of proposed RT-MBD algorithm by extensive numerical experiments. First, the performance of RT-MBD is measured by ARL functions, i.e., mean time between false alarms and mean time of detection delay. Then we compare the performance of proposed RT-MBD with existing algorithms under abrupt malicious behavior by operation characteristic curves. In the following numerical experiments, the prior probabil-

ity of PU's absence is set to be $P_0 = 0.7$, and the sensing performance of CRs is $\mathbf{S} = \begin{pmatrix} 0.8 & 0.2 \\ 0.2 & 0.8 \end{pmatrix}$.

5.1 The ARL Functions of RT-MBD

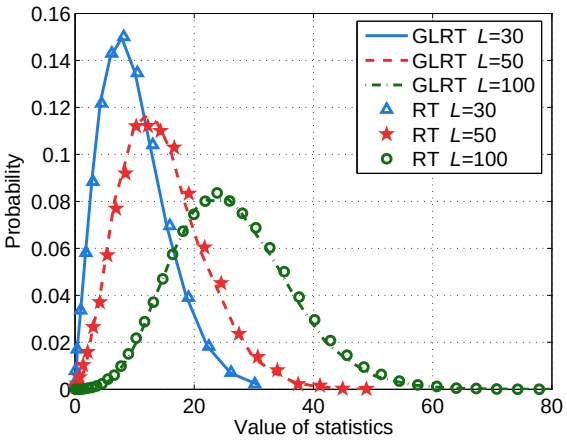

Fig. 2. Empirical probability mass function RT statistic.

In Fig. 2, the empirical probability mass functions (pmfs) of RT statistic and modified GLRT statistic (i.e., $2\ln T_{\text{GLRT}}$) based on 10^4 individual experiments are presented. The length of sensing reports are set to be $L = 30, 50, 100$, and behavior parameter $\boldsymbol{\theta}_{\text{M}} = (1,1)^T$. As shown in the figure, the empirical pmfs of the two statistics are very close. It verifies the statement in Section 3 that the statistics has a same asymptotic distribution, and it is an important premise to substitute T_{GLRT} by T_{RT} to simplify GLRT-MBD.

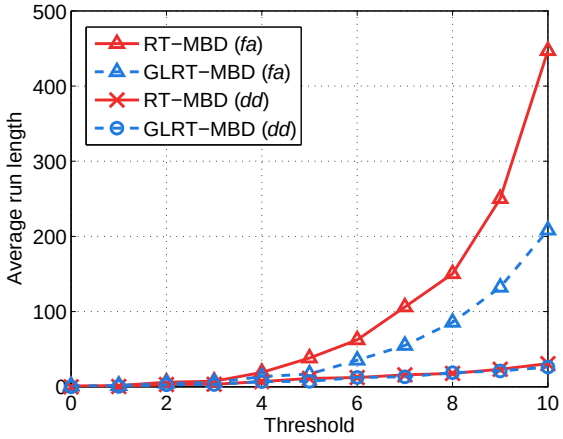

Fig. 3. Average run length functions of RT-MBD and GLRT-MBD (fa: mean time between false alarms; dd: mean time of detection delay).

Fig. 3 demonstrates the values of average run length functions of RT-MBD and GLRT-MBD with different threshold $\eta = 0, 1, \cdots, 10$. The statistic of GLRT-MBD is doubled in the experiment to compare the ALR functions with that of RT-MBD in the same scale of thresholds. The true value of behavior parameter $\boldsymbol{\theta}_{\text{M}} = (1,1)^T$. It can be seen that mean time of detection delay (the curve with circles and the curve with crosses) of the two algorithms are almost overlapped. Whereas the mean time between false alarms of RT-MBD (the solid curve with triangles) is larger than that of GLRT-MBD (the dashed curve with triangles). It is because that the expectation of statistic $g_{\text{RT}}(t)$ is smaller than that of $g_{\text{GLRT}}(t)$ when $\boldsymbol{\theta} = (0,0)^T$. With the same threshold, statistic $g_{\text{GLRT}}(t)$ tends to exceed the threshold within shorter sensing slots than $g_{\text{RT}}(t)$ after the algorithm starts. Therefore, mean time between false alarms of RT-MBD is larger than that of GLRT-MBD, and this conclusion has been discussed in Subsection 4.3.

5.2 Operating Characteristic Curves

In this subsection, to evaluate performance of RT-MBD and other algorithms, the operating characteristic curves are presented.

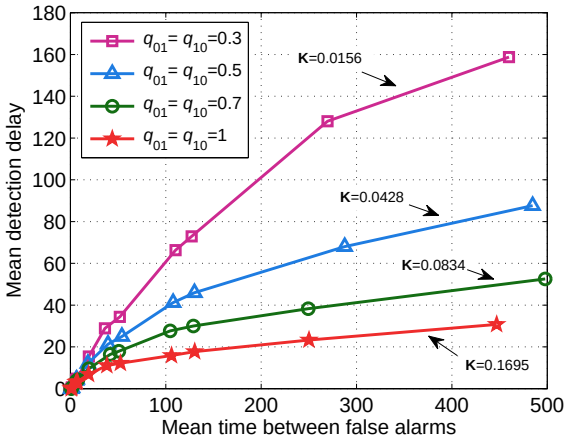

Fig. 4. Operating characteristic curves of RT-MBD under malicious behavior with various parameters.

Fig. 4 shows operating characteristic curves of RT-MBD, where the x-axis denotes mean time between false alarms and y-axis denotes mean time of detection delay. In this experiment, we reveal the relation between the performance of RT-MBD and the Kullback information of behavior parameter. Therefore, it is unnecessary to test the performance under all the possible values of behavior parameter $\boldsymbol{\theta}_{\text{M}}$, and several values, i.e., $\boldsymbol{\theta}_{\text{M}} = (0.3,0.3)^T, (0.5,0.5)^T, (0.7,0.7)^T, (1,1)^T$, are tested as examples. According to (28), corresponding Kullback information of the parameter is derived as $\mathbf{K} = 0.0156, 0.0428, 0.0834, 0.1695$ (bits). By analyzing the simulation results, we have the conclusion that malicious behavior with larger Kullback information is more different from honest behavior than others, and it can be detected more quickly with constraint of a certain false alarm. For example, when mean time between false alarms is fixed, the curve of $\boldsymbol{\theta}_{\text{M}} = (1,1)^T$ (the curve with stars) has the best performance, i.e., the lowest mean time of detection delay. Simulation results in Fig. 4 validate the analysis of (27).

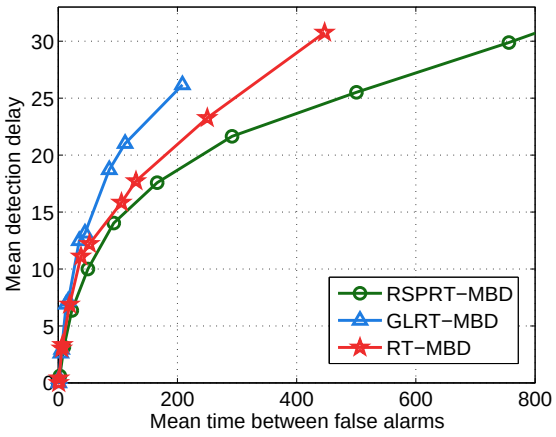

Fig. 5. Operating characteristic curves of different online MBD algorithms.

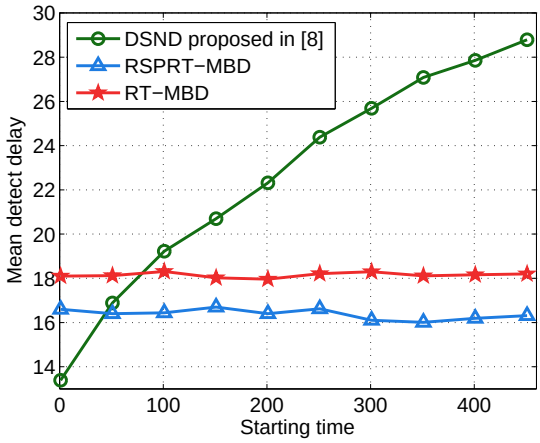

Fig. 6. Performance of different detection algorithms under abrupt malicious behavior.

Fig. 5 provides operating characteristic curves of several online MBD algorithms including proposed RT-MBD. The behavior parameter is $\boldsymbol{\theta}_{\mathrm{M}} = (1,1)^T$. It can be seen that RSPRT-MBD (the curve with circles) achieves the lowest detection delay with constraint of a certain mean time of false alarms among these algorithms, because RSPRT-MBD is assumed have complete prior information of malicious behavior. Unlike RSPRT-MBD, both of GLRT-MBD and RT-MBD operate under unknown behavior parameter, and they do not perform as well as the complete prior information algorithm. Moreover, as analyzed in Subsection 4.3, statistic $g_{\mathrm{RT}}(t)$ of RT-MBD has lower expectation under honest behavior than that of GLRT-MBD. It has larger mean time between false alarms under a given threshold (see Fig. 3). Then the mean time of detection delay of RT-MBD is lower than that of GLRT-MBD with constraint of the same false alarm rate. This conclusion is also validated by simulation result in the figure, i.e., the curve of RT-MBD (the curve with stars) is lower than that of GLRT-MBD.

To evaluate performance of proposed RT-MBD under abrupt malicious behavior, we compare RT-MBD with existing MBD algorithm. In Fig. 6, malicious behavior with unknown starting time is considered, and DSND algorithm[2] [8] is tested as an example. In this numerical experiment, the mean time between false alarms is set to be $\beta = 180$ sensing slots (corresponding false alarm rate is $\alpha = 0.0056$) for all the tested algorithms, and behavior parameter is $\boldsymbol{\theta}_{\mathrm{M}} = (1,1)^T$. Before malicious behavior starts, the checked CR acts as an honest user. As shown in the figure, the proposed RT-MBD (the curve with stars) achieves a mean time of detection delay about 18 sensing slots, and it is hardly affected by honest behavior before malicious behavior starts. Because of complete prior information, RSPRT-MBD achieves a lower mean time of detection delay than RT-MBD, which is about 16 sensing slots. However, the DSND is interfered by the honest behavior before attacking time, and detection delay grows with increasing of starting time of malicious behavior. It indicates that traditional MBD algorithms such as DSND are not fit for detecting malicious behavior with unknown staring time.

Furthermore, we notice that when starting time of malicious behavior is earlier than 80 sensing slots, DSND performs better than RT-MBD. It is because that Kullback information between honest behavior and malicious behavior in DSND is larger than that of RT-BMD. But this Kullback information bonus is canceled out when malicious behavior occurs after the MBD starts for a certain length of sensing slots, i.e., 80 sensing slots.

6. Conclusions

In this paper, we investigate the malicious behavior detection in collaborative spectrum sensing of cognitive radio networks. The more practical malicious behavior with unknown parameter and unknown starting time is considered. To alleviate impacts of honest behavior before malicious behavior starts, we propose a Rao test-based malicious behavior detection (RT-MBD) algorithm, based on change detection theory. The performance of the proposed algorithm is analyzed mathematically, and the performance bounds of mean time between false alarms and mean detection delay are provided. In the simulation section, we test the performance of RT-MBD and have the conclusion that malicious behavior with larger Kullback information can be detected more quickly after it starts with constraint of a fixed mean time of false alarms. Moreover, the simulation results prove that the proposed RT-MBD is not interfered by honest behavior before attack starts, and it is more agile than existing MBD algorithms.

Acknowledgements

This work is supported by the national basic research program (973) of China (2009CB320400), the national nat-

[2]DSND is a typical one of the algorithms that detect malicious behavior based on historical sensing reports of CRs ignoring honest behavior before attacking time. Algorithms proposed in [9] and [10] have the same property as DSND. Similar results for these algorithms could be derived.

ural science fund of China (60932002 and 61172062), and the natural science fund of Jiangsu, China (BK2011116).

References

[1] HAYKIN, S. Cogniteive radio: brain-empowered wireless communications. *IEEE Journal on Selected Areas in Communications*, 2005, vol. 23, no. 2, p. 201 - 220.

[2] MITOLA, J. *Software radio architecture*. John Wiley & Sons, 2000.

[3] MA, J., ZHAO, G., LI, Y. Soft combination and detection for cooperative spectrum sensing in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 2008, vol. 7, no. 11, p. 4502 - 4507.

[4] GHASEMI, A., SOUSA, E. Collaborative spectrum sensing for opportunistic access in fading environments. In *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*. Baltimore (USA), 2005, p. 131 - 136.

[5] MISHRA, S. M., SAHAI, A., BRODERSEN, R. W. Cooperative sensing among cognitive radios. In *IEEE International Conference on Communications*. Istanbul (Turkey), 2006, p. 1658 - 1663.

[6] BALDINI, G., STURMAN, T., BISWAS, A., R., LESCHHORN, R., GÓDOR, G., STREET, M. Security aspects in software defined radio and cognitive radio networks: a survey and a way ahead. *IEEE Communications Surveys & Tutorials*, 2012, vol. 14, no. 2, p. 355 - 379.

[7] JEONG, S. S., JEON, W. S., JEONG, D. G. Collaborative spectrum sensing for multiuser cognitive radio systems. *IEEE Transactions on Vehicular Technology*, 2009, vol. 58, no. 5, p. 2564 - 2569.

[8] LI, H., HAN, Z. Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks. *IEEE Transactions on Wireless Communications*, 2010, vol. 9, no. 11, p. 3554 - 3565.

[9] VEMPATY, A., AGRAWAL, K., CHEN, H., VARSHNEY, P. Adaptive learning of Byzantines' behavior in cooperative spectrum sensing. In *IEEE Wireless Communications and Networking Conference (WCNC)*. Cancun (Mexico), 2011, p. 1310 - 1315.

[10] YAO, J., WU, Q., WANG, J. Attacker detection based on dissimilarity of local sensing reports in collaborative spectrum sensing. *IEICE Transactions on Communications*, 2012, vol. E95-B, no. 9, p. 3024 - 3027.

[11] FENG, S., ZHENG, X., YAO, J., DING, G. Seeking justice: lapsed reputation-based cooperative spectrum sensing with lasting trusted nodes assistance. *Proceedings of IEEE WCSP*, 2012.

[12] PAGE, E. Continuous inspection schemes. *Biometika*, 1954, vol. 41, p. 100 - 115.

[13] LORDEN, G. Procedures for reacting to a change in distribution. *Annals of Mathematical Statistics*, 1971, vol. 42, no. 6, p. 1897 - 1908.

[14] KAY, S., M. *Fundamentals of Statistical Signal Processing: Detection Theory*. Prentice Hall, 1998.

[15] KHAN, Z., LEHTOMAKI, J., UMEBAYASHI, K., VARTIAINEN, J. On the selection of the best detection performance sensors for cognitive radio networks. *IEEE Letters on Signal Processing*, 2010, vol. 17, no. 4, p. 359 - 362.

[16] DIGHAM, F. F., ALOUINI, M. S., SIMON, M. K. On the energy detection of unknown signals over fading channels. *IEEE Transactions on Communications*, 2007, vol. 55, no. 1, p. 21 - 24.

[17] LETAIEF, K. B., ZHANG, W. Cooperative communications for cognitive radio networks. *Proceedings of the IEEE*, 2009, vol. 97, no. 5, p. 878 - 893.

[18] MIN, A. W., KIM, K., SHIN, K. G. Robust cooperative sensing via state estimation in cognitive radio networks. *IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*. Aachen (Germany), 2011, p. 185 - 196.

[19] KAY, S. M. *Fundamentals of Statistical Signal Processing: Estimation Theory*. Prentice Hall, 1998.

[20] LORDEN, G. On excess over the boundary. *Annals of Mathematical Statistics*, 1970, vol. 41, no. 2, p. 520 - 527.

[21] LORDEN, G. Open-ended tests for Koopman-Darmois families. *Annals of Mathematical Statistics*, 1973, vol. 1, no. 4, p. 633 - 643.

About Authors ...

Junnan YAO was born in 1983. He received his B.S. and M.S degrees from Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China, in 2005 and 2009. He is currently pursuing the Ph.D. degree in communications and information system at the PLA University of Science and Technology, Nanjing, China. His research interests are in wireless communications and signal processing. He is particularly interested in security issues in spectrum sensing.

Qihui WU was born in 1970. He received his B.S. degree in communications engineering, M.S. degree and Ph.D. degree in communications and information system from Institute of Communications Engineering, Nanjing, China, in 1994, 1997 and 2000, respectively. He is currently professor at the PLA University of Science and Technology, China. His current research interests are algorithms and optimization for cognitive wireless networks and soft-defined radio.

Shuo FENG received his B.S. degree (with honors) in electronic engineering from University of Electronic Science and Technology of China, Chengdu, China, in 2011. He is currently pursuing his M.S. degree in communications and information system in Institute of Communications Engineering, PLA University of Science and Technology, Nanjing, China. His research interests focus on cognitive radio networks, wireless communications and security.

Jinlong WANG was born in 1963. He received his B.S. degree in wireless communications, M.S.degree and Ph.D. degree in communications and electronic systems from Institute of Communications Engineering, Nanjing, China, in 1983, 1986 and 1992, respectively. He is currently professor at the PLA University of Science and Technology, China. He is also the cochairman of IEEE Nanjing Section. He has published widely in the areas of signal processing for communications, information theory, and wireless networks. His current research interests include wireless communication, cognitive radio and soft-defined radio.