Zhang *et al. EURASIP Journal on Advances in Signal Processing* 2014, **2014**:81
http://asp.eurasipjournals.com/content/2014/1/81

EURASIP Journal on Advances in Signal Processing
a SpringerOpen Journal

RESEARCH Open Access

# Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing

Linyuan Zhang[†], Qihui Wu[*], Guoru Ding[*†], Shuo Feng and Jinlong Wang

**Abstract**

In cognitive radio networks, spectrum sensing data falsification (SSDF) attack is a crucial factor deteriorating the detection performance of cooperative spectrum sensing. In this paper, we propose and analyze a novel *probabilistic soft* SSDF attack model, which goes beyond the existing models for its generalization. Under this generalized SSDF attack model, we firstly obtain closed form expressions of global sensing performance at the fusion center. Then, we theoretically evaluate the performance of the proposed attack model, in terms of destructiveness and stealthiness, sequentially. Numerical simulations match the analytical results well. Last but not least, an interesting trade-off between destructiveness and stealthiness is discovered, which is a fundamental issue involved in SSDF attack, however, ignored by most of the previous studies.

**Keywords:** Cognitive radio; Spectrum sensing data falsification attack; Destructiveness; Stealthiness

## 1 Introduction

Cognitive radio (CR) has been regarded as a promising technology to improve the spectrum utilization [1]. To enable CR, cooperative spectrum sensing, among multiple spectrum sensors, is one of the key technologies [2]. However, due to the openness of low-layer protocol stack of CR, the reliability of cooperative spectrum sensing is challenged by many security threats [3].

The most well-known security threat is the spectrum sensing data falsification (SSDF) attack [4], where abnormal or malicious spectrum sensors falsify their true sensing results. The main goal of SSDF attack can be roughly expressed as two points. One point is to decrease the global detection probability for disturbing the normal operation of the primary user (PU). The other is to increase the global probability of false alarm with the purpose of wasting the access opportunities of the honest secondary users (SUs).

Previous studies on SSDF attack modeling can be generally grouped into two classes: hard SSDF attack and soft SSDF attack. Briefly, in hard SSDF attack, malicious SUs falsify their local binary decisions [5-8], while in soft SSDF attack, malicious SUs falsify their received energy values. Compared to hard SSDF attack, soft SSDF attack is generally more powerful and elusory for its relatively larger value space [9-12], since malicious SUs falsify real energy observations, rather than binary decisions, to mislead the fusion center (FC).

Three soft SSDF attack models have been widely adopted to test various secure sensing algorithms: Always Yes [13], Always No [14,15], and Always Adverse [16]. In *Always Yes* soft SSDF attack, an attacker raises its local observations by injecting a positive offset in every sensing slot. In *Always No* attack, an attacker decreases its local observations by injecting a negative offset in every sensing slot. In *Always Adverse* attack, an attacker firstly performs a local binary hypothesis testing between $H_0$ and $H_1$ by comparing its energy observation with a predefined threshold, with $H_0$ denoting the case that the primary signal is absent and $H_1$ otherwise; then, the malicious SU raises its observations when its local binary decision is $H_0$ and decreases its observations when its decision is $H_1$. One main limitation of the existing soft SSDF attack models is that they are oversimplified and not general enough to serve as the baseline for the design of counter-attack or secure sensing algorithms.

Motivated by the observations above, in this paper, we start with an objective to develop a more general soft SSDF attack model, which should go beyond the existing

*Correspondence: wqhqhw@163.com; dingguoru@gmail.com
[†]Equal contributors
College of Communications Engineering, PLA University of Science and Technology, Yudao Road, Nanjing 210007, China

models and include them as special cases. We also consider that each attacker should be smart to have dual goals in mind: (i) causing harmful disturb to cooperative spectrum sensing and (ii) protecting itself against being easily detected. Specifically, the main contributions of this paper are as follows:

- Propose a generic probabilistic soft SSDF attack model and derive the corresponding closed-form expressions of global sensing performance at the fusion center.
- Analyze the destructiveness of the proposed attack model under three general scenarios and obtain the corresponding optimal attack strategies.
- Define a stealthiness metric and analyze the stealthiness of the proposed attack model under a classical secure sensing algorithm.
- Discover an interesting trade-off between destructiveness and stealthiness, which is a fundamental issue involved in SSDF attack, however, ignored by most of the previous studies.

The remainder of this paper is organized as follows. Section 2 presents the spectrum sensing preliminaries. In Section 3, we formulate the proposed probabilistic soft SSDF attack model and present the analysis of its impacts on the sensing performance. Analytical results on destructiveness and stealthiness of the proposed attack model are provided in Sections 4 and 5, respectively. Numerical results are given in Section 6, and conclusions are provided in Section 7.

## 2 Spectrum sensing preliminaries

As shown in Figure 1, we consider a cooperative spectrum sensing system consisting of $N$ SUs and a FC. Each SU conducts energy detection and transmits its observation to the FC. At the FC, the global decision is made based on the combination of observations. In particular, there are some malicious SUs reporting falsified observations to the FC to deteriorate the spectrum sensing performance.

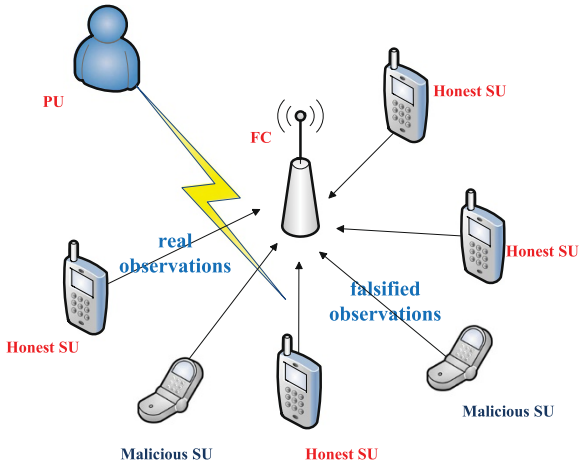


**Figure 1 Cooperative spectrum sensing system.** PU, primary user; SU, secondary user; FC, fusion center.

For a given frequency band, spectrum sensing is generally formulated as a binary hypotheses as follows:

$$\begin{aligned} H_0 &: r_i(t) = n_i(t), \quad i = 1, 2 \ldots, N \\ H_1 &: r_i(t) = h_i(t)s_i(t) + n_i(t), \quad i = 1, 2 \ldots, N, \end{aligned} \tag{1}$$

where $H_0$ denotes the case that the primary signal is absent and $H_1$ denotes the case that PU is present, $N$ is the number of SUs, $r_i(t)$ is the $t$-th sample of the $i$-th SU's received signal, $s_i(t)$ is the PU's transmit signal, $h_i(t)$ is the channel gain, and $n_i(t)$ denotes the additive white Gaussian noise (AWGN).

With an energy detector, the collected energy observation at the $i$-th SU can be given as $x_{Ei} = \sum_{t=1}^{2U} |r_i(t)|^2$, where $U = TW$ is the time-bandwidth product. According to the central limit theorem, when $U$ is large enough (e.g., $U >> 10$), $x_{Ei}$ can be well approximated as a Gaussian random variable under both hypotheses $H_0$ and $H_1$ as follows [14,16,17]:

$$\begin{cases} H_0 : x_{Ei} \sim N\left(u_{0i}, \sigma_{0i}^2\right) \\ H_1 : x_{Ei} \sim N\left(u_{1i}, \sigma_{1i}^2\right), \end{cases} \tag{2}$$

where $u_{0i} = 2U$, $\sigma_{0i}^2 = 4U$, $u_{1i} = 2U(\gamma_i + 1)$, $\sigma_{1i}^2 = 4U(2\gamma_i + 1)$ and $\gamma_i$ is the received SNR of the $i$th SU.

The local binary decision $d_i$ at the $i$-th SU can be obtained by comparing its energy observation with a local threshold $\eta_i$,

$$x_{Ei} \underset{d_i=H_0}{\overset{d_i=H_1}{\gtrless}} \eta_i. \tag{3}$$

At the FC, a weighted combination is generally used to obtain the global decision $D$ as follows:

$$x_E = \sum_{i=1}^{N} w_i x_{Ei} \underset{D=H_0}{\overset{D=H_1}{\gtrless}} \eta_f \tag{4}$$

where $\eta_f$ is the global threshold at the FC and $w_i \in [0, 1]$ is the weight assigned to the $i$-th SU by the FC, and $\sum_{i=1}^{N} w_i = 1$.

## 3 Probabilistic soft SSDF attack

In this section, we will propose a generic soft SSDF attack model and present the analysis of its impacts on the sensing performance. Before going into deep analysis, we declare that a generic and effective SSDF attack model should at least have the following features:

- Attackers should be able to exploit their local sensing results to implement effective attacks, and the

imperfection of the local sensing results should also be considered.

- Attackers should be able to jointly consider harmfully disturbing the FC to obtain wrong decisions and reliably protecting itself from being easily detected, by properly adjusting attack parameters.

### 3.1 The proposed attack model

Based on considerations previously mentioned, a *probabilistic soft SSDF attack model* is proposed as follows. Firstly, an attacker (say, the $i$-th SU) makes its local binary decision via (3). Then, it utilizes a probability $p_i$ to decide whether to perform attack. If it decides to attack, it will randomly produce a Gaussian value as sensing result to report; otherwise, it will hold its true observation. Mathematically, this attack model can be written as

| Local observation | Local decision | Reported result |
|---|---|---|
| $x_{Ei}$ | $H_0$ | $\begin{cases} \xrightarrow{p_i} x \sim N(u_{2i}, \sigma_{2i}^2) \\ \xrightarrow{1-p_i} x = x_{Ei} \end{cases}$ |
| $x_{Ei}$ | $H_1$ | $\begin{cases} \xrightarrow{p_i} x \sim N(u_{3i}, \sigma_{3i}^2) \\ \xrightarrow{1-p_i} x = x_{Ei} \end{cases}$ |

(5)

where $u_{2i}$ and $\sigma_{2i}^2$, respectively, denote the mean and variance when the local decision of the $i$-th SU is $H_0$ (i.e., PU is absent), $u_{3i}$ and $\sigma_{3i}^2$ denote the mean and variance when the local decision is $H_1$. Obviously, for an honest SU, the attack probability equals to zero. For a malicious SU, the attack probability $p_i \in (0, 1)$. Naturely, the two mean values of random distributions have such a relation: $u_{2i} \geq u_{3i}$, as the attacker generally falsifies sensing results by reversing them. To facilitate the following analysis, we define $(u_{2i}, u_{3i})$ as the attack strength and consider the case $\sigma_{2i}^2 = \sigma_{3i}^2 = \sigma_{1i}^2$.

The attack model in (5) is general enough to include the existing models as special cases, via properly adjusting the attack parameters $(u_{2i}, u_{3i}, p_i)$. For example, Always No [13], Always Yes [14,15], and Always Adverse attacks [16] can be realized when $(u_{2i}, u_{3i}, p_i)$ is set as $(u_{0i}, u_{0i}, 1)$, $(u_{1i}, u_{1i}, 1)$ and $(u_{1i}, u_{0i}, 1)$, respectively. In particular, the attack probability $p_i$ can make the proposed attack more elusory and flexible.

### 3.2 Local sensing performance under probabilistic soft SSDF attack

For the proposed attack model in the Section 3.1, the probability density function (PDF) of the reported result by the $i$-th malicious SU, under hypothesis $H_0$ and $H_1$, can be respectively calculated as

$$\begin{aligned} g_{H_0 i}(x) = & \lim_{\Delta \to 0} \frac{1}{\Delta} \left[ \int_x^{x+\Delta} f\left(\frac{x-u_{0i}}{\sigma_{0i}}\right) dx\,(1-p_i) \right. \\ & + \int_x^{x+\Delta} f\left(\frac{x-u_{2i}}{\sigma_{2i}}\right) dx \left(1 - Q\left(\frac{\eta_i - u_{0i}}{\sigma_{0i}}\right)\right) p_i \\ & \left. + \int_x^{x+\Delta} f\left(\frac{x-u_{3i}}{\sigma_{3i}}\right) dx Q\left(\frac{\eta_i - u_{0i}}{\sigma_{0i}}\right) p_i \right] \\ = & f\left(\frac{x-u_{0i}}{\sigma_{0i}}\right)(1-p_i) + \left(1 - Q\left(\frac{\eta_i - u_{0i}}{\sigma_{0i}}\right)\right) \\ & \times f\left(\frac{x-u_{2i}}{\sigma_{2i}}\right) p_i + Q\left(\frac{\eta_i - u_{0i}}{\sigma_{0i}}\right) f\left(\frac{x-u_{3i}}{\sigma_{3i}}\right) p_i, \end{aligned} \tag{6}$$

$$\begin{aligned} g_{H_1 i}(x) = & \lim_{\Delta \to 0} \frac{1}{\Delta} \left[ \int_x^{x+\Delta} f\left(\frac{x-u_{1i}}{\sigma_{1i}}\right) dx\,(1-p_i) \right. \\ & + \int_x^{x+\Delta} f\left(\frac{x-u_{2i}}{\sigma_{2i}}\right) dx \left(1 - Q\left(\frac{\eta_i - u_{1i}}{\sigma_{1i}}\right)\right) p_i \\ & \left. + \int_x^{x+\Delta} f\left(\frac{x-u_{3i}}{\sigma_{3i}}\right) dx Q\left(\frac{\eta_i - u_{1i}}{\sigma_{1i}}\right) p_i \right] \\ = & f\left(\frac{x-u_{1i}}{\sigma_{1i}}\right)(1-p_i) + \left(1 - Q\left(\frac{\eta_i - u_{1i}}{\sigma_{1i}}\right)\right) \\ & \times f\left(\frac{x-u_{2i}}{\sigma_{2i}}\right) p_i + Q\left(\frac{\eta_i - u_{1i}}{\sigma_{1i}}\right) f\left(\frac{x-u_{3i}}{\sigma_{3i}}\right) p_i, \end{aligned} \tag{7}$$

where $f\left(\frac{x-u_i}{\sigma_i}\right)$ represents the PDF of the Gaussian variable $x$ with the mean $u_i$ and standard deviation $\sigma_i$, $Q(x)$ is the Gaussian Q-function and $\eta_i$ is local threshold.

### 3.3 Global sensing performance under probabilistic soft SSDF attack

In a cooperative spectrum sensing system with a FC and $N$ SUs, among which the first $k$ SUs are malicious attackers, the FC fuses results from both malicious SUs and honest SUs via Equation 4. The fusion result's PDF, under hypothesis $H_0$ and $H_1$, can be respectively calculated as

$$\begin{aligned} g_{mH_0}(x) = & \sum_{\mathrm{m_1}=[0,2,3]} \cdots \sum_{\mathrm{m_k}=[0,2,3]} a_{m_1 1} a_{m_2 2} \cdots a_{m_k k} \\ & \cdot f\left( \frac{x - w_1 u_{m_1 1} - w_2 u_{m_2 2} \cdots - w_k u_{m_k k} - u_{h0}}{\sqrt{{w_1}^2 \sigma_{m_1 1}^2 + {w_2}^2 \sigma_{m_2 2}^2 \cdots + {w_k}^2 \sigma_{m_k k}^2 + \sigma_{h0}^2}} \right), \end{aligned} \tag{8}$$

$$\begin{aligned} g_{mH_1}(x) = & \sum_{\mathrm{m_1}=[1,2,3]} \cdots \sum_{\mathrm{m_k}=[1,2,3]} b_{m_1 1} b_{m_2 2} \cdots b_{m_k k} \\ & \cdot f\left( \frac{x - w_1 u_{m_1 1} - w_2 u_{m_2 2} \cdots - w_k u_{m_k k} - u_{h1}}{\sqrt{{w_1}^2 \sigma_{m_1 1}^2 + {w_2}^2 \sigma_{m_2 2}^2 \cdots + {w_k}^2 \sigma_{m_k k}^2 + \sigma_{h1}^2}} \right). \end{aligned} \tag{9}$$

In (8) and (9), we have

$$a_{0i}=1-p_i, a_{2i}=p_i\left[1-Q\left(\frac{\eta_i-u_{0i}}{\sigma_{0i}}\right)\right], a_{3i}=p_iQ\left(\frac{\eta_i-u_{0i}}{\sigma_{0i}}\right),$$
$$b_{1i}=1-p_i, b_{2i}=p_i\left[1-Q\left(\frac{\eta_i-u_{1i}}{\sigma_{1i}}\right)\right], b_{3i}=p_iQ\left(\frac{\eta_i-u_{1i}}{\sigma_{1i}}\right)$$
$$u_{h0}=\sum_{i=k+1}^{N} w_iu_{i0}, {\sigma_{h0}}^2=\sum_{i=k+1}^{N} {w_i}^2\sigma_{i0}^2, u_{h1}=\sum_{i=k+1}^{N} w_iu_{i1}, {\sigma_{h1}}^2=\sum_{i=k+1}^{N} {w_i}^2\sigma_{i1}^2. \tag{10}$$

Let $P_f$ and $P_d$ denote the probabilities of detection and false alarm at the FC, respectively, which can be obtained as

$$P_f=\Pr\{x_E\geq\eta_f|H_0\}$$
$$=\sum_{\mathrm{m_1}=[0,2,3]}\cdots\sum_{\mathrm{m_k}=[0,2,3]} a_{m_11}a_{m_22}\cdots a_{m_kk}\cdot \cdot Q\left(\frac{\eta_f-w_1u_{m_11}-w_2u_{m_22}\cdots-w_ku_{m_kk}-u_{h0}}{\sqrt{{w_1}^2\sigma_{m_11}^2+{w_2}^2\sigma_{m_22}^2\cdots+{w_k}^2\sigma_{m_kk}^2+\sigma_{h0}^2}}\right), \tag{11}$$

$$P_d=\Pr\{x_E\geq\eta_f|H_1\}$$
$$=\sum_{\mathrm{m_1}=[1,2,3]}\cdots\sum_{\mathrm{m_k}=[1,2,3]} b_{m_11}b_{m_22}\cdots b_{m_kk}\cdot \cdot Q\left(\frac{\eta_f-w_1u_{m_11}-w_2u_{m_22}\cdots-w_ku_{m_kk}-u_{h1}}{\sqrt{{w_1}^2\sigma_{m_11}^2+{w_2}^2\sigma_{m_22}^2\cdots+{w_k}^2\sigma_{m_kk}^2+\sigma_{h1}^2}}\right). \tag{12}$$

## 4 Destructiveness analysis

In this section, we evaluate the impacts of the three model parameters $p_i, u_{2i}, u_{3i}$ on the proposed attack model's destructiveness. Specifically, we analyze three general and actual scenarios in sequence:

(i) *Probabilistic attack*: The optimal attack probability is derived to cause the largest harm to FC's detection performance.
(ii) *Contention attack*: Setting appropriate attack strength, a malicious SU implements the optimal attack to maximize the global probability of false alarm to waste access opportunities of honest SUs.
(iii) *Interference attack*: With specific attack strength, a malicious SU conducts the optimal attack with the purpose of minimizing the global probability of detection to disturb the normal operation of the primary user.

Furthermore, without loss of generality, in the following analysis, the weight $w_i$ is set as $1/N$.

### 4.1 Probabilistic attack

Consider a scenario that a malicious SU aims to deteriorate spectrum sensing performance of the system, raising $P_f$ and reducing $P_d$. Here, we analyze the impacts of the attack probability $p_i$ on performing the above attack objective. The problem can be expressed as:

$$\max_{p_i}\{(1-P_d)P(H_1)+P_fP(H_0)\},$$
$$\text{subject to } u_{2i}=u_{1i}, u_{3i}=u_{0i}. \tag{13}$$

**Theorem 1.** *For the given attack strength* $(u_{2i}, u_{3i})=(u_{1i}, u_{0i})$*, the probability of detection* $P_d$ *decreases with the attack probability* $p_i$ *and the probability of false alarm* $P_f$ *increases with* $p_i$*.*

*Proof.* Given $(u_{2i}, u_{3i})=(u_{1i}, u_{0i}), \forall\Delta>0$, we have

$$P_f(p_i+\Delta)-P_f(p_i)$$
$$=\sum_{\mathrm{m_1}=[0,2,3]} a_{m1}\cdots\sum_{\mathrm{m_i}=[0,2,3]}\left[a_{mi}(p_i+\Delta)-a_{mi}(p_i)\right]\cdots\sum_{\mathrm{m_k}=[0,2,3]} a_{m_kk}Q\left(\frac{\eta_f-\sum_{l=1}^{k}u_{m_il}-u_{h0}}{\sqrt{\sum_{l=1}^{k}\sigma_{m_il}^2+\sigma_{h0}^2}}\right)$$
$$>\sum_{\mathrm{m_1}=[0,2,3]} a_{m1}\cdots\sum_{\mathrm{m_{i-1}}=[0,2,3]} a_{m(i-1)}\sum_{\mathrm{m_{i+1}}=[0,2,3]} a_{m(i+1)}\sum_{\mathrm{m_k}=[0,2,3]} a_{m_kk}$$
$$\cdot\left\{-\Delta\left(1-Q\left(\frac{\eta_i-u_{0i}}{\sigma_{0i}}\right)\right)Q\left(\frac{\eta_f-\sum_{n\neq i}w_nu_{m_n1}-w_iu_{0i}-u_{h0}}{\sqrt{\sum_{n\neq i}{w_n}^2\sigma_{m_nn}^2+{w_i}^2\sigma_{0i}^2+\sigma_{h0}^2}}\right)\right.$$
$$\left.+\Delta\left[1-Q\left(\frac{\eta_i-u_{0i}}{\sigma_{0i}}\right)\right]Q\left(\frac{\eta_f-\sum_{n\neq i}w_nu_{m_n1}-w_iu_{2i}-u_{h0}}{\sqrt{\sum_{n\neq i}{w_n}^2\sigma_{m_nn}^2+{w_i}^2\sigma_{1i}^2+\sigma_{h0}^2}}\right)\right\}. \tag{14}$$

Furthermore, we have

$$\begin{aligned}
&\because \sigma_{1i}^2 > \sigma_{0i}^2, u_{1i} > u_{0i}, \Delta > 0, i = 1, \cdots, k.\\
&\therefore Q\left(\frac{\eta_f - \sum\limits_{n\neq i} w_n u_{m_n 1} - w_i u_{0i} - u_{h0}}{\sqrt{\sum\limits_{n\neq i} {w_n}^2 \sigma_{m_n n}^2 + {w_i}^2 \sigma_{0i}^2 + \sigma_{h0}^2}}\right)\\
&\quad < Q\left(\frac{\eta_f - \sum\limits_{n\neq i} w_n u_{m_n 1} - w_i u_{2i} - u_{h0}}{\sqrt{\sum\limits_{n\neq i} {w_n}^2 \sigma_{m_n n}^2 + {w_i}^2 \sigma_{1i}^2 + \sigma_{h0}^2}}\right)\\
&\therefore P_f\left(p_i + \Delta\right) - P_f\left(p_i\right) > 0
\end{aligned}$$

Consequently, the probability of false alarm $P_f$ increases with the attack probability $p_i$. Similarly, we can obtain $P_d\left(p_i + \Delta\right) - P_d\left(p_i\right) < 0$, and thus the probability of detection $P_d$ decreases with $p_i$. Therefore, the detection error probability $P_e = \{(1 - P_d) P\left(H_1\right) + P_f P\left(H_0\right)\}$ increases with $p_i$. □

Note that Theorem 1 without taking into account any defense or secure sensing algorithms at the FC, obviously, a malicious SU with a high attack probability is prone to being easily found out for its low stealthiness, which will be further studied in the next section.

### 4.2 Contention attack

Consider a scenario that a malicious SU intends to contend with honest SUs for secondary access opportunities, i.e., to induce the FC to maximize the probability of false alarm, which can be expressed as follows:

$$\begin{aligned}
&\max_{(u_{2i}, u_{3i})} P_f,\\
&\text{subject to } P_d = \beta \in (0, 1).
\end{aligned} \tag{15}$$

To simplify proofs, we assume that there exists a single malicious SU (i.e., the $i$-th SU) in the system. Simultaneously, to partially ensure the stealthiness of attack behaviors, attack strength is limited (see Appendix).

**Theorem 2.** *Given the probability of detection as $P_d = \beta$ and the attack probability as $p_i = p_a$, the probability of false alarm $P_f$ increases with $u_{2i}$.*

*Proof.* For a given probability of detection at the FC, we have

$$P_d(u_{2i}, u_{3i}) = \beta. \tag{16}$$

Take the derivation of both sides, we have

$$\frac{du_{3i}}{du_{2i}} = -\frac{b_{2i} f\left(\frac{N\eta_f - u_{2i} - N u_{h1}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h1}^2}}\right)}{b_{3i} f\left(\frac{N\eta_f - u_{3i} - N u_{h1}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h1}^2}}\right)}. \tag{17}$$

From (11), we have

$$\begin{aligned}
\frac{dP_f}{du_{2i}} = {} & a_{2i} f\left(\frac{N\eta_f - u_{2i} - N u_{h0}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h0}^2}}\right)\\
& - a_{3i} f\left(\frac{N\eta_f - u_{3i} - N u_{h0}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h0}^2}}\right)\frac{du_{3i}}{du_{2i}}.
\end{aligned} \tag{18}$$

Based on limitation of attack strength in the Appendix, we have

$$\begin{cases}
\dfrac{a_{2i}}{a_{3i}} > 1 > \dfrac{b_{2i}}{b_{3i}}\\
\left|\dfrac{N\eta_f - u_{2i} - N u_{h0}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h0}^2}}\right| < \left|\dfrac{N\eta_f - u_{3i} - N u_{h0}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h0}^2}}\right|\\
\left|\dfrac{N\eta_f - u_{3i} - N u_{h1}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h1}^2}}\right| < \left|\dfrac{N\eta_f - u_{2i} - N u_{h1}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h1}^2}}\right|.
\end{cases} \tag{19}$$

$$\therefore \frac{b_{3i} f\left(\frac{N\eta_f - u_{3i} - N u_{h1}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h1}^2}}\right)}{b_{2i} f\left(\frac{N\eta_f - u_{2i} - u_{h1}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h1}^2}}\right)} > 1 > \frac{a_{3i} f\left(\frac{N\eta_f - u_{3i} - N u_{h0}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h0}^2}}\right)}{a_{2i} f\left(\frac{N\eta_f - u_{2i} - N u_{h0}}{\sqrt{\sigma_{1i}^2 + N^2 \sigma_{h0}^2}}\right)}. \tag{20}$$

$$\therefore \frac{dP_f}{du_{2i}} > 0. \tag{21}$$

□

Theorem 2 points out that the global probability of false alarm can reach the maximum when $u_{2i}$ reaches the available maximum. This theorem provides us with an approach to derive the optimal solution of attack strength to the optimization in (15). Fixed $P_d$ provides an implicit function about $u_{3i}$ and $u_{2i}$ whose range is limited in the Appendix. Then based on Theorem 2, the optimal value can be selected from the set of $(u_{2i}, u_{3i})$ satisfying the function.

### 4.3 Interference attack

Consider another scenario that a malicious SU aims to bring harmful interference to disturb the normal operation of the PU, i.e., to minimize the probability of detection, which can be formulated as

$$\begin{aligned}
&\min_{(u_{2i}, u_{3i})} P_d,\\
&\text{subject to } P_f = \alpha \in (0, 1).
\end{aligned} \tag{22}$$

**Theorem 3.** *Given the probability of false alarm as $P_f = \alpha$ and the attack probability as $p_i = p_a$, the probability of detection decreases with $u_{3i}$.*

*Proof.* For a given probability of false alarm at the FC, we have

$$P_f(u_{2i}, u_{3i}) = \alpha. \tag{23}$$

Take the derivation of both sides, we have

$$\frac{du_{2i}}{du_{3i}} = -\frac{b_{3i} f\left(\frac{N\eta_f - u_{3i} - Nu_{h1}}{\sqrt{\sigma_{1i}^2 + N^2\sigma_{h1}^2}}\right)}{b_{2i} f\left(\frac{N\eta_f - u_{2i} - Nu_{h1}}{\sqrt{\sigma_{1i}^2 + N^2\sigma_{h1}^2}}\right)}.$$

From (12), it can be calculated as follows:

$$\frac{dP_d}{du_{3i}} = a_{3i} f\left(\frac{N\eta_f - u_{3i} - Nu_{h0}}{\sqrt{\sigma_{1i}^2 + N^2\sigma_{h0}^2}}\right)\frac{du_{2i}}{du_{3i}} - a_{2i} f\left(\frac{N\eta_f - u_{2i} - Nu_{h0}}{\sqrt{\sigma_{1i}^2 + N^2\sigma_{h0}^2}}\right) \tag{24}$$

Based on the results in (19) and (20), we finally have

$$\frac{dP_d}{du_{3i}} < 0. \tag{25}$$

□

Theorem 3 points out that the global probability of detection can reach the maximum when $u_{3i}$ reaches the available minimum. This theorem provides us with an approach to derive the optimal solution of attack strength to the optimization in (22). Fixed $P_f$ provides an implicit function about $u_{3i}$ and $u_{2i}$ whose range is limited in Appendix. Then based on Theorem 3, the optiaml value can be selected from the set of $(u_{2i}, u_{3i})$ saitisfying the function.

## 5 Stealthiness analysis

In the previous section, analysis on destructiveness is done without taking into consideration any defense or secure sensing algorithms at the FC, while in this section, we consider that a classical secure sensing algorithm developed in [18] is adopted at the FC to find out the potential attackers. Therefore, stealthiness of the proposed attack model should further be studied.

Current secure algorithms at the FC mainly leverage history sensing results to identify malicious SUs [3]. To ensure the generality of the stealthiness analysis, a classical algorithm developed in [18] is chosen in this paper. Breifly, we first review this algorithm as follows.

Initially, all SUs are treated as reliable ones with a reputation value of $r_i(0)$. Then, the reputation value of the $i$-th SU at the $k$-th time slot is updated as [18]

$$r_i(k) = r_i(k-1) + (-1)^{d_i(k)+D(k)} \tag{26}$$

where $D(k)$ represents the global decision at the FC and $d_i(k)$ is the $i$-th SU's local decision at the $k$-th time slot. When the reputation value is lower than a discarded threshold $\lambda$, the SU is identified as a malicious one; otherwise, it is treated as a honest one. In [18], $r_i(0) = \lambda + \triangle$, where $\lambda$ is set as 1 and $\triangle$ is set as 4. At the $k$-th time slot, the local decision of the $i$-th SU is obtained as follows:

$$\Gamma_i(k) \underset{d_i(k)=H_0}{\overset{d_i(k)=H_1}{\gtrless}} \eta_i \tag{27}$$

where

$$\Gamma_i(k) = \ln \frac{\Pr(x_{Ei}(k)\,|H_1)}{\Pr(x_{Ei}(k)\,|H_0)}$$

The global decision $D(k)$ is calculated as

$$\Gamma(k) = \sum_{j\in S(k)} w_j(k)\Gamma_i(k) \underset{D(k)=H_0}{\overset{D(k)=H_1}{\gtrless}} \eta_f \tag{28}$$

where $S(k)$ represents the set of SUs with the reputation values larger than the threshold $\lambda$, and

$$w_j(k) = \frac{r_j(k-1)}{\sum_{i\in S(k)} r_i(k-1)}. \tag{29}$$

Through analysis about the previous algorithm, we define a stealthiness metric $\psi$ as follows:

$$\psi(k) = \begin{cases} \dfrac{\frac{1}{N_m}\sum_{i=1}^{N_m} r_i^m(k)}{\frac{1}{N-N_m}\sum_{j=1}^{N-N_m} r_j^h(k)}, & \sum_{i=1}^{N_m} r_i^m(k) > 0 \\ 0, & \text{otherwise} \end{cases} \tag{30}$$

where $N_m$ is the number of malicious SUs, $r_i^m(k)$ denotes the reputation value of the $i$-th malicious SU, and $r_i^h(k)$ denotes the reputation value of the $i$-th honest SU. We choose honest SUs as a baseline and the FC hardly distinguish a malicious SU from malicious ones when the stealthiness metric is close to 1, that is to say, the malicious SU has good stealthiness. Deeper analysis is done in the next section.

## 6 Performance evaluation and discussions

In this section, numerical simulations are used to verify the analytical results on destructiveness and stealthiness of the proposed probabilistic soft SSDF attack model.

In the following simulations, the cooperative spectrum sensing system consists of a FC and $N$ SUs, among which $N_m$ SUs are malicious. The average received SNR is set as -7 dB and the local threshold is obtained by setting the

local false alarm probability as 0.1. The time bandwidth product $U$ is 100. The probability of primary signal being present is set as $P(H_1) = 0.5$. Without loss of generality, in the following simulations, for all malicious SUs, we set $A = 1.1u_{1i}, B = 0.9u_{0i}, u_{2i} = u_2, u_{3i} = u_3, \forall i = 1, \ldots, N_m$.

### 6.1 Destructiveness evaluation

Figure 2 shows the global sensing performance at the FC under the proposed SSDF attack model, in terms of global detection error probability $P_e$, defined as

$$P_e = P(H_1)(1 - P_d) + P(H_0)P_f. \tag{31}$$

In the simulation, $N = 10, N_m = 3$. Curves with four groups of attack strengths $(u_2, u_3)$ are plotted. We also plot the curve without malicious SUs as the baseline. It is shown in Figure 2 that (i) the global detection error probability increases with the attack probability, (ii) when the attack strength increases, i.e., increasing of $u_2$ and/or decreasing of $u_3$, the global detection error probability increases, and (iii) simulations match the theoretical results very well.

Figure 3 shows the global false alarm probability versus different detection probabilities, when the malicious SU implements contention attack as discussed in Section 4.2. In the simulation, the attack probability is set as 0.7 and the optimal values of attack strength $(u_2, u_3)$ is obtained according to Theorem 2. Remind that in Theorem 2, we consider the case that there is a single malicious SU in the system and we set $N = 5, N_m = 1$. Other two curves are also presented for comparison when $0.95u_2$ and $0.9u_2$ are set lower than the optimal value $u_2$, $u_3^*$ and $u_3^{**}$ are correspondingly calculated for the given $P_d$. It can be observed in Figure 3 that the global false alarm probability $P_f$ gets its maximum when the malicious SU implements contention attack.

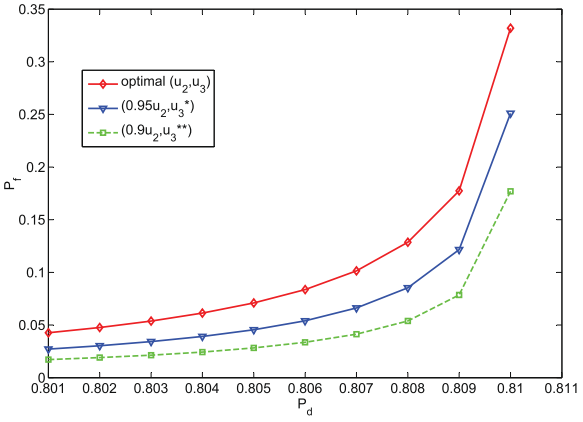


**Figure 3 Global detection performance at the FC under contention attack.** $N = 5, N_m = 1$.

Figure 4 shows the global detection probability versus different false alarm probabilities when the malicious SU implements interference attack as discussed in Section 4.3. In the simulation, the attack probability is set as 0.7 and optimal value of attack strength $(u_2, u_3)$ is obtained according to Theorem 3. Remind that in Theorem 2, we consider the case that there is a single malicious SU in the system and we set $N = 5, N_m = 1$. Other two curves are also presented for comparison when $1.01u_3$ and $1.02u_3$ are set larger than the optimal value $u_3$, $u_2^*$ and $u_2^{**}$ are correspondingly calculated for the given $P_f$. As shown in Figure 4, the global detection probability $P_d$ gets the minimum when the malicious SU implements interference attack.

### 6.2 Stealthiness evaluation

In this subsection, we study the impact of the attack probability on stealthiness of the proposed attack model. The

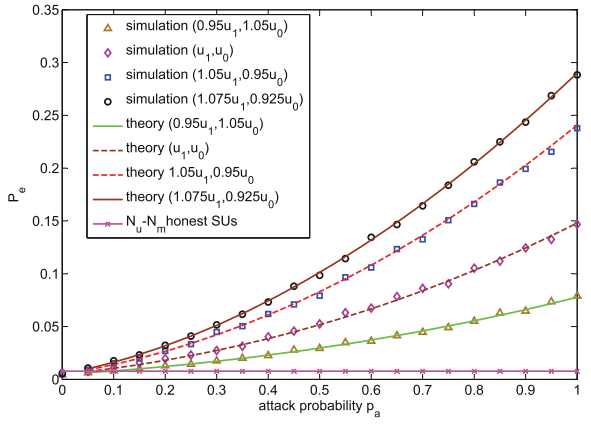


**Figure 2 Global detection performance at the FC under different attack probabilities.** $N = 10, N_m = 3$.

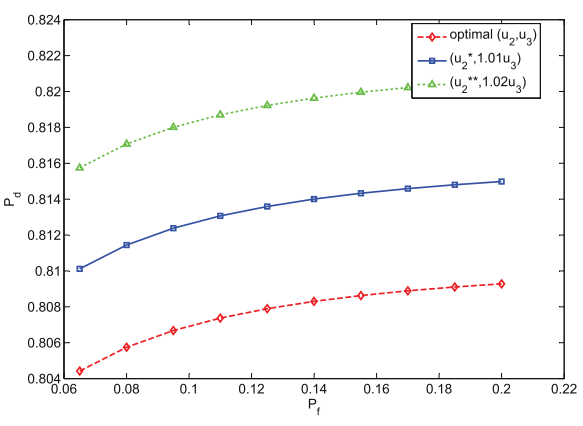


**Figure 4 Global detection performance at the FC under interference attack.** $N = 5, N_m = 1$.

attack strength is set as $u_2 = u_1, u_3 = u_0$, and $N = 10, N_m = 3$.

Figure 5 shows the evolution of the stealthiness metric, defined in (30), under different attack probabilities. Two main observations are as follows:

- After a few sensing slots, the stealthiness metric restrains itself to a constant value $\psi$ for each given attack probability $p_a$.
- Malicious users' stealthiness deteriorates with the attack probability $p_a$.

Mathematically, denote $k$ as the index of the sensing slot, the first observation above can be rewritten as:

$$\exists \text{ constant } M \in \mathbb{R}, k > M, \psi(k) = \psi = h(p_a) \tag{32}$$

As shown in Figure 5, the secure algorithm is not sufficiently valid to probabilistic attack. Essentially, the secure algorithm in [18] uses a reputation accumulation mechanism based on history decision information. However, the reputation accumulating process is ruined by such malicious SUs that may behave in a honest manner, then turn malicious at the next moment. Furthermore, there exists a probability of collision $p_c(k)$, with which the $i$-th malicious SU's local decision $d_i^m(k)$ is inconsistent with FC's global decision $D(k)$, which can be denoted as

$$\begin{aligned} p_c(k) &= P(d_i^m(k) \neq D(k)) \\ &= P(H_0)P(d_i^m(k) \neq D(k)|H_0) + P(H_1)P(d_i^m(k) \neq D(k)|H_1) \end{aligned} \tag{33}$$

Simultaneously, there is a collision between FC's global decision and a honest user's local decision with a probability $p_c{}'(k)$ during the $k$-th sensing slot as well. Consistent with the stealthiness metric, the collision probabilities restrain themselves to constant values as well.

$$\exists M, k > M, \begin{cases} p_c(k) = p_c \\ p_c{}'(k) = p_c{}'. \end{cases} \tag{34}$$

Furthermore, we can obtain the relation between collision probabilities and the stealthiness metric as follows

$$\psi = \frac{p_c{}'}{p_c}. \tag{35}$$

The second observation above is opposite to the results in Figure 2. Briefly, destructiveness in Figure 2 increases with the attack probability while stealthiness in Figure 5 decreases with the attack probability. Consequently, there should be a trade-off between stealthiness and destructiveness with respect to the attack probability.

Motivated by this discovery, we further plot Figure 6, which shows the global detection error probability $P_e$ of the robust defense or secure sensing algorithm developed in [18], under the proposed probabilistic soft attack model. In the simulation, $N = 10, N_m = 3$.

Although the $x$-axis and $y$-axis of Figures 2 and 6 are of the same content, their results are quite different. The main reason behind the differences lies on the fact that the secure sensing algorithm developed in [18] is adopted at the FC in producing Figure 6 to discard the detected malicious SUs before the global fusion. It is observed in Figure 6 that with defense or secure sensing algorithms into consideration, there generally exists an optimal attack probability $p_a \in (0, 1]$, not necessarily equal to 1.

Taking the curve with the attack strength $(u_1, u_0)$ as an example and comparing it with the curve without malicious SUs, we can divide the attack probability into three intervals:

- An interval with a low attack probability than the first point drawn as a circle in Figure 6, named *role reversal interval*, where malicious SUs' participation does not pose harm to FC's global fusion, but is beneficial to it.
- An interval of a high attack probability than the second point drawn as a square, named *exposure*

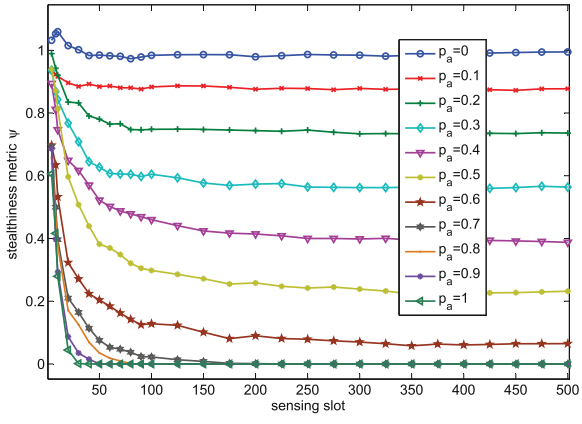


**Figure 5 Stealthiness under different attack probabilities.** $N = 10, N_m = 3$.

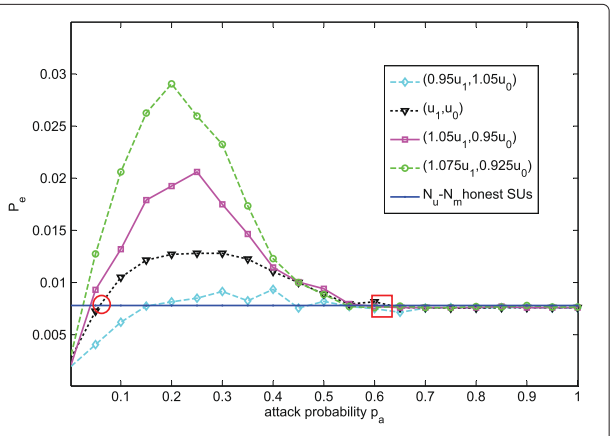


**Figure 6 Relationship between attack performance and attack probability with destructiveness and stealthiness into consideration.** $N = 10, N_m = 3$.

*interval*, where attackers are found out and removed, and their powerful attack action is nearly transparent to FC for their low stealthiness.

- An interval of a medium attack probability between the above two points, named *favorable attack interval*, where effective but stealthy attack can be implemented.

## 7 Conclusions

In this paper, a generic and novel probabilistic soft SSDF attack model has been proposed. In the proposed attack model, a malicious SU has a certain probability, varying from 0 to 1, to conduct attacks. Under this generalized SSDF attack model, we firstly obtained closed-form expressions of the global sensing performance at the fusion center. Then, we theoretically evaluated the performance of the proposed attack model, in terms of destructiveness and stealthiness, sequentially. Moreover, numerical simulations match the analytical results well. An interesting trade-off between destructiveness and stealthiness has also been discovered, which is a fundamental issue involved in SSDF attack, however, ignored by most of the previous studies.

## Appendix

### Limitation of attack strength

An extremely large or small value viciously reported by malicious users will bring about huge damage for the fusion center without any defense schames, but such attack behaviors are very prone to be identified. So, before studying optimal attack parameters' setting, we list restricted conditions as follows:

$$\begin{cases} A \geqslant u_{2i} \geqslant u_{3i} \geqslant B & (a) \\ N\eta_f - u_{h1} < \dfrac{u_{3i} + u_{2i}}{2} < N\eta_f - u_{h0} & (b) \end{cases} \tag{36}$$

where $A$ and $B$ are constants. In the condition $(a)$, attack stength are restricted within certain intervals determined by the constants $A$ and $B$ and the relationship of size between $u_{2i}$ and $u_{3i}$ is referred to before, revealing the attack intention. Further, the condition $(b)$ is used to avoid the large deviation from honest reports through the inter-constraint relationship between $u_{2i}$ and $u_{3i}$, and the two sides of the inequation can be used to denote the residual of FC's threshold minus the honest means.

#### Competing interests

The authors declare that they have no competing interests.

#### Acknowledgements

This work is supported in part by the National Natural Science Foundation of China under Grant No. 61172062 and No. 61301160 and in part by Jiangsu Province Natural Science Foundation under Grant No. BK2011116.

Received: 2 March 2014 Accepted: 20 May 2014
Published: 31 May 2014

#### References

1. J Mitola, Cognitive radio: an integrated agent architecture for software defined radio. Ph.D. Dissertation, KTH (2000)
2. Q Wu, G Ding, J Wang, YD Yao, Spatial-temporal opportunity detection in spectrum-heterogeneous cogntive radio networks: two-dimensional sensing. IEEE Trans. Wireless Commun. **12**(2), 516–526 (2013)
3. H Rifa Pous, MJ Blasco, C Garrigues, Review of robust cooperative spectrum sensing techniques for cognitive radio networks. Wireless Personal Commun. **67**(2), 175–198 (2012)
4. R Chen, JM Park, YT Hou, Toward secure distributed spectrum sensing in cognitive radio networks. IEEE Commun. Mag. **46**(4), 50–55 (2008)
5. F Penna, Y Sun, L Dolecek, D Cabric, Detecting and counteracting statistical attacks in cooperative spectrum sensing. IEEE Trans. Signal Process. **60**(4), 1806–1822 (2012)
6. JN Yao, Q Wu, J Wang, Attacker detection based on dissimilarity of local reports in collaborative spectrum sensing. IEICE Trans. Commun. **9**, 3024–3027 (2012)
7. H Li, Z Han, Catch me if you can: an abnormality detection approach for collaborative spectrum sensing in cognitive radio networks. IEEE Trans. Wireless Commun. **9**(11), 3554–3565 (2010)
8. A Vempaty, L Tong, P Varshney, Distributed inference with byzantine data: state-of-the-art review on data falsification attacks. IEEE Signal Process. Mag. **30**(5), 65–75 (2013)
9. F Farmani, MA Jannat-Abad, R Berangi, Detection of SSDF attack using SVDD algorithm in cognitive radio networks, in *IEEE Third International Conference on Computational Intelligence, Communication Systems and Networks (CICSyN)*: 26–28 July 2011 (IEEE, Bali, 2011), pp. 201–204
10. AW Min, KG Shin, X Hu, Secure cooperative sensing in IEEE 802.22 WRANs using shadow fading correlation. IEEE Trans. Mobile Comput. **10**(10), 1434–1447 (2011)
11. G Ding, Q Wu, YD Yao, JL Wang, YY Chen, Kernel-based learning for statistical signal processing in cognitive radio networks: Theoretical foundations, example applications, and future directions. IEEE Signal Process. Mag. **30**, 126–136 (2013)
12. S Cui, Z Han, S Kar, TT Kim, H Poor, A Tajer, Coordinated data-injection attack and detection in smart grid. IEEE Signal Process. Mag. **29**(5), 106–115 (2012)
13. R Chen, JM Park, K Bian, Robust distributed spectrum sensing in cognitive radio networks, in *INFOCOM*. 13-18 April 2008; Phoenix, AZ (IEEE, 2008), pp. 1876–1884
14. Y Han, Q Chen, JX Wang, An enhanced DS theory cooperative spectrum sensing algorithm against SSDF attack, in *IEEE Vehicular Technol.ogy Conference (VTC Spring)*. 6–9 May 2012; Yokohama (IEEE, 2012), pp.1–5
15. P Kaligineedi, M Khabbazian, VK Bhargava, Secure cooperative sensing techniques for cognitive radio systems, in *IEEE International Conference on Communications*. 19–23 May 2008; Beijing (IEEE, 2008), pp. 3406–3410
16. N Nguyen-Thanh, I Koo, A robust secure cooperative spectrum sensing scheme based on evidence theory and robust statistics in cognitive radio. IEICE Trans. Commun. **12**, 3644–3652 (2009)
17. H Urkowitz, Energy detection of unknown deterministic signals. Proc. IEEE. **55**(4), 523–531 (1967)
18. K Zeng, P Paweczak, D Cabric, Reputation-based cooperative spectrum sensing with trusted nodes assistance. IEEE Commun. Lett. **14**(3), 226–228 (2010)

doi:10.1186/1687-6180-2014-81
**Cite this article as:** Zhang *et al.*: Performance analysis of probabilistic soft SSDF attack in cooperative spectrum sensing. *EURASIP Journal on Advances in Signal Processing* 2014 **2014**:81.