Received December 9, 2017, accepted January 10, 2018, date of publication January 15, 2018, date of current version March 9, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2793906

MAC Based Energy Efficiency in Cooperative Cognitive Radio Network in the Presence of Malicious Users

JIANXIN DAI[1], JUAN LIU[2], CUNHUA PAN[3], JIANGZHOU WANG[4], (Fellow, IEEE), CHONGHU CHENG[2], and ZHILIANG HUANG[5]

[1]School of Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
[2]College of Telecommunications and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[3]Queen Mary University of London, London E1 4NS, U.K.
[4]School of Engineering and Digital Arts, University of Kent, Canterbury CT2 7NZ, U.K.
[5]College of Mathematics, Physics, and Information Engineering, Zhejiang Normal University, Jinhua 321004, China

Corresponding author: Cunhua Pan (c.pan@qmul.ac.uk)

This work was supported in part by the Postdoctoral Research Funding Plan in Jiangsu Province under Grant 1501073B, in part by the Natural Science Foundation of Nanjing University of Posts and Telecommunications under Grant NY214108, in part by the Natural Science Foundation of China under Grant 61401399 and Grant 61701254, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20170901, and in part by the Open Research Fund of National Mobile Communications Research Laboratory, Southeast University under Grant 2016D05 and Grant 2017D06.

ABSTRACT In cognitive radio networks, cooperative spectrum sensing (CSS) is generally adopted for improving spectrum sensing accuracy to increase spectrum utilization and avoid interference with the primary users. However, some malicious secondary users (SUs) may affect the CSS performance by inducing false observation bits for fusion. The message authentication code (MAC) is a promising technique to avoid the damage from the spectrum sensing data falsification (SSDF) attacks. In this paper, as both the more spectrum sensing nodes and the MAC reporting bits result in extra energy consumption, we propose an energy efficiency model to capture the effects of the length of MAC and the number of cooperative SUs under independent and collaborative SSDF attacks, respectively, and analyze the existence of the optimal length of MAC and the optimal number of cooperative SUs that can achieve the maximum value of energy efficiency, respectively. Simulation results are provided to show that the CSS scheme based on MAC can resist SSDF attacks and the accuracy of the theoretical analysis is also validated.

INDEX TERMS Cooperative spectrum sensing, spectrum sensing data falsification (SSDF) attack, message authentication code, energy efficiency.

I. INTRODUCTION

To further improve the spectrum utilization and meet the individual communications services, cognitive radio has emerged as an intelligent technology in the future wireless communication system [1]–[5]. In the cognitive radio networks (CRNs), the vacant licensed spectrum of primary users (PUs) can be utilized by secondary users (SUs) through the spectrum sensing (SS). Many methods have been used to improve the performance, for example, Li *et al.* proposed an effective antenna selection algorithm to significantly improve the performance of interference alignment based CRNs in [3]. Relative to individual spectrum sensing, cooperative spectrum sensing (CSS), which is generally applied in CRNs, can improve the spectrum sensing accuracy even more [6]. Whereas adversaries can compromise some sensor nodes to send false sensing consequences on the basis of the wireless broadcast nature, where spectrum sensing data falsification (SSDF) attacks significantly create CRNs vulnerability [7], [8]. In SSDF attacks, in order to reduce spectrum utilization and degrade overall network performance, compromised nodes may mislead the channel availability decision by operating independently or cooperatively [9]. So as to avoid the damage from SSDF attack, researchers have proposed many countermeasures in CRNs including radio propagation characteristics [10], incentive-based mechanisms [11], trust/reputation based approaches [12], consensus-based approaches [13], [14], hidden Markov models (HMMs)-based malicious user detection approaches [15], a modified combinatorial optimization identification (COI) [16], data cleansing approaches [17] and clustering based methods [18], [19]. However, few related papers consider symmetric cryptographic mechanism, which can produce a message authentication code (MAC) to verify the spectrum sensing data reports [20], [21], because MAC is a low-overhead secure CSS protocol.

Recently, people have paid more attention to energy-efficiency, which is defined as the ratio of the rate to the total power consumption. Energy efficiency is important to CRNs since it is a precedent condition to attain high utilization of the batteries. Cooperative spectrum sensing can improve the spectrum sensing accuracy, but the energy consumption of SUs would linearly increase with the number of sensor nodes which participate in spectrum sensing [22]. In general, when all sensor nodes participate in spectrum sensing, it can maximize the spectral efficiency but may not maximize the energy efficiency. Hence, there have been some literature studying the energy efficient maximization and secure problem for SSDF in CRNs [20]–[24]. A cooperative spectrum sensing scheme was proposed to obstruct SSDF attacks in two attack cases (i.e., independent and cooperative SSDF attacks), and increase the energy efficiency in CRNs [23]. The consequent gain in energy-efficiency is analyzed and evaluated for the CRNs with a frame structure accommodating CSS and cooperation in primary PU's transmission or opportunistic SUs' transmission while maintaining the same SS reliability and target PU's transmission rate [24]. On the other hand, the fusion center (FC), which is responsible for obtaining and processing the local decisions and then making the final decision, needs the information reported by MAC, so using MAC requires extra energy consumption to provide some additional bits. It is for this reason that the number of the additional security bits should be optimized to achieve the maximum energy efficiency [20]. In [21], the objective of energy efficiency maximization was studied with the constraints of CSS report distance, message bit length and report error rate. In addition, the optimal value of message bits was decided only in the K-out-of-N fusion rule with $K = 1$. Therefore, it is critical to study the maximum energy efficiency through jointly optimizing the number of sensor nodes and the number of the additional security bits. In this paper, a MAC based energy efficient cooperative spectrum sensing scheme is proposed to obstruct SSDF attacks and enhance the energy efficiency in CRNs. On the whole, the main contributions of this paper are three aspects.

- We discuss the CSS problems under independent and collaborative SSDF attacks, respectively, and adopt a low-overhead symmetric cryptographic mechanism that reduces the effects of the malicious users on energy efficiency.
- The energy efficiency optimization problem is formulated, where the design variables are the number of cooperative sensor nodes and the number of the additional security bits as design variables. The relations between energy efficiency and two variables is theoretically analyzed under two types of SSDF attacks, respectively.
- Extensive simulation results on the energy efficiency performance along with performance comparison are reported in the different cases.

The rest of this paper is organized as follows: proposed system model is presented in Section II. Section III analyzes the optimization problem and its solution. Numerical results are then provided in Section IV, and the paper is concluded in Section V.

II. SYSTEM MODEL

Consider a CRN with a PU and N SUs, as shown in Figure 1. The cognitive users opportunistically utilize the channels whenever they are idle and perform cooperative spectrum sensing to figure out the presence or absence of primary users over different time slots. A data fusion center gathers the individual binary decisions by the cognitive nodes to make the final decision on spectrum sensing results.

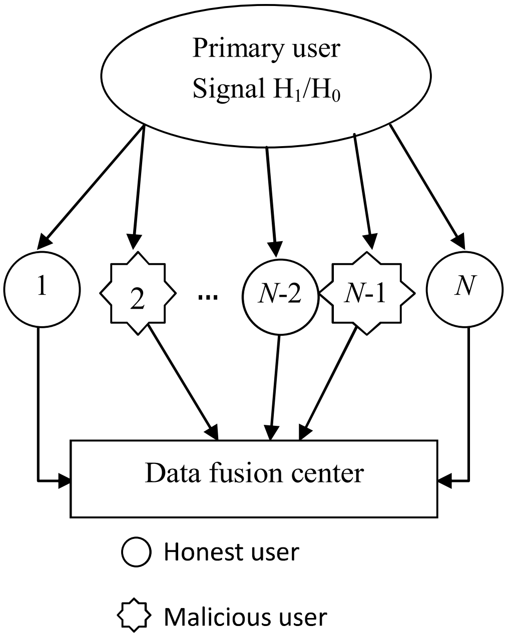


FIGURE 1. CR networks system model in the presence SSDF attack.

A. CSS AND DECISION RULE

Each sensor performs local spectrum sensing independently. The communications between PU transmitter and receiver are carried out with the probability $1 - P_0$, where P_0 is the probability of the channel being idle. To avoid the act of colliding with PU, each SU carries out cyclic energy detection in the target bands. The detection can be transformed into a binary hypothesis problem, in which H_0 indicates that the channel is idle and H_1 indicates that the channel is busy. An energy detector is utilized to integrate the received signal in bandwidth $f_s/2$ over the sensing period τ. The sensor i will decide whether the channel is occupied by PUs or not through comparing the collected energy E_i with a predefined threshold ε_i. The decision is given by

$$D_i = \begin{cases} 1 & E_i > \varepsilon_i \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

The false alarm probability P_f and detection probability P_d of the sensor are defined as

$$P_f = \Pr\{D_i = 1|H_0\} = \Pr\{E_i > \varepsilon_i|H_0\} \tag{2}$$

$$P_d = \Pr\{D_i = 1|H_1\} = \Pr\{E_i > \varepsilon_i|H_1\} \tag{3}$$

which can be written by a Q-function as

$$P_f = Q(\frac{\varepsilon - f_s\tau}{\sqrt{2f_s\tau}}) \tag{4}$$

$$P_d = Q(\frac{\varepsilon - f_s\tau - \gamma}{\sqrt{2f_s\tau + 4\gamma}}) \tag{5}$$

where $\gamma = \sigma_x^2/\sigma_n^2$ is the received signal-to-noise ratio.

The cooperative spectrum sensing performed by multiple sensors can solve the hidden terminal problem as a result of shadowing or multipath fading. Each sensor independently carries out spectrum sensing and comes to a decision. They transmit the decisions to the base station. The base station fuses these decisions to reach the final decision based on some fusion rules, where there are 'OR', 'AND' and 'K/N' [26]. The 'OR' rule can be expressed as

$$Q_d = 1 - \prod_{i=1}^{N}(1 - P_{d,i}), \tag{6}$$

$$Q_f = 1 - \prod_{i=1}^{N}(1 - P_{f,i}) \tag{7}$$

The 'AND' rule can be expressed as

$$Q_d = \prod_{i=1}^{N} P_{d,i}, \tag{8}$$

$$Q_f = \prod_{i=1}^{N} P_{f,i}. \tag{9}$$

And the 'K/N' rule can be expressed as

$$Q_d = \Pr\{D_i = 1|H_1\} = \Pr\left\{\sum_{i=1}^{N} D_i \geq k|H_1\right\}, \tag{10}$$

$$Q_f = \Pr\{D_i = 1|H_0\} = \Pr\left\{\sum_{i=1}^{N} D_i \geq k|H_0\right\}. \tag{11}$$

If M $(M < K < N)$ malicious users exist and they are of the same type, the binary hypothesis test of the system is:

$$\Phi = \sum_{i=1}^{N-M} D_i + \sum_{j=1}^{M} \omega_j \begin{cases} \geq K & H_1 \\ \leq K & H_0 \end{cases} \tag{12}$$

where D_i is the report of SU$_i$ given by (1), ω_j is the report of MU$_j$.

B. ATTACK MODEL

In SSDF attacks, the false spectrum sensing results can be independently or collaboratively sent by the compromised nodes to misdirect the global decision of cooperative spectrum sensing. Two types of SSDF attacks are introduced as follows.

1) INDEPENDENT SSDF ATTACK

Independent SSDF (I-SSDF) attack means to that each node compromised by adversary independently reports its sensing consequence with specific probabilities.

Case 1: Always free Malicious Attack

All malicious users send the '0' to data fusion center. In this case, the detection probability and false alarm probability by the $K/(N - M)$ rule are written as follows, respectively,

$$P_D(M, N) = \sum_{j=K}^{N-M} \binom{N-M}{j} P_d{}^j(1 - P_d)^{N-M-j}, \tag{13}$$

$$P_F(M, N) = \sum_{j=K}^{N-M} \binom{N-M}{j} P_f{}^j(1 - P_f)^{N-M-j}. \tag{14}$$

Case 2: Always busy Malicious Attack

All malicious users send the '1' to data fusion center. In this case, the detection probability and false alarm probability by the $(K - M)/(N - M)$ rule can be written as follows, respectively,

$$P_D(M, N) = \sum_{j=K-M}^{N-M} \binom{N-M}{j} P_d{}^j(1 - P_d)^{N-M-j}, \tag{15}$$

$$P_F(M, N) = \sum_{j=K-M}^{N-M} \binom{N-M}{j} P_f{}^j(1 - P_f)^{N-M-j}. \tag{16}$$

Case 3: Always wrong Malicious Attack

Each malicious user always sends the opposite of the original sensing result to data fusion center. In this case, the detection probability and false alarm probability can be obtained as follows, respectively,

$$P_D(M, N) = \sum_{j=K}^{N-M} \binom{N-M}{j} P_d{}^j(1 - P_d)^{N-M-j} \tag{17}$$

$$P_F(M, N) = \sum_{j=K-M}^{N-M} \binom{N-M}{j} P_f{}^j(1 - P_f)^{N-M-j}. \tag{18}$$

2) COLLABORATIVE SSDF ATTACK

In collaborative SSDF (C-SSDF) attack, those nodes compromised the adversaries, which are selected for spectrum sensing, can collaboratively send false sensing consequences to misdirect the global decision. In particular, they can first interflow their sensing results with each other and collaboratively come to a consistent decision about the licensed channel availability by the L/M rule. Then, the nodes compromised the adversaries report the opposite consistent decision to the data fusion center.

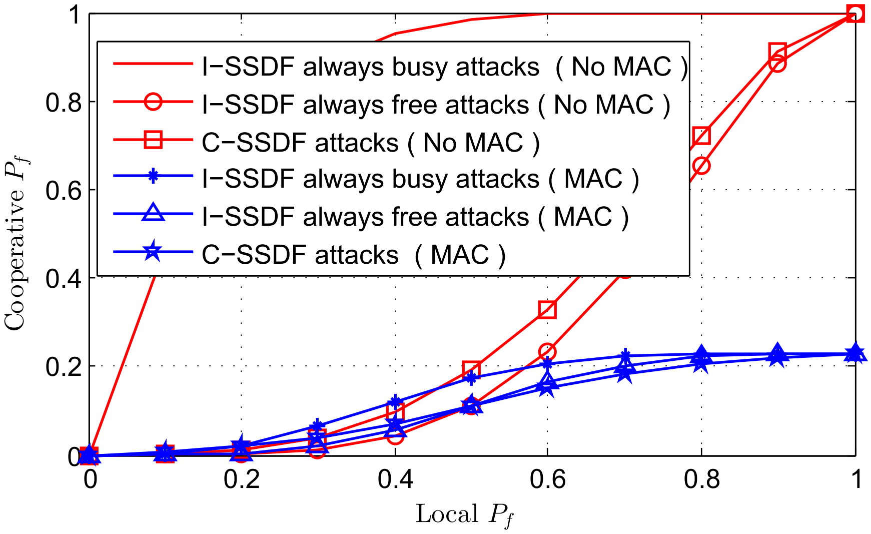


FIGURE 2. The performance comparison of cooperative spectrum sensing system with anti SSDF attack.

Under the L/M fusion rule, the cooperative detection probability $P_{D,m}$ and false alarm probability $P_{F,m}$ of the malicious users are:

$$P_{D,m} = \sum_{i=L}^{M} \binom{M}{i} {P_d}^i (1 - P_d)^{M-i}, \tag{19}$$

$$P_{F,m} = \sum_{i=L}^{M} \binom{M}{i} {P_f}^i (1 - P_f)^{M-i}, \tag{20}$$

where $L = \lceil (M+1)/2 \rceil$, and symbol $\lceil z \rceil$ indicates the smallest integer value greater than z. Let $\alpha = \frac{M}{N}$. Thus, for each node compromised by adversaries under C-SSDF attacks, the cooperative detection probability $P_D(M, N)$ and false alarm probability $P_F(M, N)$, can be unified as

$$P_D(M, N) = (1 - \alpha)P_{D,h} + \alpha(1 - P_{D,m}), \tag{21}$$

$$P_F(M, N) = (1 - \alpha)P_{F,h} + \alpha(1 - P_{F,m}), \tag{22}$$

where

$$P_{D,h} = \sum_{i=Q}^{N-M} \binom{N-M}{i} {P_d}^i (1 - P_d)^{N-M-i}, \tag{23}$$

$$P_{F,h} = \sum_{i=Q}^{N-M} \binom{N-M}{i} {P_f}^i (1 - P_f)^{N-M-i}, \tag{24}$$

$$Q = \lceil (1 - \alpha)K \rceil \,. \tag{25}$$

C. SECURITY MECHANISM TO RESIST SSDF

MAC, also called cryptographic checksum, is used to check on the reported spectrum sensing information. MAC produces a data package of n bits and sends with original data [20]. The MAC is computed with a Hash function using the spectrum sensing reported information as follows:

$$\mathrm{MAC} = C_T(S), \tag{26}$$

where S is local sensing result of 1 bit, the encryption key T is shared between legitimate SUs and FC. Each SU uses generation function to figure the MAC of B-1 bits, and then sends the total B bits data to FC. The FC deduces the MAC of received message on the basis of the same function and encryption key and then compares them with the received MAC to formalize whether the sensing information has been altered.

To resist a replay attack [25], we alter the generation function as

$$\mathrm{MAC} = C_T(S\,|Seq.Number\,) \tag{27}$$

where the *Seq.Number* is expressed as the sequence number of CSS. The value of the *Seq.Number* is renovated through the FC as broadcasting the common control information, but the malicious users are unable to learn about.

To send the SSDF attack resoundingly, the malicious users can randomly produce MAC with an intercept probability $P_x = 1/2^{B-1}$. When MAC length is increased, the SSDF intercept probability of the malicious SU is decreased, and thus security can be guaranteed. Hence the global secure detection probability and global secure false alarm probability in this case can be formulated as follows:

$$P_{D,\mathrm{sec}} = \sum_{i=1}^{M} \binom{M}{i} {P_x}^i (1 - P_x)^{M-i} P_D(i, N), \tag{28}$$

$$P_{F,\mathrm{sec}} = \sum_{i=1}^{M} \binom{M}{i} {P_x}^i (1 - P_x)^{M-i} P_F(i, N). \tag{29}$$

Define the total error probability as

$$P_{E,\mathrm{sec}} = P_{M,\mathrm{sec}} + P_{F,\mathrm{sec}}, \tag{30}$$

where

$$P_{M,\mathrm{sec}} = \sum_{i=1}^{M} \binom{M}{i} {P_x}^i (1 - P_x)^{M-i} (1 - P_D(i, N)). \tag{31}$$

Figure 2 shows the impact of the cooperative spectrum sensing on the cooperative false alarm probability when the

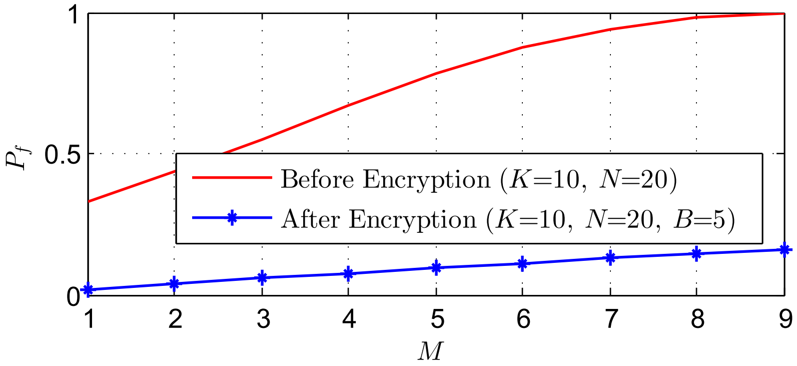


FIGURE 3. Cooperative false alarm probability versus the number of malicious users with anti SSDF attack.

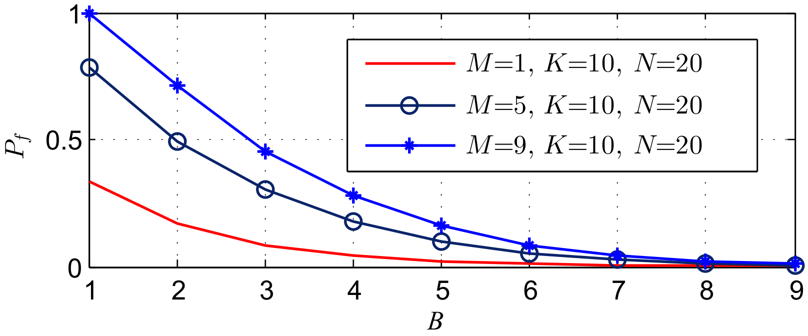


FIGURE 4. Cooperative false alarm probability versus the encrypted information.

system is attacked by SSDF under the K/N criterion. It can be seen that encryption can greatly reduce the cooperative false alarm probability, i.e., the false alarm probability with MAC decreases by 0.79 when the local false alarm probability is 0.5 for always busy independent malicious attack.

Figure 3 shows the relationship between the false alarm probability and the number of malicious users before and after encryption under the same fusion rule ('K/N'). It can be observed that the probability of false alarm increases with the number of malicious users. Before encryption, the resulting effect of the malicious users on the false alarm probability is large. For example, the malicious user number increases from 1 to 10, the probability of false alarm before encryption increases by 0.66, but the probability of false alarm after encryption only increases by a factor of 0.15.

Figure 4 shows the relationship between the probability of false alarm and the amount of encrypted information. As can be seen from the figure, the probability of cooperative false alarm decreases as the amount of encrypted information increases. It is also observed that more malicious users lead to higher false alarm probability.

D. ENERGY CONSUMPTION MODEL

In CRNs, when sensor nodes carry out spectrum sensing, data transmission/reception and idle listening, they always consume energy. In this paper we focus on studying the energy efficiency as sensor nodes execute spectrum sensing. The energy consumption of spectrum sensing is composed of two parts: energy consumption in sensing the spectrum and sensing results transmission. Since a binary local decision is used in the spectrum sensing result, the energy consumption of transmitting the sensing results, compared to the energy consumption of spectrum sensing, is very small and can be ignored [25]. The energy consumption of spectrum sensing becomes crucial for the CRNs when cooperative spectrum sensing is adopted. According to [25], the total energy consumption arisen from spectrum sensing can be simply written as

$$E = E_{\text{css,sec}} + E_t, \tag{32}$$

where $E_{\text{css,sec}} = Ne_s + NBe_r$, e_s is the energy consumption arisen from one SU in sensing and e_r is the energy consumption arisen from transmitting 1-bit data to the FC, E_t is the energy consumed by transmitting.

III. ANALYSIS ON ENERGY EFFICIENCY OF SSDF

The optimization objective is the energy efficiency maximization of cooperative spectrum sensing under the security requirements. The global secure detection probability and global secure false alarm probability can be used to scale the effects of attack on the performance of system. Therefore, the energy efficiency in secure CSS can be obtained by

$$\mu_{\text{sec}} = \frac{P_0(1 - P_{F,\text{sec}})RT}{E_{\text{css,sec}} + E_t} \tag{33}$$

where $P_0(1 - P_{F,\text{sec}})$ is the probability that the spectrum is detected correctly when it is not used by PU, R is the transmission rate in bps, T is the transmission time.

By using MAC to resist SSDF attack, we design the energy efficiency maximization by optimizing the number of cooperative spectrum sensing nodes N and the number of the additional security bits. Specifically, the optimization problem is mathematically stated as follows:

$$\max_{B,N} \mu_{\text{sec}} = \max_{B,N} \frac{P_0(1 - P_{F,\text{sec}})RT}{E_{\text{css,sec}} + E_t}. \tag{34}$$

Define function $f(x) = \sum_{i=0}^{N} \binom{N}{i} x^i (1 - P_f)^{N-i}$, $P_f < 1$, $x \in (0, P_f]$, $N > 1$. By using the binomial theorem, we have

$$f(x) = (x + 1 - P_f)^N. \tag{35}$$

Lemma 1: There exists $q \in (0, P_f]$, such that

$$\sum_{j=K}^{N} \binom{N}{j} P_f^j (1 - P_f)^{N-j} = \sum_{j=0}^{N} \binom{N}{j} q^j (1 - P_f)^{N-j}. \tag{36}$$

Proof: Please see Appendix A.

A. RELATION BETWEEN ENERGY EFFICIENCY AND THE NUMBER OF COOPERATIVE SPECTRUM SENSING NODES

We assume that both the number of malicious users and the amount of encrypted information are constants, and then μ_{sec} is a function of variable that is the number of cooperative spectrum sensing nodes. Note that $\frac{dE}{dN} = e_s + Be_r$. Denote $\frac{\partial \mu_{\text{sec}}}{\partial N}$ as the partial derivative of the energy efficiency taken with respect to N, which is given by

$$\frac{\partial \mu_{\text{sec}}}{\partial N} = -\frac{P_0 RT \left[E P'_{F,\text{sec}}(N) + (1 - P_{F,\text{sec}})(e_s + Be_r) \right]}{E^2}, \tag{37}$$

where $P'_{F,\text{sec}}(N)$ can be derived by Lemma 1 as follows.

Case 1: Independent SSDF Attack

By Lemma 1, $P_{F,\text{sec}}(N)$ can be expressed as

$$P_{F,\text{sec}}(N) = (q+1-P_f)^N \left(\frac{P_x}{q + 1 - P_f} + 1 - P_x \right)^M. \tag{38}$$

For notation simplicity, we define $A \triangleq q + 1 - P_f$, $\xi \triangleq P_0 RT$. So we have

$$P'_{F,\text{sec}}(N) = A^N \left(\frac{P_x}{A} + 1 - P_x \right)^M \ln(q + 1 - P_x). \tag{39}$$

In this case, we can prove that the energy efficiency has a unique maximal value for N, and there is only one root of equation $\frac{\partial \mu_{\text{sec}}}{\partial N} = 0$.

Since $q < P_f$, $q + 1 - P_x < 1$. Therefore $P'_{F,\text{sec}}(N) < 0$, and the global secure false alarm probability $P_{F,\text{sec}}(N)$ decreases with the increase of the number of SUs. It can be derived that $\lim_{N\to\infty} \frac{\partial \mu_{\text{sec}}}{\partial N} < 0$ and $\lim_{N\to 0} \frac{\partial \mu_{\text{sec}}}{\partial N} > 0$ for any value of N. Hence, there must exist an optimal number of cooperative spectrum sensing nodes that can maximize the energy efficiency, and the root of equation $\frac{\partial \mu_{\text{sec}}}{\partial N} = 0$ exists.

Setting $\frac{\partial \mu_{\text{sec}}}{\partial N} = 0$, it is derived that

$$A^N \left(\frac{P_x}{A} + 1 - P_x \right)^M = \frac{e_s + Be_r}{(e_s + Be_r) - E \ln A}. \tag{40}$$

Then, we get

$$Y(N) = \Omega(N), \tag{41}$$

where

$$Y(N) \triangleq A^N \left(\frac{P_x}{A} + 1 - P_x \right)^M, \tag{42}$$

$$\Omega(N) \triangleq \frac{e_s + Be_r}{(e_s + Be_r) - E \ln A}. \tag{43}$$

Obviously, both $Y(N)$ and $\Omega(N)$ are decreasing. Since $1 > A = q + 1 - P_f > 0$, we have $\frac{P_x}{A} > P_x$ and $\ln A < 0$. We can obtain that

$$Y(0) = \left(\frac{P_x}{A} + 1 - P_x \right)^M > 1, \tag{44}$$

$$\Omega(0) = \frac{e_s + Be_r}{(e_s + Be_r) - E_t \ln A} < 1\,, \tag{45}$$

$$\lim_{N\to\infty} Y(N) = 0\,, \tag{46}$$

$$\lim_{N\to\infty} \Omega(N) = 0\,, \tag{47}$$

$$\lim_{N\to\infty} \frac{Y(N)}{\Omega(N)} = 0\,. \tag{48}$$

$Y(N)$ is an infinitesimal of higher order than $\Omega(N)$ as N goes to infinity. So there must exist N_0 such that $Y(N) < \Omega(N)$ in $(N_0, +\infty)$.

Based on the above analysis, it can be concluded that $Y(N)$ only intersects $\Omega(N)$ once. Therefore, the root of equation $\frac{\partial \mu_{\text{sec}}}{\partial N} = 0$ is unique, and the energy efficiency is an unimodal function and there exists only one optimal value of N that maximizes μ_{sec}.Thus, Bisection method [27], [28] can be used to obtain the optimal number of cooperative spectrum sensing nodes.

Case 2: Collaborative SSDF Attack

Similarly using Lemma1, $P_{F,\text{sec}}(N)$ can be expressed as

$$P_{F,\text{sec}}(N) = \alpha (q_1 + 1 - P_f)^N \left(\frac{P_x}{A} + 1 - P_x \right)^M + (1 - \alpha)\left(1 - (q_2 + 1 - P_f)^M\right) \tag{49}$$

where $0 < q_1,\ q_2 < P_f$. So we have

$$P'_{F,\text{sec}}(N) = \alpha (q_1 + 1 - P_f)^N \left(\frac{P_x}{A} + 1 - P_x \right)^M \ln(q_1 + 1 - P_x)\,. \tag{50}$$

Analogously to the case 1, it also can be proved that the energy efficiency is a unimodal function and there exists only one optimal value of N that maximizes μ_{sec} in Case 2.

B. RELATION BETWEEN ENERGY EFFICIENCY AND THE AMOUNT OF INFORMATION ENCRYPTION

Assume that both the number of malicious users and the number of cooperative spectrum sensing nodes are constants, μ_{sec} is a function with a variable B that is the amount of encrypted information. Problem (34) can be rewritten as

$$\max_{B} \mu_{\text{sec}}(B) = \max_{B} \frac{R(B)}{P(B)}. \tag{51}$$

The methodological analysis used in [29] to solve the fractional optimization can be consulted here to solve Problem (51). First, we regulate a function as

$$f(B, \lambda) = R(B) - \lambda P(B), \tag{52}$$

where λ is an arbitrary positive number. We regulate another function as follows

$$g(\lambda) = \max_{B} f(B, \lambda). \tag{53}$$

If $g(\lambda)$ is a monotonically decreasing function in terms of λ, the optimal solution of Problem (51) exists at $g(\lambda) = 0$ [29].

Theorem 1: $g(\lambda)$ is a monotonically decreasing function of λ.

Proof: Please see Appendix B.

Theorem 2: The root of equation $g(\lambda) = 0$ is the maximum value of energy efficiency. And the optimal solution of problem (51) uniquely exists when $f(B, \lambda) = 0$.

Proof: Please see Appendix C.

It is difficult to obtain the solution of such problem in a closed form expression. Hence the solution can be computed by the iterative search algorithm. With a given number of cooperative spectrum sensing nodes, we can simply use the following bisection algorithm (Algorithm 1) to solve Problem (51) over an interval $[0, B_0]$, which is known to contain B^*.

Algorithm for finding the optimal B^*

```
Initialize a feasible $B$, $B \in [0, B_0]$, $\lambda_{\min}$, $\lambda_{\max}$, tolerance $\varepsilon$, iteration number $n = 1$;
Repeat
    a) $\lambda \leftarrow (\lambda_{\min} + \lambda_{\max})/2$
    b) Find optimal $B^*$ maximizing $f(B, \lambda)$ by bisection algorithm;
    c) If $g(\lambda) > 0$, $\lambda_{\max} \leftarrow \lambda$
    else $\lambda_{\min} \leftarrow \lambda$;
Until $\lambda_{\max} - \lambda_{\min} < \varepsilon$;
Output $B^*$.
```

where ε is a predefined small constant to control the accuracy of convergence.

IV. SIMULATION RESULTS

In this section, performance results are presented through numerical results. All channels are modeled by the product of path-loss and independent Rayleigh fading with complex normal distribution $\mathcal{CN}(0, 1)$ [30], [31]. The path loss in decibels is modeled as $38.46+35\log_{10}(d)$, where d is measured in meters [6]. All simulation results are obtained by averaging over 200 channel realizations. The main system parameters are given in Table 1.

TABLE 1. Main simulation parameters.

Parameters	Value
Probability of ideal channel P_0	0.6
Data rata R	200Kbps
Transmission time T	0.4s
Channel Bandwidth B	3KHz
Sensing period τ	2ms
Energy consumed by one SU in sensing e_s	1J/bit
Energy consumed when transmit 1-bit data to the FC e_r	0.01J/bit
Energy consumed by transmission E_t	0.01J/bit
Tolerance ε	10^{-4}

The effect on the achievable energy efficiency is shown in Figure 5 when the legitimate SUs do not employ any security algorithm and employ MAC algorithm, respectively. The energy efficiency is drawn versus the fusion rule threshold K for different numbers of malicious users M. It is visible that the energy efficiency is lowered as increasing Ms. It can be observed that the threshold K plays an important rule to make a reduction in the effect of the malicious users. In the case of insecure CSS, for $M \geq K$, the energy efficiency is zero since P_f is one according to (18), and hence no data will be transmitted. But increasing K can relieve the influence on energy efficiency. In Figure 5, MAC clearly addresses the malicious effects on the CSS, in which the energy efficiency achieved by the proposed secure CSS is explored versus the fusion rule threshold K for $B = 4$. The curve can be attributed to the MAC effects that are the increase in the successfully transmitted data since MAC lowers the false alarm probability.

Figure 6 is simulated to show the energy efficiency versus number of cooperating SUs under I-SSDF attacks, and Figure 7 shows the energy efficiency versus number of cooperating SUs under C-SSDF attacks. We can conclude that it is not always helpful to use all the available SUs in CSS. To enhance the energy efficiency, there is a deficiency to detect the optimal number of cooperating SUs. We can predicate that increasing M lowers the achievable energy efficiency since the more malicious users increase the false alarm probability.

The energy efficiency using MAC based CSS is explored in Figure 8 under I-SSDF attacks and in Figure 9 under C-SSDF attacks considering the number of the reported bits B for $K = 6$ and different numbers of malicious users, respectively. It can be seen from the figures, along with the increase of the number of the reported bits B, the efficiency increases first and then decreases, that is to say, there is the optimal reported bits B that maximizes energy efficiency.

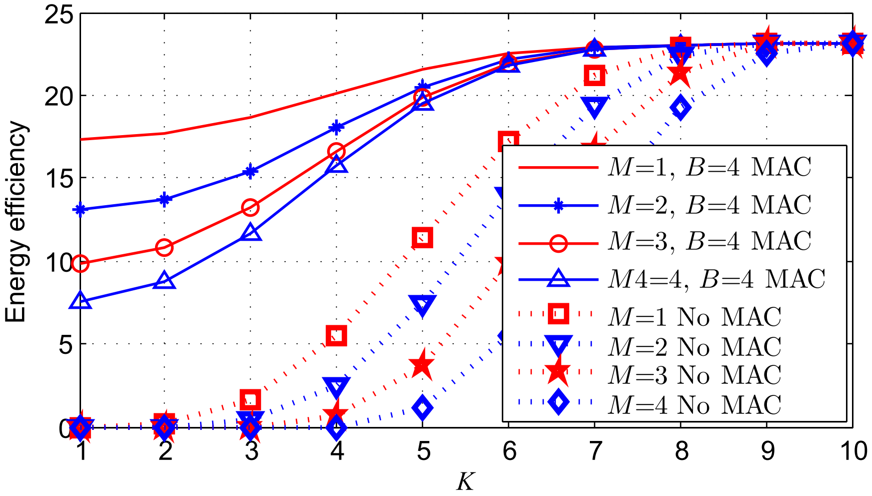


FIGURE 5. The energy efficiency versus the fusion rule threshold for multiple numbers of malicious uses.

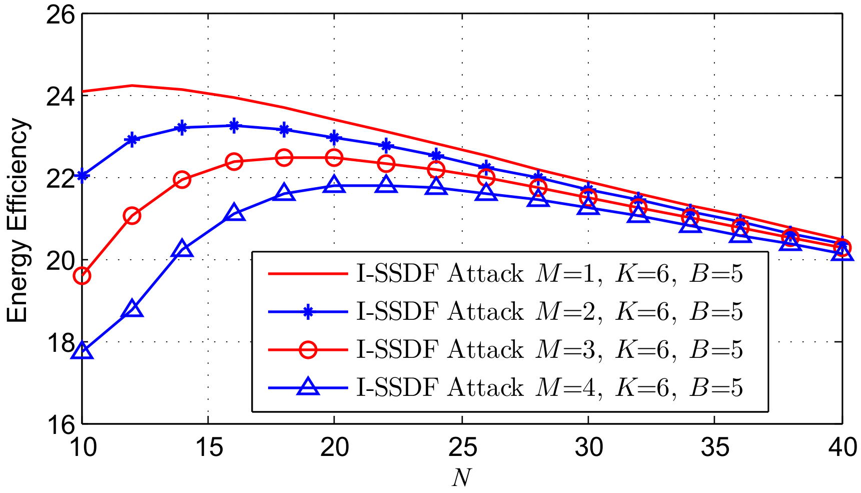


FIGURE 6. The energy efficiency versus the number of secondary users under I-SSDF attacks.

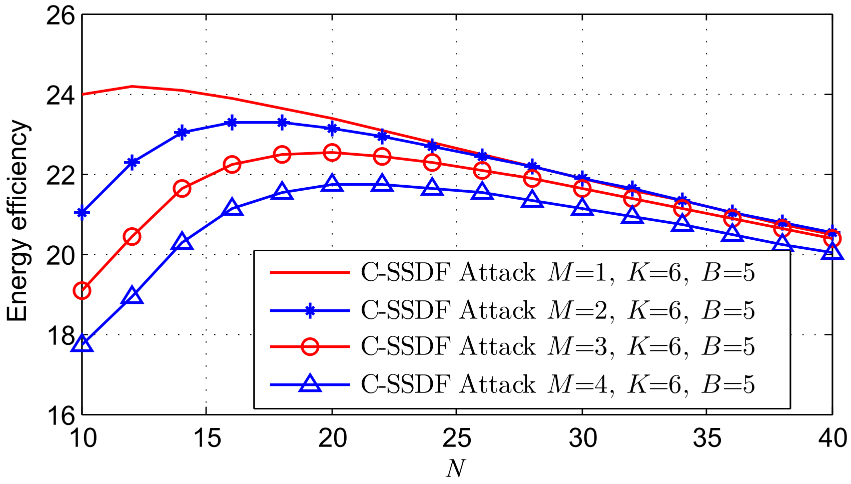


FIGURE 7. The energy efficiency versus the number of secondary users under C-SSDF attacks.

Figure 10 compares the energy efficiency versus the number of the reported bits B for $M = 4$ and $K = 6$ under two types of attacks. The C-SSDF attack lowers the energy efficiency since the accuracy of the cooperative spectrum sensing under C-SSDF attacks is lower than that under I-SSDF attacks.

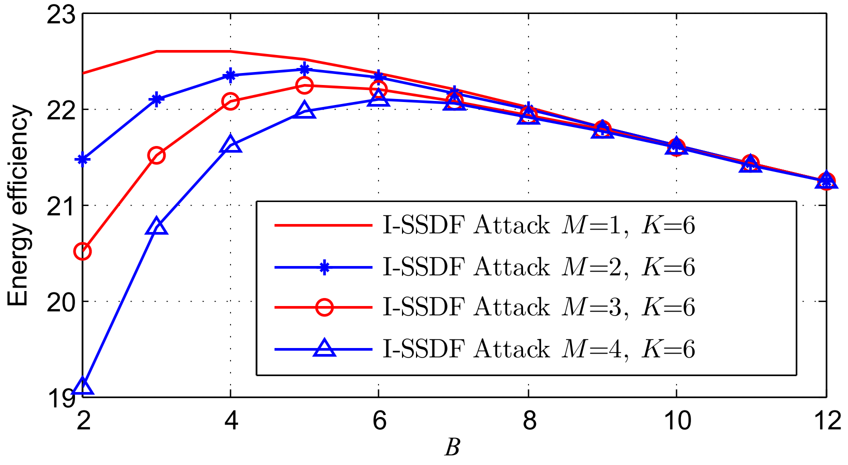


FIGURE 8. The energy efficiency versus encryption information under I-SSDF attacks.

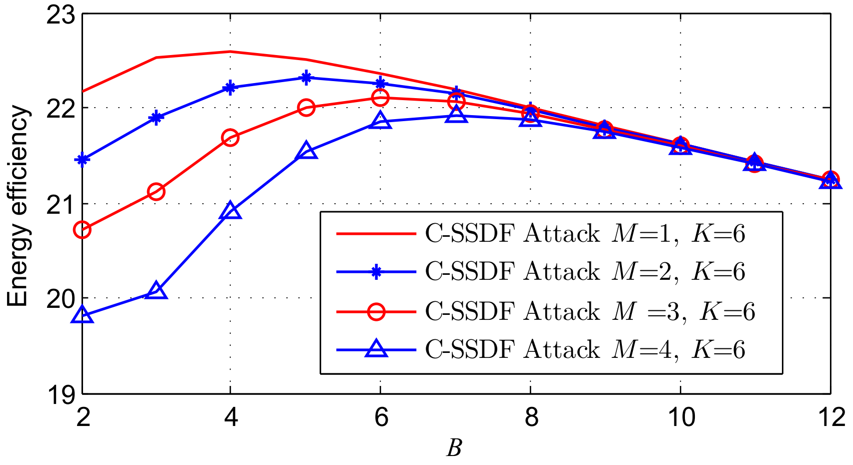


FIGURE 9. The energy efficiency versus encryption information under C-SSDF attacks.

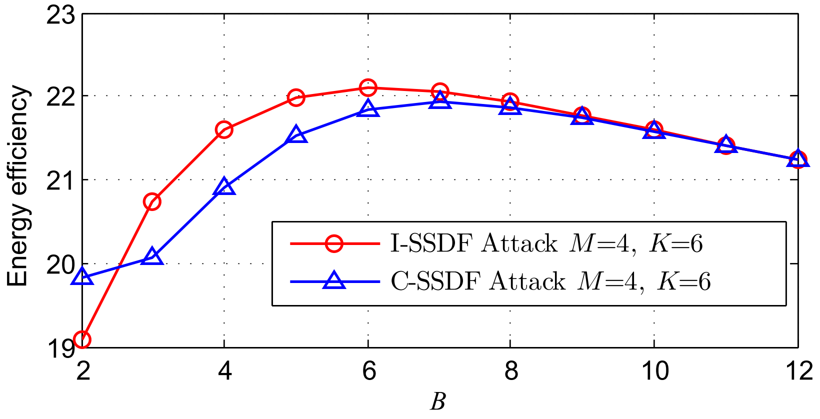


FIGURE 10. The comparison of energy efficiency versus encryption information under two types of attacks.

V. CONCLUSION

In this paper, we have studied the energy efficiency in the secure cooperative spectrum sensing for CRNs and investigated the impacts of independent and collaborative SSDF attacks on the accuracy of cooperative spectrum sensing. To resist SSDF attack, MAC is adopted to reduce the effects of the malicious users. The analysis and simulations show that the number of malicious users, the number of spectrum sensing nodes and the number of the reported bits have significant impacts on the accuracy of cooperative sensing results. Then the concept of energy efficiency is defined in terms of the number of cooperative sensor nodes and the number of the additional security bits as design variables. Simulation results have showed that there exist only one optimal number of cooperative sensor nodes and optimal value of security bits that can maximize the energy efficiency, respectively. Simulation results have verified the efficiency of the proposed MAC based CSS.

APPENDIX A
PROOF OF LEMMA 1

Proof: Since $N > 1$, $f(x)$ is a monotonically increasing and continuous function in $(0, P_f]$. So we have

$$0 < f(x) \leq f(P_f) = 1. \tag{54}$$

Note that

$$\begin{aligned} 0 &< \sum_{j=K}^{N} \binom{N}{j} P_f^j (1-P_f)^{N-j} \\ &< \sum_{j=0}^{N} \binom{N}{j} P_f^j (1-P_f)^{N-j} = 1. \end{aligned} \tag{55}$$

By using the intermediate value theorem, there exists $q \in (0, P_f]$ such that

$$f(q) = \sum_{j=K}^{N} \binom{N}{j} P_f^j (1-P_f)^{N-j}, \tag{56}$$

namely,

$$\sum_{j=K}^{N} \binom{N}{j} P_f^j (1-P_f)^{N-j} = \sum_{j=0}^{N} \binom{N}{j} q^j (1-P_f)^{N-j}. \tag{57}$$

APPENDIX B
PROOF OF THEOREM 1

Proof: For given $f(B, \lambda) = 0$, we have

$$\frac{\partial f(B,\lambda)}{\partial \lambda} = -P(B) = -\left(Ne_s + NBe_r + E_t\right) < 0. \tag{58}$$

Thus, $f(B, \lambda)$ is a monotonically decreasing function of λ for any B. For any positive number Δ, we have

$$f(B,\lambda) > f(B, \lambda + \Delta). \tag{59}$$

Since

$$g(\lambda) = \max_B f(B,\lambda) \geq f(B,\lambda) > f(B,\lambda+\Delta), \quad \forall B, \tag{60}$$

it is derived that

$$g(\lambda) > \max_B f(B,\lambda+\Delta) = g(\lambda+\Delta). \tag{61}$$

Therefore, $g(\lambda)$ is a monotonically decreasing function of λ.

APPENDIX C
PROOF OF THEOREM 2

Proof: According to (33) and (52), for any B, we have

$$f\left(B, \mu_{\text{sec}}(B)\right) = 0. \tag{62}$$

We define B_{opt} as the optimal solution of (51). Since $\mu_{\text{sec}}(B_{opt})$ is the maximum value of energy efficiency, $\lambda = \mu_{\text{sec}}(B_{opt})$ is the largest value of λ that can satisfy $f(B, \lambda) = 0$.

Then, we define λ^* as the root of $g(\lambda) = 0$, i.e., $g(\lambda^*) = 0$. And B^* is the corresponding value that maximizes $f(B, \lambda^*) = 0$. Since $g(\lambda)$ is a monotonically decreasing function of λ, for any value $\bar{\lambda}$ that satisfies $\bar{\lambda} > \lambda^*$, we have

$$g(\bar{\lambda}) = \max_B f(B, \bar{\lambda}) < 0. \tag{63}$$

Thus, any $\bar{\lambda} > \lambda^*$ is unable to satisfy $f\left(B, \bar{\lambda}\right) = 0$. Hence, λ^* is the largest value that can satisfy $f(B, \lambda) = 0$, and we can get $\lambda^* = \mu_{\text{sec}}(B_{opt})$ and $B^* = B_{opt}$. Therefore, the root λ^* of $g(\lambda) = 0$ is the maximum value of energy efficiency.

The second order derivative of $f(B, \lambda)$ with respect to B for any λ can be computed as

$$\frac{\partial^2 f(B,\lambda)}{\partial B^2} = -P_0 RT \frac{\partial^2 P_{F\,\text{sec}}}{\partial B^2}. \tag{64}$$

Case 1: Independent SSDF Attack

According to Lemma1, $P_{F,\text{sec}}(B)$ can be expressed as

$$P_{F,\text{sec}}(B) = A^N \left(1 + \frac{P_f - q}{A} P_x\right)^M, \tag{65}$$

where $0 < q < P_f$. Since $P_x = 1/2^{B-1}$, $P_x{}' = -\frac{\ln 2}{2^{B-1}}$, So we yield

$$\begin{aligned} &\frac{\partial^2 f(B,\lambda)}{\partial B^2} \\ &= -\xi M \frac{(\ln 2)^2}{2^{B-1}} \left(P_f - q\right)(A)^{N-1} \left(1 + \frac{P_f - q}{A}\frac{1}{2^{B-1}}\right)^{M-1} \\ &\quad - \xi M^2 (M-1) \left(\frac{\left(P_f - q\right)\ln 2}{2^{B-1}}\right)^2 (A)^{N-2} \\ &\quad \times \left(1 + \frac{P_f - q}{A}\frac{1}{2^{B-1}}\right)^{M-2} < 0. \end{aligned} \tag{66}$$

So $f(B, \lambda)$ is a concave function in terms of B, and the optimal solution of (51) is uniquely exists.

Case 2: Collaborative SSDF Attack

Similarly using Lemma1, $P_{F,\text{sec}}(B)$ can be expressed as

$$\begin{aligned} P_{F,\text{sec}}(B) &= \alpha\left(q_1 + 1 - P_f\right)^N \left(\frac{P_x}{A} + 1 - P_x\right)^M \\ &\quad + (1-\alpha)\left(1 - \left(q_2 + 1 - P_f\right)^M\right), \end{aligned} \tag{67}$$

where $0 < q_1, q_2 < P_f$. For notation simplicity, we define $A_1 \triangleq q_1 + 1 - P_f, A_2 \triangleq q_2 + 1 - P_f$. So we yield

$$\begin{aligned} &\frac{\partial^2 f(B,\lambda)}{\partial B^2} \\ &= -\xi M\alpha \frac{(\ln 2)^2}{2^{B-1}} \frac{P_f - q}{A} {A_1}^N \left(1+\frac{P_f-q}{A}\frac{1}{2^{B-1}}\right)^{M-1} \\ &\quad - \xi M^2 (M-1)\alpha \left(\frac{\ln 2}{2^{B-1}}\frac{P_f-q}{A}\right)^2 {A_1}^N \\ &\quad \times \left(1+\frac{P_f-q}{A}\frac{1}{2^{B-1}}\right)^{M-2} < 0. \end{aligned} \tag{68}$$

So $f(B, \lambda)$ is also a concave function in terms of B, and the optimal solution of (51) is uniquely exists.

REFERENCES

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Comput. Netw.*, vol. 50, no. 13, pp. 2127–2159, 2006.

[2] N. Zhao, F. R. Yu, H. Sun, and M. Li, "Adaptive power allocation schemes for spectrum sharing in interference-alignment-based cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 5, pp. 3700–3714, May 2016.

[3] X. Li, N. Zhao, Y. Sun, and F. R. Yu, "Interference alignment based on antenna selection with imperfect channel state information in cognitive radio networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 7, pp. 5497–5511, Jun. 2016.

[4] H. Men, N. Zhao, M. Jin, and J. M. Kim, "Optimal transceiver design for interference alignment based cognitive radio networks," *IEEE Commun. Lett.*, vol. 19, no. 8, pp. 1442–1445, Aug. 2015.

[5] C. Pan, J. Wang, W. Zhang, B. Du, and M. Chen, "Power minimization in multi-band multi-antenna cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 13, no. 9, pp. 5056–5069, Sep. 2014.

[6] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, "Cooperative spectrum sensing in cognitive radio networks: A survey," *Phys. Commun.*, vol. 4, no. 1, pp. 40–62, Mar. 2011.

[7] Y. Cai, Y. Mo, K. Ota, C. Luo, M. Dong, and L. T. Yang, "Optimal data fusion of collaborative spectrum sensing under attack in cognitive radio networks," *IEEE Netw.*, vol. 28, no. 1, pp. 17–23, Jan./Feb. 2014.

[8] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *IEEE Wireless Commun.*, vol. 19, no. 6, pp. 106–112, Dec. 2012.

[9] G. Baldini, T. Sturman, A. R. Biswas, R. Leschhorn, G. Godor, and M. Street, "Security aspects in software defined radio and cognitive radio networks: A survey and a way ahead," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 2, pp. 355–379, 2nd Quart., 2012.

[10] S. Liu, Y. Chen, W. Trappe, and L. J. Greenstein, "ALDO: An anomaly detection framework for dynamic spectrum access networks," in *Proc. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 675–683.

[11] S. Sodagari, A. Attar, V. C. M. Leung, and S. G. Bilén, "Denial of service attacks in cognitive radio networks through channel eviction triggering," in *Proc. IEEE GLOBECOM*, Dec. 2010, pp. 1–5.

[12] A. S. Rawat, P. Anand, H. Chen, and P. K. 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.

[13] S. Liu, H. Zhu, S. Li, X. Li, C. Chen, and X. Guan, "An adaptive deviation-tolerant secure scheme for distributed cooperative spectrum sensing," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Dec. 2012, pp. 603–608.

[14] H. Tang, F. R. Yu, M. Huang, and Z. Li, "Distributed consensus-based security mechanisms in cognitive radio mobile ad hoc networks," *IET Commun.*, vol. 6, no. 8, pp. 974–983, May 2012.

[15] X. He, H. Dai, and P. Ning, "HMM-based malicious user detection for robust collaborative spectrum sensing," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 11, pp. 2196–2208, Nov. 2013.

[16] Z. Qin, Q. Li, and G. Hsieh, "Defending against cooperative attacks in cooperative spectrum sensing," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2680–2687, Jun. 2013.

[17] G. Ding *et al.*, "Robust spectrum sensing with crowd sensors," *IEEE Trans. Commun.*, vol. 62, no. 9, pp. 3129–3143, Sep. 2014.

[18] M. Ghaznavi and A. Jamshidi, "A reliable spectrum sensing method in the presence of malicious sensors in distributed cognitive radio network," *IEEE Sensors J.*, vol. 15, no. 3, pp. 1810–1816, Mar. 2015.

[19] C. S. Hyder, B. Grebur, L. Xiao, and M. Ellison, "ARC: Adaptive reputation based clustering against spectrum sensing data falsification attacks," *IEEE Trans. Mobile Comput.*, vol. 13, no. 8, pp. 1707–1719, Aug. 2014.

[20] S. Althunibat *et al.*, "On the trade-off between security and energy efficiency in cooperative spectrum sensing for cognitive radio," *IEEE Commun. Lett.*, vol. 17, no. 8, pp. 1564–1567, Aug. 2013.

[21] J. Bao, Y. Wang, and L. Li, "A spectrum sensing data falsification countermeasure strategy in energy-efficient CRN," in *Proc. 8th Int. Conf. IEEE Wireless Commun. Signal Process. (WCSP)*, Oct. 2016, pp. 1–5.

[22] S. A. Mousavifar and C. Leung, "Energy efficient collaborative spectrum sensing based on trust management in cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 14, no. 4, pp. 1927–1939, Apr. 2015.

[23] J. Ren, Y. Zhang, Q. Ye, K. Yang, K. Zhang, and X. S. Shen, "Exploiting secure and energy-efficient collaborative spectrum sensing for cognitive radio sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 10, pp. 6813–6827, Oct. 2016.

[24] S. Chatterjee, S. P. Maity, and T. Acharya, "Energy efficiency in cooperative cognitive radio network in the presence of malicious users," *IEEE Syst. J.*, to be published.

[25] M. Zhu and S. Martínez, "On the performance analysis of resilient networked control systems under replay attacks," *IEEE Trans. Autom. Control*, vol. 59, no. 3, pp. 804–808, Mar. 2014.

[26] Y.-C. Liang, Y. Zeng, E. C. Y. Peh, and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Trans. Wireless Commun.*, vol. 7, no. 4, pp. 1326–1337, Apr. 2008.

[27] H. Ren, N. Liu, C. Pan, and C. He, "Energy efficiency optimization for MIMO distributed antenna systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2276–2288, Mar. 2017.

[28] H. Hu, H. Zhang, and Y. C. Liang, "On the spectrum- and energy-efficiency tradeoff in cognitive radio networks," *IEEE Trans. Commun.*, vol. 64, no. 2, pp. 490–501, Feb. 2016.

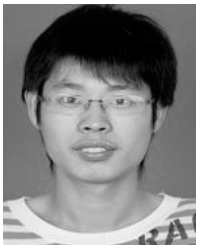
[29] Y. Pei, Y.-C. Liang, K. C. Teh, and K. H. Li, "Energy-efficient design of sequential channel sensing in cognitive radio networks: Optimal sensing strategy, power allocation, and sensing order," *IEEE J Sel Areas Commun.*, vol. 29, no. 8, pp. 1648–1659, Sep. 2011.

[30] H. Zhu, "Performance comparison between distributed antenna and microcellular systems," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 6, pp. 1151–1163, Jun. 2011.

[31] H. Zhu, "Radio resource allocation for OFDMA systems in high speed environments," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 4, pp. 748–759, May 2012.

JIANXIN DAI received the B.S. degree from the Mathematics Department, Nanjing Normal University, China, in 1995, the M.S. degree in communications science from the Nanjing University of Posts and Telecommunications, China, in 2007, and the Ph.D. degree in electronic engineering from the National Mobile Communications Research Laboratory, Southeast University, Nanjing, China, in 2014. From 2015 to 2017, he held a postdoctoral position with the Nanjing University of Posts and Telecommunications, China. From 2016 to 2017, he was an Academic Visitor with the University of Kent, U.K. From 2009 to 2017, he was an Associate Professor with the Nanjing University of Posts and Telecommunications, China. His current research interests include C-RAN, mm-Wave communications, massive MIIMO systems, and cognitive radio networks.

JUAN LIU received the B.E. degree from the School of Electrical Engineering, Yancheng Institute of Technology, China, in 2016. She is currently pursuing the M.Eng. degree with the College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, China. Her research interests include spectrum sensing and cognitive radio networks.



CUNHUA PAN received the B.S. and Ph.D. degrees from the School of Information Science and Engineering, Southeast University, Nanjing, China, in 2010 and 2015, respectively. From 2015 to 2016, he was a Research Associate with the University of Kent, U.K. He currently holds a postdoctoral position with the Queen Mary University of London, U.K. His research interests include C-RAN, mm-Wave communications, NOMA, D2D, large-scale MIMO, and cloud computing. He is a TPC member of the IEEE ICC and GLOBECOM from 2015 to 2017.

JIANGZHOU WANG (F'17) is currently the Head with the School of Engineering and Digital Arts, and a Professor of Telecommunications, University of Kent, U.K. He has authored over 200 papers in international journals and conferences in the areas of wireless mobile communications and three books. He is an IET Fellow. He was a recipient of the Best Paper Award from the 2012 IEEE GLOBECOM and was an IEEE Distinguished Lecturer from 2013 to 2014. He was the Technical Program Chair of the 2013 IEEE WCNC in Shanghai and the Executive Chair of the 2015 IEEE ICC in London. He serves/served as an Editor for a number of international journals. For example, he was an Editor for the IEEE Transactions on Communications from 1998 to 2013, and was a Guest Editor for the IEEE Journal on Selected Areas in Communications and the IEEE Communications Magazine. He is currently an Editor for *Science China Information Sciences*.

CHONGHU CHENG received the B.Sc., M.Sc., and Ph.D. degree from the Department of Radio Engineering, Southeast University, Nanjing, China, in 1983, 1986, and 1993, respectively. From 1994 to 1996, he was a Post-Doctoral Research Scientist with the Department of Information Electric, Zhejiang University. From 1999 to 2001, he was invited to work with the Telecommunication Research Institute of the Ministry of Posts and Telecommunications. Since 2001, he has been with the Nanjing University of Posts and Telecommunications, where he is currently a Professor. His research interests include computational electromagnetic, microwave passive circuits, and small antenna.

ZHILIANG HUANG was born in Wuhan, China, in 1981. He received the B.Sc. degree from the Wuhan Institute of Technology, Wuhan, China, in 2004, the M.Sc. degree from Zhejiang Normal University, Jinhua, 2009, and the Ph.D. degree from Southeast University, Nanjing, 2013. In 2013, he joined the College of Mathematics, Physics, and Information Engineering, Zhejiang Normal University. From 2015 to 2016, he was a Visiting Scholar with Bilkent University, Ankara, Turkey. His research interests include meta-heuristic algorithms and error-correcting codes.