Throughput and Interference for Cooperative Spectrum Sensing: A Malicious Perspective

Jipeng Gan[1], Jun Wu[1,2,3,4*], Jia Zhang[1], Zehao Chen[1], and Ze Chen[1]
[1] School of Communication Engineering, Hangzhou Dianzi University
Hangzhou, Zhejiang 310018 China
[e-mail: gan19081311@163.com]
[2] National Mobile Communications Research Laboratory, Southeast University
Nanjing, Jiangsu 211189 China
[3] Artificial Intelligence Key Laboratory of Sichuan Province, Sichuan University of Science and Engineering
Yibing, Sichuan 643002 China
[4] College of Information Science and Electronic Engineering, Zhejiang University
Hangzhou, Zhejiang 310058 China
[e-mail: wojames2011@163.com]
*Corresponding author: Jun Wu

Received July 8, 2021; revised October 2, 2021; accepted October 24, 2021; published November 30, 2021

Abstract

Cognitive radio (CR) is a feasible intelligent technology and can be used as an effective solution to spectrum scarcity and underutilization. As the key function of CR, cooperative spectrum sensing (CSS) is able to effectively prevent the harmful interference with primary users (PUs) and identify the available spectrum resources by exploiting the spatial diversity of multiple secondary users (SUs). However, the open nature of the cognitive radio networks (CRNs) framework makes CSS face many security threats, such as, the malicious user (MU) launches Byzantine attack to undermine CRNs. For this aim, we make an in-depth analysis of the motive and purpose from the MU's perspective in the interweave CR system, aiming to provide the future guideline for defense strategies. First, we formulate a dynamic Byzantine attack model by analyzing Byzantine behaviors in the process of CSS. On the basis of this, we further make an investigation on the condition of making the fusion center (FC) blind when the fusion rule is unknown for the MU. Moreover, the throughput and interference to the primary network are taken into consideration to evaluate the impact of Byzantine attack on the interweave CR system, and then analyze the optimal strategy of Byzantine attack when the fusion rule is known. Finally, theoretical proofs and simulation results verify the correctness and effectiveness of analyses about the impact of Byzantine attack strategy on the throughput and interference.

This work is supported by the open research fund of National Mobile Communications Research Laboratory, Southeast University (No. 2022D16), Fundamental Research Funds for the Provincial Universities of Zhejiang (No. GK209907299001-023), Open Fund Project of Sichuan Provincial Key Laboratory of Artificial Intelligence (No. 2021RYJ07), and 2020 Annual Teachers' Professional Development Project of Domestical Visiting Scholars in Institutions of Higher Education (No. FX2020009).

http://doi.org/10.3837/tiis.2021.11.019 **ISSN : 1976-7277**

Keywords: Cooperative spectrum sensing, Byzantine attack, Malicious perspective, Throughput and interference.

1. Introduction

Due to the rapid advances in wireless communication systems, the demand for spectrum resources has increased sharply, so the spectrum resources cannot meet the needs of wireless devices and applications. And yet, in another respect, it has been proved by Federal Communications Commission (FCC) research that the spectrum scarcity is a direct consequence of the underutilization of the frequency spectrum by primary users (PUs) either temporally or spatially in fact. Therefore, cognitive radio (CR) is proposed to enable secondary users (SUs) to communicate in the authorized frequency band, with the aim of not affecting the PU's normal operation [1]. In a interweave CR operation mode [2], CR allows secondary users (SUs) using spectrum sensing methods to detect whether the PU's signal is present or not [3], and then the SUs opportunistically access the channel (when the PU is absent, which presents that the channel is underutilized by the PU) but without causing excessive interference to the primary network. Therefore, CR is able to solve the dilemma between the spectrum underutilization and scarcity [4].

However, due to the inherent nature of wireless propagation, the single-node spectrum sensing is prone to be affected by many factors, such as shadow effect, multipath fading, etc., the spectrum sensing performance is prone to be affected. In view of this, cooperative spectrum sensing (CSS) uses the spatial diversity of SUs to improve the spectrum sensing performance by the diversity gain, which significantly increases the sensing accuracy. Now it has become the primary method for the fusion center (FC) to detect whether the PU occupies the spectrum. In the CSS, SUs sends the original observations (soft-combining) or their local decisions (hard-combining) to the FC, and then the FC makes a global decision about the PU's status through a specific fusion rule [5]. There is no doubt that CSS is able to improve the accuracy of the PU detection. However, it opens a hole to the malicious users (MUs) who take part in the spectrum sensing and submit falsified sensing information to the FC to implement Byzantine attack. Through Byzantine attack, MUs mislead the FC to make wrong global decision by submitting falsified sensing information, thereby causing the following effects: on the one hand, MUs can prevent normal users (NUs) from occupying spectrum resources the in order to selfishly access the channel; on the other hand, MUs allure NUs to access the channel when the PU is using it and then cause excessive interference to the PU's normal communication.

Therefore, protecting CSS from Byzantine attack is indispensable and devising a comprehensive and in-depth analysis on the characteristics and impact of Byzantine attack becomes essential.

1.1 Related Work

The area of CSS has been a very active field of research in the past, security problems in CRNs have gained attention only in the last decade. Both [6] and [7] used a trusted node assistance to verify the correctness of reputation and data of participating CSS nodes, with the aim of securing CSS. In [8], the FC allocates a reasonable weight value (depending on historical sensing behavior of nodes) according to the submitted observations' evaluation to make the global decision. In [9], an algorithm was proposed by Z. Sun et al. to select better sensing strategies either collaboratively or independently. In [10], M. Ningrinla et al. proposed a lightweight intrusion detection scheme and intrusion detection scheme using the Markov chain model based on historical spectrum sensing data to detect intrusion and identify Byzantine attackers. In [11][12], a reputation-based strategy is proposed by A. S. Rawat et al. to identify Byzantine attackers, but Byzantine attack identification can take effect in the proposed system when the malicious percentage is less than 50%. Nevertheless, the above-mentioned methods either rely heavily on the assistance of a third-party trusted node or are only applicable for small-scale Byzantine attack scenarios. In fact, the reliable trusted node is not easy to obtain in a realistic CRN, this assumption appears to be too ideal. Otherwise, since a low percentage of MUs cannot compromise the FC, most of existing Byzantine identification algorithms adopt the FC's global decision as the evaluation criterion of the reputation management mechanism [13], apparently, they overlook the possibility of large-scale Byzantine attack.

Compared to the ideal assumptions in the aforementioned works, an incentive method based on peer-peer prediction was proposed by Y. Gan et al. to identify and punish attackers and encourage SU to send accurate reports in [14]. An incentive-compatible mechanism was designed by W. Wang et al. to provide a moderate punishment to MUs based on the moral hazard principal-agent model in [15]. With the prior knowledge of attack behaviors, the closed-form expressions of the identification performance was derived by L. Zhang et al. in [16]. Considering that the unavailable prior knowledge, the maximized likelihood estimation is made based on the extended sensing to optimize the optimal performance. In [17], J. Wu et al. proposed a low-complexity sequential 0/1 defense strategy against strategic Byzantine attack for CSS. Both [18] and [19] made use of estimation algorithm to estimate attack parameters, aiming to adopt appropriate defense strategies. In contrast to the simplified hostile scenario, the above works consider some relatively complex and flexible Byzantine attack strategies from various aspects, and then propose corresponding defense strategies by means of estimation algorithms. But for some special attack model (i.e., probabilistic Byzantine attack), estimation algorithms have to take a long sensing observation period and then confirms attack parameters before deploying defense strategies.

Bedsides, J. Ren et al. proposed an algorithm which take Byzantine attack and energy efficiency into consideration in [20]. F. Ye et al. made use of evidence theory and credibility calculation where evaluates the holistic credibility of SUs from both the real-time difference and statistical sensing behavior of SUs in [21] to propose a CSS method. In [22], W. Hashlamoun et al. proposed a mechanism to mitigate the Byzantine attack by partitioning sensors into groups and measured the CSS performance by introducing a weighted Kullback-Leibler divergence indicator. Unfortunately, [20-24] only consider the simple always attack, such as always yes/no/false attack, but in fact, for a rational MU, the always attack is more aggressive and easily identified by the FC's defense strategy. Otherwise, numerous efforts on Byzantine attack identification and removal for CSS have been made in [25-26] and references therein.

1.2 Our Contributions

Through analyses on the above literature, many efforts have been devoted to studying Byzantine attack for CSS, few studies consider rational Byzantine attackers from the malicious perspective. Because of the incomplete analysis of Byzantine behavior, the defensive strategy or algorithms always have various unrealistic assumptions and some limitations, hence CSS also poses many new research challenges.

The previous works always start with the CSS security to deal with Byzantine attack and fail in considering the motives and purpose of MUs, in this paper, we relax the requirements of the parameters on Byzantine attack, and reconsider Byzantine attack behaviors in CSS. Further, we make an in-depth analysis on the impact of Byzantine attack of the achievable throughput of CRNs and interference to the PU under various scenarios. In summary, the main contributions of this paper can be summarized as follows:

- We start with Byzantine behaviors in CSS to develop a dynamic Byzantine attack model from the malicious perspective. Under this generalized attack model, the MU can conduct various attack strategies by arbitrarily adjusting attack parameters and does not have any restrictions. Since the proposed dynamic Byzantine attack model does not have any ideal assumptions, it provides a more extensive analysis in various complex scenarios.
- Under two scenarios where the fusion rule is unknown or known for MUs, the blind problem and the impact of Byzantine attack on the throughput and interference are taken into account. When the fusion rule is unknown, according to the proposed attack model, we derive the minimal percentage of MUs and condition of which making the FC blind. When the fusion rule is known, we analyze the impact of Byzantine attack on the achievable throughput of CRNs and interference to the PU, and conduct the optimal attack strategy to obtain maximal throughput and interference.
- Finally, we simulate the real effect of Byzantine attack parameters on CRNs in the various scenarios, and by a series of numerical simulations, we corroborate correctness and effectiveness of theoretical analyses about the impact of Byzantine attack strategy on the throughput and interference from the malicious perspective.

1.3 Organization

The remainder of this paper is organized as follows. Section 2 introduces the system model, including the spectrum sensing, Byzantine attack model, and throughput evaluation. In Section 3, the blind condition of making the FC blind is analyzed and derived when the fusion rule is unknown. Section 4 analyzes the optimal attack strategy to maximize the achievable throughput and interference when the fusion rule is known. Simulation results are provided in Section 5 to verify our theoretical analyses. Finally, conclusions and further work are drawn in Section 6.

2. System Model

In this section, the spectrum sensing model based on an interweave operation mode is presented in an infrastructure-based CRN. Following the spectrum sensing model, we propose a dynamic Byzantine attack model according to Byzantine behaviors from the MU's perspective. Then on the basis of the periodic spectrum sensing frame structure, we further evaluate the achievable throughput as the performance metric of CRNs, respectively.

2.1 Spectrum Sensing Model

We consider an infrastructure-based CRN in an interweave operation mode, which consists of a FC, a PU, N several collaborative SUs, and the malicious percentage ρ, as shown in **Fig. 1**. In order to realize the detection for the PU, all SUs make use of the local spectrum sensing methods to detect the PU signal. According to the binary hypothesis test problem, at the k-th sensing interval, the received sampled signal $y_i(n)$ of the i-th SU can be described as

$$y_i(n) = \begin{cases} u_i(n), & H_0 \\ h_i(k)s(n) + u_i(n), & H_1 \end{cases} \tag{1}$$

where H_0 and H_1 represent the two hypotheses that the licensed frequency band is idle or occupied (i.e., the PU is absent or present), $u_i(n)$ is the additional white Gaussian noise (AWGN) with mean zero and variance σ_u^2, $s(n)$ is the SU's received signal transmitted by the PU, $h_i(n)$ is the channel gain, $s(n)$ and $u_i(n)$ are assumed to be independent.

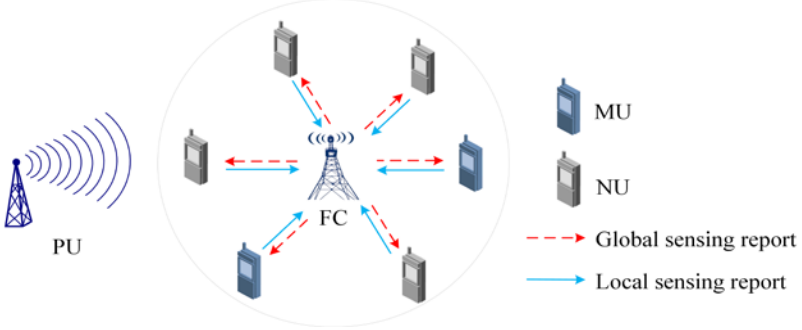

Fig. 1. CSS in the presence of MUs.

Currently, there are a variety of local spectrum sensing methods, including energy detection, matched filter, cyclostationary detection, and wavelet detection. Among these methods, the energy detection is commonly adopted because it does not require the PU signal's prior information and has a low implementation complexity. Then, the test statistic $y_i(t)$ for energy detector at the k-th sensing interval is calculated as

$$T_i(k) = \sum_{t=1}^{S} |y_i(t)|^2 \tag{2}$$

According to the central limit theorem, $T_i(k)$ can be approximated by a Gaussian distribution (when the number of samples S is large enough) as follows [27]

$$T_i(k) = \begin{cases} \mathcal{N}(S\sigma_u^2, 2S\sigma_u^4), & H_0 \\ \mathcal{N}(S(\gamma_i(k)+1)\sigma_u^2, 2S(\gamma_i(k)+1)^2\sigma_u^4), & H_1 \end{cases} \tag{3}$$

where $\gamma_i(k)$ is the signal-to-noise ratio (SNR) of the PU measured at the i-th SU.

Assuming that τ represents the sensing time, the received signal is sampled at sampling frequency f_s, therefore the local spectrum sensing performance for the i-th SU, i.e., the local false alarm probability and the local detection probability are respectively given by

$$P_{f,i} = P(T_i(k) > \lambda | H_0) = Q\left(\left(\frac{\lambda}{\sigma_u^2} - 1\right)\sqrt{\tau f_s}\right) \tag{4}$$

$$P_{d,i} = P(T_i(k) > \lambda | H_1) = Q\left(\left(\frac{\lambda}{\sigma_u^2} - \gamma_i(k) - 1\right)\sqrt{\frac{\tau f_s}{2\gamma_i(k)+1}}\right) \tag{5}$$

where $Q(\cdot)$ is the complementary distribution function of the standard Gaussian, λ is the predetermined threshold.

2.2 Byzantine Attack Model

After all SUs individually performs the spectrum sensing, they should continue submitting a binary decision to the FC for the global decision making. Though cooperative paradigms mitigate the negative effect of the nature of wireless propagations, but open a door for different attacks, such as Byzantine attack. In Byzantine attack, the MU sends falsified local decision report about the PU status to the FC and intentionally confuse the FC.

Many efforts have been devoted to studying Byzantine attack in CSS, including attack model and defense strategies, i.e., [24] and references therein. To be specific, Byzantine attack model has received far less attention than Byzantine defense, such as, many researches only focus on simple always yes/no/false attacks without dealing with more sophisticated malicious behaviors. There is no doubt that such an always attacker is easy to be identified and removed from CSS. This is to say, if the analysis on Byzantine attack behavior is not thorough enough, it is impossible to conduct a robust defense strategy.

To formulate a more generalized and flexible Byzantine attack model, we conduct theoretical study to dissect Byzantine behaviors of MUs. In details, when the MU deliberately sends falsified spectrum sensing data to the FC, its final goal is to force the FC into making a wrong global decision. On the one hand, when a MU has detected that the PU is absent, it falsifies the decision report 0 into 1 and then deceives the FC into declaring the global decision as 1. As a result, the FC broadcasts that the PU is using the channel, then NUs cannot access the channel to avoid causing interference to the PU, and can only continue spectrum sensing in the next sensing frame. Finally, the MUs can exclusively occupy the channel that is not actually being used by the PU. On the other hand, when a MU has detected that the PU is present, the MU falsifies the decision report 1 into 0, its objective is to induce the FC to announce the global decision 1 into 0. This is to say, the FC may inform SUs that the PU is absent and they can access the channel, but in fact the PU is still using the channel, thereby causing harmful interference to the PU.

The above two situations are the most extreme impact of Byzantine attacks on CSS. In consideration of their own attack risks, MUs do not always adopt such extreme attack strategies because extreme attack strategies will soon fail to deploy due to low reputation in common reputation-based methods. From a long-term perspective, the intermittent or interval attack strategies will not be discovered immediately, the MU has a certain degree of concealment and remains in CRNs for a long time [28]. In this regard, we start with a probabilistic attack strategy to develop a generalized and flexible Byzantine attack model.

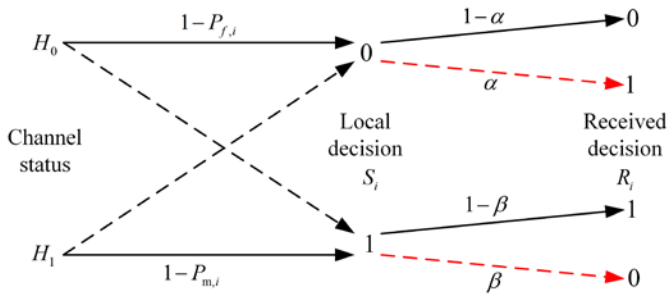

Fig. 2. Dynamic Byzantine attack model.

MUs are equipped with the same spectrum sensing capability as NUs, the NU honestly submits a binary decision report to the FC while the MU submits a falsified decision report with a certain probability after all SUs perform the local spectrum sensing, as shown in **Fig. 2**. In details, when the local decision S_i is 0, the MU submits 1 to the FC with the probability α; when $S_i = 1$, the MU submits 0 to the FC with the probability β. From the malicious perspective, the MU can conduct various attack strategies by varying the flipping probability α and β from 0 to 1. Such as, when $\alpha = 1$ or $\beta = 1$, the Byzantine attack is the always yes or always no attack at this time while it is the always false attack when $\alpha = \beta = 1$. In other words, such an always attack is a kind of particular case of our proposed attack model. It should be noted that the MU can be regarded as the NU when $\alpha = \beta = 0$ because it did not launch attack.

According to the proposed dynamic Byzantine attack, a couple of flipping probabilities α and β can be expressed as

$$\alpha = P(R_i = 1|S_i = 0) \tag{6}$$

$$\beta = P(R_i = 0|S_i = 1) \tag{7}$$

For the sake of simplicity, MUs are assumed to be independent of each other and have the same flipping probability, then the false alarm probability and the miss detection probability for a MU can be obtained as

$$P_f^m = (1 - P_f)\alpha + P_f(1 - \beta) \tag{8}$$

$$P_m^m = (1 - P_m)\beta + P_m(1 - \alpha) \tag{9}$$

Taking Byzantine attack into consideration in CSS, the false alarm probability P_{fa} and the miss detection probability P_{ma} at the FC can be respectively expressed as

$$P_{fa} = \rho P_f^m + (1 - \rho)P_f \tag{10}$$

$$P_{ma} = \rho P_m^m + (1 - \rho)P_m \tag{11}$$

where the detection probability $P_{da} = 1 - P_{ma}$.

Different from that α and β are regarded as the false alarm attack and miss detection attack parameter and assumed to be the same in [10], the flipping probabilities α and β are independent of each other in this paper. To be specific, A. Sharifi and M. Niya treat the malicious percentage ρ as the attack intensity in [29], obviously, the flipping probability is confused with the malicious percentage. In summary, unlike the existing attack model, our proposed dynamic Byzantine attack model does not have no any special assumption on attack parameters.

2.3 Throughput Evaluation

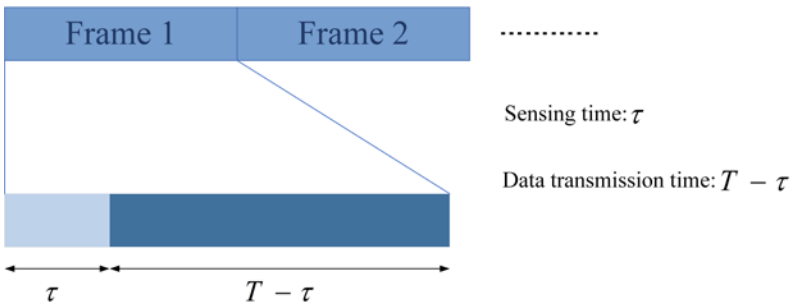

Fig. 3. Periodic spectrum sensing frame structure of CRN.

Next, we further introduce a periodic spectrum sensing frame structure to evaluate the achievable throughput of CRNs [30]. Each frame (the frame duration is T) consists of a sensing slot (the sensing time is τ) and a data transmission slot (data transmission time is $T - \tau$), as

shown in **Fig. 3**. Based on the spectrum sensing frame structure, a brief of some assumptions and parameters are provided to evaluate the throughput in the data transmission time. Let C_0 and C_1 represent the average throughput of CRNs in the absence or presence of the PU [30], respectively, P_s is the received power of SU, N_0 is the noise power and P_p is the interference power of PU measured at the SU, then [30]

$$C_0 = \log_2\left(1+\frac{P_s}{N_0}\right) \tag{12}$$

$$C_1 = \log_2\left(1+\frac{P_s}{P_p+N_0}\right) \tag{13}$$

In order to take the CSS performance into consideration, we further adopt the majority rule at the FC, which is based on the majority of the individual decisions [31]. Depending on the majority rule, then the global false alarm and detection probability can be given by [31][32]

$$Q_f = \sum_{n=K}^{N}\binom{N}{n}P_{fa}^{n}\left(1-P_{fa}\right)^{N-n} \tag{14}$$

$$Q_d = \sum_{n=K}^{N}\binom{N}{n}P_{da}^{n}(1-P_{da})^{N-n} \tag{15}$$

where the global miss detection portability $Q_m = 1 - Q_d$.

According to the global decision (the FC broadcasts that the PU is absent) made by the FC, there are following cases where SUs are allowed to access the channel.

Case 1: when the FC correctly decides that the PU is absent, the SU is allowed to access the channel underutilized by the PU, then the average throughput of CRN for **Case 1** can be expressed as

$$R_0 = \frac{T-\tau}{T}P(H_0)\left(1-Q_f\right)C_0 \tag{16}$$

where $P(H_0)$ represents the probability of hypothesis H_0.

Case 2: when the FC wrongly decides that the PU is absent, the miss detection occurs, according to the global decision, the SUs still access the channel being used by the PU but will cause the harmful interference to the PU, the average throughput of CRN for **Case 2** is given by

$$R_1 = \frac{T-\tau}{T}P(H_1)(1-Q_d)C_1 \tag{17}$$

where $P(H_1)$ represents the probability of hypothesis H_1.

Through above analyses, the average throughput of CRN can be represented by

$$R = \frac{T-\tau}{T}\left(P(H_0)(1-Q_f)C_0 + P(H_1)(1-Q_d)C_1\right) \tag{18}$$

Following the above description and analyses about CSS and Byzantine attack, we further provide a comprehensive investigation on the impact of Byzantine attack in the following section.

3. Scenario I: Unknown Fusion Rule

This section considers a scenario where the MU does not know the fusion rule adopted by the FC. Because of unknown fusion rule, the MU launches Byzantine attack but cannot obtain the global CSS performance. In view of this, we discuss Byzantine attack from the local spectrum sensing performance next.

MUs intend to destroy the operation of CR through Byzantine attack, in order to achieve this goal, MUs need to perform local spectrum sensing like other NUs, and then flip the original sensing decision and submit them to the FC, thereby misleading the FC to make wrong global decision regarding the PU's status. If possible, MUs will make the FC completely unable to decide on the channel status, but this needs to make an in-depth analysis on characteristics of Byzantine attack. In fact, there are a number of different MU identification and mitigation algorithms methods to defend against Byzantine attack threats but fail in considering characteristics of Byzantine attack itself. For example, regardless of the defense strategy, to what extent can MUs degrade the performance of the FC, and what is the relationship between the attack ratio ρ and the flipping probabilities α and β?

In order to solve above issues, we introduce a blind conception about the FC's decision ability. In the view of the Bayesian framework, when the received decision does not provide any information about the hypotheses to the FC, we regard that the FC is blind at this time. That is to say, the global decision is completely independent of the hypothesis test. Meanwhile, it should be noted that the random guess of the FC can also have 50% accuracy, hence the condition to make the FC blind can be stated as $P(\boldsymbol{R}|H_0) = P(\boldsymbol{R}|H_1)$ where $\boldsymbol{R} = [R_1, \ldots, R_i, \ldots, R_N]$. Assuming that each SU's sensing observation is subject to conditional independent and identically distribution, then the blind condition of which MUs make the FC become $P_{fa} = P_{da}$. Therefore, we have

$$\rho P_f^m + (1-\rho)P_f = 1 - \rho P_m^m - (1-\rho)P_m \tag{19}$$

Hence, the FC becomes blind if

$$\rho = \frac{1}{\alpha + \beta} \tag{20}$$

To be specific, we can see from (20) that when MUs launch always false attack (i.e., $\alpha = \beta = 1$), the minimum percentage of MUs to make the FC blind is $\rho = 0.5$. Otherwise, when MUs only launch always yes attack ($\alpha = 1$) or always no attack ($\beta = 1$), it is impossible to make the FC blind unless MUs are spread all over the network.

The above blind condition is derived without defense strategies, but in front of defense strategies, MUs still can adjust their own attack strategies (the attack ratio and the flipping probability) to obtain attack benefit (i.e., exclusively occupying the channel or causing harmful interference to the PU) and ensure security [29]. For example, on the one hand, when the MU represents the minority, three kinds of always attack have been widely studied and easily identified. In fact, MUs should consider that the flipping probability is less than 1 (i.e., $\alpha = \beta = 0.5$), then will not be eliminated because of aggressive attacks; On the other hand, when MUs are in the majority, most defense strategies cannot defend against such a large-scale Byzantine attack, therefore the flipping probability can be varied from 0 to 1.

4. Scenario I I: Known Fusion Rule

This section takes the scenario II where the MU knows the fusion rule adopted by the FC into account. According to the majority rule, MUs would want to deteriorate the CSS performance, thereby occupying spectrum resources or causing harmful interference to the PU. The malicious goal is to obtain the optimal attack strategy that maximizes the MU's throughput and interference to the PU.

4.1 The SU's Average Throughput

Before proceeding with analyses on the MU's average throughput and interference to PU, the SU's average throughput of CRN is provided. Following (18) and the interweave CR framework, the average throughput for a SU is represented by

$$R_l = \frac{T-\tau}{T}\frac{1}{N}\left(P(H_0)(1-Q_f)C_0 + P(H_1)(1-Q_d)C_1\right) \tag{21}$$

When MUs intend to minimize R_l, then the minimization problem can be described as

$$\min_{\alpha,\beta} \frac{T-\tau}{T}\frac{1}{N}\left(P(H_0)(1-Q_f)C_0 + P(H_1)(1-Q_d)C_1\right) \tag{22}$$

For a fixed β, the partial derivative of R_l with respect to α can be obtained as

$$\frac{\partial R_l(\alpha,\beta)}{\partial \alpha} = -\frac{T-\tau}{T}\frac{1}{N}\left(P(H_0)C_0\frac{\partial Q_f}{\partial \alpha} + P(H_1)C_1\frac{\partial Q_d}{\partial \alpha}\right) \tag{23}$$

where $\frac{\partial Q_f}{\partial \alpha}$ and $\frac{\partial Q_d}{\partial \alpha}$ can be obtained by the following algebraic manipulations,

$$\begin{aligned}
\frac{\partial Q_f}{\partial \alpha} &= \binom{N}{K}\left(K\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}\left(1-P_{fa}\right)^{N-K} - (N-K)\cdot\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K}\left(1-P_{fa}\right)^{N-K-1}\right) \\
&\quad + \binom{N}{K+1}\left((K+1)\frac{\partial P_{fa}}{\partial \alpha}\cdot P_{fa}^{K}\left(1-P_{fa}\right)^{N-K-1} - (N-K-1)\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K+1}\right. \\
&\quad \left.\cdot\left(1-P_{fa}\right)^{N-K-2}\right) + \cdots + \binom{N}{N}\left(N\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{N-1} - 0\right) \\
&= \frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}\left(1-P_{fa}\right)^{N-K}\left[\left(\binom{N}{K}K - \frac{P_{fa}}{1-P_{fa}}(N-K)\right) + \binom{N}{K+1}\right. \\
&\quad \left.\cdot\left((K+1)\frac{P_{fa}}{1-P_{fa}} - (N-K-1)\frac{P_{fa}^2}{\left(1-P_{fa}\right)^2}\right)\right] \\
&= \frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}\left(1-P_{fa}\right)^{N-K}\left[\left(\binom{N}{K}K - \frac{P_{fa}}{1-P_{fa}}(N-K)\right)\right. \\
&\quad \left. + \frac{P_{fa}}{1-P_{fa}}\binom{N}{K+1}\left((K+1) - (N-K-1)\cdot\frac{P_{fa}}{1-P_{fa}} + \cdots\right]\right.
\end{aligned} \tag{24}$$

Because of $\binom{N}{K}\frac{K}{N} = \binom{N-1}{K-1}$, then

$$\begin{aligned}
\frac{\partial Q_f}{\partial \alpha} &= \frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}\left(1-P_{fa}\right)^{N-K}\left[\binom{N}{K}K + \left[-\frac{P_{fa}}{1-P_{fa}}\binom{N}{K}\cdot(N-K)\right.\right. \\
&\quad \left.\left. + \frac{P_{fa}}{1-P_{fa}}\binom{N}{K+1}(K+1)\right] + \cdots\right] \\
&= \frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}\left(1-P_{fa}\right)^{N-K}\left[\binom{N-1}{K-1}N + \frac{P_{fa}}{1-P_{fa}}\left[\binom{N}{K+1}\cdot(K+1)\right.\right. \\
&\quad \left.\left. - \binom{N}{K}(N-K)\right] + \cdots\right] \\
&= \frac{\partial P_{fa}}{\partial \alpha}\left(1-P_{fa}\right)^{N-K}\left[\binom{N-1}{K-1}N + \frac{P_{fa}}{1-P_{fa}} * 0\right] \\
&= N\binom{N-1}{K-1}\frac{\partial P_{fa}}{\partial \alpha}P_{fa}^{K-1}\left(1-P_{fa}\right)^{N-K}
\end{aligned} \tag{25}$$

Similarly, we also have $\frac{\partial Q_d}{\partial \alpha} = N\binom{N-1}{K-1}\frac{\partial P_{da}}{\partial \alpha}P_{da}^{K-1}(1-P_{da})^{N-K}$.

Then, we have the following result

$$\frac{\partial R_l(\alpha,\beta)}{\partial \alpha} = -\binom{N-1}{K-1}\rho\frac{T-\tau}{T}P(H_1)C_1P_m\,(1-P_{da})^{N-K} \cdot P_{da}^{K-1}\left[\frac{P(H_0)C_0}{P(H_1)C_1}\frac{(1-P_f)P_{fa}^{K-1}(1-P_{fa})^{N-K}}{P_mP_{da}^{K-1}(1-P_{da})^{N-K}}+1\right] \quad (26)$$

By observing (26), we can easily get $\frac{\partial R_l(\alpha,\beta)}{\partial \alpha} < 0$. The proof of $\frac{\partial R_l(\alpha,\beta)}{\partial \beta} > 0$ is similar to that of $\frac{\partial R_l(\alpha,\beta)}{\partial \alpha} < 0$.

Therefore, it is concluded that the optimal attack strategy to minimize the SU's average throughput is $\alpha = 1, \beta = 0$. Since $C_0 > C_1$, R_0 dominates the achievable throughput.

4.2 The MU's Average Throughput and Interference to the PU

Now, the impact of Byzantine attack on benefit of the MU itself is an issue of our concern. From the MU's perspective, there are two modes of Byzantine attack, such as, sleep mode and action model. In the sleep mode, the MU does not launch Byzantine attack, i.e., $\alpha = \beta = 0$, but it detects the PU's presence or absence by means of the local spectrum sensing technology as well as other NUs, and also obtains spectrum resources from it or causes certain interference to the PU. In the action mode, the MU launches Byzantine attack, with the aim of occupying more spectrum resources and causing excessive interference to the PU.

Next, we further elaborate on how the MU achieves the average throughput and causes harmful interference to the PU from CSS process in the interweave CR system. A brief description of following situations about the MU's average throughput and interference to the PU can be described as

Situation 1: When the FC's global decision is 1, the PU is also present, all SUs are not allowed to access the channel at the current frame. According to the principle of the interweave CR system, SUs have to sense the availability of another channel in the next sensing frame.

Situation 2: When the FC's global decision is 0, but in fact the PU is present and the FC still informs SUs to access the PU's channel, thereby causing harmful interference to the normal activities of PU at this time.

Situation 3: When the FC's global decision is 1, and the PU is absent, then NUs have to switch to another channel and continue spectrum sensing in the next frame while MUs exclusively occupy the channel at the current frame.

Situation 4: When the FC's global decision is 0 and the PU is also absent, all SUs including MUs and NUs are allocated to spectrum resources being underutilized by the PU at the current frame.

In front of the above four situations, the next question that arises is how to evaluate the MU's average throughput and interference to the PU according to the interweave CR system model. In **Situation 1**, since the FC's global decision 1 is consistent with the real status of the PU, neither NUs nor MUs can use the channel currently being used by the PU, nor can it cause interference to the PU. Hence, both the MU's average throughput and interference to the PU are 0.

In **Situation 2**, all SUs are announced that the channel can be accessed because the global decision is 0, but the PU is present. It is apparent that SU accessing the channel being used by the PU will cause harmful interference to the PU's normal communication. In order to quantify

the interference to the PU, we use the average throughput expression to describe it as

$$R_I = \frac{T-\tau}{T}\frac{1}{N}P(H_1)(1-Q_d)C_1 \tag{27}$$

In this situation, all SUs access the channel without knowing the PU's presence, (27) can also be regarded as the available throughput of each SU (assuming that each SU is evenly allocated throughput). But from the perspective of the interweave CR framework, this situation should be avoided because the interference to the PU must be constraint. Hence, from the malicious perspective, the average throughput under this situation is equivalent to the interference to the PU.

In **Situation 3**, it should be noted that even if the MU does not launch Byzantine attack, the false alarm may occur at the FC because of the nature of wireless propagations, i.e., noise. Only because of Byzantine attacks, MUs have more opportunities to access the idle channel. Therefore, regardless of whether there is the Byzantine attack, MUs can exclusively occupy the idle channel of the current frame. Since the spectrum resource allocation problem is out of the scope of this work, we consider that ρN MUs evenly allocate spectrum resource for the sake of simplicity, then the average throughput for each MU in this situation can be expressed as

$$R_{m01} = \frac{T-\tau}{T}\frac{1}{\rho N}P(H_0)Q_f C_0 \tag{28}$$

In **Situation 4**, since the FC correctly decides that the PU is absent, then both NUs and MUs will access the idle channel and equally allocate spectrum resources. Therefore, then the average throughput for each MU in the situation is given as

$$R_{m00} = \frac{T-\tau}{T}\frac{1}{N}P(H_0)\left(1-Q_f\right)C_0 \tag{29}$$

Through above analyses of the MU's average throughput and interference to the PU, then the throughput sum R_m can be obtained by

$$R_m = R_{m01} + R_{m00} \tag{30}$$

For a MU, the final goal is to maximize the interference to the PU R_I and the throughput R_m. Apparently, the smaller the detection probability Q_d, the greater R_I, in other words, the flipping probability α has noting to do with R_I and only $\beta = 1$ makes R_I maximize. As for R_m, we take the partial derivative of R_m with respect to α and β.

For a fixed β, we have the partial derivative of R_m with respect to α by some simple algebraic manipulations

$$\frac{\partial R_m}{\partial \alpha} = \frac{\partial R_{m01}}{\partial \alpha} + \frac{\partial R_{m00}}{\partial \alpha} = \frac{T-\tau}{T}\frac{1}{N}\left(\frac{1}{\rho}-1\right)P(H_0)\frac{\partial Q_f}{\partial \alpha} \tag{31}$$

Similar to (31), for a fixed α, we have the partial derivative of R_m with respect to β is

$$\frac{\partial R_m}{\partial \beta} = \frac{T-\tau}{T}\frac{1}{N}\left(\frac{1}{\rho}-1\right)P(H_0)\frac{\partial Q_f}{\partial \beta} \tag{32}$$

Since $\rho \in [0,1]$, it is easy to obtain $\frac{\partial R_m}{\partial \alpha} > 0$ and $\frac{\partial R_m}{\partial \beta} < 0$, then it is can be concluded that the optimal attack strategy to maximize the MU's average throughput is $\alpha = 1, \beta = 0$. This conclusion we have obtained through mathematical analysis are consistent with intuitive feelings. These analyses laid the groundwork and guidance for the future analysis of MUs' optimal attack strategy under a defense mechanism.

5. SIMULATION RESULTS

In the section, we provide a series of numerical simulation results to corroborate the concreteness and effectiveness of our theoretical analysis on the achievable throughput and interference to the PU from the MU's perspective. Unless otherwise specified, the values of important simulation parameters are shown in **Table 1**.

Table 1. Simulation parameters

Parameters	**Symbol**	**Value**
Number of SUs	N	20
Percentage of MUs	ρ	0.4
Local spectrum sensing performance	P_f	0.2
	P_d	0.8
Frame duration	T	20ms
Sensing duration	τ	1ms
Probability of the hypotheses H_0 and H_1	$P(H_0)$	0.8
	$P(H_1)$	0.2
Sampling frequency	f_s	6MHz
SNR for secondary transmission	SNR_S	20dB
SNR for primary transmission	SNR_P	-15dB

As shown in **Fig. 4**, we display the impact of Byzantine attack on the achievable throughput R_l under various flipping probabilities. It can be seen that there is a negative correlation between the SU's average throughput and α, and a positive correlation between the SU's average throughput and β. Therefore, as expected, the optimal attack strategy to minimize the SU's average throughput is $\alpha = 1, \beta = 0$ from the malicious perspective.

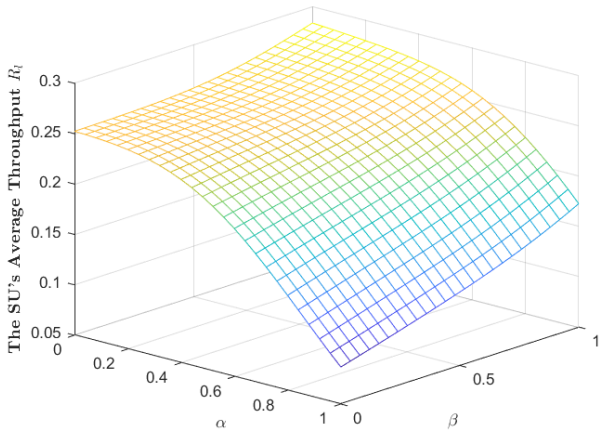

Fig. 4. The SU's average throughput of CRNs v. s. the flipping probability.

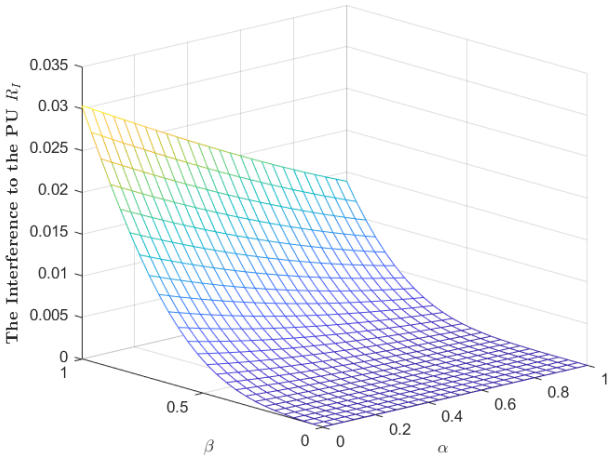

Fig. 5. The interference to the PU v. s. the flipping probability.

Since the FC incorrectly declares that the PU is absent but in fact present, SUs still access to the channel being used by the PU according to the FC's decision, thereby causing excessive interference to the PU's normal communication. **Fig. 5** illustrates the impact of Byzantine attack on the interference to the PU R_I under various flipping probabilities. It is apparent that the flipping probability β has a negative impact on R_I while the flipping probability α has a positive impact on it. Since the interference to the PU is determined by the global miss detection probability, that is, the larger Q_m, the larger R_I. According to (9), we know that the flipping probability β is larger, the miss detection probability of a MU is larger, while the flipping probability α is smaller the miss detection probability of a MU is smaller. Hence, we can see from **Fig. 5** that α increases R_I for a fixed β while β decreases R_I for a fixed α. Therefore, MUs can maximize the interference to the PU when $\alpha = 0, \beta = 1$.

Next, the MU's average throughput R_{m01} and R_{m00} under **Situation 3** and **4** are compared in **Fig. 6**. In **Situation 3**, an increasing α improves R_{m01} for a fixed β while an increasing β decreases R_{m01} for a fixed α. It is worth noting that though a pair of the flipping probabilities have a positive and negative impact on R_{m01}, it is apparent that the effect of α on R_{m01} growth rate is greater than β. Especially, when $\alpha \leq 0.2\beta$, $R_{m01} = 0$. This demonstrates that a small α has little impact on R_{m01} because of cooperative gain. In contrast to simulation results of R_{m01}, an increasing α decreases R_{m01} for a fixed β while an increasing β improves R_{m00} for a fixed α in **Situation 4**. To be specific, R_{m00} keeps in 0.256 when $\alpha \leq 0.2\beta$, but R_{m00} gradually decreases as α and β further increases or decreases respectively.

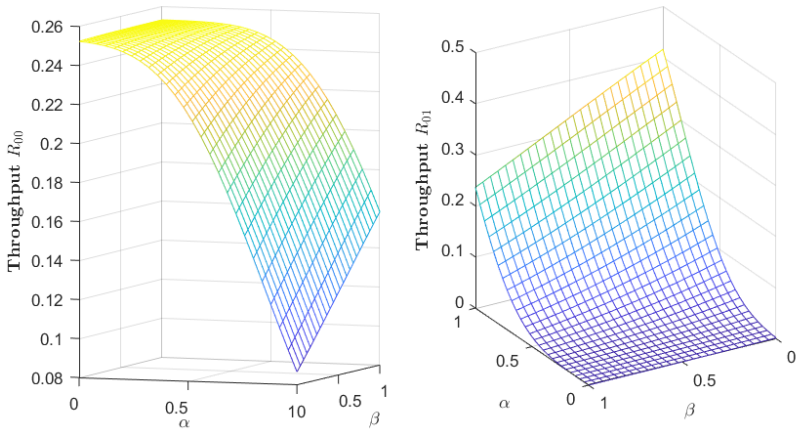

Fig. 6. The MU's average throughput v. s. the flipping probability.

In summary, the optimal attack strategy is $\alpha = 1, \beta = 0$ in **Situation 3** and $\alpha = 0, \beta = 1$ in **Situation 4.** Comparing with the interference to the PU in **Situation 2** and the relatively low throughput in **Situation 4**, MUs can exclusively occupy the idle channel in **Situation 3**, it is inspiring for MUs to launch Byzantine attack, and especially explore the secondary usage for that frequency band by increasing the flipping probability α. From **Fig. 6** and **Fig. 7**, the changing trend of the total throughput R_m following the flipping probability is similar to that of R_{m01}, apparently, (26) dominates the MU's throughput.

The previous series of simulation results on the MU's average throughput and the interference to the PU are only presented in a scenario where there are fewer MUs. Below we will further consider the MU's average throughput when MUs represents the majority, i.e., $\rho = 0.8$, as shown in **Fig. 8**. At this time, the malicious ratio and the flipping probability satisfy $\rho \geq 1/(\alpha + \beta)$, the MU's average throughput R_m remains the same, that is, MUs completely make the FC blind. However, the blind scenario does not increase the MU's throughput, but reduces it. This is because the FC's global decision is still reliable in the non-blind scenario, each MU also occupies more spectrum resources according to the global decision. In the blind scenario, on the one hand, the increase in the number of MUs reduces the average throughput, on the other hand, MUs still decide whether to access the channel based on the unreliable global decision, the gains outweigh the losses.

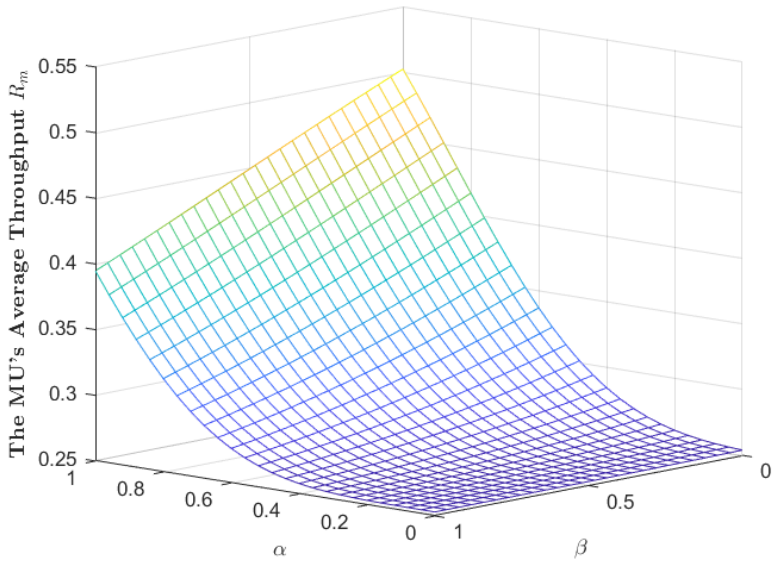

Fig. 7. The MU's average throughput when $\rho = 0.4$.

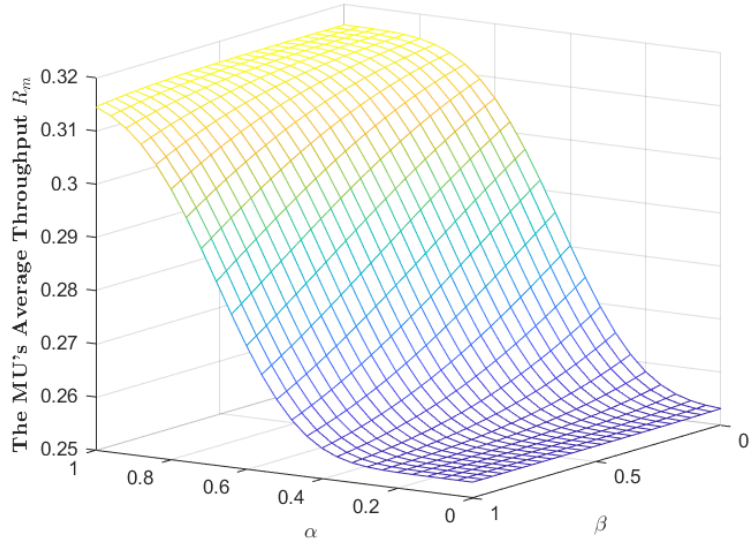

Fig. 8. The MU's average throughput when $\rho = 0.8$.

6. Conclusions and Further Work

In this paper, we established a dynamic Byzantine attack model in an interweave CR system from a malicious perspective, which can conduct various Byzantine attack by design different malicious ratios and flipping probabilities, and further derive the condition of which MUs make the FC blind. Then, we theoretically analyze the optimal attack strategy under two scenarios where MUs know that the FC adopts the fusion rule, with aim to minimize other SU's average throughput and maximize their own average throughput and the interference to

the PU. Finally, a series of numerical simulation results are presented to verify the correctness and effectiveness of our theoretical analysis on Byzantine attack.

Our work is different from most existing works in that we provide recent advances and open research directions on applying the FC and Byzantine attack in various scenarios and cases, focusing on the optimal attack strategy as well as the optimal defense strategy for CSS. In the follow-up work, we will consider the wise MU's optimal attack strategy when FC adopts a defense mechanism. This is an interesting problem worth exploring in the future. At the same time, these preliminary works pave the way for the follow-up robust defense strategy.

Acknowledgement

The authors declare that they have any commercial or associative interest that represents a conflict of interest in connection with the work submitted.

References

[1] X. L. Huang, Y. Xu, J. Wu and W. Zhang, "Non-cooperative spectrum sensing with historical sensing data mining in cognitive radio," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 10, pp. 8863-8871, Oct. 2017. Article (CrossRef Link)

[2] J. Wu, Y. Chen, P. Li, J. Zhang, C. Wang, J. Tang et al., "Optimisation of virtual cooperative spectrum sensing for UAV-based interweave cognitive radio system," *IET Communications*, vol. 15, no. 10, pp. 1368-1379, Jan. 2021. Article (CrossRef Link)

[3] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 1, pp. 116-130, Mar. 2009. Article (CrossRef Link)

[4] G. I. Tsiropoulos, O. A. Dobre, M. H. Ahmed and K. E. Baddour, "Radio resource allocation techniques for efficient spectrum access in cognitive radio networks," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 1, pp. 824-847, Oct. 2016. Article (CrossRef Link)

[5] S. Nallagonda, Y. R. Kumar and P. Shilpa, "Analysis of hard-decision and soft-data fusion schemes for cooperative spectrum sensing in Rayleigh fading channel," in *Proc of 2017 IEEE 7th International Advance Computing Conference*, Hyderabad, India, pp. 220-225, 2017. Article (CrossRef Link)

[6] K. Zeng, P. Pawelczak and D. Cabric, "Reputation-based cooperative spectrum sensing with trusted nodes assistance," *IEEE Communications Letters*, vol. 14, no. 3, pp. 226-228, Mar. 2010. Article (CrossRef Link)

[7] Y. Al-Mathehaji, S. Boussakta, M. Johnston and H. Fakhrey, "Defeating SSDF attacks with trusted nodes assistance in cognitive radio networks," *IEEE Sensors Letters*, vol. 1, no. 4, pp. 1-4, Aug. 2017. Article (CrossRef Link)

[8] X. Luo, "Secure cooperative spectrum sensing strategy based on reputation mechanism for cognitive wireless sensor networks," *IEEE Access*, vol. 8, pp. 131361-131369, Jul. 2020. Article (CrossRef Link)

[9] Z. Sun, Z. Xu, Z. Chen, X. Ning and L. Guo, "Reputation-based spectrum sensing strategy selection in cognitive radio Ad Hoc networks," *Sensors*, vol. 18, no. 12, pp. 4377, Dec. 2018. Article (CrossRef Link)

[10] N. Marchang, A. Taggu and A. K. Patra, "Detecting Byzantine attack in cognitive radio networks by exploiting frequency and ordering properties," *IEEE Transactions on Cognitive Communications and Networking*, vol. 4, no. 4, pp. 816-824, Dec. 2018. Article (CrossRef Link)

[11] P. Anand, A. S. Rawat, H. Chen and P. K. Varshney, "Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks," in *Proc of International Conference on COMmunication Systems and NETworks (COMSNETS)*, Bangalore, India, pp. 1-9, 2010. Article (CrossRef Link)

[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 Transactions on Signal Processing*, vol. 59, no. 2, pp. 774-786, Feb. 2011. Article (CrossRef Link)
[13] J. Wu, Y. Yu, T. Song and J. Hu, "Robust reputation management mechanism in cooperative spectrum sensing, " *Electronics Letters*, vol. 55, no. 21, pp. 1128-1130, Oct. 2019. Article (CrossRef Link)
[14] Y. Gan, C. Jiang, N. C. Beaulieu, J. Wang and Y. Ren, "Secure collaborative spectrum sensing: A peer-prediction method," *IEEE Transactions on Communications*, vol. 64, no. 10, pp. 4283-4294, Oct. 2016. Article (CrossRef Link)
[15] W. Wang, L. Chen, K. G. Shin and L. Duan, "Thwarting intelligent malicious behaviors in cooperative spectrum sensing," *IEEE Transactions on Mobile Computing*, vol. 14, no. 11, pp. 2392-2405, Nov. 2015. Article (CrossRef Link)
[16] L. Zhang, G. Nie, G. Ding, Q. Wu, Z. Zhang and Z. Han, "Byzantine attacker identification in collaborative spectrum sensing: A robust defense framework," *IEEE Transactions on Mobile Computing*, vol. 18, no. 9, pp. 1992-2004, Sept. 2019. Article (CrossRef Link)
[17] J. Wu, Y. Yu, T. Song and J. Hu, "Sequential 0/1 for cooperative spectrum sensing in the presence of strategic Byzantine attack," *IEEE Wireless Communications Letters*, vol. 8, no. 2, pp. 500-503, Apr. 2019. Article (CrossRef Link)
[18] A. A. Sharifi and M. Mofarreh-Bonab, "Spectrum sensing data falsification attack in cognitive radio networks: An analytical model for evaluation and mitigation of performance degradation," *AUT Journal of Electrical Engineering*, vol. 50, no. 1, pp. 43-50, 2018. Article (CrossRef Link)
[19] J. Wu, T. Song, Y. Yu, C. Wang and J. Hu, "Generalized Byzantine attack and defense in cooperative spectrum sensing for cognitive radio networks," *IEEE Access*, vol. 6, pp. 53272-53286, Aug. 2018. Article (CrossRef Link)
[20] 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 Transactions on Wireless Communications*, vol. 15, no. 10, pp. 6813-6827, Oct. 2016. Article (CrossRef Link)
[21] F. Ye, X. Zhang, Y. Li and C. Tang, "Faithworthy collaborative spectrum sensing based on credibility and evidence theory for cognitive radio networks," *Symmetry*, vol. 9, no. 3, pp. 36, Mar. 2017. Article (CrossRef Link)
[22] W. Hashlamoun, S. Brahma and P. K. Varshney, "Mitigation of Byzantine attacks on distributed detection systems using audit bits," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 18-32, Mar. 2018. Article (CrossRef Link)
[23] J. Parras and S. Zazo, "Learning attack mechanisms in wireless sensor networks using Markov decision processes," *Expert Systems with Applications*, vol. 122, pp. 376-387, May 2019. Article (CrossRef Link)
[24] H. O. Shazly, A. Saafan, H. E. Badawy and H. M. E. Hennawy, "Performance of analysis cognitive radio with cooperative sensing under malicious attacks over Nakagami faded channels," *Wireless Engineering and Technology*, vol. 7, no. 2, pp. 67-74, Apr. 2016. Article (CrossRef Link)
[25] L. Zhang, G. Ding, Q. Wu, Y. Zou, Z. Han and J. Wang, "Byzantine attack and defense in cognitive radio networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1342-1363, Apr. 2015. Article (CrossRef Link)
[26] S. Kar, S. Sethi and M. K. Bhuya, "Security challenges in cognitive radio network and defending against Byzantine attack: A survey," *International Journal of Communication Networks and Distributed Systems*, vol. 17, no. 2, pp. 120-146, Sep.2016. Article (CrossRef Link)
[27] P. Verma and B. Singh, "On the decision fusion for cooperative spectrum sensing in cognitive radio networks," *Wireless Networks*, vol. 23, pp. 2253-2262, May. 2016. Article (CrossRef Link)
[28] J. Wu, Y. Yu, H. Zhu, T. Song and J. Hu, "Cost-benefit tradeoff of Byzantine attack in cooperative spectrum sensing," *IEEE Systems Journal*, vol. 14, no. 2, pp. 2532-2543, Jun. 2020. Article (CrossRef Link)

[29] A. A. Sharifi and M. J. Musevi Niya, "Defense against SSDF attack in cognitive radio networks: Attack-aware collaborative spectrum sensing approach," *IEEE Communications Letters*, vol. 20, no. 1, pp. 93-96, Jan. 2016. Article (CrossRef Link)
[30] Y. Liang, Y. Zeng, E. C. Y. Peh and A. T. Hoang, "Sensing-throughput tradeoff for cognitive radio networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 4, pp. 1326-1337, Apr. 2008. Article (CrossRef Link)
[31] J. Wu, T. Song, Y. Yue, C. Wang and J. Hu, "Sequential cooperative spectrum sensing in the presence of dynamic Byzantine attack for mobile networks," *PloS one*, vol. 13, no. 7, Jul. 2018. Article (CrossRef Link)
[32] B. Kailkhura, Y. S. Han, S. Brahma and P. K. Varshney, "Distributed Bayesian detection in the presence of Byzantine data," *IEEE Transactions on Signal Processing*, vol. 63, no. 19, pp. 5250-5263, Oct. 2015. Article (CrossRef Link)

Jipeng Gan is studying at School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include cognitive radio networks, network security, game theory.

Jun Wu received the Ph.D. degree in Information and Communication Engineering from Southeast University, Nanjing, China, in 2018. He joined School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China, where he is currently a Lecturer from 2019. He has published over 20 IEEE/IET journal papers and conference papers, including IEEE Systems Journal, IEEE TVT, IEEE CL, IEEE WCL, IEEE Access, IET Communications and IEEE ICC, IEEE VTC. His current research interests include unmanned aerial vehicle, cognitive radio networks, internet of things, sequential detection, network security, machine learning and blockchain. He also severed as a reviewer for IEEE TCCN, IEEE Systems Journal, IEEE TVT, IEEE WCL, IET Communications and ETRI Journal etc., and a TPC member in several IEEE conferences.

J ia Zhang is studying at School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include cognitive radio networks, unmanned aerial vehicle, spectrum sensing.

Zehao Chen is studying at School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include cognitive radio networks, unmanned aerial vehicle, spectrum sensing, network security.

Ze Chen is studying at School of Communication Engineering, Hangzhou Dianzi University, Hangzhou, China. His research interests include cognitive radio networks, unmanned aerial vehicle, spectrum sensing, network security.