ANTI-JAMMING PERFORMANCE OF COGNITIVE RADIO NETWORKS UNDER MULTIPLE UNCOORDINATED JAMMERS IN FADING ENVIRONMENT

Wednel Cadeau and Xiaohua Li

Department of Electrical and Computer Engineering
State University of New York at Binghamton
Binghamton, NY 13902
{wcadeau1, xli}@binghamton.edu

ABSTRACT

In this paper, we study both the jamming capability of the cognitive-radio-based jammers and the anti-jamming capability of the cognitive radio networks (CRN), by considering multiple uncooperative jammers and independent Rayleigh flat-fading propagations. A Markov model of CRN transmission is set up for the cross-layer analysis of the anti-jamming performance. The transitional probabilities are derived analytically by considering a smart jamming attack strategy. Average throughput expression is obtained and verified by simulations. The results indicate that CRN communications can be extremely susceptible to smart jamming attacks targeting the CRN spectrum sensing and channel switching procedures.

Key words: cognitive radio networks, dynamic spectrum access, transmission power, jamming, throughput

1. INTRODUCTION

Cognitive radio networks (CRN) have attracted great attention recently as a means to resolve the critical spectrum shortage problem [1]. With dynamic spectrum access (DSA) techniques, CRN can be granted access of spectrum secondarily, i.e., as long as it can guarantee no interference to any primary user (PU) who is using this spectrum at this time in this location [2] [3]. This means that the cognitive radios have to periodically sense the spectrum to detect the primary user's activity. They have to vacate the channel immediately whenever PU activity is detected.

In this paper, we focus on the anti-jamming performance of CRN. On the one hand, jammers can greatly enhance their jamming capability by exploiting the cognitive radio technology, especially the flexible physical-layer and MAC-layer functions. In contrast, CRN may become more susceptible to jamming attacks because of some unique requirements in the physical- and MAC-layers, such as the requirement of channel vacating when detecting any primary user signals. On the other hand, the capability of hopping among many channels gives CRN a unique advantage of improving their anti-jamming performance. Therefore, the anti-jamming performance is a new and interesting research topic in CRN.

There have been extensive research results published in CRN, including areas such as spectrum sensing, transmission/modulation design, theoretical performance/capacity analysis, MAC/Network layer protocols, hardware/testbed development, security, etc. However, there have been very limited study on the anti-jamming capability although many people have pointed out its importance for a secure and reliable CRN [2] [3].

Conventionally, anti-jamming study is conducted in the Physical-layer via some anti-jamming modulations, such as spread spectrum, or in the layers above MAC via channel switching. However, even if a CRN has an anti-jam PHY-layer transmission scheme, it may still be sensitive to jamming because of the unique property of CRN, i.e., CRN has to vacate a channel even in the presence of slight jamming or interference [4]. This means that a jammer can use low energy signals to jam multiple channels at the same time. In addition, even if the CRN can apply channel hopping to avoid jamming, such schemes may be costly since new channel setup and switching in CRN may be time-consuming due to the required timing/frequency synchronization, channel estimation, handshaking for information exchange and network setup. The key problem is that the available channels may be time-varying, and the information about the available channels may not be identical among the CRN nodes. If not carefully designed, the channel switching procedure can greatly reduce the throughput of the CRN, or even make the CRN useless.

In contrast, for a jammer that uses similar cognitive radio device to conduct jamming attacks, the capability of conducting fast channel switching will enhance its jamming capability because it can easily jam multiple channels at the same time. In [5], we reported our preliminary study of the jamming capability of the jammer and the anti-jamming capability of the CRN. Nevertheless, such work was simplified by assuming additive white Gaussian noise (AWGN) channel and by considering one jammer only with a simple CRN transmission and jamming model. In this paper, we extend such study to include the more general Rayleigh flat fading channel model, and to consider multiple jammers. More over, we derive more accurate analytical results by considering a Markov model of CRN transmissions.

The organization of this paper is as follows. In Section 2, we give the models of the CRN transmission and the cognitive-radio-based jammer. Then in Section 3, we analyze jamming and anti-jamming performance in terms of CRN throughput and jamming probabilities. Simulations are conducted in Section 4. Conclusions are then given in Section 5.

2. CRN TRANSMISSION MODEL AND JAMMER MODEL

As shown in Fig. 1, typical CRN transmission modes include PU sensing period (in a sensing slot with duration T_s), data packet

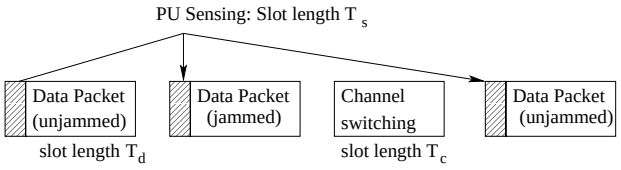

Fig. 1. Illustration of CRN transmission modes.

transmission period (in a data slot with duration T_d), and channel switching period (in a channel switching slot with duration T_c). If the PU is sensed as absent, then the CRN uses this channel to transmit a data packet; otherwise the CRN conducts channel negotiation in order to switch to a new channel. PU sensing duration T_s is usually much shorter than the data packet duration T_d, so the normal jamming-free transmission can guarantee high enough throughput. However, the channel switching duration T_c is usually long, since the CRN nodes have to conduct a sequence of synchronization, channel setup, handshaking and network setup procedure before a new channel can be settled. Therefore, T_c is usually much longer than T_d. This situation is even worse if we realize that the CRN nodes may not share identical spectrum white space information among them because of sensing errors or practical unsymmetrical signal propagations. For simplicity, we do not consider the case when the CRN nodes have backup channels in memory for faster switching. The CRN may have many channels to select from, depending on the activity of the PU. The large number of channels is one of the primary advantages of CRN to combat jamming.

In contrast to [5] where a simple CRN transmission session was assumed so that each jamming strategy was designed to jam only one of the transmission modes, in this paper we consider a more general jamming scenario where some or all of the three transmission modes may be jammed simultaneously, depending on the jamming strategy. The jamming strategy is unified to be modelled by a single parameter: the jamming signal duration T_j.

Specifically, if the PU is sensed as absent, then the CRN continues to use this channel to transmit a data packet; otherwise the CRN switches to another channel. If the data packet transmission is successful, then the CRN conducts PU sensing again; otherwise, the CRN will initiate channel switching. If the channel switching procedure is successful, then the CRN conducts PU sensing before deciding whether to conduct data transmission. The CRN will re-do the channel switching when the previous channel switching procedure is jammed.

Fig. 2 shows the Markov model for this CRN transmission scenario, where $p_s,\ p_d,\ p_c$ are the probabilities of the CRN in the spectrum sensing, data transmission and channel switching modes, respectively. The transitional probabilities $p_{js},\ p_{jd},\ p_{jc}$ are the probabilities that the spectrum sensing, data transmission and channel switching procedures are jammed, respectively. We need to first derive such transitional probabilities.

We assume that the minimum workable signal-to-interference-plus-noise ratio (SINR) for the data transmission and channel switching procedures are Γ_d and Γ_c, respectively. Usually Γ_c is smaller than Γ_d because the CRN may adopt some more reliable transmission techniques (albeit with lower data rate) such as spread spectrum modulations to increase the reliability of channel switching and to reduce the probability of interfering primary users [6]. In contrast, during the PU sensing procedure, there may only be jamming signals besides noise, so we assume a minimum interference-to-noise ratio (INR) Γ_s for the CRN to determine whether the channel is available or not.

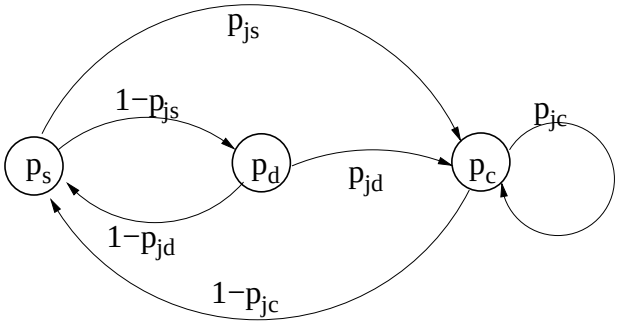

Fig. 2. Markov model for CRN transmission under various jamming probabilities.

We make the following assumptions about the jammers. 1) There are multiple jammers who do not cooperate. 2) Each jammer uses devices that have similar capabilities as a CRN node, including spectrum sensing and RF transceiving. 3) The jammers do not know the secret keys the CRN is using for channel selection and communication. Under the assumptions, since the jammers do not know the channel used by the CRN (we do not consider the smart sensing/detection of the jammers), the only way left for the jammers is to randomly select a channel to jam.

Since the jammers can fastly switch channels, they may choose to jam multiple channels simultaneously. We assume that the jammers use jamming signals with shorter duration T_j and fixed signal power P_j when they want to jam multiple channels, instead of using lower jamming power with fixed jamming signal duration. We also assume that the demodulation and signal detection of the CRN receiver depends on the average SINR received during the entire slot.

We assume that each jammer has the same transmission power $P_j = P_s$ as the CRN, where P_s is the CRN node's transmission power. Usually each jammer does not know the channel used by the CRN, nor know other jammers. So it has to randomly select some channels to jam. The jammers can use fast channel switching to jam more channels within a regular data/PU-sensing/channel-switching slot. Since the jamming duration T_j is smaller, the overall jamming signal power in this slot is also lower. The total number of channels a jammer can transmit jamming signals to depends on the ratio of the CRN transmission slot length and jamming signal length.

Conventionally, jamming is successful only if the SINR of the CRN receiver is less than certain threshold. In CRN case, however, jamming may be more easily deployed and more effective. For example, a smart jammer can selectively jam/interfere with the PU sensing slot. As long as the jamming signal emitted to the PU sensing slot makes the INR larger than the sensing threshold Γ_s, the CRN must vacate the channel and take the time-consuming channel switching procedure to negotiate a new one.

In this paper, instead of considering just one jammer as [5], we consider J jammers. Each of them adopts the above jamming strategy independently. However, we assume that all the jammers adopt the same jamming parameters P_j and T_j in order to simplify the analysis. In our case, the jamming strategy is parameterized by

T_j. Smaller T_j means the jammers try to jam more channels simultaneously and target more toward jamming PU sensing slot. Larger T_j means the jammers try to focus on fewer channels and target more toward jamming all the CRN transmission slots including the data slots. The former is similar to the "light jamming strategy" in [5], while the latter is similar to the "strong jamming strategy" in [5]. However, since the CRN and jamming models in this paper are somewhat different from those in [5], the results may also be different.

As an anti-jamming performance metric, we consider the average throughput R of the CRN, which can be calculated from the probabilities of the three states in Fig. 2 and the corresponding slot lengths. Note that only the data packet transmission mode with successful (unjammed) data transmission is counted toward the average throughput. In the next section, we will analyze the jamming probabilities before deriving this throughput.

3. JAMMING AND ANTI-JAMMING PERFORMANCE ANALYSIS

3.1. Jamming probabilities

Consider a CRN communication system, where a pair of CRN transmitter and receiver is conducting transmission at unit data throughput. A group of J jammers, each with the similar channel sensing and transmission capability as a cognitive radio, want to jam the CRN transmission so as to reduce the throughput.

First, we consider the data packet session with slot length T_d and SINR requirement Γ_d. The effect of jamming can be measured by the CRN receiver's SINR. If there are k jamming signals, each with duration T_j, in this slot, then the SINR can be defined according to the following equation

$$\gamma_d(k) = \frac{P_s \alpha_s^2 T_d}{\sum_{\ell=1}^{k} P_j \alpha_\ell^2 \min\{T_d, T_j\} + N T_d} \tag{1}$$

where α_s^2 is the Rayleigh flat fading channel (power) coefficient of the CRN, α_ℓ^2 is the Rayleigh flat fading channel (power) coefficient of the ℓth jamming signal, N is the power of the additive white Gaussian noise (AWGN). We assume that the channel power coefficients α_s^2, α_ℓ^2 are independent exponential random variables with unit mean.

Note that the index ℓ denotes the ℓth jamming signal. Each jammer may produce multiple jamming signals within this data slot $T_j < T_d$. However, only some of these jamming signals are injected to the right channel used by the CRN in this slot. Assume there are k jamming signals that accidently fall into this CRN channel. The number of jamming signals k is limited to

$$0 \le k \le K_d \triangleq J \left\lceil \frac{T_d}{T_j} \right\rceil, \tag{2}$$

where $\lceil x \rceil$ is the minimum integer that is no less than x. The case of $k = 0$ means that there is no jamming signal.

Assume there are M white space channels available for secondary spectrum access (without PU activity in this session). Then the probability that there are k jamming signals in this CRN channel follows the binomial distribution

$$P_d[k] = \binom{K_d}{k} p_j^k (1 - p_j)^{K_d - k}, \tag{3}$$

where

$$p_j = \frac{1}{M} \tag{4}$$

is the probability that a jammer chooses the same channel as the CRN with an evenly distributed random pick from an overall of M white space channels.

For simplicity, we do not consider the white space detection errors of the CRN and jammers. White space detection errors may make the available white space channels less for CRN. However, for the jammers, a safer approach might be just to jam every one of the M white space channels. In addition, we do not consider the time-varying nature of the white spaces due to primary user activity. For notational simplicity, we also assume that the channel power coefficients α_ℓ^2 are independent among all the $\ell = 1, \cdots, k$ even though some of the jamming signals are from the same jammer. This is reasonable because such jamming signals are transmitted in different time.

Since the minimum workable SINR for the data session is assumed to be Γ_d, a successful jamming means that

$$\gamma_d(k) < \Gamma_d \tag{5}$$

We have the following analytical results for the probability of successful jamming of the data session.

Proposition 1. If there are k jamming signals with the same jamming duration T_j in a data slot of duration T_d, under the assumption of independent Rayleigh flat fading channels, the probability that the data session is jammed is

$$P[\gamma_d(k) < \Gamma_d] = 1 - e^{-\frac{N\Gamma_d}{P_s}} \left(1 + \frac{P_j \min\{T_d, T_J\}}{P_s T_d} \Gamma_d\right)^{-k}. \tag{6}$$

Proof. Substituting (1) into (5), we can change (5) into $z < \Gamma_d$ where

$$z = \frac{1}{N} P_s \alpha_s^2 - \frac{P_j \min\{T_d, T_j\}}{N T_d} \Gamma_d \sum_{\ell=1}^{k} \alpha_\ell^2. \tag{7}$$

Since all the Rayleigh flat fading channel coefficients are independent, α_s^2 is an exponential random variable with unit mean, i.e., its probability density function is

$$f_{\alpha_s^2}(x) = \begin{cases} e^{-x}, & x \ge 0 \\ 0, & \text{else} \end{cases}, \tag{8}$$

while $Y = \sum_{\ell=1}^{k} \alpha_\ell^2$ follows Erlong distribution $Y(k, 1)$ with probability density function

$$f_Y(y) = \begin{cases} \frac{y^{k-1} e^{-y}}{(k-1)!}, & y \ge 0 \\ 0, & \text{else} \end{cases}. \tag{9}$$

Due to the independence assumption, their joint distribution is

$$\begin{aligned} f_{\alpha_s^2, Y}(x, y) &= f_{\alpha_s^2}(x) f_Y(y) \\ &= \begin{cases} e^{-x} \frac{y^{k-1} e^{-y}}{(k-1)!}, & x \ge 0, y \ge 0 \\ 0, & \text{else} \end{cases}. \end{aligned} \tag{10}$$

Then, the probability $P[\gamma_d(k) < \Gamma_d]$ can be evaluated as

$$P[z < \Gamma_d] = \int \int_{z < \Gamma_d} f_{\alpha_s^2, Y}(x, y)\, dx\, dy \tag{11}$$

$$= \int_0^\infty \frac{y^{k-1}e^{-y}}{(k-1)!}\,dy \int_0^{\frac{N}{P_s}\Gamma_d\left(1+\frac{P_j\min\{T_d,T_j\}}{NT_d}y\right)} e^{-x}\,dx$$
$$= \int_0^\infty \frac{y^{k-1}e^{-y}}{(k-1)!}\left[1-e^{-\frac{N\Gamma_d}{P_s}}e^{-\Gamma_d\frac{P_j\min\{T_d,T_j\}}{P_sT_d}y}\right]dy$$
$$= 1-\frac{e^{-\frac{N\Gamma_d}{P_s}}}{(k-1)!}\int_0^\infty y^{k-1}e^{-\left(1+\frac{P_j\min\{T_d,T_j\}}{P_sT_d}\Gamma_d\right)y}\,dy$$

The integration in the last equation can be changed into the integration of the Erlong probability density function. Then, according to the property of the Erlong distribution, we can derive (6). □

Note that from (6), we have

$$P[\gamma_d(0)<\Gamma_d] = 1-e^{-\frac{N\Gamma_d}{P_s}}, \tag{12}$$

which is the same as the result we can derive directly from (1) and (5) when there is no jamming signal.

Averaging over all possible k, the average probability that the data session is jammed can be written as

$$p_{jd} = \sum_{k=0}^{K_d} P[\gamma_d(k)<\Gamma_d]P_d[k]. \tag{13}$$

Similarly, for the channel switching procedure with duration T_c and minimum workable SINR Γ_c, we can derive the jamming probability as follows.

Proposition 2. For the channel switching slot of duration T_c, under the assumption of independent Rayleigh flat fading channels and identical jamming signal duration T_j for all the jammers, the probability that this channel switching session is jammed is

$$p_{jc} = \sum_{k=0}^{K_c} P[\gamma_c(k)<\Gamma_c]P_c[k], \tag{14}$$

where the maximum number of jamming signals in this session is

$$K_c = J\left[\frac{T_c}{T_j}\right], \tag{15}$$

the jamming probability with k jamming signals is

$$P[\gamma_c(k)<\Gamma_c] = 1-e^{-\frac{N\Gamma_c}{P_s}}\left(1+\frac{P_j\min\{T_c,T_J\}}{P_sT_c}\Gamma_c\right)^{-k}. \tag{16}$$

and the probability of having k jamming signals is

$$P_c[k] = \binom{K_c}{k} p_j^k(1-p_j)^{K_c-k}. \tag{17}$$

Proof. We can drive equations (14)-(17) by following directly (1)-(11). We just need to replace T_d and Γ_d with T_c and Γ_c, respectively. □

In contrast to the data packet transmission and the channel switching sessions, the spectrum sensing session is different. We need to consider the interference (jamming) to noise ratio (INR) $\gamma_s(k)$ for a white space channel without primary user activity. Usually the CRN is highly sensitive in PU sensing, which means there is an extremely small INR threshold Γ_s, and $\gamma_s(k) \geq \Gamma_s$ means that the jammers successfully disguise primary users to force the CRN to conduct channel switching. In our case, this means that the spectrum sensing session is jammed, and the CRN nodes have to initiate the channel switching procedure.

The INR under k jamming signals is defined as

$$\gamma_s(k) = \frac{\sum_{\ell=1}^{k} P_j\min\{T_s,T_j\}\alpha_\ell^2}{NT_s}. \tag{18}$$

Proposition 3. For the channel sensing slot of duration T_s, under the assumption of independent Rayleigh flat fading channels and identical jamming signal duration T_j for all the jammers, the probability that this channel sensing session is jammed is

$$p_{js} = \sum_{k=0}^{K_s} P[\gamma_s(k)\geq\Gamma_s]P_s[k], \tag{19}$$

where the maximum number of jamming signals in this session is

$$K_s = J\left[\frac{T_s}{T_j}\right], \tag{20}$$

the jamming probability with k jamming signals is

$$P[\gamma_s(k)\geq\Gamma_s] = 1-\frac{\gamma(k,a)}{(k-1)!} = \sum_{n=0}^{k-1}\frac{1}{n!}e^{-a}a^n, \tag{21}$$

where the parameter $a = \frac{NT_s\Gamma_s}{P_j\min\{T_s,T_j\}}$ and $\gamma(k,a)$ is the lower incomplete Gamma function. The probability of having k jamming signals is

$$P_s[k] = \binom{K_s}{k} p_j^k(1-p_j)^{K_s-k}. \tag{22}$$

Note that $P[\gamma_s(0)\geq\Gamma_s]=0$ when there is no jamming signal.

Proof. Equations (20) and (22) can be derived similarly as $P_d[k]$ in (2) and (3) by just replacing T_d with T_s. To derive equation (21), from the INR definition (18) we have

$$\gamma_s(k) = \frac{P_j}{NT_s}\min\{T_s,T_j\}\sum_{\ell=1}^{k}\alpha_\ell^2. \tag{23}$$

Since $Y = \sum_{\ell=1}^{k}\alpha_\ell^2$ follows Erlong distribution $Y(k,1)$ with probability density function (9), we can derive

$$P[\gamma_s(k)\geq\Gamma_s] = P\left[Y\geq\frac{NT_s\Gamma_s}{P_j\min\{T_s,T_j\}}\right] = 1-\int_0^{\frac{NT_s\Gamma_s}{P_j\min\{T_s,T_j\}}} f_Y(y)\,dy \tag{24}$$

From the property of the Erlong distribution, the integration in (24) leads to (21). Then (19) is directly available. □

3.2. Average throughput

With the jamming probabilities p_{jd},p_{jc},p_{js} derived in equations (13), (14) and (19), respectively, all the transitional probabilities in the Markov model shown in Fig. 2 are then available. According to the steady state property of the Markov model, we can calculate the probabilities of the three states p_s, p_d and p_c by solving the

following equation

$$\begin{bmatrix} -1 & 1-p_{jd} & 1-p_{jc} \\ 1-p_{js} & -1 & 0 \\ p_{js} & p_{jd} & p_{jc}-1 \end{bmatrix} \begin{bmatrix} p_s \\ p_d \\ p_c \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}. \quad (25)$$

This equation has infinitely many solutions. However, we also need a constraint

$$p_s + p_d + p_c = 1, \quad (26)$$

which will constraint the problem to have a unique solution in most cases.

With some deductions, we can readily solve (25) and (26). For example, the system stays in data packet transmission session with probability

$$p_d = \frac{(1-p_{js})(1-p_{jc})}{2-p_{jc}+(p_{jd}-p_{jc})(1-p_{js})}. \quad (27)$$

However, some of the data packet transmissions are lost due to successful jamming. Considering the jamming probability p_{jd}, we know that on average, with probability $p_d(1-p_{jd})$, the data packet transmission is successful, which contribute to average throughput.

With the state probabilities, we can define the normalized average throughput of the CRN transmission as

$$R = \frac{p_d(1-p_{jd})T_d}{p_sT_s + p_dT_d + p_cT_c}. \quad (28)$$

Proposition 4. With the normalized average throughput definition (28) and the Markov model stead-state equation (25), the throughput of CRN transmission under jamming parameter T_j is

$$R = \frac{(1-p_{js})(1-p_{jc})(1-p_{jd})T_d}{(1-p_{jc})T_s+(1-p_{js})(1-p_{jc})T_d+(p_{jd}+p_{js}-p_{jd}p_{js})T_c}. \quad (29)$$

Proof. From (25), we can represent p_d and p_c by p_s as

$$\begin{aligned} p_d &= (1-p_{js})p_s \\ p_c &= \frac{p_{jd}+p_{js}-p_{jd}p_{js}}{1-p_{jc}}p_s \end{aligned}$$

Substituting them into (28), we can derive (29). □

4. SIMULATIONS

In this section, we use simulations to verify the analysis results derived in Section 3, specifically, the normalized average throughput R and the probability of transmitting unjammed data packets $p_d(1-p_{jd})$. We used the following parameters in the simulations: $M = 100$, $J = 10$, $T_d = 5$, $T_c = 10$, $T_s = 0.25$, $\Gamma_d = 15$dB, $\Gamma_c = 10$ dB, $\Gamma_s = -15$ dB, $P_s = P_j = -80$ dBm, $N = -100$ dBm. This mainly simulates a system with a large number of available channels.

First, we use simulations to verify that the analysis results will fit the simulated results. For this purpose, we used Monte-Carlo simulations to simulate the CRN transmissions and the jammers, with channel coefficients and white space channel pickups randomly generated. For the jammers, we evaluate the jamming signal duration T_j from 0 (jamming-free) up to the duration of T_c since T_c is the longest slot length. For the theoretical results, we used equations (29) to calculate R and used equations (13) and (27) to calculate $p_d(1-p_{jd})$.

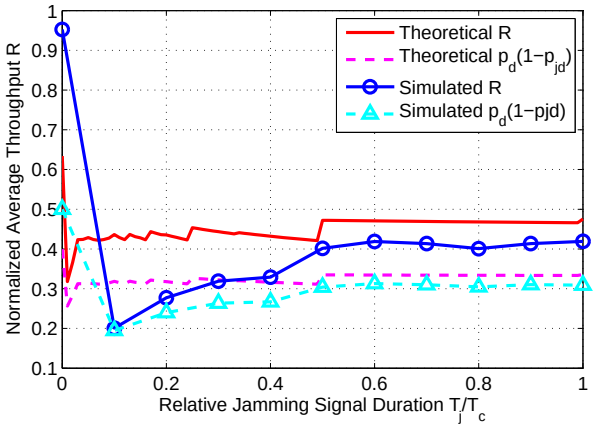

Fig. 3. Comparison of simulation results to the theoretical analysis results of the average throughput and the probability of transmitting unjammed data packets.

The simulation results are shown in Fig. 3. From the results, we can see that the theoretical analysis results fit well to the simulated results, which demonstrates the validity of the modelling and analysis. Secondly, compared to the jamming-free throughput ($T_j/T_c = 0$) which is near unity, the throughput drastically reduces to just below 0.3 when facing 10 smart jammers that used small T_j. This indicates that even with 100 channels to hop from, the CRN throughput still suffers from detrimental effect from jamming. Thirdly, it shows that smaller jamming duration T_j is more effective in terms of successful jamming than larger jamming duration. This is because by using smaller jamming duration, the jammers targeted toward the PU sensing session, and can effectively mitigate the large number of channels that the CRN can hop to. Therefore, the CRN is more susceptible to smart jamming attacks than conventional wireless networks. Finally, if we compare this result with respect to the results in [5], we can clearly see that multiple jammers can greatly enhance their jamming capability.

Next, we evaluate the anti-jamming performance of CRN when the CRN can hop among more white space channels. For the total number of channels M from 1 to 1000, we calculate the theoretical throughput under four different jamming conditions with relative jamming signal duration $T_j/T_c = 0.05$ or 0.5, and with number of jammers $J = 1$ or 10. The results are shown in Fig. 4. From the figure, we can see that while increasing the channel number M can drastically increase the anti-jamming capability of CRN, such a benefit tends to saturate after tens of channels have been used. Even with 1000 white space channels, the average throughput are still just around 0.6. In contrast, the jammers can mitigate this benefit by just using a few more jammers. This can be clearly seen in Fig. 5. With a few jammers, the CRN requires a huge number of white space channels in order to guarantee certain throughput which is already low, usually less than 0.5. This indicates the advantage of smart jammers over the CRN.

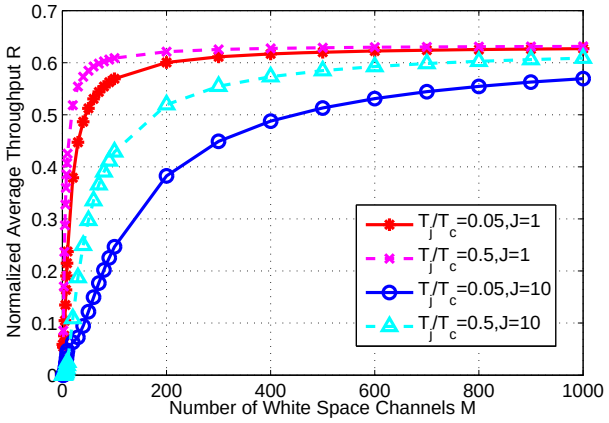

Fig. 4. Average throughput as function of number of white space channels, under various jamming conditions.

5. CONCLUSIONS

In this paper, we extend our existing research in [5], i.e., jamming performance analysis of CRN, from single-jammer in AWGN channel into multiple jammers in Rayleigh flat fading channels. Both the jamming and anti-jamming performance are analyzed by deriving expressions of the CRN average throughput and jamming probabilities. We used a Markov model of the CRN transmission with three states, and calculated the steady-state probabilities to derive the average throughput. We verified the analysis results by simulating CRN transmissions in random jammers. The results indicate that the CRN are extremely susceptible to smart jammers which try to jam the CRN's spectrum sensing procedure.

6. REFERENCES

[1] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty. "NeXt genera-tion/dynamic spectrum access/cognitive radio wireless networks: a survey," *Comput. Netw.*, 50(13):2127-2159, 2006.

[2] M. McHenry, E. Livsics, T. Nguyen and N. Majumdar, "XG dynamic spectrum access field test results," *IEEE Commun. Mag.*, vol. 45, no. 6, pp. 51-57, June 2007.

[3] C. Cordeiro, K. Challapali, D. Birru and S. Shankar, "IEEE 802.22: An introduction to the first wireless standard based on cognitive radios," *J. of Commun.*, vol. 1, no. 1, Apr. 2006.

[4] R. Chen, J.-M. Park, and J. H. Reed, "Defense against primary user emulation attacks in cognitive radio networks," *IEEE J. on Select. Areas in Commun.*, Special Issue on Cognitive Radio Theory and Applications, Vol. 26, No. 1, Jan. 2008.

[5] X. Li and W. Cadeau, "Anti-jamming performance of cognitive radio networks," *Proc. of the 45th Annual Conf. on Information Sciences & Systems (CISS)*, Johns Hopkins Univ., Blatimore, MD, March 2011.

[6] X. Li and J. Hwu, "A frequency hopping spread spectrum transmission scheme for uncoordinated cognitive radios," *Proceedings of the IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP'2009)*, Taipei, Taiwai, April 19-24, 2009.

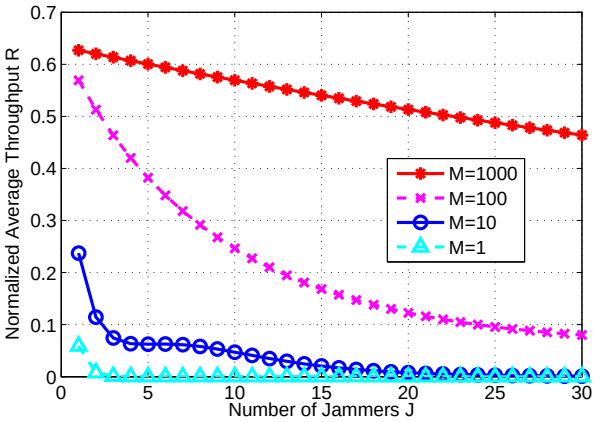

Fig. 5. Average throughput as function of number of jammers J, when the CRN has various number of white space channels. $T_j/T_c = 0.05$.