ANTI-JAMMING PERFORMANCE OF COGNITIVE RADIO NETWORKS

Xiaohua Li and Wednel Cadeau

Department of Electrical and Computer Engineering
State University of New York at Binghamton
Binghamton, NY 13902
{xli, wcadeau1}@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. We first setup the models of cognitive-radio-based jammers and the cognitive radio network transmissions. We then analyze various jamming attack strategies where the jammer spends various powers in order to jam various transmission slots of the cognitive radio networks. Average throughput and jamming probability are derived and verified by simulations. Strength and weakness of jammer and cognitive radio networks are then discussed, which will be useful to guide the anti-jamming cognitive radio network design.

Index Terms— 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. 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-layer, 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.

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 a unique property of CRN, i.e., CRN has to vacate a channel even in the presence of slight jamming or interference. 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 conduct fast channel switching will enhance its jamming capability because it can easily jam multiple channels at the same time.

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 probability. 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, a typical CRN node transmission involves transmitting a data packet (in a data slot) followed by a PU sensing period (in a sensing slot). If the PU is sensed as absent, then the node continues to use this channel; otherwise the CRN node switches to another channel. If a data packet transmission is jammed, then the CRN will initiate channel switching through a sequence of synchronization, channel setup, handshaking and network setup procedure before the data packet can be transmitted again. 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.

We make the following assumptions about the jammer. 1) The jammer uses devices that have similar capabilities as CRN nodes, including spectrum sensing and RF transceiving. A number of such jamming devices could be used by the jammer depending on how strong the attacker is or how much cost the jammer is willing to pay to jam the communication. 2) When the CRN switches to a new channel, it will take some time for a jammer to sense the spectrum and to find out which channel this CRN is using. Specifically, if

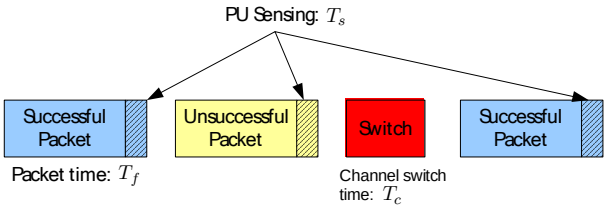


Fig. 1. Illustration of a transmission session of a CRN node.

this time period is longer than the time period the CRN spends in a channel, then the only alternative for the jammer is to randomly select channels to jam. Therefore, the CRN's channel switching rate directly impacts its anti-jam capability while at the same time affects its transmission bandwidth efficiency. 3) We also assume that 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 jammer), the only way left for the jammer is to randomly select a channel to jam. However, since the jammer can fastly switch channels, it may choose to jam multiple channels simultaneously. We assume that the jammer uses jamming pulses shorter than a slot duration when it wants to jam multiple slots at the same time, instead of using lower jamming power. We also assume that the demodulation and signal detection of the CRN receiver depends on the average signal to interference plus noise ratio (SINR) received during the entire slot.

We assume that the jammer has the same transmission power $P_J = P_s$ as the CRN. There are various ways for the jammer to conduct jamming, from conventional jamming (which uses all the transmission power to jam one channel) to more intelligent jamming approaches. Usually the jammer does not know the channel used by the CRN, so it has to randomly jamming some of the channels. In addition, the jammer can use fast channel switching to jam more channels within a slot, but at a relatively lower jamming signal level. The total number of channels a jammer can transmit depends on the ratio of the data slot length and jamming slot length. Obviously, by simultaneously jamming more channels, the jammer is more likely to hit the channel used by the CRN, but the CRN node will suffer less interference. Conventionally, the jamming is successful only if the SINR of the CRN node is less than certain threshold. Therefore, the number of simultaneously jammed channels can not be too large in practice.

However, a smart jammer can selectively jam/interfere with the PU sensing slot only. As long as the interference signal emitted to the PU sensing slot makes the SNR larger than the sensing threshold, the CRN must vacate the channel and switch to a new one.

Therefore, there are three typical jamming strategies for the jammer:

J1. Strong jamming strategy where the purpose is to completely jam any transmission;

J2. Light jamming strategy where the purpose is to inject a slight signal into the channel sensing time period to cause the CRN to switch channels;

J3. Smart jamming strategy where the purpose is to jam both channel sensing and channel switching slots.

The first strategy is effective but can only jam one or several channels simultaneously. The second strategy is more like a conventional PU emulation attack [4], while the third approach is more than a PU emulation attack at that the short channel switching procedure will be jammed completely. In the next section, we will analyze the performance of the CRN under each of the three jamming attacks. As evaluation metric, we will derive the average throughput of the CRN node, and the jamming probability.

3. JAMMING AND ANTI-JAMMING PERFORMANCE ANALYSIS

3.1. CRN Performance under Strong Jamming Strategy

Consider a CRN communication system, where a pair of CRN transmitter and receiver is conducting transmission at unit data rate. A jammer, with the similar channel sensing and transmission capability as the CR, wants to jamming the above transmission. In this subsection, we consider the Strategy J1. The effect of jamming can be measured by the CRN receiver's SINR, which can be evaluated according to the following equation

$$\gamma = \frac{P_s T_f}{P_J T_J + N T_f} = \frac{P_s}{P_J \frac{T_J}{T_f} + N}, \quad \text{for } 0 \le T_J \le T_f \qquad (1)$$

where P_s is the transmission power of the CRN (more accurately, the received signal power in CRN receiver), P_J is the transmission power of the jammer (or more accurately, the received jamming signal power by the CRN receiver), N is noise, T_f is the CRN's transmission time period, and T_J is the jamming time period.

The CRN can detect multiple usable channels, and pick one of them to use. The jammer does not know which channel the CRN is using, so it must try to jam multiple channels in turn. Therefore, the time it spends in jamming a channel, T_J , is usually less than the CRN's communication time. Without loss of generality, we just use T_f in equation (1), which is the duration of a data transmission slot, since the receiver may need to receive the entire data packet before it can conduct demodulation and decoding. If the jamming time T_J is too small, then according to (1), it may not reduce the SINR effectively. Therefore, this expression limits the rate of jamming channel switching the jammer can take. We assume that there is an SINR threshold Γ_0 such that if the SINR is less than this threshold, i.e.,

$$\gamma < \Gamma_0 \qquad (2)$$

then the CRN transmission is completely jammed, and the CRN has to switch channel.

As shown in Fig. 1, consider a single session of the CRN transmission where the CRN conducts the data transmission for T_f seconds at unit data rate. If it is not jammed, then it continues to conduct another session of transmission. If it is jammed, then the CRN need to spend another time T_c to switch to a new channel and retransmit the data packet using anther session with duration T_f. Since the jammer normally can not track perfectly the CRN's channel switching, we can reasonably assume that this next transmission session will be successful. In this case, the throughput of CRN transmission is reduced to

$$R = \frac{1 - P[J]P[\gamma < \Gamma_0]}{1 + \frac{T_c}{T_f} P[J]P[\gamma < \Gamma_0]} \qquad (3)$$

where $P[J]$ denotes the probability that the jammer successfully interfere the channel used by the CRN, $P[\gamma < \Gamma_0]$ is the probability that the received SINR is less than the receiving threshold Γ_0 and thus causes channel switching and data retransmission.

The duration T_c includes the time used for ACK/Backoff when

the first data session is jammed, new channel sensing/negotiation, communications setup (such as oscillator stabilizing, frequency/channel estimation), and link/network setup. Depending on the reliability of the CRN design, some of the above procedures may be avoided for faster switching. However, the time duration T_c may not be small (or may even be much larger than T_f) in practice.

Note that the equation (3) is describing the throughput of the case when the CRN transmission is jammed. Depending on the jamming time period T_J and the total number of possible channels used by CRN, the successful jamming probability should be considered to obtain the correct expected throughput.

An important remaining task is to deriving the jamming probability $P[J]$. Assume there are a total of M_w white space channels available. Because of the spectrum sensing errors, the CRN detects M_c channels as available to use, whereas the jammer detects M_J channels that the CRN may use. The reason that there is certain mismatch between the channels detected by the CRN and those detected by the jammer is due to the false-positive and false-negative probability of the spectrum sensors.

For a channel that is within the M_w available channels, if the CRN detected is as not available, then this is false-negative. Similarly for the jammer. Let the false-negative probabilities of the CRN and the jammer be p_{cf} and p_{Jf}, respectively. On the other hand, if a channel that is not within the M_w available channels is detected by the CRN or the jammer as available, then we have false-positive. Let the false-positive probabilities of the CRN and the jammer be p_{cp} and p_{Jp}, respectively. Then we have

$$M_J = M_w(1 - p_{Jf}) + (M - M_w)p_{Jp}, \tag{4}$$

and similarly,

$$M_c = M_w(1 - p_{cf}) + (M - M_w)p_{cp}, \tag{5}$$

where M is the total number of channels (which may usually be a very large number).

In general, such false probabilities may be small. In particular, the jammer may intentionally increase its false positive probability and reduce its false negative probability so as to make sure that its detected available channel set is larger (and include) those of the CRN. Obviously, this may increase its chance of jamming the CRN. However, it may need to try jamming more channels, which may reduce its probability of jamming the CRN.

Though the jammer knows that there are M_J channels that the CRN may use, it may not know which channel the CRN is using now. Therefore, the jammer has to jam each channel in turn. When it happens to jam the right channel, then the CRN has to switch its channel, which is a costly procedure, as shown by (3). If it does not jam the right channel, nothing happens, and the jammer simply wastes its transmission power and time. In the next, we want to derive the probability that the jammer can jam the right channel under this setting.

Let us consider first the jammer randomly select one channel to jam. The probability that the CRN is accidently using this channel is

$$P[1] = \frac{M_w(1 - p_{Jf})(1 - p_{cf})}{M_c M_J}. \tag{6}$$

Note that $M_w(1-p_{Jf})(1-p_{cf})$ is the number of available channels (within the M_w available channels) that are detected correctly by both the CRN and the jammer.

Obviously, during one session, if jamming only one channel, the probability of jamming the CRN (which is $P[1]$ in (7)) may be extremely low. In order to increase its jamming probability, the jammer may need to jam multiple channels. Assume that all such jamming channels are selected independently, then the probability of jamming the right CRN channel in K times is

$$P[J] = 1 - \left(1 - \frac{M_w(1 - p_{Jf})(1 - p_{cf})}{M_c M_J}\right)^{\frac{T_f}{T_J}}. \tag{7}$$

3.2. CRN Performance under Light Jamming Strategy

In this subsection, we consider another possible jamming strategy of the jammer, i.e., Strategy J2: the jammer uses light transmission power to jam the CRN. Although the jamming power is very small and does not normally prevent the successful data packet transmission, it will still make the CRN to switch channels since the CRNs may take the jamming signal as being the primary user signal.

Consider the CRN transmission session as shown in Fig. 1. The CRN's conduct transmission in term of slots. Each data packet slot has transmission during T_f. At the end of each data packet transmission slot, there is a short slot T_s used for the CRN to conduct spectrum sensing to see if there is primary user becoming active. If primary user is sensed, then this channel must be vacated. The channel switching time T_c may be short or long, depending on system realization. For example, a typical channel vacating time is less than 0.5 second. In a normal communication scenario, since the primary user may become active in a previously vacated channel with very low probability, the channel switching happens also with extremely low probability. As a result, even if the data packet slot length T_f is small, much less than the switching time T_c, the throughput reduction is still very small. However, in case of jamming, it will become completely different, since the jamming's objective is try to increase the frequency of channel switching.

We assume that the required CRN communication SNR is Γ_0, which is also the maximum interference level that the jammer can create. We also assume that the minimum sensing sensitivity of the CRN (for detecting the primary user) is an SNR of $\Gamma_{\min}$. Usually $\Gamma_{\min} \ll \Gamma_0$. We also assume that the jammer can not jam the channel switching procedure, because the CRNs may simply skip any jamming during this phase, or this phase is conducted by some special spread spectrum transmission so the interference to primary users is guaranteed low.

During a fixed time period T, the jammer has a total of transmission energy $P_s T \times 1$ (CRN transmission power by data packet length by one channel). Since the jammer can use lower transmission power in this case, it can jam multiple channels instead of one channel. In addition, it may not need to stay on the same channel for the entire packet period, but rather, it will stay on the same set of channels just for time T_J, where the jamming time $T_J \ll T$. Furthermore, since we consider the extremely low jamming power case only, the jamming energy spent on the data packet transmission phase usually does not matter. What is matter is the jamming energy spent inside T_s. As a result, there is usually no point for the jammer to jam the same channel for too long (in fact, it can be shown that shorter time jamming is better than long time jamming in this case). Therefore, we assume

$$T_J \le T_s. \tag{8}$$

The total number of channels G that the jammer can jam simultaneously can be obtained follows,

$$P_J T_J G \le P_s T, \tag{9}$$

where P_J is the jamming power per channel, T_J is the jamming

period per channel, P_s is the highest transmission power of the CRN and the jammer, T a slot length. Note that both the left hand side and the right hand side of (9) is the energy (or total transmission power), normalized by the channel bandwidth. We have usually also

$$\frac{P_s}{N} \geq \Gamma_0, \tag{10}$$

where N is the noise power, and Γ_0 is the required CRN transmission SNR. Note that we have averaged out both the large scale fading and small scale fading. Details about the fading will be considered in future research.

When the CRN transmission channel is jammed, the CRN receiver's SINR is (1). Note that we consider only the SINR during the primary user sensing (spectrum sensing) phase. Under our assumption, this SINR is usually large, i.e.,

$$\gamma \geq \Gamma_0 \tag{11}$$

can usually be satisfied, so even if jammed, the data packet can still be successfully transmitted. Similarly, the CRN can conduct reliable channel switching handshaking. However, the jammer will be detected by the CRN (as the primary user) if

$$\gamma > \Gamma_{\min}. \tag{12}$$

In other words, if (12) is satisfied, then channel switching procedure is initiated by the CRN, which introduces extra time and thus reduce transmission throughput. Otherwise, channel switching procedure will not be initiated. By taking the equality signs in (9) and (10), and replace the results into (11) and (12), we can get

$$\gamma = \frac{P_s}{N} \times \frac{1}{1 + \frac{\Gamma_0}{G}\frac{T}{T_s}}. \tag{13}$$

The average throughput is determined by the probability that the CRN communication channel will be correctly jammed and the jamming induced SINR satisfied (12). The jamming probability can still be derived similarly as in (7).

Note that even if the channel is jammed, the data communication is still successful. The CRN just needs to negotiate a channel switching. This is usually a quite fast procedure, but it still needs time spent in handshaking, carrier switching, oscillator stabilization, channel estimation, carrier frequency estimation, etc. Under jamming, the throughput becomes

$$R_J = R\frac{T_f + T_s}{T_f + T_s + T_c}. \tag{14}$$

An important property is that the next data packet transmission can be jammed with the same probability again. Therefore, the jamming probability and the throughput among the data packet periods are independent from each other. On the other hand, the channel switch procedure is assumed as jamming resilient, primarily due to its lower data rate transmission requirement. This simplifies the consideration. However, jamming may be addressed as elongating the channel switching time. The total average throughput in light jamming case can then be derived as

$$R = \frac{1}{1 + \frac{T_c}{T_s}P[J]P[\gamma > \Gamma_{\min}]}. \tag{15}$$

3.3. CRN Performance under Smart Jamming Strategy

In this subsection, we consider another possible jamming strategy of the jammer, i.e., Strategy J3: the jammer uses mid-level transmission power to jam the CRN. The objective is to jam the spectrum sensing slot and the channel switching slot. By injecting an interference into the channel sensing slot, the CRN will have to conduct channel switching, which wastes time and reduce throughput. This is similar to the case J2. However, in this new jamming strategy, the jammer also tries to jam the channel switching procedure. Here the objective is to jam the beginning of the channel switching procedure so as to break the handshaking conducted by the CRN nodes. As we know, such handshaking is critically needed for CRN nodes because they may have asymmetric knowledge about the available channels. In previous subsection, the channel switch slot length T_c may be small. But if this is jammed successfully, the CRN has to use some more time-consuming procedure to re-start communications. Therefore, we have to introduce a much larger channel switching slot length T_w in this case.

Nevertheless, besides such an important unique point, all the necessary derivation procedure is similar to those in the previous subsection. Following a similar procedure, we can derive the average throughput of the CRN as

$$R = \frac{1}{1 + P[J]P[\gamma > \Gamma_{\min}]\left\{P[\gamma_c < \Gamma_0]\frac{T_w}{T_f} + P[\gamma_c \geq \Gamma_0]\frac{T_c}{T_f}\right\}}. \tag{16}$$

When comparing the equation (16) with (15), we have introduced the probabilities $P[\gamma_c < \Gamma_0]$ and $P[\gamma_c \geq \Gamma_0]$, which denotes the probability that the SNR γ_c of the channel switching slot is less than the SNR threshold Γ_0 or not. Obviously, the jamming signal level should be large enough in order to cause $P[\gamma_c < \Gamma_0]$ so as to jam the channel switch procedure. Note that the jammer usually just needs to jam the initial stage of the channel switching procedure. Without loss of generality, we can assume the SNR γ_c is the average SNR during time period T_c. Equation (16) shows that the CRN throughput depends on the probability that the jammer correctly jams the PU sensing and channel switching slots and on the duration of the PU sensing and channel switching slots.

4. SIMULATIONS

In this section, we use simulations to verify the analysis results derived in Section 3, specifically, the jamming probability and the average throughput under the three jamming strategies. In addition, we simulate the two typical CRN systems:

C1. The commercial IEEE 802.22 system that exploits spectrum holes in TV broadcasting channels [3];

C2. The military XG system [2].

The first system features long data frame T_f, long channel switching slots T_c,T_w, and a smaller number of available channels M_w. On the other hand, the second system features short data frame T_f, a large number of available channels M_w, and relatively short channel switching slots T_c,T_w. Note that the difference between T_c and T_w is depending on whether the handshaking between the CRN nodes is jammed or not. If not jammed, then the time of channel switching is relatively short, as T_c. If this handshaking is jammed, then because of the asymmetric information about available channels between the CRN nodes, the channel switching time duration will be much longer, as T_w.

We denote the IEEE 802.22 like system as "CR Model 1", while the XG like system as "CR Model 2". By simulating these two different CRN models, we can readily see how the CRN protocol parameters affect the anti-jamming performance under various jamming strategies.

For the CR Model 1, we use the following parameters: $M = 10$, $M_w = 5$, $p_{jf} = p_{jp} = p_{cf} = p_{cp} = 0.05$, $T_f = 60, T_w = 30, T_c = 0.5, T_s = 0.025$, $\Gamma_0 = 15$dB, $\Gamma_{\min} = -15$ dB, $G = 10$, $P_s = -80$ dBm, $N = -100$ dBm. This mainly simulates a system with smaller number of available channels. For the CR Model 2, it shares some same parameters as the first model, but has the following different parameters: $M = 1000$,$M_w = 500$, $T_f = 5, T_w = 10, T_c = 0.3$, $G = 100$. This mainly simulates a system with a large number of available channels.

In all the simulations, the jamming slot duration T_J is a variable. We derive the throughput and jamming probability under various T_J. This way, we can see the importance for the jammer to select the best jamming parameters besides the jamming strategy.

In the first experiment, we simulated the two CR models under Jamming Strategy J1. The results are shown in Fig. 2. The curves marked as "theory" denote theoretical analysis results, calculated by equations (3) and (7). The curves marked as "sim" denote simulation results, or results obtained via simulating a large number of CRN transmission sessions under the jamming sessions. From the Fig. 2, we can clearly see that the analysis results match well with the simulation results, which indicates the validity of the analysis expressions. In addition, from the figure, we can clearly see that by using a large number of channels, the CRN can effectively mitigate jammers with jamming strategy J1, as the normalized throughput is almost unit while the jamming probability is almost 0. This means the transmission is reliable even if there are multiple jammers instead of one jammer as we analyzed and simulated. On the other hand, if the number of channels is small, then the transmission can be successfully jammed as long as the jammer's jamming slot length is chosen carefully. In fact, with multiple jammers, it is pretty flexible for the jammers to choose their jamming slot lengths. To the view point of the jammer, Strong Jamming Strategy J1 may not be a good jamming strategy.

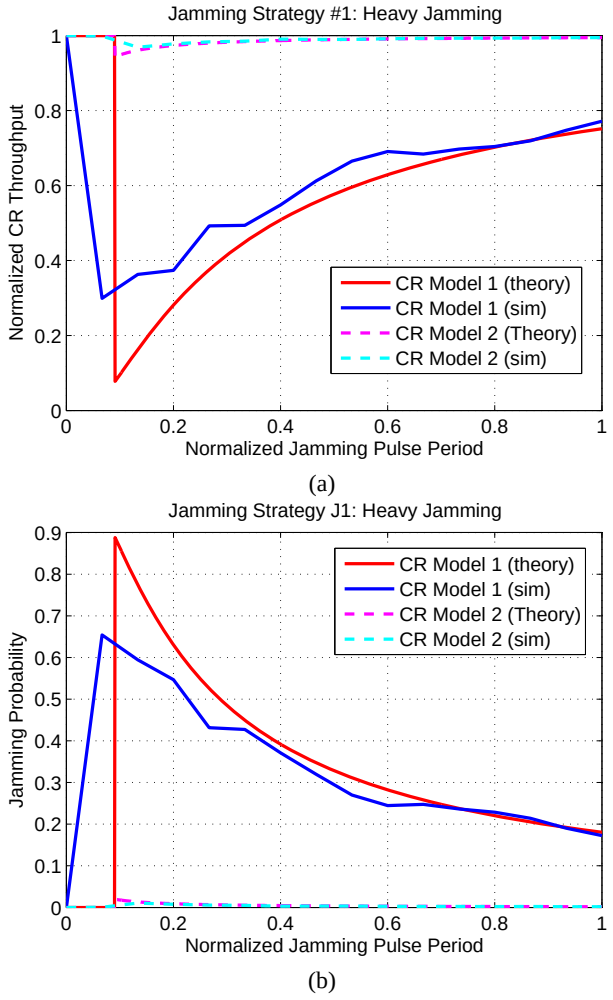


Fig. 2. CRN throughput (a) and jamming probability (b) under Jamming Strategy J1.

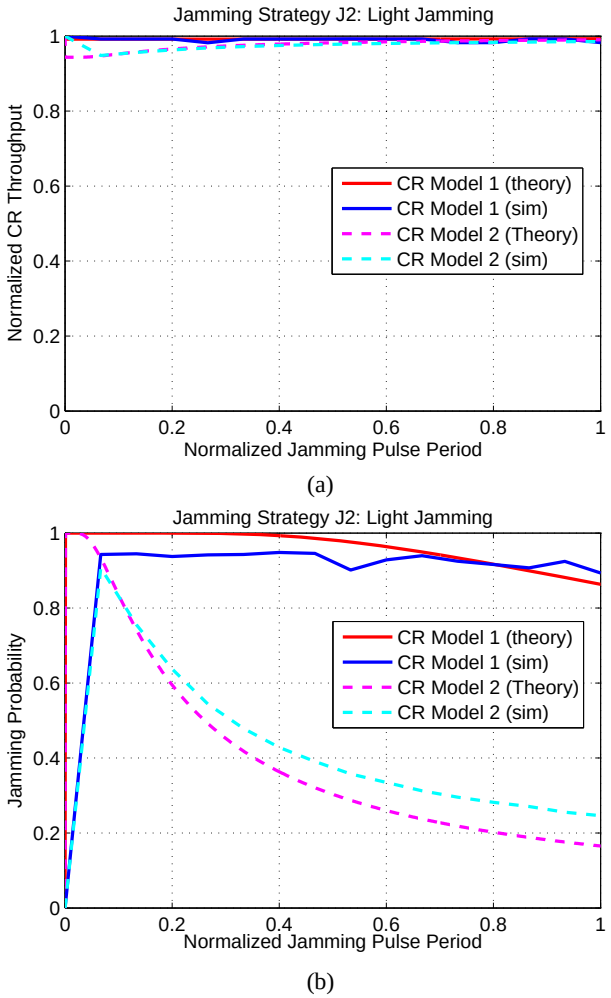
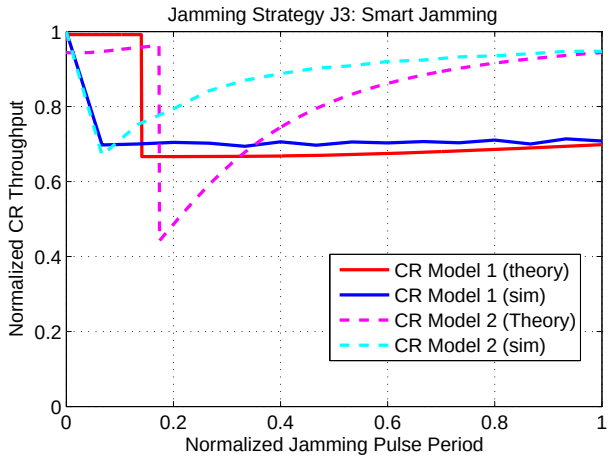
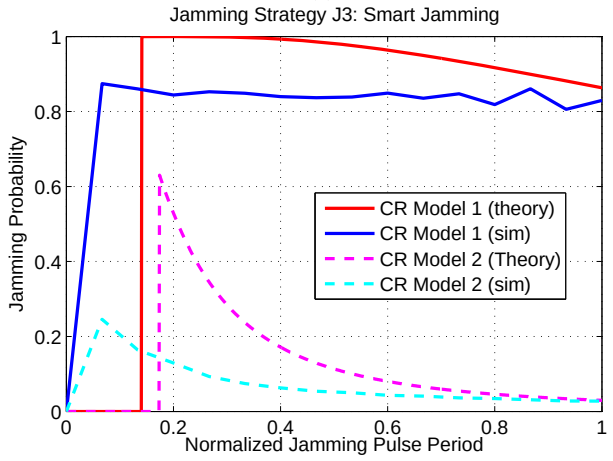


Fig. 3. CRN throughput (a) and jamming probability (b) under Jamming Strategy J2.

In the second experiment, we simulate the two CR models under the Jamming Strategy J2. The results are shown in Fig. 3. Although the jamming probability is high (which just means that with high probability the jammer can inject interfering signals into the channels used by the CRN), the throughput may not reduce too much for the CR Model 1. However, the CR model 2 may easily get jammed in this case. This can be explained by that all the data transmission can get through, and the only throughput reduction effect is due to the channel switch procedure. Since the CR model 1 has a relatively long data slot length but relatively small channel switching slot length, its throughput may not be affected severely. This is completely different from CR model 2 where the data slot length is small. Note that there is an assumption that the CRN can always find a channel to vacate to, even for CR model 1 with has a small number of channels to hop to. This result indicates the importance of optimizing the slot lengths of various MAC-layer slots. This also indicates that the conventional Primary User Emulation Attack can be easily dealt with by adjust the slot lengths, as long as there is always spare channels to use.



(a)



(b)

Fig. 4. CRN throughput (a) and jamming probability (b) under Jamming Strategy J3.

In the third experiment, we simulate the two CR models under the Jamming Strategy J3. The results are shown in Fig. 4. From the result, we can clearly see that this is the best jamming strategy in terms of jammers, as none of the models can have reliable transmissions as long as the jammer chooses jamming period appropriately. The jammer can simply use smaller jamming period (which increases) and a large enough jamming signal to jam CRN's channel switching procedure. From the figure, we can see that a single jammer can cause both CRN models reduce their throughput to 50%-70%. Therefore, a few jammers can easily jam and block the CRN transmissions. This is when CRN can really suffer from jamming, which indicates that anti-jamming design is a challenging issue for CRN.

5. CONCLUSIONS

In this paper, we modelled the CRN transmission sessions and the jammers, and analyzed the jamming and anti-jamming performance by deriving expressions of the CRN average throughput and jamming probability under three jamming strategies. We verified the analysis results by simulating the three jamming strategies in two typical CRN models. The results indicate that the anti-jamming is a challenging task in CRN. CRN needs to use more channels and to enhance the anti-jamming capability of the PU sensing procedure to mitigate jamming attacks.

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.