Secure Transmission Power of Cognitive Radios for Dynamic Spectrum Access Applications

Xiaohua Li, Jinying Chen, Fan Ng
Dept. of Electrical and Computer Engineering
State University of New York at Binghamton
Binghamton, NY 13902
{xli,fngnone1}@binghamton.edu, chjy@cdut.edu.cn

***Abstract*—One of the major concerns of cognitive radios when used for secondary spectrum access is the potential of interfering primary users, considering especially that cognitive radios may be misbehaved or under malicious attacks. In this paper, we present a method for a cognitive radio to secure its transmission power purely from its physical-layer received signals. Built into the transceiver hardware as an independent self-check procedure, this method can guarantee the avoidance of excessive interference of cognitive radios to primary users even when the more flexible upper-layer software or policy regulator is compromised under attacks. Analysis and simulations show that the secure transmission power determined by this procedure can be very close to the ideal secondary transmission power in many practical situations, so the proposed method is helpful to guarantee both the efficiency and the security of cognitive radios.**

I. Introduction

Cognitive radios (CR) have attracted great attention recently as a means to resolve the critical spectrum shortage problem. After the Federal Communications Commission (FCC)'s seminal report [1], it is know well known that spectrum access is more of a problem than physical scarcity of the spectrum, and that more flexible spectrum access techniques instead of the conventional command-and-control regulations should be adopted. Under this general theme, dynamic spectrum access (DSA) based on cognitive radio techniques [2] becomes a promising approach [3].

DSA and CR techniques have many potential commercial and military applications. An immediate commercial application under developing is the exploitation of some of the less utilized TV spectrum. The TV band is attractive not only because TV broadcasting has regular and predictable schedule of occupancy, but also because TV broadcasting is currently under digitalization with some TV bands to be freed. By the year 2009 in USA and 2010 in Europe, all the TV signals will be digital, which will reduce the bandwidth requirement and give more opportunity to DSA and CR techniques.

The idea of DSA has also be investigated in DARPA in the so-called NeXt Generation (XG) program [4]. For military applications the benefits of DSA and CR can be both spectrum efficiency and security. For instance, a subdivision under General Dynamics, the C4 system, has developed a CR called AN/USC-61(c) system for US Navy, which has approximately 750 sub-channels between 2MHz and 2GHz for operation. All of these projects have the similar objective of utilizing the spectrum more efficiently.

In DSA networks, secondary spectrum access can be granted in various ways. One of the ways is for secondary users to utilize the spectrum "white space" which primary users do not use during some time period and in some place [5]. This may require an accurate model of the primary users' activity [3]. Another way is to allow the secondary users to utilize the same spectrum at the same time and the same place with the primary users, where the spectrum is called "gray space". Obviously, this latter way can potentially provide a much higher capacity for secondary users, albeit it may introduce certain interference to primary users. To limit the interference, the secondary users may adopt an underlay approach in which they transmit at low enough power so as to guarantee a small enough interference to primary users. An example is the ultra-wideband (UWB) transmission. An alternative approach is overlay, in which the secondary users either schedule their transmission power so that their interference to primary users is limited to an acceptable level [6], or exploit special coding techniques such as dirty paper coding so that they can use a portion of transmission power to help the primary users while using the rest of the power to transmit their own information [7]. In this paper, we focus on an overlay approach similarly to [6].

One of the major issues for the wide deployment of CR and DSA techniques is the security problem. It is well known that security is a big challenge for wireless communications [8]. The challenge is even more serious with respect to CR and DSA. CR have the flexibility of adjusting transmission parameters which conventional transceivers do not have. This posts a new threat to interfere primary users when allowed for secondary spectrum access [9]. A special concern is the interference to critical infrastructures such as police and emergency bands. Many CR may have built-in capability of occupying these bands since they are assumed to be able to use these bands as secondary users when there are no primary users or in some special emergency situations. Furthermore, the capability of wide range spectrum sensing may provide malicious users with a powerful tool of eavesdropping. The flexible access to a wide range of spectrum and modulation types may allow self-fish users to overuse spectrum resources or to jam a particular channel [10]. The very nature of the

operation of CR, which depends on downloadable/adjustible software and complex policy regulations [11], makes the guarantee of security a difficult task.

The security issue has been raised in a vast amount of literatures as a big challenge [3], [5], [9]. However, there have been very few research results to address this issue so far. Before the wide deployment of CR, the security issue must be well studied and resolved.

In this paper, we address one of the primary aspects of the security issue of CR when used for secondary spectrum access, i.e., guarantee the avoidance of excessive interference to primary users. Especially, interference must be constrained even if the CR are under attack or have been taken control by malicious users through downloadable software. We will propose a way for the CR to avoid using a transmission power in a transmission bandwidth that creates uncontrollable interference to primary users, even if the software of the CR is compromised. A unique feature is that our method exploits the physical-layer signals and can be built into the transceiver hardware, independently from upper-layer software or policy regulators. Hardware-based security is usually much more difficult for attackers to compromise than software-based security. While an attacker may easily alter software, he/she may not be able to change an integrated circuit. In addition, each CR uses the proposed method individually, rather than requiring networking or cross-talking. This can also avoid many potential security weaknesses.

In this paper, we focus on presenting the new method in a DSA network where secondary spectrum access is allowable as long as the interference to primary users is within a certain threshold. Obviously, this includes as a special case the listen-before-talk schemes [4] where the secondary users access the spectrum only when there is no primary activity. To allow this more broader secondary spectrum access, we assume that the primary system can tolerate certain interference, i.e., there is some redundancy in primary receiver's destine signal-to-noise ratio (SNR). Some capacity results for this type of DSA are shown in [6] [12]. For simplicity, we consider a cellular-style transmission for primary users. Secondary users are allowed to conduct transmission at the same time and the same frequency as the primary users. We then derive the secure transmission power allowable for secondary users, where the security means that the secondary transmission power will not create interference to any primary users above an allowable threshold.

The organization of this paper is as follows. In Section II, we give the system model. In Section III, we analyze the secure transmission power by a geometric method for each single secondary user. The comparison between the secure transmission power and ideal transmission power is conducted in Section IV. Simulations are conducted in Section V. Conclusions are then given in Section VI.

II. DSA SYSTEM MODEL

We consider a cellular-like primary system, where in a cell there is a base station that communicates with M mobile users. We denote the base station as primary user T_{p0} and the mobile users as primary users T_{pi}, $i = 1, \cdots, M$. In addition, there are a number of secondary users which are denoted as T_{si}, $i = 0, 1, \cdots$, as shown in Fig. 1. In this paper, we consider the case that each of users (T_{p0}, T_{pi}, and T_{si}) has a transmitter and a receiver, and thus can and in fact does conduct both transmitting and receiving. This is the situation of a cellular system or wireless LAN. Nevertheless, the results can be readily extended into the systems where there is only broadcast-type transmissions from T_{p0} to T_{pi}, such as in TV broadcasting systems, with slight modifications, as addressed in Section III.

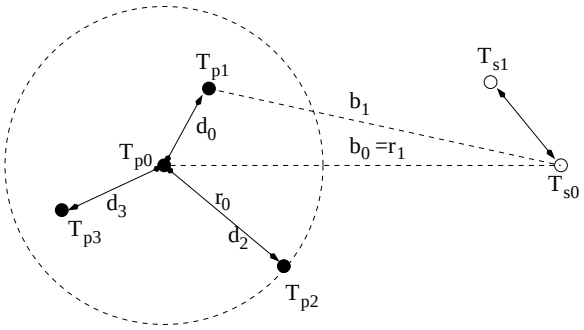

Fig. 1. Secondary spectrum access network consists of a cell with primary users (base station T_{p0} and mobile users T_{pi}), and some secondary users with CR (T_{si}).

We put the base station T_{p0} in the center of a cell with radius r_0. We assume that all the other primary mobile users are uniformly distributed inside the cell. We also assume that the secondary users lie outside of the cell just for mathematical simplicity.

The transmission distances between the base station and the mobile users are denoted as d_i, whereas the distances between the primary users and the secondary user T_{s0} are denoted as b_i. For simplicity, we assume that all the primary users use a transmission power P_0. In contrast, the secondary users' transmission power may be different, and we denote the transmission power of T_{s0} as P_1, which is what we are interested in.

We assume that both the number M and the positions of the primary users are unknown to the secondary users. Nevertheless, the secondary users can listen to the signals of all the primary users because each primary user (base station or mobile users) conduct both transmission and receiving. We do not require the secondary users to be able to discriminate the signals from different primary users.

The base station and mobile users conduct transmission with a slotted transmission protocol, where each one take turns to conduct transmission. For secondary users, we assume that they can conduct listening or transmission in any slot. The transmission power of the secondary users should be determined appropriately so that all the primary receivers can still work. In other words, while secondary transmission degrades the primary users' SNR, such a degradation should be smaller than certain threshold.

We assume that the primary system is designed with certain redundancy in SNR. Specifically, the primary receiver's SNR is no less than Γ_0 when there is no secondary transmission, while the smallest workable SNR for primary users is $\Gamma_0 - \Delta\Gamma$. So there is a redundancy of $\Delta\Gamma$ to tolerate the interference from secondary transmissions.

For most practical primary systems, the maximum transmission power P_0, the maximum transmission distance (cell size) r_0, the SNR Γ_0 and the SNR redundancy $\Delta\Gamma$ are specified in technical standards. Therefore, these parameters are available to secondary users. Considering that these parameters of the primary systems do not change for years once the standards are set, the secondary users can in fact build them into the hardware of their CR. We will show that a table of these parameters, when integrated with the received signals of the CR, can be used to determine the secure secondary transmission power P_1.

III. Secure transmission power for secondary users

If there is no secondary transmission, then the primary mobile user T_{pi}, $i = 1, \cdots, M$, has a baseband discretized received signal

$$\tilde{y}_{pi}(n) = \sqrt{P_0 g_i} s_{p0}(n) + v_{pi}(n), \tag{1}$$

where g_i denotes the path loss gain

$$g_i = K d_i^{-\alpha}, \tag{2}$$

with a constant K and a path loss exponent α. The signal $s_{p0}(n)$ is transmitted from the base station. For the receiver of the base station, we have similar formulations. Because we are interested in the long term SNR and transmission power in this paper, we omit the small-scale fading. But rather, we consider the large-scale path loss g_i only. The phase of the propagation channel is included into the transmitted signal $s_{p0}(n)$. The noise is denoted by $v_{pi}(n)$. Without loss of generality, we assume that all the signals $s_{pi}(n)$ have unit power, and all the channel noises $v_{pi}(n)$ have a power N. As a result, the SNR is determined by the transmission power P_0 and path loss g_i, as shown below

$$\tilde{\gamma}_{pi} = \frac{P_0 g_i}{N} \geq \Gamma_0. \tag{3}$$

Note that the primary system is designed to satisfy the SNR Γ_0.

If the secondary user T_{s0} also transmits while the primary user T_{pi} is receiving, then the signal received by T_{pi} becomes

$$y_{pi}(n) = \sqrt{P_0 g_i} s_{p0}(n) + \sqrt{P_1 f_i} s_{s0}(n) + v_{pi}(n), \tag{4}$$

where the path loss gain f_i is

$$f_i = K b_i^{-\alpha}. \tag{5}$$

For simplicity, we assume the parameters K and α are identical among all the users.

Under secondary spectrum access, the SNR of the primary user T_{pi} becomes

$$\gamma_{pi} = \frac{P_0 g_i}{P_1 f_i + N}. \tag{6}$$

Obviously, secondary spectrum access reduces the primary user's SNR. In order to tolerate secondary spectrum access, we exploit the primary system's link margin which is described by the SNR redundancy $\Delta\Gamma$. Therefore, the SNR (6) under secondary spectrum access just needs to satisfy

$$\gamma_{pi} \geq \Gamma_0 - \Delta\Gamma. \tag{7}$$

The secondary user T_{s0} can also listen to the primary user's transmission, which gives the signal

$$y_{s0}(n) = \sqrt{P_0 f_i} s_{pi}(n) + v_{s0}(n). \tag{8}$$

From the signal $y_{s0}(n)$, the secondary user can estimate both the noise power $N = E[|v_{s0}(n)|^2]$ and the primary user's signal power (after propagation attenuation)

$$Q_i = P_0 f_i. \tag{9}$$

Note that we have assumed channel reciprocity in terms of the path loss gain, i.e., the forward channel has the same path loss gain as the backward channel. Nevertheless, we do not require the small-scale fading channels be reciprocal.

Because the secondary user T_{s0} does not know the position of the primary users, it does not know d_i or g_i. To derive a secure secondary transmission power, the secondary user has to consider the worst case, i.e., the primary transmission distance is the maximum value r_0. In this sense, from the view point of T_{s0}, the primary user T_{pi} should have an SNR that satisfies

$$\gamma_{pi} \geq \hat{\gamma}_{pi} = \frac{P_0 \hat{g}_i}{P_1 f_i + N} \geq \Gamma_0 - \Delta\Gamma \tag{10}$$

where the maximum primary transmission distance r_0 is applied to derive path loss

$$\hat{g}_i = K r_0^{-\alpha}. \tag{11}$$

Obviously, as long as $\hat{\gamma}_{pi} \geq \Gamma_0 - \Delta\Gamma$ can be satisfied, the primary user can receive reliably.

From (10) and (9), the transmission power P_1 of the secondary transmitter must satisfy

$$\frac{P_0 \hat{g}_i}{P_1 \frac{Q_i}{P_0} + N} \geq \Gamma_0 - \Delta\Gamma. \tag{12}$$

From (12), we can derive a rule for determining the secure secondary transmission power

$$P_1 \leq \frac{P_0}{Q_i} \left(\frac{P_0 \hat{g}_i}{\Gamma_0 - \Delta\Gamma} - N \right). \tag{13}$$

According to (13), each secondary transmitter can determine its transmission power P_1 from its knowledge of the primary transmission power P_0, maximum primary transmission distance r_0 (which gives $\hat{g}_i$), the nominal primary system SNR Γ_0, the link margin (SNR redundancy) $\Delta\Gamma$, as well as its

own estimates of noise power N and primary signal power Q_i which can be estimated from its own received signals.

The procedure of using (13) to determine the allowable secondary transmission power can be implemented into the physical-layer transceiver hardware of cognitive radios. Each cognitive radio just needs to store a table of primary system's transmission frequency band, max transmission power, max transmission distance (cell size), and SNR requirements. The cognitive radio can determine the maximum allowable transmission power from its own received signals based on these *a priori* parameters. Furthermore, when there are multiple primary users, the cognitive radio just needs to choose the smallest allowable transmission power estimated during a sequence of slots. Because primary users take turns to occupy slots to conduct transmission, after certain time period, each cognitive radio will have listened the transmission of each of them.

One of the major advantages of this implementation is that the transmission power determination procedure is secure against software attacks. In practice it is more difficult for attackers to change hardware, especially the VLSI circuits, than to modify software. This is especially critical for cognitive radios where the operating software is usually assumed to be downloadable, and the policy regulation may be complex. The guarantee of software security may not be an easy task. In contrast, with the help of our proposed procedure, the transceiver hardware can help guarantee a secure secondary transmission power to avoid excessive interference, even if the software is compromised.

Another advantage of the proposed implementation is that each cognitive radio determines the secure transmission power individually, without resorting to networking or cross-talking among the cognitive radios. This can greatly enhance security against network-based attacks.

So far, the proposed scheme exploits the primary system's max transmission power P_0 and max transmission distance r_0 simultaneously. This requirement can be reduced to some extent. For some primary systems, if P_0 is not available, then the secondary user can replace P_0 by using (3). In this case, the power determination rule (13) can be modified to

$$P_1 \leq \frac{N^2\Gamma_0\Delta\Gamma}{Q_i\hat{g}_i(\Gamma_0-\Delta\Gamma)}. \tag{14}$$

On the other hand, if r_0 is not available, then the secondary user can replace r_0 also by using (3), which changes the power determination rule (13) into

$$P_1 \leq \frac{P_0N\Delta\Gamma}{Q_i(\Gamma 0-\Delta\Gamma)}. \tag{15}$$

Note that if (3) achieves equality, which means that the primary system is designed to barely satisfy the targeting SNR on the boundary, then the secondary transmission power P_1 determined from the three equations (13)-(15) are identical. Otherwise, the transmission power determined from (14)-(15) is smaller than that determined from (13), which means certain loss of secondary transmission capacity.

Note also that the equations (13)-(15) address the general situation where the secondary transmission happens simultaneously with the primary transmission, which means a spectrum "gray space" is used by CR. This automatically include the spectrum "white space" access as a special case, as happened in listen-before-talk schemes. In the latter case, since the primary signal power Q_i measured by the CR becomes zero or extremely small, the secondary transmission power P_1 becomes large. Therefore, the CR just needs to choose a transmission power that is curtained by some predefined threshold, or that is deemed sufficient for desirable secondary channel capacity.

The above derivation is conducted based on a cellular-like primary system, where all primary users conduct transmissions whose signals can be listened and exploited by the secondary CR. If the primary system is a TV-like broadcasting system where many receivers passively received signals from a base station, then the worst case primary receiver has to be considered by the CR when determining the secure transmission power. In this case, the CR usually knows the primary transmitter's signal power, from which and the cell size, the CR can deduct the distance of it from a worst case receiver, and then apply rules similar to (13), just with certain slight modifications. Details will be reported elsewhere.

IV. Ideal transmission power of secondary users

Because the secondary transmission power determination rules (13)-(15) consider the maximum primary transmission distance, which is in fact the worst case, the secure transmission power determined this way may be smaller than the maximum allowable transmission power. This surely may come at certain loss of secondary transmission power and capacity. In order to study the degree of this loss, in this section we derive the ideal transmission power by considering all possible primary transmission distances, rather than the worst case only.

Let the distance between T_{p0} and T_{s0} be r_1, and the primary mobile users are distributed uniformly in the cell of radius r_0. If there are primary receivers that are close to T_{s0}, then the transmission power of T_{s0} has to be small. The transmission power of T_{s0} depends on the position of the primary users. Since the secondary users do not have knowledge about the exact locations of the primary users, we evaluate the expected transmission power of T_{s0}, averaged over the uniform distribution of primary users.

Considering that M primary users are uniformly distributed inside the circle of radius r_0 around the primary base station T_{p0}, the cummulative distribution of the case that all the primary users are located out of a circle of radius x around T_{p0} can be modelled as

$$F(x) = \left(1-\frac{\pi x^2 - A_0}{\pi r_0^2 - A_0}\right)^M, \tag{16}$$

where $x_0 \leq x \leq r_0$ and $A_0 = \pi x_0^2$. Note that we have assumed that the secondary users know that all the primary users have a distance at least x_0 to the primary base station. The distance

constraint is reasonable in practice considering the far-field effect of antenna transmissions. Based on (16), the probability density that there are primary users with distance x to T_{p0} but there is no primary user closer to T_{p0} than x is

$$f(x) = -\frac{dF(x)}{dx} = \frac{2\pi M x}{\pi r_0^2 - A_0}\left(1 - \frac{\pi x^2 - A_0}{\pi r_0^2 - A_0}\right)^{M-1}. \quad (17)$$

Note that the negative sign in (17) is to guarantee a positive density.

Proposition 1. Consider the case that the minimum distance between T_{p0} and primary mobile users T_{pi} is x. Let the transmission power of T_{p0} be P_0. The maximum transmission power of T_{s0} is

$$P_1(x) \le (x + r_1)^{\alpha}\left(\frac{P_0}{\Gamma_0 - \Delta\Gamma}x^{-\alpha} - \frac{N}{K}\right), \quad (18)$$

where the equality can be achieved when the minimum of the primary mobile users' SNR equals $\Gamma_0 - \Delta\Gamma$, i.e., when

$$\frac{KP_0x^{-\alpha}}{KP_1(x + r_1)^{-\alpha} + N} = \Gamma_0 - \Delta\Gamma \quad (19)$$

Proof. See [12]. □

The upper bound $P_1(x)$ means that some primary mobile users' SNR will not be satisfied whenever the transmission power of T_{s0} becomes larger than $P_1(x)$, when the primary mobile users are randomly distributed.

Considering all possible x, we can derive the upper bound of the expected secondary transmission power. When evaluating average transmission power, it might be better to use the decibel value directly, because this can avoid the case that an extremely large transmission power will over-shadow many small transmission powers during averaging. Therefore, we use

$$P_1(x)(\mathrm{dB}) = 10\log_{10}\left[(x + r_1)^{\alpha}\left(\frac{P_0}{\Gamma_0 - \Delta\Gamma}x^{-\alpha} - \frac{N}{K}\right)\right]. \quad (20)$$

The decibel value of the upper bound of the expected ideal secondary transmission power can thus be derived from

$$\begin{aligned} P_1(\mathrm{dB}) &= \int_0^{r_0} P_1(x)(\mathrm{dB})f(x)dx \\ &= \int_{x_0}^{r_0} 10\log_{10}\left[(x + r_1)^{\alpha}\left(\frac{P_0}{\Gamma_0 - \Delta\Gamma}x^{-\alpha} - \frac{N}{K}\right)\right] \\ &\quad \times \frac{2\pi M x}{\pi r_0^2 - A_0}\left(1 - \frac{\pi x^2 - A_0}{\pi r_0^2 - A_0}\right)^{M-1} dx. \end{aligned} \quad (21)$$

From (21), we can evaluate the ideal secondary transmission power $P_1(\mathrm{dB})$ numerically.

To compare the ideal secondary transmission power with the secure transmission power, a closed-form solution of (21) is more desirable. Nevertheless, a closed-form evaluation of the integration in (21) is intractable. Therefore, we consider some necessary simplifications. First, we let $x_0 = 0$, so $A_0 = 0$. Then, we consider only the noiseless case with $N = 0$. After some tedious but straight-forward integration deduction from (21), we can obtain

$$\begin{aligned} P_{1,N=0}(\mathrm{dB}) &= 10\log_{10}\frac{P_0}{\Gamma_0 - \Delta\Gamma}\left(\frac{r_0}{r_1}\right)^{-\alpha} \\ &\quad + 5[\psi(M+1) - \psi(1)]\log_{10}e^{\alpha} \\ &\quad + 10\left[\frac{\sqrt{\pi}M\Gamma(M)r_0}{2\Gamma\left(M + \frac{3}{2}\right)r_1}\,{}_2F_1\left(\frac{1}{2}, 1, M + \frac{3}{2}, \frac{r_0^2}{r_1^2}\right)\right. \\ &\quad \left. - \frac{r_0^2}{2(M+1)r_1^2}\,{}_2F_1\left(1, 1, M + 2, \frac{r_0^2}{r_1^2}\right)\right]. \end{aligned} \quad (22)$$

Note that $\Gamma(\cdot)$, ${}_2F_1(\cdot)$ and $\psi(\cdot)$ denote Gamma function, Hypergeometric function, and PolyGamma function, respectively. From (22), we clearly see that the ideal secondary transmission power increases with the ratio r_1/r_0, but in general decreases with the number of primary users M. Large path loss exponent α is helpful for secondary spectrum access.

Under similarly the noiseless condition, the secure transmission power (13) can be reduced into

$$P_{1,N=0,b_i} = \frac{P_0}{\Gamma_0 - \Delta\Gamma}\left(\frac{r_0}{b_i}\right)^{-\alpha}. \quad (23)$$

If the number of primary mobile users is large enough, or after a sufficiently long time when the mobile users keep moving, then it is possible the CR will obtain a smallest power, which happens when a primary mobile user gives a distance of $b_i = r_1 - r_0$. Therefore, the smallest secure transmission power is

$$P_{1,N=0,b_i=r_1-r_0} = \frac{P_0}{\Gamma_0 - \Delta\Gamma}\left(\frac{r_0}{r_1 - r_0}\right)^{-\alpha}. \quad (24)$$

Therefore, if we compare (23) or (24) to (22), the secure transmission power is roughly lower than the ideal transmission power. However, their difference becomes smaller when the distance r_1 becomes larger, or the CR is farther away from the cell. In addition, the difference becomes smaller when the number of primary mobile users M becomes larger. We will verify such observations by simulations in Section V.

V. Simulations

In this section, we use simulations to compare the ideal secondary transmission power and the secure secondary transmission power obtained from (13). The ideal secondary transmission power is simulated under an assumption slightly different from Section IV, i.e., we assume that the primary transmission distances d_i are known to the secondary users in simulations. The ideal secondary transmission power can thus be calculated by using $g_i = Kd_i^{-\alpha}$ instead of $\hat{g}_i = Kr_0^{-\alpha}$ as in (13). As a result, the ideal secondary transmission power obtained in simulations should be even higher than those predicted in Section IV.

In simulations, we have made the base station to have a distance r_1 which is various times of $r_0 = 1000$ meters from the secondary user, and all the M primary users are randomly generated inside the primary cell with the radius

r_0. The primary transmission power is $P_1 = 100$ watts, and the noise power is $N = 5 \times 10^{-10}$ watts. The gains of all the antennas are 1, and the path loss exponent is $\alpha = 3$ for simulating an urban cellular radio environment. We let $\Gamma_0 = 20$ dB be the primary user's targeting SNR, whereas a 3 dB degradation of SNR is tolerable when accommodating secondary transmissions.

In the first experiment, we have tried various distance r_1 to evaluate the difference between the ideal transmission power and the secure transmission power for various number of primary users. As shown in Fig. 2, when the number of primary users becomes large, the difference becomes small. For example, when there are 20 primary users uniformly distributed inside the cell, the difference between the two transmission powers are usually less than 3 dB. This indicates that the efficiency of the secure transmission power determination scheme is high while guaranteeing security.

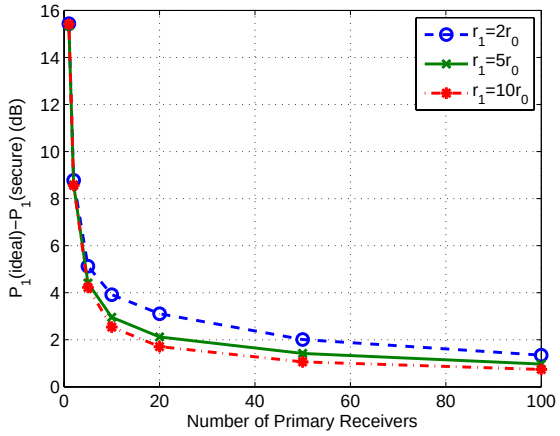

Fig. 2. Difference between ideal transmission power and secure transmission power for various primary-secondary distance r_1 and various number of primary users.

In the second experiment, we pick $r_1 = 5r_0$ and $M = 20$, and evaluate the cummulative distributions of the ideal transmission power and secure transmission power. As shown in Fig. 3, with up to 80% probability, the secure transmission power determined by the proposed scheme is less than 3 dB smaller than the ideal transmission power determined when all the system parameters are known. This result also shows the high efficiency of the secure transmission power determination scheme.

VI. Conclusion

In this paper, we propose a physical-layer power determination scheme for cognitive radios in secondary spectrum access applications. With this scheme, each cognitive radio is able to determine a secure transmission power that avoids excessive interference to primary users. The secure transmission power is determined based on certain standard parameters of primary systems, and based on the signals received by the CR itself. A unique feature of the proposed scheme is that it can be conveniently built into the transceiver hardware. The independence from the higher-layer software means that it can help guarantee the security of cognitive radios even when the software becomes compromised.

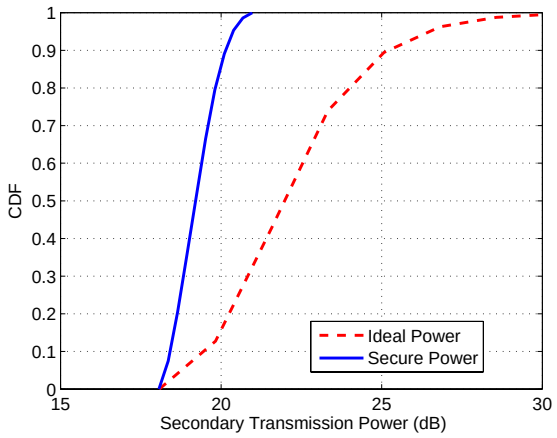

Fig. 3. Cummulative distribution of the ideal transmission power and secure transmission power.

References

[1] Federal Communications Commission, "Spectrum Policy Task Force," Rep. ET Docket no. 02-135, Nov. 2002.

[2] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 2, pp. 201-220, Feb. 2005.

[3] Q. Zhao and B. M. Sadler, "A survey of dynamic spectrum access," *IEEE Singal Processing Mag.*, vol. 24, no. 3, pp. 79-89, May 2007.

[4] 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.

[5] Y. Xing, R. Chandramouli, S. Mangold and S. Shankar, "Dynamic spectrum access in open spectrum wireless networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 3, pp. 626-637, Mar. 2006.

[6] M. Gastpar, "On capacity under receive and spatial spectrum-sharing constraints," *IEEE Trans. Info. Theory*, vol. 53, no. 2, pp. 471-487, Feb. 2007.

[7] N. Devroye, P. Mitran and V. Tarokh, "Achievable rates in cognitive radio channels," *IEEE Trans. Info. Theory*, vol. 52, no. 5, pp. 1813-1827, May 2006.

[8] X. Li, J. Hwu and E. P. Ratazzi, "Using antenna array redundancy and channel diversity for secure wireless transmissions," *Journal of Commun.*, vol. 2, no. 3, pp. 24-32, May 2007.

[9] J. Chapin and D. C. Sicker, "Safety and certification for new radio technologies," *IEEE Commun. Mag.*, vol. 44, no. 9, pp. 30-32, Sept. 2006.

[10] R. Chen and J.-M. Park, "Ensuring trustworthy spectrum sensing in cognitive radio networks," *IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, Sept. 2006.

[11] D. Wilkins, et al., "Policy-based cognitive radios," to appear, *IEEE Wireless Commun.*, 2007.

[12] X. Li, J. Hwu and N. Fan, "Transmission power and capacity of secondary users in a dynamic spectrum access network," *IEEE Military Communications Conference (MILCOM'2007)*, Orlando, FL, Oct. 29-31, 2007.