Pseudorandom Time-Hopping Anti-Jamming Technique for Mobile Cognitive Users

Nadia Adem, Bechir Hamdaoui, and Attila Yavuz
School of Electrical Engineering and Computer Science
Oregon State University, Corvallis, Oregon 97331
Email:ademn,hamdaoui,attila.yavuz@eecs.oregonstate.edu

***Abstract*—The 5G wireless networks will support massive connectivity mainly due to device-to-device communications. An enabling technology for device-to-device links is the dynamical spectrum access. The devices, which are equipped with cognitive radios, are to be allowed to reuse spectrum occupied by cellular links in an opportunistic manner. The dynamical spectrum availability makes cognitive users switch between channels, which leads to communication overhead, delay, and energy consumption. The performance degrades even more in the presence of security threats. It is important to countermeasure security threats while meeting a desired quality of service. In this paper, we analytically model the impact of spectrum dynamics on the performance of mobile cognitive users in the presence of cognitive jammers. The spectrum occupancy is modeled as a two-state Markov chain. Channels are modeled as double fading. Our contribution is proposing a pseudorandom time hopping technique to countermeasure jamming. We achieve an analytical solution of jamming probability, switching and error probability. Based on our findings, our proposed technique out performs the frequency hopping anti-jamming technique in a number of performance metrics.**

I. Introduction

5G wireless networks will support 1,000-fold gains in capacity. Deployment of networks with such a massive capacity poses many challenges, among which radio resource management is the most significant. The challenge is even more acute with the introduction of device-to-device communications [2]. 5G will support connections for at least 100 billion devices [6]. The support of massive capacity and connectivity becomes even more challenging when security concerns are taken into account. An enabling technology for device-to-device links is the reuse of spectrum occupied by cellular links [2]. In addition to cellular users, which are the primary users of spectrum, the communicating devices, which implement the cognitive radios, access the channels opportunistically. The dynamical spectrum access improves the spectrum utilization. However, the lack of access priority makes communication between cognitive users more vulnerable to security attacks.

A. Motivations

The availability of resources to cognitive users varies over time depending on primary users behaviors. The process of identifying and exploiting spectrum access opportunities causes performance degradation. Achieving a desired quality of service in cognitive networks while handling a security attack, e.g. jamming, is a challenge. Jamming attacks are more detrimental than other types of attacks [11]. Jammers can completely disrupt the communication between legitimate users. Jammers can utilize their transmission capabilities over the limited resources accessible by cognitive users. The challenge of maintaining a desired quality of service is even more acute when legitimate users are in motion. Due to the mobility of users, communication channel becomes both frequency and time dispersive. In this paper, we are proposing a pseudorandom time hopping anti-jamming scheme for cognitive users which are in motion. Our scheme out performs frequency hopping anti-jamming schemes.

B. Limitations of Existing Anti-jamming Techniques

A large number of resource management schemes have been recently proposed in the context of cognitive networks. However, few of those take into account security attacks like jamming. Most of the anti-jamming schemes existing in the literature rely on frequency hopping technique and its variations (e.g. [10] and [12]). We see anti-jamming methods based on frequency hopping to be unpractical in the context of cognitive networks for the following reasons.

- The coordinated frequency hopping schemes, where cognitive users follow a pre-share key to hop between channels whenever the last assigned channel is jammmed, are unpractical. Due to lack of access priority, a cognitive user is required to vacate a channel whenever a primary user reclaims the spectrum usage right. Consequently, the user needs to identify some other idle channel and switch to that channel. High primary user activities leads to high switching rate, which in turn causes communication delay, and energy consumption. The performance degrades even more with frequency hopping anti-jamming schemes.
- Anti-jamming techniques based on frequency-hopping can lead to a high probability of jamming. High primary user activities decrease the number of channels accessible by cognitive users, hence a jammer has more chance to hit their channels.
- The uncoordinated frequency hopping, where no agreement made between the transmitter and receiver on the hopping pattern, drastically degrades communication efficiency. Consequently, it is unpractical in cognitive networks where the resources are scarce.
- It is not necessary that cognitive users have access to multiple channels, which is a requirement for the frequency hopping anti-jamming methods.
- Spread spectrum based techniques which require a relatively large bandwidth are not applicable in cognitive networks since spectrum availability is volatile.

C. Summary of Contributions

In this paper, we introduce a jamming resiliency for communication links between cognitive mobile users. The channel occupancy is modeled as a Markov chain. The fading channel is modeled as a double fading channel. The anti-jamming technique is based on a pseudorandom time hopping. In the proposed scheme, the capacity of a channel is subdivided into n portions, where a user sends its data over one portion. The allocation is done by dividing the time axis into frames. Each frame is divided into slots of fixed length (e.g., one bit or one packet long). A user is constrained to only one slot per a frame. As time goes, a user keeps hopping between time slots. The allocation of the slots is made psedorandom according to a private key.

To the best of our knowledge, the idea of defending against jammers by distributing the data in time secretly has not been considered. We obtain the analytical solution for switching, jamming, and bit error probability. We compared the analysis of our scheme with the frequency hopping system. To the best of our knowledge, countermeasuring jamming while taking into account the mobility of users and the impact of the anti-jamming scheme on the switching process has not been addressed in the literature. Below we summarize the advantages of the proposed technique.

- The system is designed to mitigate the time-varying effects of the channel caused by the mobility of users. The slot duration is carefully selected to mitigate the frequency dispersive effects of the channel. The slot duration should be small so that the channel variations within the slot are small.
- The frame duration is larger than the channel's time coherent duration to guarantee independence between frames.
- Selective diversity can be the criteria for allocating the slot to combat fading effect. The channel level crossing rate, which is the rate at which the transmitted signal envelope crosses a specified level, and duration of fades, which is the average duration of time during which signal envelope remains below a certain level, can be considered to allocate the slot with the best quality.
- Our scheme provides a jamming resiliency for cognitive networks with arbitrary number of accessible channels. There is no assumption on the minimum-required number of channels as is the case for most of the other anti-jamming schemes. However, for multi-channel system, users can access more than a channel simultaneously to speed up data transmission.
- Cognitive users vacate a channel only if a primary user is detected. Hence, the switching overhead in our technique is less than that for frequency hopping anti-jamming schemes. The jamming resiliency can be improved even more by making switching between channel follow a secret pattern derived from the same key pre-shared between the transmitter and receiver.
- The primary users' activity is considered in the design of slot duration so that the average transmission delay and switching probability are as desired.
- The proposed system has a great flexibility to be accessed by multiple users. Different slots can be assigned to different users.
- Our technique is out performing the frequency hopping based schemes in different metrics, including switching, service, and bit error probability.

II. System Model

A. Channel Model

Cognitive users have access to N channels licensed to some primary users. The occupancy of each channel is modeled as a two-state Markov chain. Cognitive user opportunistically utilizes the spectrum. The average channel idle and busy interval (denoted by $\overline{T}_{idle}$ and $\overline{T}_{busy}$ respectively) are independent and exponentially distributed with parameters u and v respectively. All the channels are assumed to be independent of each other and identical. Channels are both frequency and time selective. The time selectivity is caused by the relative motion between the two communicating entities. We consider the mobile-to-mobile channel model described in [3].

The model of primary users applies to users in cellular networks. It is popular to model arrival of calls as a Poisson process (i.e., exponentially distributed interarrival times), and the probability distributions of call durations as exponential [15]. Successive interarrival times and call durations are independent of each other in this model.

B. Attacker Model

- A jammer is assumed to have limited resources. It has limited power, denoted by J, within each time frame duration, denoted by T_f.
- The attacker should not jam primary users , as they are the licensed users since that might cause a penalty on the attacker.
- The jammer has a similar capability with legitimate cognitive users. Jammer senses to and switches between channels.
- The jammer chooses to jam the entire frame duration (i.e., continuous time jamming), or a few slots within a frame (i.e., partial-time jamming).

III. Proposed Scheme

In the proposed pseudorandom time hopping communication system, the available channel capacity is subdivided into a number of time slots n. The allocation is done by dividing the time axis into frames. Each frame is divided into n slots of one bit long. A user's transmitted signal occupies one of the available slots. The selection of the time slot is made pseudorandomly according to a private key pre-shared between the transmitter and receiver.

A block diagram of the transmitter and receiver system is shown in Fig. 1. In any signaling interval, cognitive user senses to the channels to identify the spectrum opportunities. According to a private key, user selects one of the unoccupied channels. Then, the slot to be occupied by the transmitted signal is determined according to the same key. For security reasons, different seeds can be used to generate different patterns over

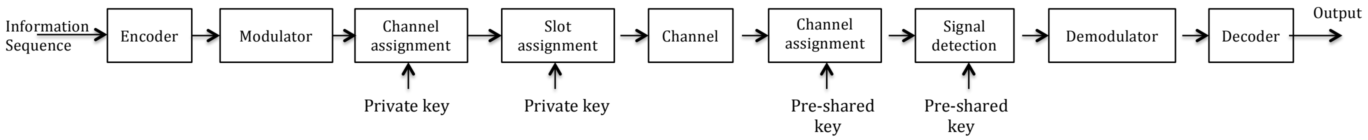

Fig. 1. Pseudorandom time hopping system block diagram

time and frequency. The transmitter pre-shares the key and seeds with the receiver, which in turn removes the pseudorandomness introduced to the transmitted signal. The modulation employed is the orthogonal frequency division multiplexing (OFDM) with N_c subcarriers where each subcarrier employs binary phase shift keying (BPSK) modulation.

We further analyze this scheme in the following section.

IV. Scheme Analysis

In this section we analyze a number of performance measures. We analyze the jamming probability and investigate its dependence on primary users' behavior. We also derive the expression of the switching and bit error probability in the presence of jamming attack.

A. Jamming Probability

The dynamical spectrum availability makes cognitive users more vulnerable to jamming. It is important to understand the nature of jamming probability and its dependence on primary users' behavior. The jamming probability has its consequence on the delay performance, and error probability and hence on the network design.

Jamming probability is the probability that the jammer hits the channel and the slot assigned to the legitimate cognitive user. At least one channel needs to be idle for the jammer to be able to jam cognitive users communication. The jammer jams m slots within a frame ($0 \leq m \leq n$). The jamming probability, denoted by P_j, is expressed as

$$P_j = \sum_{i=1}^{N} \binom{N}{i} \frac{m}{in} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} \tag{1}$$

The graph of this equation for different primary users' behavior in case of continuous time jamming (i.e., $m = n$) is shown in Fig. 2. It is observed that P_j changes drastically as primary users activity changes. The jammer is gaining from the volatile availability of spectrum. For high levels of primary users activity (i.e., the ratio between u and v which means that $\overline{T}_{busy}$/ $\overline{T}_{idle}$ is high), the average number of unoccupied channels can be much less than the total number of channels, giving the jammer a higher chance to disrupt the communication of the legitimate users. Another observation we can make is that P_j can be low when there are few channels and u/v is relatively high. The reason is that the resources are lacking for both the legitimate user and the attacker, i.e., the jammer is not able to jam because of lack of access opportunities. Low P_j might seem appealing, but the lack of access opportunities leads to higher transmission delay.

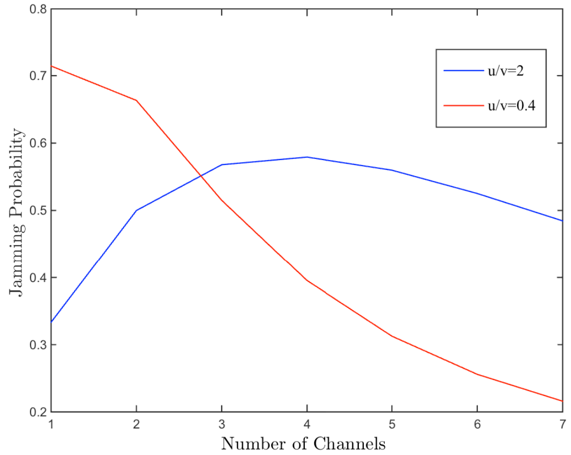

Fig. 2. Jamming probability vs number of channels

B. Switching Probability

In the time hopping system no switching is performed due to the presence of a jammer. In other words, if the jammer gets to access the same channel the legitimate user uses, the user is not required to switch to another channel. The probability of performing switching at any frame is written as

$$P_{sw} = \frac{\lambda}{\mu} \sum_{i=1}^{N-1} \binom{N-1}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} \tag{2}$$

λ is the probability that the legitimate user has information to send within a frame duration. μ is the service probability, which is the probability that there is at least one primary user channel idle for at least one time slot. μ can be expressed as $\sum_{i=1}^{N} \binom{N}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} e^{-uT_s}$.

In Fig. 3, we plot the switching probability for our system along with the corresponding probability in frequency hopping systems where legitimate users are required to vacate a channel whenever it is jammed. [12], [10] and some other existing works assume that successful channel jamming leads to switching. In Fig. 3, we set $u = 2$, $v = 1$, and slot duration $T_s = 100$ msec. It is observed that switching probability for the time hopping system is relatively low. Because of high jamming probability, the switching probability of frequency hopping system is much

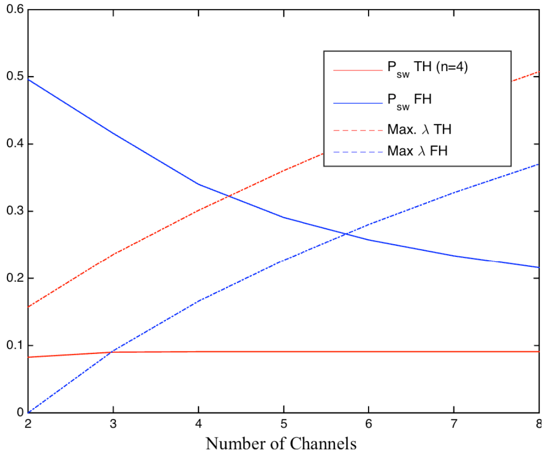

Fig. 3. Switching probability vs number of channels

higher than that for the time hopping, especially with few channels. In the same figure, we plot the service probability μ for both time and frequency systems. In case the data queues up at the transmitter (which is usually the case since the access is opportunistic), the maximum probability of having some data sent within a frame (λ) should not exceed the service probability (μ) for the queue to be stable. From Fig. 3, we conclude that in the frequency hopping system, the switching is performed in a higher probability with a lower service probability. In other words, the amount of data that can be served in the frequency hopping system is less than that for the time hopping system. This is a key thing to observe as one might think that we are sacrificing the throughput for the anti-jamming resilience in the time hopping system. However, our findings show that this is not true.

C. Error Probability

In this subsection we evaluate the probability of error as a performance metric. We investigate the probability of error for the additive white Gaussian noise (AWGN) channel and double fading channel. The jamming signal is modeled as a Gaussian random process with zero mean. Similar model is commonly considered in the literature (e.g., [12], [13], and [14]).

1) Error Probability in AWGN Channel: The jammer jams ρ_J fraction of the total frame time, ρ_J equals m/n. If the jamming power per frame is J, then the received jmmaing-signal variance per slot is $\frac{J}{\rho_J}$. Assuming that the jamming power dominates the noise, the probability of error is given by

$$P_e = \sum_{i=1}^{N} \binom{N}{i} \frac{m}{in} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} Q\Big(\sqrt{\frac{2mE_s}{nP_j}}\Big) \quad (3)$$

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt$ and E_s is the symbol energy.

The jammer can select m that causes the worst legitimate users performance. To be able to do so, jammer needs to estimate the legitimate user bit energy. In Fig. 4, for a different values of E_s/J we plot the probability of error versus the fraction of jammed slots within a frame. As expected, as the legitimate user power to the attacker power ratio increases, the attacker needs to focus its power over less number of slots to be able to successfully jam. Otherwise, the attacker wastes its power without degrading the performance of legitimate user significantly.

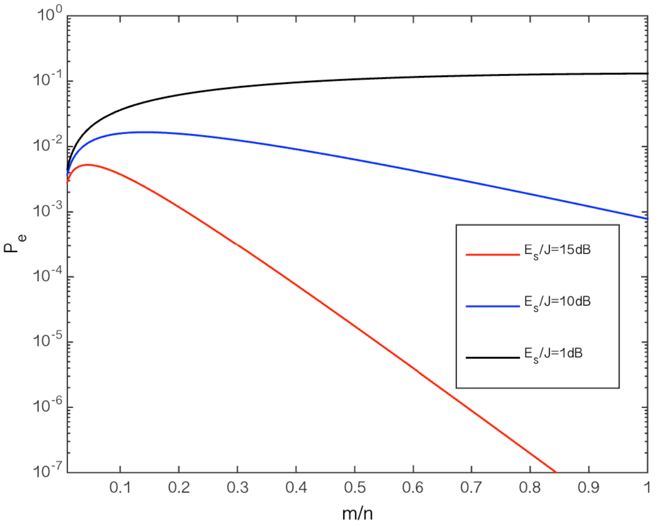

Fig. 4. Error probability vs ratio of the jammed slots within a frame

2) Error Probability in Double Fading Channel: Within each OFDM subcarrier the channel is assumed to be non-selective Rayleigh fading with zero mean Gaussian channel gain α. The cross correlation between l^{th} subcarrier channel gain at time $t+\tau$ ($\alpha_l(t+\tau)$) and the and k^{th} subcarrier channel gain at time t ($\alpha_k(t)$) $R_{\alpha_l \alpha_k}(\tau)$ can be factorized into two factors $R_t(\tau)$ and $R_f(\tau)$. While $R_t(\tau)$ represents the temporal correlation of the channel gain, $R_f(\tau)$ represents the correlation across subcarriers. We consider the mobile-to-mobile model described in [3] to characterize our channel. $R_t(\tau)$ in this model is expressed as $2J_0(2\pi f_{m1}\tau)J_0(2\pi f_{m2}\tau)$. Where $J_0(.)$ is the zero order Bessel function. f_{m1}, and f_{m2} are the maximum Doppler frequency due to motion of the transmitter and receiver respectively. f_{m2} can be represented in terms of f_{m1} as af_{m1}, where $0 \leq a \leq 1$. a can also be viewed as the ratio between the transmitter speed and receiver speed. The power spectral density corresponding to $R_t(\tau)$ is given in [4]. The multipath power intensity profile which describes the frequency selectivity of the channels is modeled as an exponential. Due to the mobility of users, channels experience frequency dispersion, leading to intercarrier interference I, where I at the ith subcarrier is expressed as

$$I = \frac{4E_sT_s^2}{\pi^2 f_{m1}\sqrt{a}} \sum_{\substack{k=0\\k\neq i}}^{K-1} \frac{1}{(k-i)^2} \Bigg[\int_0^{(1-a)f_{m1}} f^2 \frac{1}{x} K(\frac{1}{x}) df + \int_{(1-a)f_{m1}}^{(1+a)f_{m1}} f^2 K(x) df \Bigg] \quad (4)$$

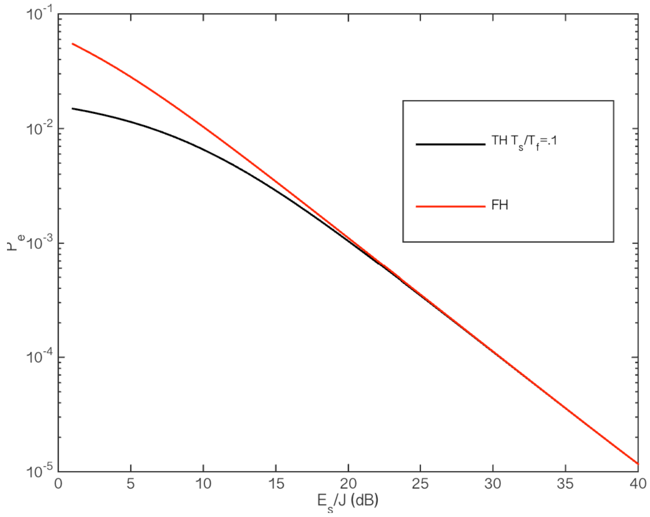

Fig. 5. Error probability vs legitimate user power to the attacker power ratio

where $x \triangleq \frac{1+a}{2\sqrt{a}}\sqrt{1-(\frac{f}{(1+a)f_{m1}})^2}$ and $K(x) \triangleq \int_0^{\pi/2}\frac{dt}{\sqrt{1-x^2 sin^2 t}}$ is the complete elliptical integral of the first kind.

The error probability is defined only if there exists an idle channel. The lack of idle channel causes a service delay. The probability that there is no service within a frame is given by $(1-\mu)$. The error probability conditioned on the availability of at least one channel for a fixed channel gain is given by

$$P_{e|\alpha} = \sum_{i=1}^{N}\binom{N}{i}\frac{1}{(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}} \left[\frac{m}{in}Q(\sqrt{\frac{2E_s|\alpha|^2}{nJ/m+I}}) + (1-\frac{m}{in})Q(\sqrt{\frac{2E_s|\alpha|^2}{I}})\right] \quad (5)$$

The unconditional error probability is given by

$$P_e = \frac{1}{2}\sum_{i=1}^{N}\binom{N}{i}\frac{1}{(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}} \left[\frac{m}{in}\left(1-\sqrt{\frac{\gamma_1}{1+\gamma_1}}\right) + (1-\frac{m}{in})\left(1-\sqrt{\frac{\gamma_2}{1+\gamma_2}}\right)\right] \quad (6)$$

where $\gamma_1 = \frac{E_s E[|\alpha|^2]}{nJ/m+I}$, and $\gamma_2 = \frac{E_s E[|\alpha|^2]}{I}$. $E[|\alpha|^2]$ which denotes the average value of $|\alpha|^2$ which is normalized to unity.

For $N = 4$, $N_c = 256$ and $u/v = 1$, in Fig. 5 and 6, we plot the error probability for the subcarrier in the middle of a channel ($i = 128$) for the case $a = 0.1$, $T_s f_{m1} = 0.001$ and $a = 0.5$, $T_s f_{m1} = 0.05$ respectively. We can observe from these figures that when the product of the maximum Doppler frequency and slot duration ($T_s f_{m1}$) along with the relative ratio between the transmitter and receiver speed (a) increase, the probability of error becomes irreducible after a certain value of E_s/J. This is an important observation in terms of energy consumption and error performance. For a given transmitter and receiver speed, if a higher quality of service is desired, an adjustment in the slot duration needs to be made since an increase in the transmission power might not improve the performance. Also we can observe that for low legitimate-to-attacker power ratio, the pseudorandom time-hopping system outperforms the frequency-hopping system. In other words, when the jamming power is relatively high, our system achieves, with less power, the same level of performance that the frequency hopping systems achieve.

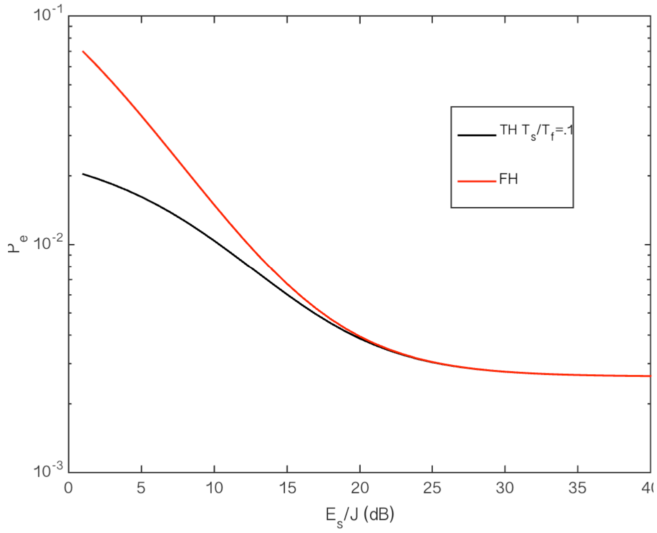

Fig. 6. Error probability vs legitimate user power to the attacker power ratio

V. Conclusions

In this paper, we have proposed a pseudorandom time hopping technique to countermeasure jamming. While taking into account jamming attacks, mobility of users, and spectrum availability dynamics, we obtained the analytical solutions of jamming, switching, and error probabilities. We showed that our anti-jamming method outperforms the frequency hopping based anti-jamming scheme in terms of jamming probability, switching, service and error probability. Our technique is energy efficient, spectrum efficient, and provides jamming resilience with little communication overhead, which makes it a strong candidate for device-to-device links in 5G networks.

References

[1] N. Adem and B. Hamdaoui, "Delay Performance Modeling and Anal. in Clustered Cognitive Radio Networks," *in Proc. IEEE Globecom*, Austin, TX, 2014, pp. 193-198.

[2] E. Hossain, IEEE Globecom Tutorial, Topic: "Evolution Toward 5G Cellular Networks: A Radio Resource and Interference Management Perspective." Austin, TX, Dec. 8, 2014.

[3] A. S. Akki, and F. Haber, "A Statistical Model of Mobile-to-Mobile Land Communication Channel," *IEEE Trans. Veh. Technol.*, vol. 35, no. 1, pp. 2–7, Feb. 1986.

[4] A. Pertrolino, J. Gomes, and G. Tavares, "A Mobile-to-Mobile Fading Channel Simulator Based on an Orthogonal Expansion,"*IEEE 67th Veh. Technol. Conf.*, Marina Bay, Singapore, May 2008., pp. 366-370.

[5] H. Yanıkömeroğlu , IEEE Globecom Tutorial, Topic: "Emerging Concepts and Technologies towards 5G Wireless Networks." Austin, TX, Dec. 12, 2014.

[6] Huawei, “5G: A technology vision,” 2013. [Online]. Available: www.huawei.com/5gwhitepaper. [Accessed: Jan. 10, 2015].

[7] F. S. P. T. Force, “ Report of the spectrum efficiency working group, ” Nov. 2002.

[8] D. Datla, A. M. Wyglinski, and G. J. Minden, “A spectrum surveying framework for dynamic spectrum access networks,” *IEEE Trans. Veh. Technol.*, vol. 58, no. 8, pp. 4158–4168, Oct. 2009.

[9] A.G. Fragkiadakis; E.Z. Tragos, I.G. Askoxylakis, “A survey on security threats and detection techniques in cognitive radio networks, ” IEEE Commun. Surv. Tutor. 2013, 15, 428–445.

[10] H. Su, Q. Wang, K. Ren and K. Xing,“ Jamming-resilient dynamic spectrum access for cognitive radio networks,” *in Proc. IEEE ICC*, 2011, pp. 1–5.

[11] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, “Jamming-resistant key establishment using uncoordinated frequency hopping,” *in Proc. IEEE symp. on security and privacy*, 2008.

[12] Li, Xiaohua ; Cadeau, W., “Anti-jamming performance of cognitive radio networks,”, *in Proc. IEEE CISS*, 2011.

[13] H. Zhang and Y. Li., “Anti-jamming property of clustered OFDM for dispersive channels, ” in Proc. MILCOM., Oct. 2003, pp:336-340.

[14] J. Proakis and M. Salehi, *Digital Communications,* 5th Edition. MCGraw-Hill, 2008.

[15] A. Al Daoud, M. Alanyali, and D. Starobinski, “Secondary pricing of spectrum in cellular CDMA networks,”*in Proc. 2nd IEEE Int. Symp. New Frontiers DySPAN* , Ireland, 2007, pp. 535–542.