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 [1]. The dynamical spectrum availability makes cognitive users switch between channels. Switching 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. 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.**

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 [1]. 5G will support connections for at least 100 billion devices [2]. 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 [1]. 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 user behaviors. The process of identifying and exploiting spectrum access opportunities causes performance degradation [3]. 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 [4]. 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. 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. [5] and [6]). We see anti-jamming methods based on frequency hopping to be inefficient 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 inefficient. 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 lead 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, thereby increasing the chances of a jammer to hit cognitive user channels.
- The uncoordinated frequency hopping, where no agreement is made between the transmitter and receiver on the hopping pattern, drastically degrades communication efficiency. Consequently, uncoordinated frequency hopping based antijamming schemes are inefficient 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 mobile cognitive users. The occupancy of primary user channels is modeled as a Markov chain. Channels are assumed to be both time and frequency dispersive. 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 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 performance of our scheme with the frequency hopping scheme. To the best of our knowledge, the impact of jamming on the switching process of mobile cognitive users has not been addressed in the literature.

Below we summarize the advantages of the proposed technique.

- The system is designed to mitigate the channel time-varying effects which is 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 user activities are 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 channel idle and busy interval 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 dispersive. The frequency dispersion is caused by the relative motion between the two communicating entities. We consider the mobile-to-mobile fading-channel model described in [7].

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 [8]. 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.
- Attacker are not disrupting the primary users' communications, as they are the licensed users.
- Jammers have similar transmission capabilities with legitimate cognitive users. Jammer senses to and switches between channels.
- Jammers choose 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 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, the 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 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_{sc} 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 user behaviors. We also derive the expression

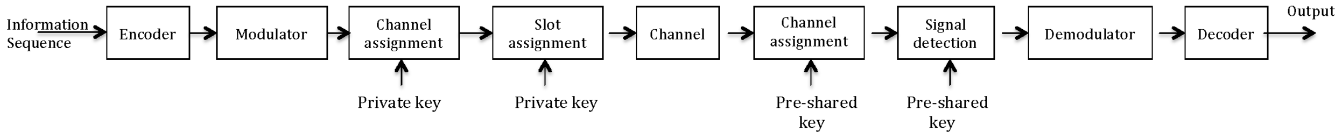

Fig. 1. Pseudorandom time hopping system block diagram

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 user behaviors. 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 a jammer hits both the channel and the slot assigned to the legitimate cognitive user. At least one channel needs to be idle for a jammer to be able to jam cognitive users communication. A channel idle time and busy time are exponentially distributed with parameters u and v respectively. The average idle and busy intervals are denoted by $\overline{T}_{idle}$ and $\overline{T}_{busy}$ respectively. The probability that there are exactly i idle channels out of the N accessible channels is given by $\frac{1}{(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}}$. A jammer jams m slots within a frame $(0 \leq m \leq n)$. The jamming probability, denoted by P_j, is expressed as

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

The graph of this equation for different primary user behaviors 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 user activities change. The jammer is gaining from the volatile availability of spectrum. For high levels of primary user activities (i.e., the ratio between u and v is high 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, which in turn gives the jammer a higher chance to disrupt the communication of 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.

B. Switching Probability

In the time hopping system no switching is performed due to the presence of a jammer. In other words, if a jammer gets to access the same channel that the legitimate user uses, the legitimate user is not required to switch to another channel.

Channels availability and user's offered load β, which is defined as the ratio between the arrival probability and service probability, determine if a channel handoff needs to be performed within a particular time frame. For stability conditions β is assumed to be less than unity [9]. The arrival probability λ is the probability that a user generates a data packet within a frame duration. The service probability μ is the probability that a cognitive user gets a channel access opportunity for at least slot duration T_s. The service probability is expressed as $(1 - \frac{1}{(1+v/u)^N})e^{-uT_s}$ [3].

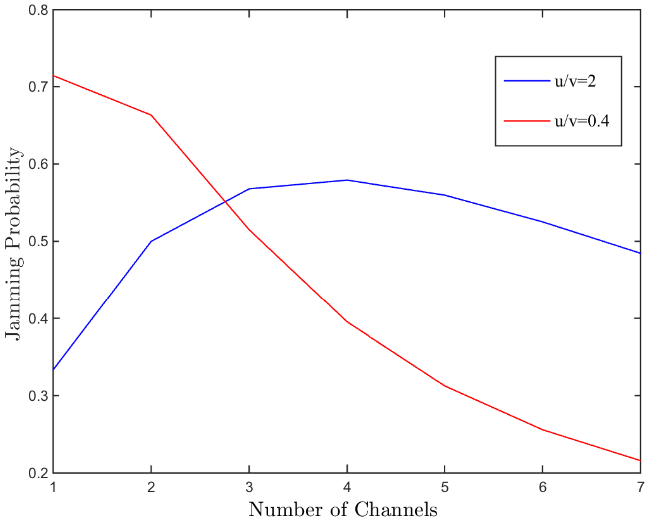

Fig. 2. Jamming probability vs number of primary user channels

The probability that a user switches between channels at any frame is the probability that the last assigned channel is busy during that frame while there is another channel idle and offered load is greater than zero. The switching probability is written as

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

In Fig. 3, we plot the switching probability for the time hopping system along with the corresponding probability in the frequency hopping system where legitimate users are required to vacate a channel whenever it is jammed. [5], [6] and some other existing works assume that successful channel jamming leads to switching. 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

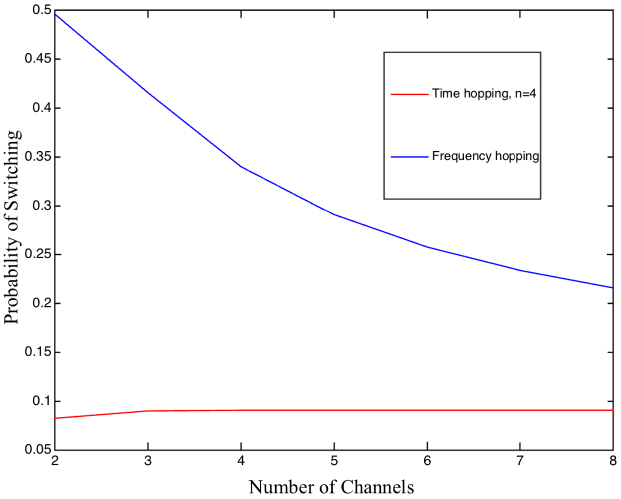

Fig. 3. Switching probability vs number of primary user channels

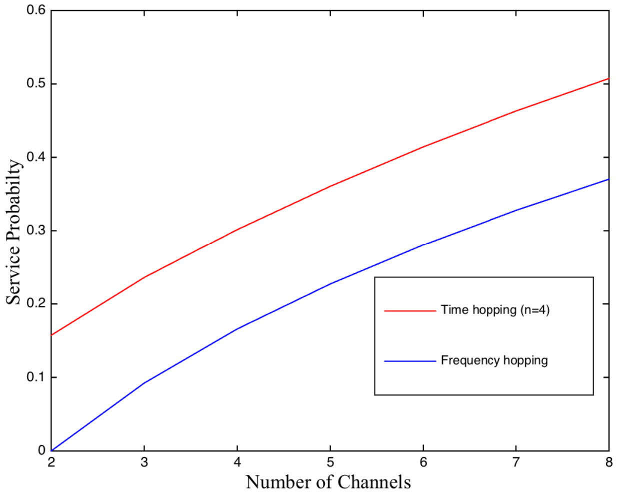

Fig. 4. Service probability vs number of primary user channels

hopping system is much higher than that for the time hopping, especially with few channels.

For the same settings considered in Fig. 3, we plot in Fig 4 the time and frequency hopping systems service probability. Fig. 3 and Fig. 4, show that in the frequency hopping system the switching probability is higher while it offers 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 in the time hopping system we are sacrificing the throughput for the anti-jamming resilience. However, our findings show that this is not true.

C. Error Probability

We investigate the probability of error for the additive white Gaussian noise (AWGN) channels and mobile-to-mobile fading channels. The jamming signal is modeled as a Gaussian random process with zero mean. Similar model is commonly considered in the literature (e.g., [6], [10], and [11]).

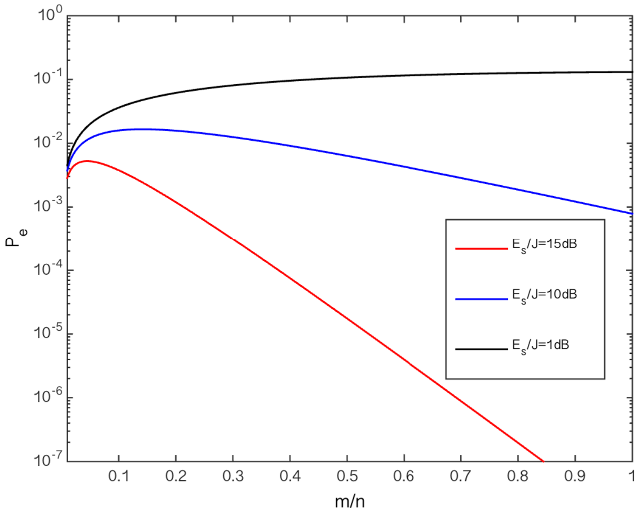

Fig. 5. Error probability vs jamming fraction

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 jamming-signal variance per slot is nJ/m. Assuming that the jamming power dominates the noise, the probability of error is given by

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

where $Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-t^2/2} dt$ and E_s is the average symbol energy. Equation (3) follows from Equation (1) and the BPSK error probability [11].

A 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. 5, for several values of E_s/J we plot the probability of error versus the jamming fraction m/n. As expected, as the legitimate-to-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.

2) Error Probability in Mobile-to-Mobile Fading Channel: Within each OFDM subcarrier the channel is assumed to be non-selective Rayleigh fading with zero mean Gaussian channel gain. 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 $(\alpha_k(t))$ 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 [7] 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 $0 \leq a \leq 1$. The power spectral density corresponding to $R_t(\tau)$ is given in [12]. The multipath power intensity profile which describes the frequency selectivity of the channels is modeled as an exponential.

Due to the mobility of users, all subchannels experience frequency dispersion, leading to intercarrier interference. The OFDM baseband signal transmitted over the channel is expressed as $s(t) = \frac{1}{\sqrt{T_s}}\sum_{i=0}^{N_{sc}-1} s_i e^{j2\pi i/T_s t}$, where $0 \leq t \leq T_s$, N_{sc} is the number of subcarriers. s_i, $i \in \{1,..,N_{sc}\}$, represents the BPSK symbol at the i^{th} subcarrier. The subcarrier symbols are assumed to be independent and identically distributed, each with zero mean and average energy E_s. The received baseband signal is expressed as $s_r(t) = \frac{1}{\sqrt{T_s}}\sum_{i=0}^{N_{sc}-1} \alpha_i(t)s_i e^{j2\pi i/T_s t} + j(t)$, where $j(t)$ is the jammer signal. The l^{th} subchannel-gain variations over time $\alpha_l(t)$ can be expressed as $\alpha_l(T_s/2) + \acute{\alpha_l}(t - T_s/2)$, $0 \leq t \leq T_s$, where $\acute{\alpha_l}$ is the l^{th} subchannel-gain first derivative [13]. To detect the l^{th} symbol, the received signal is passed through a correlator tuned to the l^{th} frequency [11]. Due to the mobility of users, all subchannels interfere with the l^{th} subcarrier. The average power of intercarrier interference at the l^{th} subchannel I_l is expressed as

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

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

The probability of error, corresponding to detecting the symbol at the l^{th} subcarrier, is defined only if there exists at least an idle primary user channel. The lack of a channel access opportunity causes a service delay [3]. The error probability conditioned on fixed subchannel gain is given by

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

Equation (5) can be derived from Equation (1) and (3). Averaging over the distribution of the subchannel gain, the unconditional error probability can be expressed as

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

where $\gamma_1 = \frac{2E_sE[|\alpha_l|^2]}{nJ/m+I_l}$, and $\gamma_2 = \frac{2E_sE[|\alpha_l|^2]}{I_l}$. $E[|\alpha_l|^2]$ which is normalized to unity denotes the average value of $|\alpha_l|^2$. Note that for a deterministic number c, the random variable $c|\alpha_l|^2$ has a chi-square probability distribution given by $c^{-1}exp(-c^{-1}|\alpha_l|^2)$.

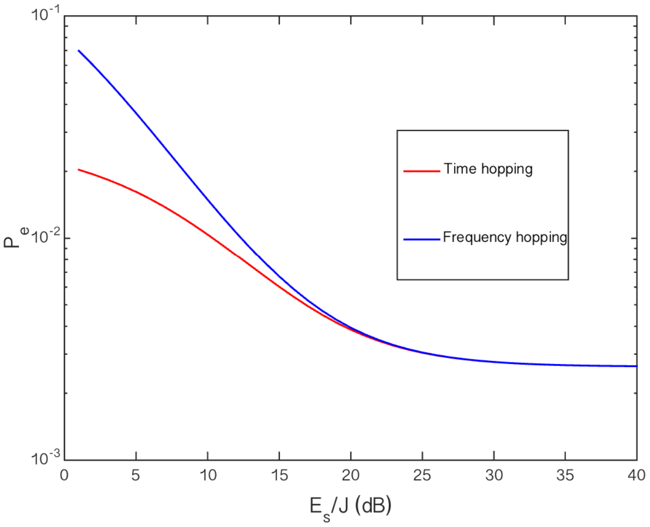

Fig. 6. Error probability vs legitimate-to-attacker power ratio

For $N = 4$, $N_{sc} = 256$, $m/n = 0.1$ and $u/v = 1$, in Fig. 6, we plot the error probability for the subcarrier in the middle of a channel (i.e., $l = 128$) for $a = 0.5$, $T_sf_{m1} = 0.05$. We can observe from the figure that due to the mobility of the users, the probability of error reaches a limit and any increase in E_s/J no longer improves the performance. This limit, which can be derived by taking the limit of Equation (6) as E_s/J goes to infinity, is referred to as the irreducible error probability [14]. 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. As the legitimate-to-attacker power ratio increases, the intercarrier interference domains the jamming effect, hence the time and frequency hopping system perform similarly.

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 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] E. Hossain, “Evolution toward 5G cellular networks: A radio resource and interference management perspective,” *IEEE Globecom Tutorial*, Austin, TX, Dec. 8, 2014.

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

[3] N. Adem and B. Hamdaoui, “Delay performance modeling and analysis in clustered cognitive radio networks,” in *Global Communications Conference (GLOBECOM), 2014 IEEE*, Dec 2014, pp. 193–198.

[4] M. Strasser, C. Popper, S. Capkun, and M. Cagalj, “Jamming-resistant key establishment using uncoordinated frequency hopping,” in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, May 2008, pp. 64–78.

[5] H. Su, Q. Wang, K. Ren, and K. Xing, “Jamming-resilient dynamic spectrum access for cognitive radio networks,” in *Communications (ICC), 2011 IEEE International Conference on*, June 2011, pp. 1–5.

[6] X. Li and W. Cadeau, “Anti-jamming performance of cognitive radio networks,” in *Information Sciences and Systems (CISS), 2011 45th Annual Conference on*, March 2011, pp. 1–6.

[7] A. Akki and F. Haber, “A statistical model of mobile-to-mobile land communication channel,” *Vehicular Technology, IEEE Transactions on*, vol. 35, no. 1, pp. 2–7, Feb 1986.

[8] A. Al Daoud, M. Alanyali, and D. Starobinski, “Secondary pricing of spectrum in cellular cdma networks,” in *New Frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on*, April 2007, pp. 535–542.

[9] H. Takagi, “Queueing analysis. discrete-time systems, vol. 3,” 1993.

[10] H. Zhang and Y. Li, “Anti-jamming property of clustered ofdm for dispersive channels,” in *Military Communications Conference, 2003. MILCOM ’03. 2003 IEEE*, vol. 1, Oct 2003, pp. 336–340 Vol.1.

[11] J. Proakis and M. Salehi, *Digital Communications*, ser. McGraw-Hill International Edition. McGraw-Hill, 2008.

[12] A. Petrolino, J. Gomes, and G. Tavares, “A mobile-to-mobile fading channel simulator based on an orthogonal expansion,” in *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, May 2008, pp. 366–370.

[13] P. Bello and B. Nelin, “The effect of frequency selective fading on the binary error probabilities of incoherent and differentially coherent matched filter receivers,” *Communications Systems, IEEE Transactions on*, vol. 11, no. 2, pp. 170–186, June 1963.

[14] P. Bello, “Correction to ”the influence of fading spectrum on the binary error probabilities of incoherent and differentially coherent matched filter receivers”,” *Communications Systems, IEEE Transactions on*, vol. 11, no. 2, pp. 169–169, June 1963.