Mitigating Jamming Attacks in Mobile Cognitive Networks Through Time Hopping

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@oregonstate.edu

Abstract

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. The dynamical spectrum availability makes cognitive users switch between channels. Switching leads to energy consumption, latency, and communication overhead in general. The performance degrades even more when the network is under jamming attack. This type of attack is one of the most detrimental attacks. Addressing jamming while maintaining a desired quality of service is a challenge. While existing anti-jamming mechanisims assume stationary users, in this paper we propose and evaluate countermeasures for mobile cognitive users. We propose two time-based techniques which, unlike other existing frequency-based techniques, do not assume accessibility to multiple channels and hence do not rely on switching to countermeasure jamming. We achieve analytical solutions of jamming, switching and error probabilities. Based on our findings, the proposed techniques out perform other existing frequency-based techniques.

I. Introduction

5G wireless networks will support 1,000-fold gains in capacity. 5G networks will also support connections for at least 100 billion devices [1]. Deployment of networks with such a massive capacity and connectivity poses many challenges, among which radio resource management is the most significant. The challenge is even more acute when security concerns are taken into account. The dynamic spectrum access provided through cognitive radios is considered as one of the enabling technologies to deploy 5G networks [2]. In addition to primary users, which have priority to access a number of communication channels, secondary users, which implement cognitive radios, may access the channels opportunistically. That in turn improves spectrum utilization which is required for achieving high capacity networks. Cognitive users can be self-managed as they are capable of observing, learning, and adapting to environment changes. The self-management is a desirable capability when it comes to deploying networks with large number of devices. However, the lack of access priority makes communication between cognitive users more vulnerable to security attacks. Mechanisms that handle security threats and take into account the volatility of resources need to be designed.

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 utilize their transmission capabilities over the limited resources accessible by cognitive users and completely disrupt the communications between them. As mobility of users makes communication channels both frequency and time dispersive, the challenge of maintaining a desired quality of service is even more acute when legitimate users are mobile. In this paper, we propose time-based anti-jamming schemes for mobile cognitive users.

B. *Related Work*

There exist quite a few recent works focusing on security attacks in cognitive networks. The primary user emulation attacks have been studied extensively, see for example [5]–[7]. A deal of effort has also been devoted to spectrum sensing security, see, e.g. [8]–[10]. Jamming attacks have also attracted research attention as they are more detrimental and they significantly degrade spectrum utilization. Most of existing jamming countermeasures assume accessibility for multiple channels and hence consider surfing between them as a way to retreat from jammers. In [11], the authors assumed that cognitive users hop among multiple channels and randomly allocate power to defend against jammers. They modeled interactions between jammers and secondary users as Colonel Blotto game. They derived hopping patterns based on Markov decisions process or some learning techniques. Similarly, the authors in [12] proposed frequency hopping based countermeasure and modeled the anti-jamming scheme as a game. Unlike [11], in [12] hopping patterns are derived based on prospect theory. The work in [13] is similar to [11]. However, while transmission power is allocated randomly in [11], the authors in [13] deployed their proposed learning algorithms to allocate power optimally. In [14], the authors assumed that jammers and legitimate users compete sequentially. They modeled their interaction as a game using Stackelberg model. In their scheme, secondary users allocate power based on estimated jamming power. [15] modeled spectrum availability and access as partially observed Markov process. The authors in [15] assumed that users learn to retreat from jammers through, similar to the other works, spectral surfing. They derived their retreating strategy based on multiple-armed bandit problem with the assumption that secondary users have same knowledge about spectrum availability and jammers. In [16], the authors also considered spectral surfing as a jamming countermeasure with the assumption that secondary users use pre-shared secret keys for channels selection.

C. Summary of Contributions

Most jamming countermeasures exist in literature are based on frequency hopping. They mainly differ in the strategies used to derive hopping patterns. Due to volatile access opportunities, frequency-based countermeasures are not the best choices in cognitive networks. Since secondary users lack spectrum-access priority, whenever a primary user claims the right to use a channel, they have to vacate it and switch to some other idle one. Mitigating jamming through spectral surfing leads to a higher switching rate. Hence, more energy consumption, delay, and communication overhead in general. In addition, high primary users activity reduces the number of channels accessible by secondary users. Hence, frequency hopping techniques become less effective as primary users become more and more active. More importantly, these techniques work only if multiple channels are accessible. None of them addresses jamming attacks when there is only one channel accessible by legitimate users. To avoid these limitations, we propose to mitigate jamming through time-based techniques. In the following we summarize the properties of our proposed countermeasures and point out their differences from existing schemes.

- We propose two time-based techniques that work with arbitrary number of channels. They can be as few as one. Existing jamming countermeasures, however, assume accessibility to multiple channels.
- Our techniques do not rely on switching and hence avoid any associated overhead.

- While existing schemes assume stationary users, we assume mobile users. One of our proposed schemes is designed to mitigate jamming and mobility effects as well (see section III-B for details).
- We obtain closed-form formulas to a number of performance metrics including jamming probability, switching probability, and error probability.
- Our findings show our proposed techniques outperform other existing frequency-based techniques.

II. Preliminaries and Models

Notations. Operator $||$ denotes the concatenation. $\lceil x \rceil$ denotes the ceiling of x. $\lfloor x \rfloor$ denotes the floor of x.

Definitions.

1) key derivation function (KDF) is a function with which an input key and other input data are used to generate keying material that can be employed by cryptographic algorithms.
2) Pseudorandom number generators (PRNG) is a deterministic algorithm used to generate a sequence of bits which looks like random sequence, given as input a short random sequence (the input seed).

Channels Model. Cognitive users have access to N channels licensed to some primary users. Cognitive users opportunistically utilize the spectrum. The occupancy of each channel is modeled as a two-state Markov chain. The average channel idle and busy interval are independent and exponentially distributed with parameters u and v respectively. All 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 channel model described in [17]. 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 [18]. Successive interarrival times and call durations are independent of each other in this model.

Secondary Users Model. We assume that there are n connections within the cognitive network at most. Each connection is established between a pair of secondary users which access spectrum opportunistically. Each user accesses no more than one channel at a time. Users operate in a

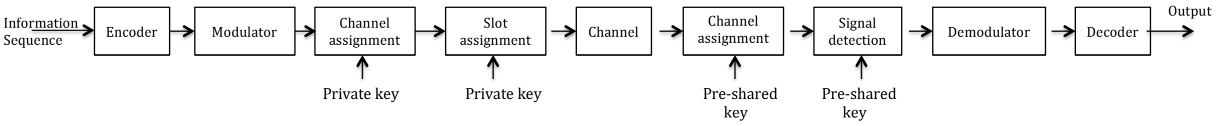

Fig. 1. Pseudorandom time hopping system block diagram

time-slotted mode. They are required to sense the spectrum periodically to avoid interfering with primary users. They also need to vacate a channel if it is detected to be occupied. More details about how users get assigned to spectrum each transmission period is given in section III.

Jamming Model. We assume that there is jammer in the cognitive network with transmission capabilities similar to secondary users. In other words, jammer is able to identify and exploit spectrum access opportunities. It intentionally disrupts the communication between secondary users. Jammer activities are required to be transparent to licensed users. This assumption is reasonable and widely-used, e.g. [16], [19], and many others consider a similar assumption. To ensure transparency, jammer, similar to legitimate users, is required to perform periodic channel sensing. In fact, we are not concerned about primary users security. We are only addressing jamming attacks in cognitive networks. Back to the model, jammer periodically sense the spectrum to identify the unoccupied channels and pick one of them randomly to launch a jamming attack. Jammer exploits its limited energy to degrade legitimate users performance either by performing partial-time or continuous-time jamming. It aims to make legitimate users switch between channels by making jammed channels unaccessible. However, our main goal is to make legitimate users avoid jamming without having them switch between channels.

III. Proposed Schemes and their Analysis

To mitigate jamming, we propose to spread a legitimate user data over time. More specifically, instead of transmitting legitimate user data continuously over time, a user transmits some data over some time, holds for some other random amount time, and then transmits again and so on. The idea is to make the transmission instants look random to jammer. In this way, we impose jammer to jam in a discontinuous way, otherwise, it wastes its limited power (more details about possible jammer interactions and their effects on performance are to discussed). This idea, which we refer to as *time hopping*, is simple yet outperform frequency hopping technique. It is also used to achieve multiple access. To apply time hopping we propose the two following schemes.

A. Private Key Based Time Hopping (PKTH)

In PKTH, we consider the capacity of a channel to be subdivided into n portions, where n is the maximum number of connections can be established between secondary users. A user is constrained to use only one portion for data transmission. The allocation is done by dividing the time axis into frames. Each frame is divided into n slots of fixed length (e.g., one bit or one packet long). According to a pairwise shared key, a user allocates one slot per a frame. A block diagram of time hopping transmitter and receiver system is shown in Fig. 1. In any signaling interval, time hopping pattern (slots to be occupied by the transmitted signal over time) and channel selections are determined as described in Algorithm 1. As we do not assume multiple channels accessibility, we only consider *time evasion* as a countermeasure in PKTH. However, in case there is more than a channel accessible by the cognitive network, users take the advantage of their pre-shared keys for spectrum access. Spectral surfing is performed to avoid interfering with primary users. To ensure security seeds used for time hopping pattern derivation are different from the ones used for spectrum access. The transmitter pre-shares the key and seeds with the receiver, which in turn removes the pseudorandomness introduced to allocate transmitted signal over time and frequency. We give a high level description of Algorithm 1 below, and discuss its complexity.

Initialization. A trusted third party, which is in our model the primary users network base station, distributes private keys among pairs of users. Keys are generated such that similarities between patterns derived from different pairs are minimal such that multiple access can be achieved [20]. Cellular network base station also assigns an identification number to each legitimate user.

Pseudorandom Numbers Generation. Using the private key along with seeds (generated by KDF using session, transmitter and receiver IDs) transmitter and receiver run PRNG to generate pseudorandom sequence of bits used for time hopping pattern derivation (denoted by $PRSeq_{TH}$) and sequence used for channel selection (denoted by $PRSeq_{CS}$).

Hopping Pattern Derivation. The generated pseudorandom sequences $PRSeq_{TH}$ and $PRSeq_{CS}$ are truncated into chunks of $\lceil \log_2 n \rceil$ and $\lceil \log_2 N \rceil$ bits long respectively. The modulo n and modulo N of the decimal numbers corresponding to resulted chunks are used to indicate the allocated slot and channel.

Algorithm 1 Time Hopping Pattern Derivation and Channel Selection Algorithm

```
    **Initialization**: Executed once after the network deployment.
 1: Cellular network base station assigns a private key to each pair of users.
 2: Users $\mathcal{X}$ and $\mathcal{Y}$ both determine the slot $g$ ($decision_{TH}$) and channel $k$ ( $decision_{CS}$) to be used for transmission. They set $a$ to be $\lceil \log_2 n \rceil$, $b$ to be $\lceil \log_2 N \rceil$, $C_{CS}$, $C_{TH}$,$A$ ,$B$ all to be one. $Seed_{CS}$ ($Seed_{TH}$) denotes seed used for channel selection (time hopping). $s$ denotes session ID. $l$ denotes the size of users $\mathcal{X}$ and $\mathcal{Y}$ private key $K$.
    **Pseudorandom Numbers Generation**: Executed by both $\mathcal{X}$ and $\mathcal{Y}$ each session.
 3: $Seed_{CS} \leftarrow KDF_K(ID_x \parallel ID_y \parallel s)$.
 4: $PRSeq_{CS} \leftarrow PRNG_K(Seed_{CS})$. Denote the binary string $PRSeq_{CS}$ by $\{x_i\}_{i=1}^{l}$.
 5: **if** $B = 0$ **then** $B \leftarrow 1$, $C_{CS} \leftarrow 1$, go to 12
 6: $Seed_{TH} \leftarrow KDF_K(ID_y \parallel s \parallel ID_x)$.
 7: $PRSeq_{TH} \leftarrow PRNG_K(Seed_{TH})$. Denote the $PRSeq_{TH}$ binary string by $\{y_i\}_{i=1}^{l}$.
 8: **if** $A = 0$ **then** $A \leftarrow 1$, $C_{TH} \leftarrow 1$, go to 20
    **Hopping Pattern Derivation**: Executed every time frame by both $\mathcal{X}$ and $\mathcal{Y}$.
 9: **if** the last assigned channel is idle **then** $decision_{CS} \leftarrow$ no switching.
10: **else**
11:     **if** $C_{CS} \leq \left\lfloor \frac{l}{b} \right\rfloor$ **then**
12:         $k \leftarrow (\sum_{j=C_{CS}}^{C_{CS}+b-1} x_j 2^j) \mod N$.
13:         $C_{CS} \leftarrow C_{CS} + 1$
14:         **if** $k^{th}$ channel is idle **then** $decision_{CS} \leftarrow$ switch to $k^{th}$ channel.
15:         **else**
16:             go to 11
17:     **else**
18:         $B \leftarrow 0$, update $s$, go to 3
19: **if** $C_{TH} \leq \left\lfloor \frac{l}{a} \right\rfloor$ **then**
20:     $g \leftarrow (\sum_{i=C_{TH}}^{C_{TH}+a-1} y_i 2^i) \mod n$. $decision_{TH} \leftarrow$ allocate $g^{th}$ slot.
21:     $C_{TH} \leftarrow C_{TH} + 1$
22: **else**
23:     $A \leftarrow 0$, update $s$, go to 6
```

Algorithm complexity: The number of accessible channels, the chance of their occupancy, the required level of security required by Algorithm 1 are all factors determine its computational complexity. The type of the employed key derivation function, KDF, and the length of the seed it generates play an important role in determining the running time of the algorithm. We assume that BLAKE hash [21] based key derivation function is applied and analyze the complexity accordingly. In BLAKE based key derivation functions, users hash some secret information (in our case a private key, their id's, and session id) using BLAKE hash function. BLAKE is one of hash functions in the final of National Institute of Standards and Technology (NIST) 2007-2012 Competition for developing cryptographic hash algorithms [22]. There are two main instances of BLAKE, BLAKE-256 and BLAKE-512. They respectively produce 256- and 512-bit digests and run with complexity $\mathcal{O}(256^{1.3})$ and $\mathcal{O}(512^{1.225})$ [21].

The complexity of the pseudorandom number generators, PRNG, algorithm is also affected by the output of the KDF (the input for the PRNG algorithm). The goal of the PRNG algorithm is to generate a number that has a pseudo-random distribution such that no efficient procedure can distinguish it from uniform distribution. The complexity of the PRNG algorithm depends on the type of procedure the generator is secure aganist. In case efficient procedures are associated with (probabilistic) polynomial time algorithm, the PRNG complexity is a polynomial time (in terms of its input, the seed) [23]. I.e., the PRNG runs in $\mathcal{O}(l_s^L)$ where l_s is the seed length, and L is an integer greater than one. Hence, the complexity of the KDF and PRNG in Algorithm 1 is $\mathcal{O}(l_s^L)$ where l_s equals either 256 or 512 depending on the used hash function. For any given session, executing lines 6-7 is enough for allocating time slot for $\lfloor l/a \rfloor$ time frames. Similarly, lines 3-4 results in allocating a channel for (at most) $\lfloor l/b \rfloor$ time frames. However, since with a probability p_{busy} a channel is occupied by a primary user, it takes $\lceil 1/p_{busy} \rceil$ operations as much, in average, to allocate a channel. The overall computational complexity of the algorithm, hence, is $\mathcal{O}(N_S N_T \left\lceil \frac{1/p_{busy}}{\lfloor l/b \rfloor} \right\rceil l_s^L)$, where N_S is the number of sessions, N_T is the number of time frame within each session assuming, without loss of generality, all sessions have the same number of frames.

To analyze the anti-jamming capabilities of the time hopping system, we assume users employ orthogonal frequency division multiplexing (OFDM) with N_c subcarriers where each subcarrier employs either coherent binary phase shift keying (BPSK) or differential phase shift keying (DPSK) modulation depending on the fading environment.

We further analyze a number of performance measures to evaluate this technique. We analyze the jamming probability and investigate its dependence on primary user behaviors. We also derive the expression of the switching and bit error probability in the presence of jamming attack.

1) 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, error probability and hence on the network design.

Jamming probability is the probability that a jammer hits both the channel and slot assigned to a legitimate 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 a channel is idle, as a result of this model, is given by $\frac{v}{(u+v)}$. Considering that there are N identical and independent channels, 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 chooses to jam a fraction ρ of each time frame. Jammer sets the value ρ to countermeasure the time hopping technique, as we will see in section III-A3 and III-B. Conditioning on the availability of i channels, the probability of jamming a channel in a given time frame is $\frac{\rho}{i}$. Recalling that the probability of the availability of i is given by $\frac{1}{(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}}$, and considering that there are $\binom{N}{i}$ possible combinations for i idle channels out of the N channels, the jamming probability, denoted by P_j, is expressed as

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

The graph of this equation for different primary user behaviors and continuous time jamming ($\rho = 1$) 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 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 legitimate users and attacker. In other words, jammer is not able to jam because of lack of access opportunities. Low

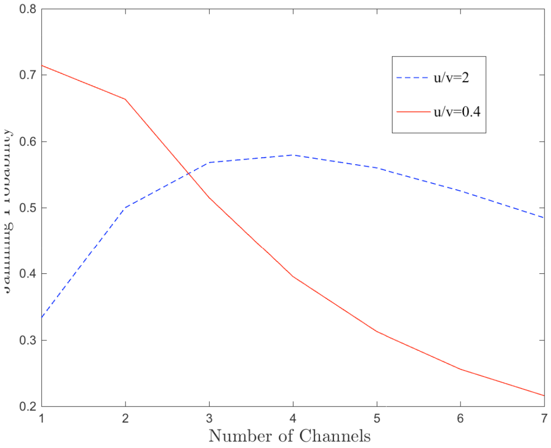

Fig. 2. Jamming probability vs number of primary user channels

P_j might seem appealing, but the lack of access opportunities leads to higher transmission delay [3].

2) Switching Probability: In the time hopping systems no switching is performed due to the presence of a jammer. In other words, if a jammer gets to access the same channel that a 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. 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, derived in [3], is the probability that at least a channel is idle (which is given by $(1 - \frac{1}{(1+v/u)^N}))$ multiplied by the probability that the channel is idle for at least a time frame (which is, considering our channel model, given by e^{-uT_s}). In other words, the service probability is expressed as [3]

$$\mu = (1 - \frac{1}{(1 + v/u)^N})e^{-uT_s} \tag{2}$$

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

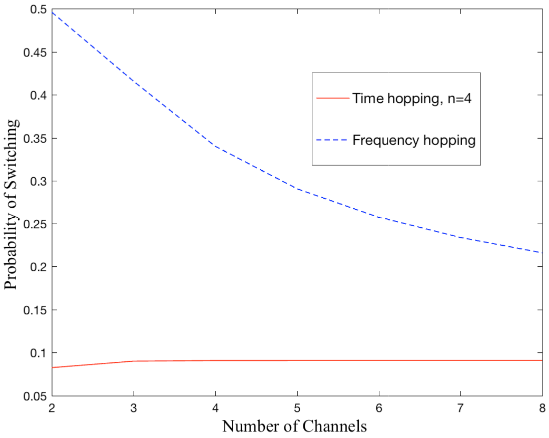

Fig. 3. Switching probability vs number of primary user channels

$$P_{sw} = \beta \sum_{i=1}^{N-1} \binom{N-1}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} \tag{3}$$

The justification behind this equation is similar to that made for Equation(1). In Equation(3), however, the limit of the sum does not exceed $N-1$. That is intuitive since, excluding the channel a user is currently assigned to, the user can only switch to one of $N-1$ channels at most. In Fig. 3, we plot the switching probability for time hopping system along with the corresponding probability in frequency hopping system where legitimate users are required to vacate a channel whenever it is jammed. [15], [16] 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 hopping system is much higher than that for the time hopping, especially with few channels.

3) 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 jamming signal model is commonly considered in the literature (e.g., [16], [24], [25]).

a) Error Probability in AWGN Channel: The jammer jams ρ fraction of the total frame time. If the jamming power per frame is J, then the received jamming-signal variance per slot

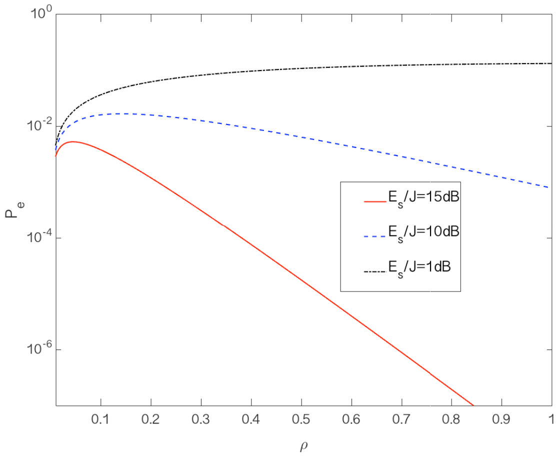

Fig. 4. Error probability vs jamming fraction

is ρJ. Assuming that the jamming power dominates the noise, the probability of error is given by

$$P_e = \sum_{i=1}^{N} \binom{N}{i} \frac{\rho}{i} \frac{1}{(v/u+1)^{N-i}} \frac{1}{(u/v+1)^{i}} Q\Big(\sqrt{\frac{2\rho E_s}{J}}\Big) \tag{4}$$

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 (4) follows from Equation (1) and the BPSK error probability [25].

Attacker sets ρ to countermeasure legitimate user anti-jamming techniques. The jammer selects ρ that causes the worst legitimate users performance. In Fig. 4, for several values of E_s/J we plot the probability of error versus jamming fraction time ρ. As legitimate-to-attacker power ratio increases, the attacker can make legitimate users performance worse by focusing its power over smaller fraction time. Otherwise, the attacker wastes its power without degrading the performance of legitimate user significantly. That is to say that by making legitimate user discontinuously transmit its data and randomly allocate data over time, we impose jammer to follow the same strategy (i.e., jam discontinuously), which is turn reduces the probability of jamming.

b) 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 [17] 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. In this model the communicating users both can be in motion. f_{m1}, and f_{m2} are the maximum Doppler frequency due to the motion of the transmitter and receiver respectively. Without loss of generality, f_{m2} can be represented in terms of f_{m1} as af_{m1}, where $0 \leq a \leq 1$. The power spectral density $PSD(f)$ corresponding to $R_t(\tau)$ is given in [26] and expressed in Equation(5). The multipath power intensity profile which describes the frequency selectivity of channels is modeled as an exponential.

$$PSD(f) = \frac{1}{\pi^2 f_{m1}\sqrt{a}} \begin{cases} \frac{1}{x}K(\frac{1}{x}) & \text{if } |f| \leq (1-a)f_{m1} \\ K(x) & (1-a)f_{m1} < |f| \leq (1+a)f_{m1} \\ 0 & |f| > (1+a)f_{m1} \end{cases} \tag{5}$$

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. Due to the mobility of users, all OFDM 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 [27]. To detect the l^{th} symbol, the received signal is passed through a correlator tuned to the l^{th} frequency. The received l^{th} symbol $\hat{s}_l$ is expressed (as in [25]) as $\frac{1}{\sqrt{T_s}}\int_0^{T_s} s_r(t)e^{-j2\pi f_l t}dt$. Where f_l is the l^{th} carrier frequency. As a result, $\hat{s}_l$ is expressed as

$$\hat{s}_l = \alpha_l(T_s/2)s_l + \frac{T_s}{2j\pi}\sum_{\substack{i=0 \\ i\neq l}}^{N_{sc}-1} \frac{\acute{\alpha_l}(T_s/2)s_l}{(i-l)} + j_l \tag{6}$$

Where j_l is the jamming signal at the $l^t h$ subcarrier. Due to the mobility of users, subchannels interfere with the l^{th} subcarrier (second term in Equation(6)). Considering the power spectral density of the channel, the average power of intercarrier interference at the l^{th} subchannel I_l is expressed as

$$I_l = \frac{4E_sT_s^2}{\pi^2 f_{m1}\sqrt{a}} \sum_{\substack{i=0 \\ i\neq l}}^{N_{sc}-1} \frac{1}{(l-i)^2}\Bigg[\int_0^{(1-a)f_{m1}} f^2\frac{1}{x}K(\frac{1}{x})df + \int_{(1-a)f_{m1}}^{(1+a)f_{m1}} f^2K(x)df\Bigg] \tag{7}$$

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

$$P_{e|\alpha_l} = \sum_{i=1}^{N}\binom{N}{i}\frac{1}{(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}} \left[\frac{\rho}{i}Q(\sqrt{\frac{2E_s|\alpha_l|^2}{\rho J+I_l}}) + (1-\frac{\rho}{i})Q(\sqrt{\frac{2E_s|\alpha_l|^2}{I_l}})\right] \tag{8}$$

Equation (8) can be derived from Equation (1) and (4). By averaging over the distribution of the subchannel gain we obtain the unconditional error probability which can be expressed as

$$P_e = \frac{1}{2}\sum_{i=1}^{N}\binom{N}{i}\frac{1}{(v/u+1)^{N-i}}\frac{1}{(u/v+1)^{i}} \left[\frac{\rho}{i}\left(1-\sqrt{\frac{\gamma_1}{1+\gamma_1}}\right) + (1-\frac{\rho}{i})\left(1-\sqrt{\frac{\gamma_2}{1+\gamma_2}}\right)\right] \tag{9}$$

where $\gamma_1 = \frac{2E_sE[|\alpha_l|^2]}{\rho J/+I_l}$, 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 $c^{-1}exp(-c^{-1}|\alpha_l|^2)$.

In Fig. 5, we plot the error probability for the subcarrier in the middle of a channel ($l = 128$). We set the number of primary user channels to four ($N = 4$), number of subcarriers to 256, ρ to 0.1, average busy to idle time to unity ($u/v = 1$), receiver to transmitter speed ratio to be 0.5 ($a = 0.5$), and the product of maximum Doppler frequency and slot duration (T_sf_{m1}) to 0.05. We observe from the figure that the probability of error reaches a limit such that any increase in E_s/J no longer improves the performance. In other words, increasing legitimate-to-jammer power ratio makes no difference after a certain threshold as mobility effects starts to dominate jamming effect. This limit, which can be derived by taking the limit of Equation

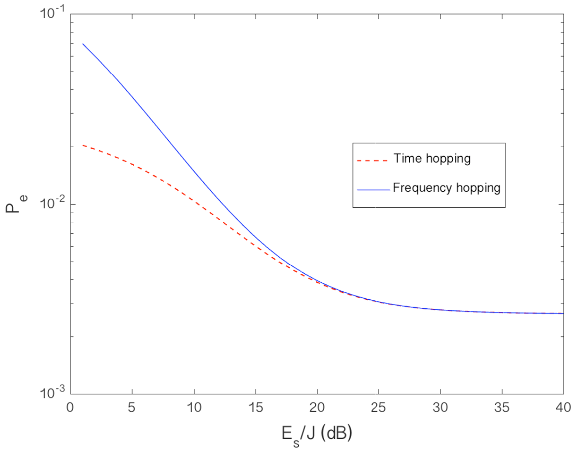

Fig. 5. Error probability vs legitimate-to-attacker power ratio

(9) as E_s/J goes to infinity, is referred to as irreducible error probability [28]. 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 (to reduce the value of $T_s f_{m1}$) so that the effect of mobility is mitigated. 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 jamming power is relatively high, our system achieves with less power the same level of performance that frequency hopping systems achieve. That is because, in the time hopping system we enforced jammer to discontinuously jam. One might think that we are not utilizing our resources, as we only allocate one slot for a legitimate user within each frame. However, our system is a multiusers system where each slot can be allocated to a different user. As legitimate-to-attacker power ratio increases, the intercarrier interference domains the jamming effect and time and frequency hopping systems perform similarly.

To overcome the performance improvement limitations and mitigate the fading channel effects, we propose another time hopping technique.

B. Selective Diversity Based Time Hopping (SDTH)

SDTH anti-jamming technique is similar to PKTH, however, in this scheme we consider the channel quality in the hopping pattern derivation. The time axis is divided into frames. The time frame is subdivided into s subframes, which are in turn divided into n_s slots. In any signaling interval, based on a shared key, a user selects a subframe. Within the selected subframe, slot to be allocated with user's transmitted signal is determined based on channel quality. Channel envelope-crossing rate, which is the rate at which the transmitted signal envelope crosses a specified level, can be a criteria for channel quality determination. Duration of fades defined as average time during which signal envelope remains below a certain level is another channel quality measure. Mobile-to-mobile channel statistical properties that can be used to determine channel quality over time are analytically characterized in [29]. In SDTH, best channel gain is our criteria for subrames slot allocation. Best gain in the sense that the allocated slot has the maximum channel gain among the subframe slots. The estimation method presented in [30] can be used to determine the channel with the best quality. Channel coherence time, which characterizes the time varying of the frequency dispersiveness caused due to mobility of users, is an important SDTH design parameter that needs to be considered in determination of slot and frame durations. The slot duration should be small (smaller than channel coherence time) so that channel variations within the slot are small. Also, since coherence time quantifies the correlation of channel gain at different times, to ensure security, frame duration should be larger than the coherence time. In other words, frame durantion should be set such that channel responses for different frames are uncorrelated.

We further analyze analytically the scheme error probability and compare it with the corresponding probability of PKTH. We will show, in different fading environments, SDTH improves the probability of error considerably over PKTH and hence over frequency hopping.

There is a correlation between channel gains at different slots in the subframes, in general. Using the probability joint distribution of channel gains at different slots to obtain the error probability is complicated and does not lead to a closed form solution. The correlation between the channel gains can be described by their joint characteristic function [31]. Considering the correlation between the n_s subframe slots, the error probability of an allocated slot is expressed as [31]

$$P_e = \int_{-\infty}^{\infty} .. \int_{-\infty}^{\infty} CF(x_1, .., x_{n_s}) f(x_1, .., x_{n_s}) dx_1 .. dx_{n_s} \tag{10}$$

$CF(x_1, .., x_{n_s})$ is the characteristic function which is defined as $E[e^{j(x_1 r_1 + .. + x_{n_s} r_{n_s})}]$. Where $r_i \triangleq |\alpha_{s_i}|^2$, and α_{s_i} is the i^{th} slot channel gain $\forall\ i \in \{1, .., n_s\}$. r_i is distributed as chi-squared with two degrees of freedom. $CF(x_1, .., x_{n_s})$ is expressed as $det(\mathbf{A})^{-1}$. where $\mathbf{A}(l, l) =$

$1 - jx_l E[r_l]$, and $\mathbf{A}(l,k) = \sqrt{cV_{r_l}V_{r_k}}\ \forall\ l,k \in \{1,..,n_s\}$. c is the correlation coefficient between r_l and r_k, V_{r_l} is the variance of the random variable r_l. $f(x_1,..,x_{n_s})$ is given by

$$f(x_1,..,x_{n_s}) = \frac{1}{(2\pi)^{n_s}} \int_0^\infty P_{e|r} h(r, x_1,..,x_{n_s}) dr \tag{11}$$

Where r is the maximum of $r_1,..,r_{n_s}$ and $h(r, x_1,..,x_{n_s})$ is given by

$$h(r, x_1,..,x_{n_s}) = \prod_{l=1}^{n_s} \Bigg[\sum_{k=1}^{n_s} (-1)^{k+1} \\ \sum_{b_1+..+b_{n_s}} \frac{j(b_1x_1 + .. + b_{n_s})}{exp(jr((b_1x_1 + .. + b_{n_s})))} \Bigg] \tag{12}$$

Depending on the fading environment, it can be difficult for coherent systems such as phase shift keying to maintain coherence over a single pulse duration. With out loss of generality, we consider differential phase shift keying modulation to express P_e. The error probability conditioned on the availability of at least one channel for a fixed r is given by

$$P_{e|r} = \frac{\rho}{2} \sum_{i=1}^{N} \binom{N}{i} \frac{1}{i\,(v/u+1)^{N-i}} \frac{1}{(u/v+1)^i} \times \\ \left(exp\Big(-\frac{E_s r}{(J/\rho + I)}\Big) - exp\Big(-\frac{E_s r}{I}\Big) \right) \\ + \frac{1}{2}\Big(1 - \frac{1}{(v/u+1)^N}\Big) exp\Big(-\frac{E_s r}{I}\Big) \tag{13}$$

Considering the error probability of DPSK [25], Equation (13) can be derived similar to Equation (4). By plugging Equation (13) and (12) into equation (11) which in turns plugged into (10) gives the closed form of the error probability for any fading environment, jamming strategy, and primary user activities level. For mathematical tractability, we evaluate SDTH error probability when number of slots within a subframe n_s is two. In this case, P_e is expressed as follows

$$P_e = \frac{2\rho}{(4\pi)^2} \Bigg[\sum_{i=1}^{N} \binom{N}{i} \frac{1}{i\,(v/u+1)^{N-i}} \frac{1}{(u/v+1)^i} \\ \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} \Big(f_1(x_1,x_2) - f_2(x_1,x_2) \Big) dx_1 dx_2 \\ + \Big(1 - \frac{1}{(v/u+1)^N}\Big) \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} f_2(x_1,x_2) dx_1 dx_2 \Bigg] \tag{14}$$

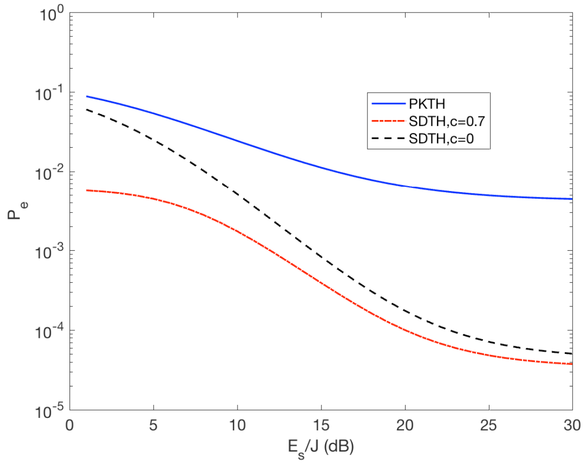

Fig. 6. Error probability vs legitimate-to-attacker power ratio

Where $f_i(x_1, x_2)$ for $i \in \{1, 2\}$ is given by

$$f_i(x_1, x_2) = \frac{1}{(x_1 E[r_1] + j)(x_2 E[r_2] + j)} \times \frac{(x_1 + x_2 - 2j\gamma_i)}{(x_1 - j\gamma_i)(x_2 - j\gamma_i)(x_1 + x_2 - j\gamma_i)} \tag{15}$$

Where $\gamma_1 = \frac{E_s E[r]}{J/\rho + I}$, and $\gamma_2 = \frac{E_s E[r]}{I}$.

In Fig. 6, we plot SDTH error probability vs legitimate-to-attacker power ratio for various values of correlation coefficient. We consider both the cases when there is no correlation between slots (c=0) and the correlation coefficient is 0.7. We assume that there are two identical primary user channels. The probability that a channel is idle is half. The fraction of jammed frame time ρ is half. The product of maximum Doppler frequency and slot duration is 0.05, the receiver-to-transmitter speed ratio is 0.5. $E[r_1]$ and $E[r_2]$ are normalized with respect to $E[r]$ each equals $4/3$, the variance of both r_1 and r_2 equal four.

Fig. 6 shows that SDTH technique reduces error probability significantly over PKTH scheme. The reduction becomes more significant as the intecarrier interference dominates jamming (i.e., as legitimate-to-attacker power ratio increases). Furthermore, we observe that a correlation between slots leads to more performance improvements. The number of slots within a frame, number of subframes, and the duration of time slots can all be designed such that slots within a subframe are correlated to maintain a desired error performance.

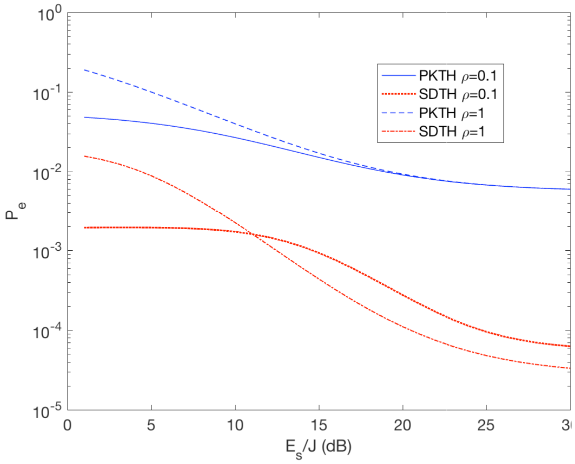

Fig. 7. Error probability vs legitimate-to-attacker power ratio

In Fig. 7, for correlation coefficient equals 0.7 and various values of jamming fraction time ρ, we plot the error probability for both PKTH and SDTH. The figure shows that in case of SDTH, when the jammer power is relatively high (i.e, E_s/J is low) as the percentage of time jammed increases, legitimate user performance can be degraded significantly. In other words, if the power of jammer is high, it can contentiously jam ($\rho = 1$) and hence the performance of legitimate user becomes worse than that if it jams partially ($\rho < 1$). However, as jammer-to-legitimate power ratio decreases, the lower the jamming fraction time, the worse the performance it can be. These observations agree with those made from Fig. 4 in the sense that jammer can lead to worst case performance depending on its power and percentage of jammed time.

IV. Conclusions and Future Work

In this paper, we have proposed two time based jamming countermeasures. 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 methods outperform the frequency hopping anti-jamming scheme in terms of switching probability, and error probability. Proposing a game theoretical approach in which we exploit the mobility of users to mitigate jamming is underway.

ACKNOWLEDGMENT

This work was supported in part by the US National Science Foundation under NSF award CNS-1162296.

REFERENCES

[1] Huawei, "5G: A technology vision," [Online]. Available: www.huawei.com/5gwhitepaper [Accessed: Nov. 25, 2015].

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

[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] D. Shan, K. Zeng, P. Richardson, and W. Xiang, "Detecting multi-channel wireless microphone user emulation attacks in white space with noise," in *Cognitive Radio Oriented Wireless Networks (CROWNCOM), 2013 8th International Conference on*, July 2013, pp. 154–159.

[6] K. Borle, B. Chen, and W. Du, "A physical layer authentication scheme for countering primary user emulation attack," in *Acoustics, Speech and Signal Processing (ICASSP), 2013 IEEE International Conference on*, May 2013, pp. 2935–2939.

[7] W.-L. Chin, C.-L. Tseng, C.-S. Tsai, W.-C. Kao, and C.-W. Kao, "Channel-based detection of primary user emulation attacks in cognitive radios," in *Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th*, May 2012, pp. 1–5.

[8] H. Li and Z. Han, "Catch me if you can: An abnormality detection approach for collaborative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE Transactions on*, vol. 9, no. 11, pp. 3554–3565, November 2010.

[9] Z. Gao, H. Zhu, S. Li, S. Du, and X. Li, "Security and privacy of collaborative spectrum sensing in cognitive radio networks," *Wireless Communications, IEEE*, vol. 19, no. 6, pp. 106–112, December 2012.

[10] A. Grissa, M.and Yavuz and B. Hamdaoui, "LPOS: locaion privacy for optimal sensing in cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2015 IEEE*, Dec 2015, pp. 1–5.

[11] Y. Wu, B. Wang, and T. Liu, K.J.R. ; Clancy, "Anti-jamming games in multi-channel cognitive radio networks," *Selected Areas in Communications, IEEE Journal on*, vol. 30, no. 1, pp. 4–15, January 2012.

[12] L. Xiao, J. Liu, Y. Li, N. Mandayam, and H. Poor, "Prospect theoretic analysis of anti-jamming communications in cognitive radio networks," in *Global Communications Conference (GLOBECOM), 2014 IEEE*, Dec 2014, pp. 746–751.

[13] K. Dabcevic, A. Betancourt, L. Marcenaro, and C. Regazzoni, "A fictitious play-based game-theoretical approach to alleviating jamming attacks for cognitive radios," in *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*, May 2014, pp. 8158–8162.

[14] L. Xiao, T. Chen, J. Liu, and H. Dai, "Anti-jamming transmission stackelberg game with observation errors," *Communications Letters, IEEE*, vol. 19, no. 6, pp. 949–952, June 2015.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] C. Chen, M. Song, C. Xin, and J. Backens, “A game-theoretical anti-jamming scheme for cognitive radio networks,” *Network, IEEE*, vol. 27, no. 3, pp. 22–27, 2013.

[20] A. Yavuz, *Lecture notes: Advanced Network Security*. Oregon State University, 2014.

[21] J.-P. Aumasson, L. Henzen, W. Meier, and R. C.-W. Phan, “Sha-3 proposal blake,” *Submission to NIST*, 2008.

[22] N. Sha, “Competition, 2007-2012,” [Online]. Available: http://csrc.nist.gov/groups/ST/hash/sha-3/index.html [Accessed: Jul. 10, 2016].

[23] O. Goldreich, “Texts in computational complexity: Pseudorandom generators,” 2006.

[24] 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, 2003, pp. 336–340 Vol.1.

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

[26] 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.

[27] 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.

[28] 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.

[29] A. Akki, “Statistical properties of mobile-to-mobile land communication channels,” *Vehicular Technology, IEEE Transactions on*, vol. 43, no. 4, pp. 826–831, Nov 1994.

[30] A. Bletsas, A. Khisti, D. Reed, and A. Lippman, “A simple cooperative diversity method based on network path selection,” *Selected Areas in Communications, IEEE Journal on*, vol. 24, no. 3, pp. 659–672, March 2006.

[31] Q. Zhang and H. Lu, “A general analytical approach to multi-branch selection combining over various spatially correlated fading channels,” *Communications, IEEE Transactions on*, vol. 50, no. 7, pp. 1066–1073, Jul 2002.