Send Orders for Reprints to reprints@benthamscience.ae

The Open Cybernetics & Systemics Journal, **2014,** *8,* **853-859**

Open Access

Modeling of Channel Jamming in Dynamic Spectrum Access Networks

Hui Sun[1], Rui Wang[1,2,*] and Yanxiao Zhao[3]

[1]*Automation Department, College of Aeronautical Automation, Civil Aviation University of China, Tianjin, 300300, P.R. China;* [2]*Electrical Engineering and Automation Department, College of Aeronautical Automation, Civil Aviation University of China, Tianjin, 300300, P.R. China;* [3]*ECE Department, South Dakota School of Mines and Technology, Rapid City, S.D, 57701, USA*

Abstract: Dynamic Spectrum Access (DSA) network is envisioned as a promising candidate to significantly improve the spectrum utilization. Due to its specific features of the DSA, however, this network is more vulnerable to security attacks than the traditional wireless networks. And channel jamming is a one of main threats to DSA networks. So far, limited works have been done in mathematical and formal modeling of the channel jamming. In this paper, we present the attempts to analyze the channel jamming behaviors in DSA networks in order to find a relationship between the number of channels, secondary users and attackers. The research focuses on jamming performance analysis in various architectures, that is, a simple DSA network and a complex DSA network with varied situations. Comparisons between theoretical and simulation results in Matlab verify that the modeling and analysis are valid.

Keywords: Attacker, channel Jamming, dynamic spectrum access (DSA), secondary user.

1. INTRODUCTION

Dynamic Spectrum Access (DSA) networks enable secondary users to access the licensed spectrum bands opportunistically. This is achieved by making secondary users to access bands when primary users are not present [1-2]. Secondary users should sense channels to find an idle one and keep sensing to follow evacuation protocol upon the return of the primary users. Based on this method, DSA networks significantly improve the spectrum utilization and relieve the issue of "spectrum scarcity" [3], however, DSA network encounters serious security problems not appeared in conventional wireless networks because of the characteristics of DSA networks. For example, in [4], authors analyze the Denial of service of attack in MAC protocols. There is an attack in spectrum sensing which is unique to CRNs and is a fundamental threat to CRNs. In this situation the attackers can imitate the signal of primary user to trick secondary users into believing that there is a primary user. In such a case, the secondary user has to find an alternate channel for communication, or leave the system when alternate channels are not available. It is primary user emulation attack (PUEA) [5]. For PUEA, malicious users emulate the primary information over the idle spectrum such that the secondary users cannot use the corresponding white bonds. This will make low spectrum utilization and inefficient cognitive network operation. Specifically, an attacker, which may be a malicious user or a selfish SU, can transmit a PU signal using its cognitive radio [6]. Paper [7] discussed that several classes of attacks and proposed the approaches for mitigating the attacks by instilling some "common sense" into radio systems.

Channel jamming is recently becoming a common threat to a DSA network [8, 9]. The malicious nodes sense the channels on channels. If an attacker detects the channel is under using, it interferes the communication of users which are on this channel. In this case, the secondary users will vacate this channel to other available ones after finishing spectrum sensing. So, the switching time and sensing time will affect the quality of communication between secondary users. If the switch time is long, the communicating quality will be inefficient.

Therefore, many researches are focusing on anti-jamming. DSA network could be more susceptible to jamming because of some unique requirements, such as secondary users have to leave from the channel if a primary user signal is detected [10]. When fake primary signal is detected, the secondary users have to vacate the current channel to find another available channel due to misdetection. Consequently, the switching time and sensing time will affect the quality of communication between secondary users. Paper [1] provided a distributed probabilistic protocol to mitigate jamming in cognitive radio networks.

There are multiple primary methods a jammer could employ to accomplish solving jamming issue. For instance, traditional jamming, Common Control Channel Jamming, and primary user emulation attack (PUEA) are easily implemented in DSA networks [11]. PUEA refers to attacks may jam the licensed band, emulate primary users and thus prevent the secondary users from utilizing the unlicensed bands and limit CN capacity [12]. To solve the jamming issue, some anti-jamming methods are proposed in [13-16]. The anti-jamming approaches can be divided into three main

1874-110X/14

categories such as network layer anti-jamming, link layer anti-jamming and physical layer anti-jamming [17]. Network coding or adding network-level redundancy is the main method to solve jamming in network layer anti-jamming. Network coding can defense against snooping and eavesdropping attacks by combining packets together and send to the receiver to enhance the throughput. Beam forming, directional antennas, and spread spectrum are used as the physical layer anti-jamming [18].

In [19], authors presented an optimal strategy through the Markov decision process. Secondary users can use proactive hopping as a defense strategy against jamming. This hopping behavior can gives DSA networks an advantage of improving their anti-jamming performance [20].

So far, most of papers discuss the anti-jamming algorithm in DSA network and simply proposed algorithms for anti-jamming. Limited works have been done in mathematical and formal modeling of the channel jamming. The contribution of this paper is mathematically modelling channel jamming and obtaining in-depth understanding of the fundamental process in jamming process. And we consider a secondary user could hop across multiple channels in order to reduce the probability of being jammed in the process. In different situations, comparisons between simulation results and theoretical analysis have been conducted to verify the effectiveness of the analysis.

The remainder part of this paper is organized as follows: The configuration of system modules is developed in Section 2. Section 3 proposes the analysis of channel jamming in detail. Section 4 presents the simulation results and the related data analysis. Conclusions and future works are summarized in Section 5.

2. SYSTEM MODELS

2.1. Channel Model

Consider a DSA network with M licensed channels which can be opportunistically used by secondary users. Each channel has two different states. One is 'Busy' when the channel is occupied and another is 'Idle' which is referred to the state that channel is empty. In this paper, we primarily focus on the behaviors of secondary users and attackers, so the effect from primary users is not considered. That is, the 'Busy' state presents that the current channel is occupied by secondary users or jammed by attackers. We also assume that all idle channels have the same features. That means secondary users do not have to check the quality of available channels before they select one.

Let *Hi* and *Ho* denote the state of channel as 'Idle' and 'Busy' respectively. Then, the state S of channel can be presented as below.

$$S_m = \begin{cases} 1, & m \overset{\text{def}}{=} H_o \\ 0, & m \overset{\text{def}}{=} H_i \end{cases}$$

2.2. Secondary User Model

Suppose that the secondary users have perfect spectrum sensing, that is, false alarm and detection error are zero and not considered. Secondary users can detect all M channels and select an idle channel randomly. In this paper, we suppose that the number of channel *(M)* is much larger than the number of secondary user pairs *(N)* ($N \leq M$). Two cases are examined. First, each channel can be occupied by only one secondary user pair. This case is called non-overlapping. Second, multiple secondary user pairs can share one channel. This is called overlapping in secondary users. If secondary users detect the existence of attackers, users leave the current channel immediately and select other available channels to continue communicating. In the overlapping situation, the non-transmission users will observe the transmitting users' behavior to vacate or not. Suppose that the switching duration from previous channel to a new one is negligible and each secondary user pair can only keep communication with a limited period in current channel. If the communication does not done in the specific period, secondary users must leave this channel and select other available channels to continue transmission.

2.3. Attacker Model

If an attacker detects the channel occupied by secondary users, it will block the communication. Once the channel state becomes idle, attackers will stop jamming and switch to other channels immediately. If no secondary users were found in a channel during this sensing period, the attacker moves to other channel until detecting secondary users. Like the secondary users' behavior, jammers have two different situations: overlapping (Attackers can be divided into several groups randomly according to multiple different methods, named "overlapping".) and non-overlapping.

Based on the models above, the throughput of secondary users just relates to the communication time and the whole process overhead. Analysis of the jamming process is discussed in next section.

3. CHANNEL JAMMING ANALYSIS

In a DSA network, M, N and L denote the number of channels, secondary users and attackers, respectively. p_a refers to the probability of attack, p_s denotes the channel selection probability of secondary users, and p_m is the channel selection probability of attackers. Assume that the duration of process T is a relatively long period and T is divided into huge amount of time slots as shown in Fig (**1**). The period of each time slot is T_m.

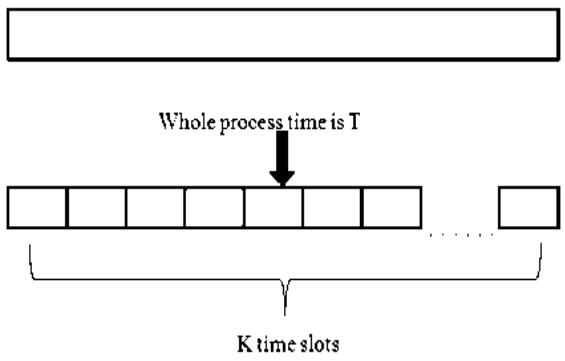

Fig (1). Process time and time slots.

Let K denotes the number of time slots:

$$K = \frac{T}{T_m}$$

In each time slot, only one behavior exists, either communication or jamming. If jamming happens on a channel, the whole transmission and effective communication are assumed to be ruined when time slot is zero. Otherwise, the duration of communication is T_m.

Now derive the successful access probability for secondary users: *Let* p_a be the attack probability, p_c be the communication probability.

$$p_c = 1 - \frac{K\{(p_a \times 0) + [(1-p_a) \times T_m]\}}{K \times T_m}$$

3.1. One Secondary user Pair vs. One Attacker

Channel selection probability of the secondary user pair is $p_s = \frac{1}{M}$. Similarly, channel selection probability of attacker is $p_m = \frac{1}{M}$. Attack probability is

$$p_a = M \times (p_s \times p_m) \quad (1)$$

3.2. Multiple Secondary user Pairs vs. Multiple Attackers

Suppose that there are N secondary user pairs, M channels and L attackers in a DSA network, where $1 < N \ll M 1 < N \leq M$ and $1 < L \ll M$. Let α denote the different ways to select L channels from M channels by attackers. Suppose that there is no overlapping happen, then

$$\alpha = C_M^L$$

The jamming behavior will not happen, if no attacker selects the channel which is occupied by secondary users. The combination for this situation is defined as β. Then,

$$\beta = C_{M-1}^L$$

So, attack probability is

$$p_\alpha = 1 - \frac{\beta}{\alpha}$$

3.3. Multiple Secondary user Pairs (Overlapping) vs. Multiple Attackers (Non-Overlapping)

Suppose that the Time Division Multiple Access (TDMA) channel access method will be used in this case. Based on TDMA strategy, it is known that the users transmit signals periodically. In this scenario, even if an attacker can find a channel which is occupied by secondary users and attack the channel, however, it does not mean that the secondary users are attacked if these users are not in their communication period.

Let p_d refer to the probability of communication duration of secondary users in the whole period of communication and p_t denote the probability of overlapping in a DSA network. Here, p_d and p_t are unknown. They depend on the spectrum band itself.

There are two jamming cases may happen while taking the overlapping case into consideration. Case one is that secondary users are under attack on a sharing channel. Case two is that secondary user pair is jammed in a channel only occupied by itself. According to the equation (1), two equations can be found.

In Case one, the attack probability is

$$p_{\alpha 1} = p_t \times p_d \times [(p_s \times p_m) \times M] \quad (2)$$

In Case two, the probability of attack is

$$p_{\alpha 2} = (1 - p_t) \times [(p_s \times p_m) \times M] \quad (3)$$

In this instance, the attack probability should be equal to the sum of the probabilities in different cases. Based on the equation (2) and (3), the probability is

$$p_\alpha = p_{\alpha 1} + p_{\alpha 2}$$

3.4. Multiple Secondary user (Non-Overlapping)vs. Multiple Attackers (Overlapping)

So far, it is only discussed that each channel is attacked by only one attacker. If the overlapping happens in attackers, the situation becomes more complicated.

Here, one secondary user pair and several attackers are proposed in a DSA network. If there is one attacker jamming the channel, no matter which attacker is, the attack is considered to be successful. Suppose that there are L attackers in a DSA network. If the overlapping is considered, we can find L different kinds of combinations of attackers. For instance, suppose that four attackers are in a four channels network. Attackers can organize four different combinations. Here, in general, R denotes the number of groups.

Let R be equal to 2 (Each group is presented using red square). The possible channels' states for the same channel are shown in Fig (**2**). There are 6 types of ways to jam a channel by two groups of attackers.

Let M denote the number of channels, and r present the possible number of the groups of the attackers specifically. Then attack probability should be p_m^r.

Therefore, the attack probabilities in different situations are shown in Table **1**.

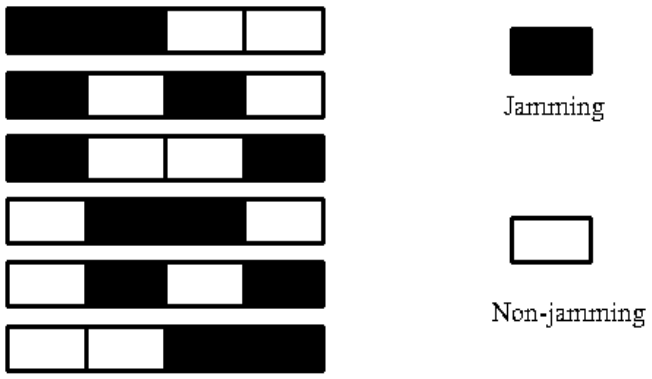

Fig (2). Channel jamming in different situation with two groups of attackers' case.

Table 1. Group attack probability and group structure.

The Number of Groups	Attack Probability	Structure of Group
1	1/4	(4)
2	2/4	(1, 3)and(2, 2)
3	3/4	(1, 2, 1)
4	4/4	(1, 1, 1, 1)

Suppose that L attackers are divided into r groups. Let p_L^r refer to the probability, then, channel selection probability of attackers is

$$p_m = \sum_{r=1}^{L} p_L^r p_m^r \quad (4)$$

From equation (1) and (4), the attack probability is

$$p_\alpha = (p_s \times \sum_{r=1}^{L} p_L^r p_m^r) \times M$$

4. NUMERICAL RESULTS

In this section, the channel jamming is simulated and the jamming performance is evaluated in various cases. All the results shown in the following figures present that the theoretical results match the simulation results very well, which demonstrates the validation of the modeling and analysis.

4.1. One User vs. One Attacker

In the first experiment, we consider one secondary user, one attacker over varied numbers of channels is considered. Fig (**3**) shows the comparisons between simulation and theoretical values in a network with up to 10 channels. Fig (**4**) shows the results in a network up to 100 channels. From both figures, it is obvious that the theoretical values match the simulation results very well, and the jamming probability is reduced while increasing the number of channels. Furthermore, the jamming probability with 100 channels line becomes smoother than that with 10 channels. This verifies the attacker has lower chance to jam a channel occupied by the user, especially with a large number of channels.

4.2. Multiple Users vs. Multiple Attackers (Non-Overlapping)

In the second experiment, multiple users and attackers are investigated in a DSA network. And channel sharing does not happen among attackers or secondary users.

The analysis in Section 3 suggests that the attack probability will be equal to 1 if the number of attackers is equal to the number of channels. If the number of channels is larger than that of attackers, the jamming probability is reduced as shown in Fig (**5**).

Table **2** shows the comparisons between the theoretical values and simulation results which are shown in Fig (**6**).

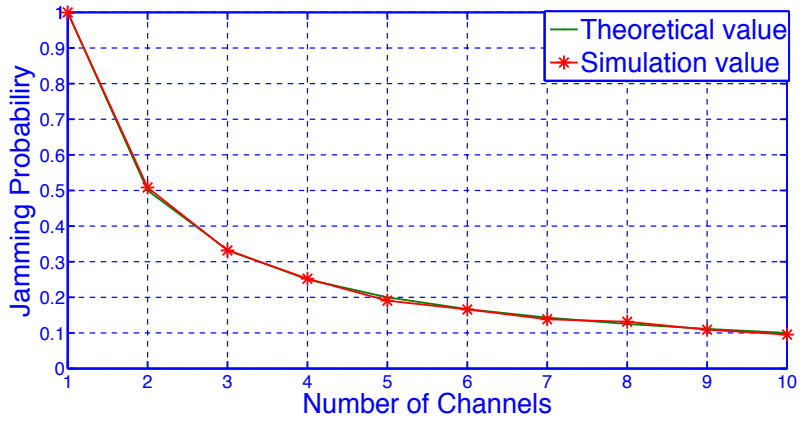

Fig (3). Comparison of jamming probability between theoretical values and simulation values (one user vs. one attacker, 10 channels).

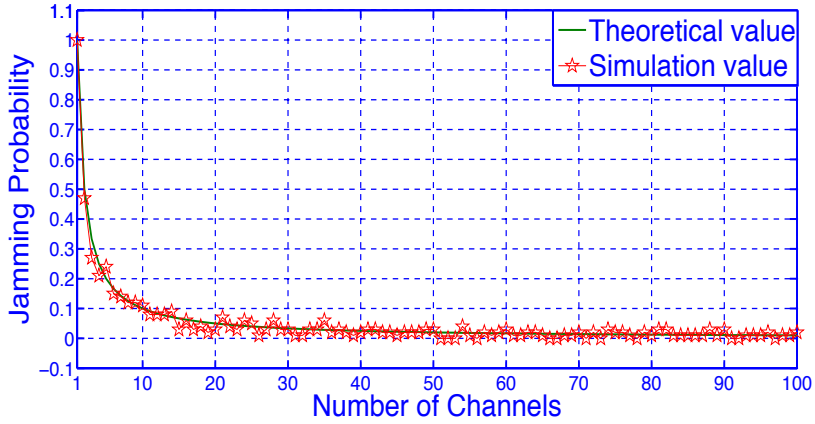

Fig (4). Comparison of jamming probability between theoretical values and simulation values (one user vs. one attacker, 100 channels).

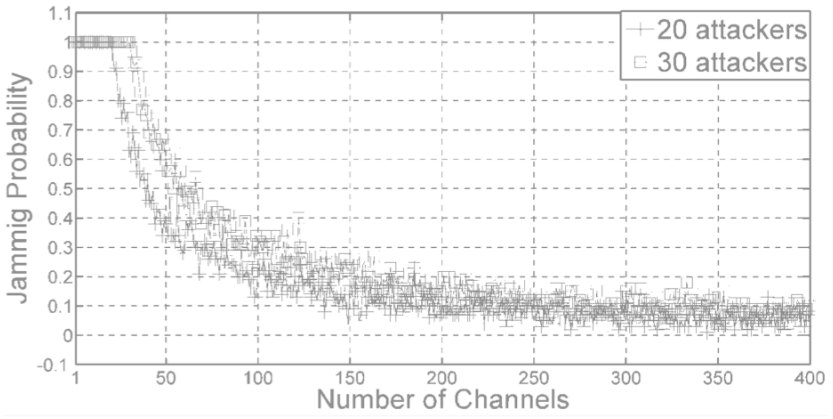

Fig (5). Comparison of jamming probability (20 vs. 30 attackers both with 3 users and 400 channels).

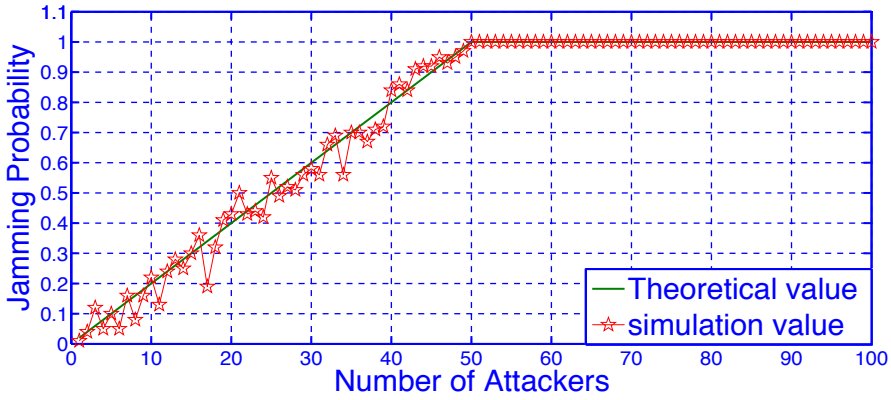

Fig (6). Comparison of jamming probability between theoretical values and simulation values (3 users vs. multiple attackers, 50 channels).

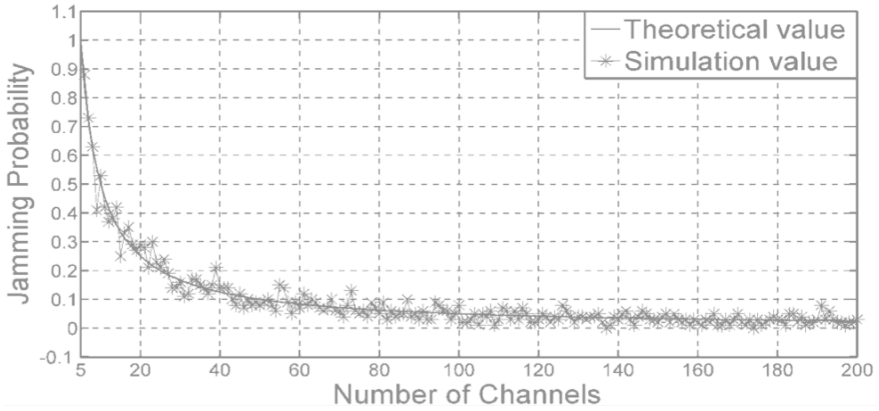

Fig (7). Comparison of jamming probability between theoretical values and simulation values (3 users (overlapping) vs. 5 attackers, 200 channels).

Fig (**6**) presents that the jamming probability will be enhanced by increasing the number of attackers. If the number of attackers is larger than the number of channels (in this experiment, the number is 50), the jamming probability of this DSA network is equal to 1. Because all channels are occupied by malicious node, in this case, the DSA network is under attacked 100 percent. 100 percent.

4.3. Multiple Secondary Users (Overlapping)

In the third experiment, the situation with multiple users and attackers is simulated in a DSA network. And the overlapping is taken into consideration among secondary users. In this case, TDMA is used in the system. Suppose

Table 2. The comparison of jamming probability between theoretical and simulation.

Number of Channels	Simulation Value	Theoretical Value
100	0.15	0.2
150	0.09	0.13
200	0.15	0.1
300	0.05	0.06
400	0.06	0.05

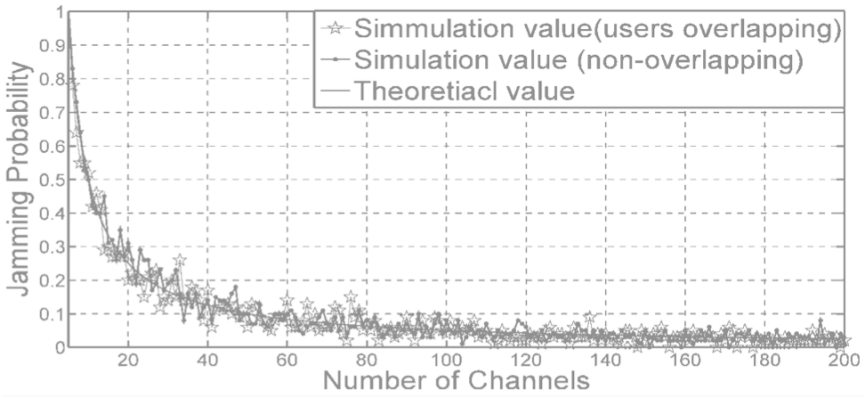

Fig (8). Comparison of jamming probability between theoretical values and simulation values (3 users vs. 5 attackers, 200 channels).

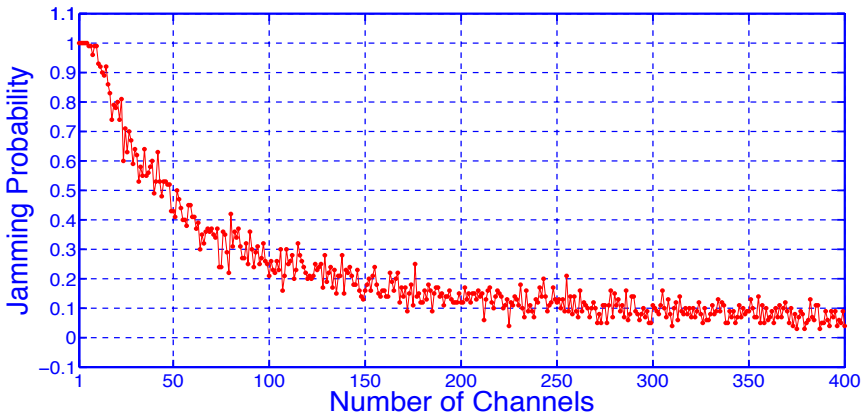

Fig (9). Simulation values (overlapping).

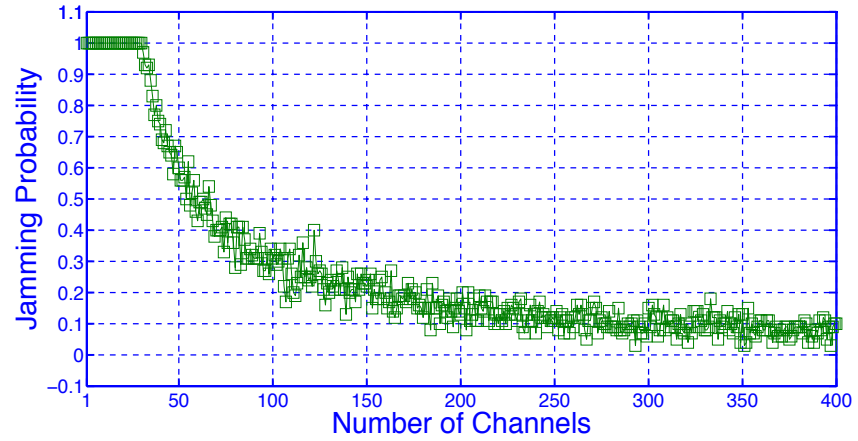

Fig (10). Simulation values (non-overlapping).

that the probability is proportional to the reciprocal of the number of secondary user pairs in a channel. The pure curve shown in Fig (**7**) is the theoretical value.

In Fig (**8**), the pure line shows theoretical values which are calculated by using mathematical methods. The line with stars displays the simulation values with overlapping situation, while the line with dots shows the non-overlapping situation. Based on this figure, we can identify that the simulation value with overlapping is larger than the simulation value without overlapping if the number of channels is not big. Simulation values are getting very close between the above two situations with the increasing of the number of channels.

4.4. Multiple Attackers with Overlapping

In the last experiment, we consider the overlapping happens in multiple attackers in a DSA network with multiple secondary users. From Fig (**9**), we can observe that jamming probability is less than 1 even the number of channels less than or equals to the number of attackers because they were separated into several groups with overlapping. And the number of groups is less than the number of channels. It is different with the non-overlapping situation shown in Fig (**10**). The jamming probability is 1 if the number of attackers is less than or equal to the number of channels.

CONCLUSION AND FUTURE WORKS

Security issue becomes a serious problem to DSA networks. Due to the unique characteristics of DSA networks, it is prone to be attacked by channel jamming [16]. In this paper, a system model has been first set up and has been analyzed the jamming behaviors according to the unique feature of secondary users, spectrum and jammers based on this model. We analyzed several different situations and compared the theoretical and simulated values. All the simulation results have shown that the proposed jamming model and theoretical analysis are validated.

In the current works, the channel quality and primary users' activity are ignored. In the future, we will consider different channel qualities and the affects from primary users in DSA networks. Also the analysis of attackers with overlapping situation will be extended.

CONFLICT OF INTEREST

The authors confirm that this article content has no conflict of interest.

ACKNOWLEDGEMENTS

This work was supported by grants from the Young Scientists Fund of the National Natural Science Foundation of China (61403395), the Natural Science Foundation of Tianjin, PR China (13JCYBJC39000), Project supported by the Scientific Research Staring Foundation for the Returned Overseas Chinese Scholars, Ministry of Education of China, Tianjin Key Laboratory of Civil Aircraft Airworthiness and Maintenance in CAUC (104003020106), the National Basic Research Program of China (2014CB744904), Scholars of Civil Aviation University of China (2012QD21x).

REFERENCES

[1] Pietro, Roberto Di, Oligeri, and Gabriele "Jamming mitigation in Cognitive radio networks", IEEE Network, v 27,n 3, p 10-15, 2013

[2] Kui Ren , Haojin Zhu , Zhu Han , Radha Poovendran. "Security in Cognitive Radio Networks", IEEE Network, May/June 2013.

[3] B. Wang and K. J. R. Liu, "Advances in Cognitive Radio Networks: A Survey", IEEE J. Sel. Topics Signal Process., vol. 5, no. 1, pp. 5–23, 2011

[4] Li Zhu and Huaibei Zhou, "Two Types of Attacks Against Cognitive Radio Network MAC Protocols", in International Conference on Computer Science and Software Engineering, 2008. vol. 4, pp. 1110-1113, 2008.

[5] LI Hongning, PEI Qingqi, MA Lichuan, "Channel Selection Information Hiding Scheme for Tracking User Attack in Cognitive Radio Networks", pp. 125-136, China Communications • March 2014

[6] ChunSheng Xin, Senior Member, IEEE and Min Song, Senior Member, IEEE, "Detection of PUE Attacks in Cognitive Radio Networks Based on Signal Activity Pattern", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 5, MAY 2014.

[7] Clancy, Charles T. and Goergen, Nathan, "Security in Cognitive Radio networks: Threats and mitigation", Proceedings of the 3rd international conference on Cognitive radio Oriented wireless networks and communications, 2008 pp 1-8

[8] Prasad, N. R.,"Secure Cognitive Networks", European Wireless Technology Conference, pp. 107-110, 2008.

[9] Qing Zhao and Brian M. Sadler, "A survey of Dynamic Spectrum Access: Signal Processing and Networking Perspectives", Acoustics, Speech and Signal Processing, 2007. ICASSP 2007. IEEE International Conference on, Vol. 4, pp. IV-1349-IV-1352, 2007.

[10] Qihang Peng, Cosman, P.C., Milstein, L.B. "Spoofing or Jamming: Performance Analysis of a Tactical Cognitive Radio Adversary", 46th Annual Conference on Information Sciences and Systems (CISS' 2012), pp. 1-6, 2012.

[11] Yuan Yuan, Bahl, P., Chandra, R., Chou, P.A., Ferrell, J.I., Moscibroda, T., Narlanka, and S.,Yunnan Wu, "KNOWS: Kognitive Networking Over White Spaces", New frontiers in Dynamic Spectrum Access Networks, 2007. DySPAN 2007. 2nd IEEE International Symposium on, pp. 416-427, 2007.

[12] Jack L. Burbank, A. Roger Hammons Jr., and Stenven D. Jones, "A Common Lexicon And Design Issue Surrounding Cognitive Radio Networks Operating In The Presence Of Jamming", Military Communications Conference, 2008. MILCOM 2008. IEEE. pp. 16-19, 2008.

[13] Beibei Wang, Yongle Wu, K.J. Ray, Clancy, T. Charles "An anti-jamming stochastic game for cognitive radio networks", IEEE Journal on Selected Areas in Communications, v 29, n 4, p 877-899, April 2011, ADVANCES IN COGNITIVE RADIO NETWORKING AND COMMUNICATIONS(II)

[14] Husheng Li and Zhu Han, "Dogfight in spectrum: Jamming and Anti-Jamming in Multichannel Cognitive Radio Systems", Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE. pp. 1-6, 2009.

[15] Yongle Wu, Beibei Wang, K.J. Ray, Clancy, T. Charles "Anti-jamming games in multi-channel cognitive radio networks", IEEE Journal on Selected Areas in Communications, v 30, n 1, p 4-15, January 2012, GAME THEORY IN WIRLESS COMMUNICATIONS

[16] Sangeeta Singh and Aditya Trivedi, "Anti-jamming in Cognitive Radio Networks Using Reinforcement Learning Algorithms", Wireless and optical Communications Networks (WOCN), 2012 Ninth International Conference on, pp. 1-5, 2012.

[17] Yi Shi and Y. Thomas Hou, "A Distributed Optimization Algrithom for Multi-hop Cognitive Radio Networks", INFOCOM 2008. The 27th Conference on Computer Communications. IEEE. pp. 1292-1300, 2008.

[18] Shabnam Sodagari and T. Charles Clancy, "An Anti-Jamming Strategy for Channel Access in Cognitive Radio Networks", GameSec'11 Proceedings of the Second international conference on Decision and Game Theory for Security, pp. 34-43, 2011.

[19] Yongle Wu, Beibei Wang, and K. J. Ray Liu, " Optimal Defense Against Jamming Attacks in Cognitive Radio networks using the Markov Decision Process Approach", Global Telecommunication Conference (GLOBECOM 2010), 2010 IEEE, pp. 1-5, 2010.

[20] Wednel Cadeau and Xiaohua Li, "Anti-jamming performance of cognitive radio networks under multiple uncoordinated jammers in fading environment", 46th Annual Conference on Information Sciences and Systems (CISS' 2012), pp. 1-6, 2012.

Received: September 16, 2014 Revised: December 23, 2014 Accepted: December 31, 2014