https://doi.org/10.33778/kcsa.2021.21.1.209

A survey on Rendezvous Algorithms in Cognitive Radio Networks Under Jamming Attacks★

Martin Robin*, Kim Yongchul**

ABSTRACT

The problem of congestion in the licensed radio channels spectrum can be solved by Cognitive Radio Networks (CRN). Several algorithms exist to ensure the rendezvous between Secondary Users (SUs), they are increasingly efficient, allowing faster rendezvous under multiple scenarios. In parallel, several jamming algorithms are developed to counter rendezvous which are also improving. The goal in CRN is to ensure the rendezvous by warding such jammers with robust algorithms. In this paper, we classify various jamming techniques and analyze the performance of various well-known rendezvous algorithms under jamming attacks.

재밍 공격 상황을 고려한 인지무선 네트워크에서의 랑데뷰 알고리즘들에 관한 분석

마틴 로빈*, 김 용 철**

요 약

허가 된 무선 채널 스펙트럼의 혼잡 문제를 해결하는 방법으로 인지무선네트워크(CRN, Cognitive Radio Networks)가 많은 주목을 받고 있다. 보조 사용자 (SU) 간의 랑데뷰를 보장하기 위해 여러 알고리즘들이 존재하며 점점 더 효율적인 알고리즘들이 개발되어 다양한 시나리오에서 빠른 랑데뷰가 가능해지고 있다. 동시에 개선되고 있는 랑데뷰 알고리즘을 공격하기 위해 여러 재밍 알고리즘들이 개발되고 있다. CRN의 목표는 강력한 알고리즘으로 이러한 재밍 공격을 최소화 하여 랑데뷰를 보장하는 것입니다. 이 논문에서는 다양한 재밍 기술들을 분류하고 잘 알려진 여러 랑데뷰 알고리즘들의 재밍공격 상황하에서의 성능을 분석하였다.

Key words : Channel Hopping Scheme, Jamming Attacks, Rendezvous Algorithms, Cognitive Radio Networks.

접수일(2021년 02월 01일), 수정일(1차: 2021년 03월 13일), 게재확정일(2021년 3월 23일)

★ 본 논문은 육군사관학교 화랑대연구소 2021년도 연구활동비 지원을 받아 연구되었음.

* 프랑스사관학교 / 전자공학과(주저자)

** 육군사관학교 / 전자공학과 교수(교신저자)

1. Introduction

With the development of wireless technologies, the radio spectrum is fully filled between licensed users like the Army or communication companies and there is very little space left for unlicensed users. But there are still frequencies unused in the allocated bands. The goal of Opportunistic Spectrum Access (OSA) with the cognitive radio networks (CRNs) is to allow unlicensed users, or secondary users (SUs) to use these spectrum holes without interfere with the licensed users or primary users (PUs). To achieve this, each SU is equipped with a cognitive radio (CR) which can detect and put the user on unused frequencies [8]. In order to exchange data between them several SUs must join the same frequency at the same time, the role of rendezvous algorithm is to make it happen. The difficulties are that users are not aware of each other presence before the rendezvous takes place, the available channels can be different for each user and change dynamically.

Most of rendezvous algorithms are based on the channel hopping (CH). With this technique the time is divided in slots, at each time slot the users change channels until there is several users on the same one at the same time.

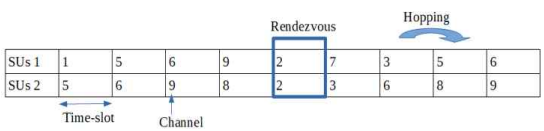

Figure 1 Channel-Hopping

A rendezvous algorithm can be centralized, it means that a server helps all users of the network to meet each other on the same channel. This is more complicated to implement than decentralized algorithms, but feasible for instance: DIMSUMNet [3]. Still, there are issues of reliability with this technique : if a problem occurs with the server nobody can connect, and it is easily jammed. That is why most rendezvous algorithms are decentralized, with no common server for the users.

Each centralized or decentralized is whether with or without a CCC (Common Control Channel). In the case of global CCC, all users, in the case of local CCC, users in the corresponding region can use the CCC to facilitate rendezvous. In practice the CCC are not used because it is difficult to code them, there is a problem of congestion if all users must go on the same channel beside one jamming attack on this channel shut down the entire network. So the algorithms most widespread and resistant to jammers are decentralized and without CCC ie blind rendezvous systems.

Then there are different scenarios for two criteria: time synchronization and channels symmetry. First time synchronization, the situation may require a synchronous or an asynchronous algorithm. The easiest scenario is the synchronous one, when all SUs start their CH sequence at the same time. This is more comfortable to implement than the asynchronous scenario where two SUs begin their CH sequence at different time, there is an offset containing entire time-slots between them. The asynchronous is the most probable scenario, the users do not join at the same time to launch their CH sequences.

SUs 1	1	2	3	4	1	2	3	4
SUs 2	Offset		1	2	3	4	1	2

Figure 2 Asynchronous scenario

Most of the time two users do not have the same available channels, depending on the location of the user in the network, it means that they can not jump on the same channels It is asymmetric. For instance SUs1 set of channels : {1,2,3,4,5} is different from SUs2 set of channels : {3,4,5,6,7}. In the symmetric scenario, all users share the same set of available channels. This model is only suitable when the SUs are close to each other. Some rendezvous algorithm can only work with symmetric scenarios and others operate with asymmetric scenarios.

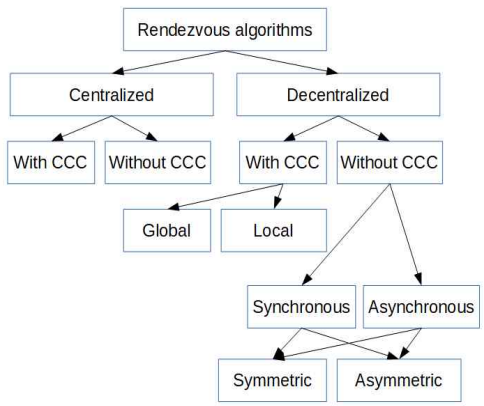

Figure 3 Categories of rendezvous algorithms

Later, we will see that few algorithms need, for instance the ID of the SU in order to differentiate them or to give them roles, like a receiver and a transmitter. Other needs two antennas per SU to work which brings more consumption of money and resources.

There are dozens of rendezvous algorithm, to analyze them we must set some criteria. The most important is the robustness of the algorithm : the rendezvous must happen even if there is a jamming attack on the network. So, we need the algorithm's probability of rendezvous between 80% and 100%. Then there are the time to rendezvous (TTR), maximum TTR (MTTR) and average TTR (ATTR), these are numbers of time-slots. Obviously MTTR only exists if there is a 100 % chance of success, and after robustness we look at the ATTR to find out the fastest scheme possible. Finally we can consider the complexity of the algorithm. This survey paper aims to classify different recent algorithms for rendezvous under jamming attacks. The second part describes the different jamming attacks that are used to disrupt CRN and the third part shows the impact of those attacks on different rendezvous algorithms.

2. Jamming attacks

Since the development of CRs, jamming attacks are a huge problem for wireless networks. Indeed, jammers use the wireless environment to interfere or prevent communications. Thus, rendezvous algorithms that are very efficient and can guarantee a rendezvous quickly, but if those are not impervious to jamming attacks, it will become unusable. That is why CCC and centralized algorithms are so sensible to these attacks, if the jammers happen to find the channel responsible of the control or the server and the whole network is down. Asynchronous and asymmetric models are the most realistic. It will be more interesting to work with algorithms of this type because SUs do not know when their future partner starts the rendezvous process and on which channel it evolves.

There are a lot of different jamming attacks and those are divided into two categories: the elementary and advanced jammers.

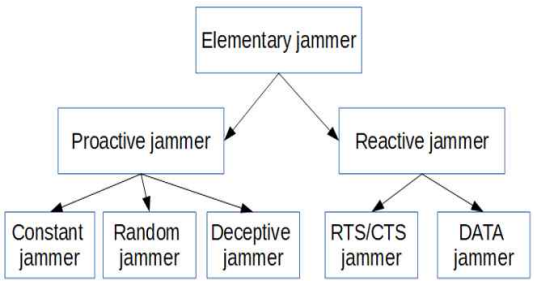

Figure 4 the different elementary jammers

Elementary jammer contains proactive and reactive jammers. The proactive strategy is to send packages of random bits on one channel to interfere and so nobody can use it. Constant jammers send bits to completely occupy all the channels at the same time, the only positive aspect is that this scheme is simple but it is not effective as it is easy to detect by realizing that all frequencies are jammed at the same time. Thus the energy required to jam all the frequencies is considerable and if the band is too large it is impossible to implement. Random jammers transmit amount of bits at random times. This algorithm alternates between two states: sleep and wake phases and saves more energy than the constant jammer, but is still quite ineffective. It is a low probability to hit an SU when the band is large but it is sometimes used when the rendezvous algorithm is unknown. The last category is deceptive jammer, as its name suggests it simulate a transmission by sending regular packets. This one is the less detectable algorithm but is still ineffective.

Reactive jammers works with SUs, it targets one channel and attack when an SU appears on it. This type is more efficient than proactive for two reasons, it saves its energy and difficult to detect as it only sends bits on the channel when the SU is there. When SUs meets, they send different messages: request-to-send (RTS) and then a clear-to-send (CTS) to initiate the transmission. Some jammers are able to detect such messages and jam the channel where the conversation takes place, so that the channel seems occupy and the SUs must move. Another reactive strategy used by data jammer is to wait and scramble the data to disrupt the transmission, hence the SUs must start again the process. This jammer can also disrupt the acknowledgment message sent after the transmission of data so the sender does not know if the other SUs receive its message, forcing to re-transmit the data packets.

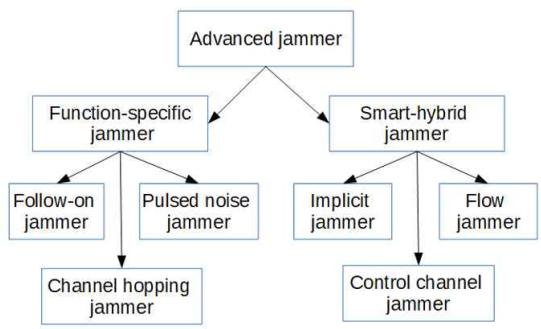

Figure 5 the different advanced jammers

Advanced jammers can be function-specific jammers (FSJ) or smart-hybrid jammer, they are more effective than elementary techniques also more complex and can be proactive or reactive.

FSJ are scheduled by the jammer before the attack takes place, they can focus on one channel to save resources or jam wide parts of the spectra, depending on their functionality. It can be Follow-On Jammer (FOJ) where all channels are used, it scans the network to find the next channel to jam and rapidly hop on it. FOJ is very difficult to

counter with its very high rate of frequency change, thus it is useful against anti-jamming frequency hopping spread spectrum (FHSS) algorithms. Channel Hopping Jammer (CHJ) is able to hop between different channels discretely and it jams multiple channels at the same time. Pulsed Noise Jammer (PNJ) is like a random elementary jammer but can attack different channels at the same time and turn off following a programmed sequence.

Smart jammers are called smart because of their efficiency and effectiveness. The goal of these jammers is to optimize their strategy by focusing on their targets. Thus, they use only the energy needed to almost certainly jam one or more channels. The strategy is to find out the CH sequence of an SU to be able to jam continuously. Control Channel Jammer (CCJ) can take control of control channels or CCC then destroy the entire channel. The second type is Implicit Jammer (IJ) which reduce the speed in the access point of the network until everything is unusable. Finally Flow Jammer (FJ) reduces the traffic flow with different jamming attacks and calculate the minimum power to scramble a packet, it optimizes and makes jamming efficient.

There are well known smart jammers such as Sequence Sensing Jamming Attack (SSJA), Channel Detecting Jamming Attack (CDJA) [4] and Multi-Radio Channel Detecting Jamming Attack (MRCDJA). SSJA is a reactive jammer and its aim is to find out the CH sequence of an SU before the rendezvous takes place. It finds the forward-hop with two listening channels and generate the subsequent CH sequences of an SU. CDJA [9] is a function-specific advanced jammer which prevent the rendezvous between several SUs by estimating the CH sequence, it is similar to SSJA as it was to designed to jam JS algorithm efficiently. It guesses the CH sequences by listening to channels and jam the channels just before the rendezvous happen on them.

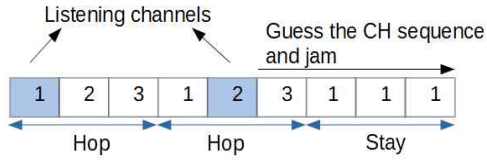

Figure 6 CDJA attack on a JS algorithm with M=3

Furthermore the jammer is able to detect which SUs are senders or receivers in a multi role algorithm. The jammer listens the first channel and then the second one. From the moment it has recovered both channels, the jammer retrieve the forward hop and starts its attack on the future channel. The jammer can estimate the channel hopping sequences within the first jump-pattern while using one or two channels. The MRCDJA is a smart jammer [17] developed to counter Enhanced Jump Stay (EJS) rendezvous algorithm but works as well against all scheme that needs additional information. It is obviously an enhanced version of CDJA. This jammer is able to do several tasks simultaneously: checking if an SU access some channel and listening or blocking many channels. MRCDJA is one of the best jamming attack scheme with its high speed and the impact on several channels at the same time. Using muptiple radios, the MRCDJA is able to detect faster the two channels for its calculation of the next hopping channel and scramble the network with precision. But it comes at a price, it needs more material for listening and more resources to make them work. In the next section we will see how and to what extent

the Rendezvous algorithms resist these jamming attacks.

3. Rendezvous algorithms

There has been extensive work on Rendezvous algorithms, and much of the work has focused on fast and guaranteed rendezvous. In this section, we review the recently proposed rendezvous algorithms for jamming resistance.

<Table 1> List of key notations

Term	Definition
M	Available channels for an SU
P	The smallest prime number greater than M
N	The number of SUs
C	The whole available channel set C= {c_1, c_2, …, c_M}

Full Random (FR) algorithm generates the CH sequences of an SU totally in random. Randomness is the best method to limit any form of jamming because the CH sequence is never deterministic. However, the FR can not guarantee rendezvous.

SSCH (Bahl et al.) [6] allows a low complexity rendezvous under synchronous and symmetric model. In this design, each SUs choose several channel and the CH sequences are determined. As it requires time synchronization and the choice of few channels by the users, this technique is not used and can be easily jammed.

Quorum-based Channel Hopping (QCH)[2] has two variations M-QCH and L-QCH [5]. They both enable rendezvous under asymmetric and synchronous model. The first design ensures ETTR by minimizing the MTTR and the second design guarantees the even distribution of the rendezvous points in terms of both time and frequency. However, these synchronous systems may not be feasible in certain types of networks, for example, ad hoc networks, which rely on a pre-existing infrastructure, such as routers. Moreover, under the assumption of synchronization, the impact of a jamming attack can be significant. Later a variation called A-QCH has been created, it is working under asymmetric and asynchronous model but only for a system with two channels which limits the application of this algorithm.

Generated Orthogonal Sequences (GOS) [4] does not work for asymmetric scenarios but do not need a time-synchronization, SUs use predefined CH sequences which are the same for all users. So the algorithm limits the number of channels used which is interesting to limit the use of a network but as there is a list of obligatory channels it can be precisely targeted by the jammer especially smart ones can easily disrupt it.

Modular Clock (MC) [1] works under symmetric model. Its variation Modified Modular Clock (MMC) enable asymmetric model. Their principle is that each user picks a proper prime number P and randomly selects a rate r which is less than P. Then the user generates its CH sequence with pre-defined modulo operations. With MMC, if the available channel sets of two nodes are different and they select two different prime numbers (say P1 and P2), the users will attempt rendezvous in any pair of channel indices in at most P1P2 time slots and thus the rendezvous is achieved under the asymmetric model. Both do not provide guaranteed rendezvous, but are effective in practice. Random jamming attack can only down the probability of rendezvous to 90% but the SSJA attack can reduce their

effectiveness to 20% rendezvous probability.

Deterministic Rendezvous Sequence (DRSEQ) is only for symmetric model, do not work under asymmetric model and guaranteed rendezvous in at most 2M+1 time-slots. Channel Rendezvous Sequence (CRSEQ) run for both but is weak under symmetric model, rendezvous for asymmetric model in at most P(3P-1). The principle works with triangle number and modular operations.

Ring-Walk (RW) [10] is a blind rendezvous algorithm. SUs walk on the ring by visiting vertices of channels with different velocities, the higher velocity SU will eventually catch the lower velocity SU. Rendezvous is under both symmetric and asymmetric model and the algorithm needs the ID of the SUs. ATTR are O(M*N) and $O(M^2*N)$ respectively for symmetric and asymmetric cases, which is not satisfactory.

Full Diversity Channel Hopping (FDCH) principle is a circular movement of the CH sequences. It has a good ATTR and maximize rendezvous diversity. It is robust under a Smart Jammer attack. Its weakness, like all the deterministic algorithms is with an asymmetric scenario. In the enhanced FDCH-Role-Based (FDCH-RB) algorithm, the rendezvous is established between a transmitter and a receiver (roles are pre-assigned before the rendezvous). Rendezvous is achieved in O(M) time-slots under asymmetric and asynchronous model. FDCH Common Strategy (FDCH-CS) is the same principle but with two cognitive radio antennas by user. ATTR is (T-1)/2 where T is the number of vertices in the ring, so T>M. This is a very good ATTR. CDJA reduces the probability of rendezvous about 90% for the FDCH-RB, 50% for the FDCH-CS. FDCH-CS is indeed more resistant to jamming attack but needs two antennas for each user which makes the algorithm far more complex and consume more resources. A combination of FDCH and FR is a good way to respond to jamming attack, especially smart jamming attack. But it does not provide a finite MTTR. With a judicious use of randomness and determination we can create a hybrid algorithm with a 90% rendezvous probability and a decent ATTR under jamming attacks but without a 100% chance of rendezvous.

Jump-Stay (JS) [7] operate under asymmetric, asynchronous scenarios and it is a blind rendezvous algorithm. Its ATTR is decent under normal circumstances, but it is vulnerable to CDJA in which the jammer can estimate the channel hopping sequences within the first jump-pattern. The jammer can compute the entire channel hopping sequence and thus reduce the rendezvous success rate from 100% to less than 20% and 10% using one and two listening channels respectively. EJS works with modulo operations, ATTR is $O(P^2)$ instead of $O(P^3)$ for the JS. It does not guarantee rendezvous under Multi-Radio Channel Detecting Jamming Attack (MRCDJA), the probability drops to 30%. Random Enhanced Jump-Stay (REJS) algorithm works under the four scenarios. It works in the same way as the EJS algorithm but by adding randomness. This algorithm has a random part which is very effective against jamming, r is randomly chosen in the channel set so each channel has equal probability of being selected. Thus, each channel has the same probability of being used as rendezvous channel.

Alternate Hop-and-Wait (AHW) [11] is a fast blind rendezvous, the goal is to minimize

ATTR. It uses the binary ID of SU to create CH sequences. When the bit equal to zero, an SU launches a Wait-Hop-Hop sequence otherwise it does Hop-Hop-Hop. We obtain the CH sequence when all bits of the ID have been used. It enable rendezvous under jamming attack (95% with 20 channels) but it does not provide guaranteed rendezvous under MRCDJA. The probability for two SUs to meet is 45%. Even if MRCDJA was created to counter EJS algorithms it is also efficient against AHW because they have similar schemes. There are three enhanced AHW algorithms by generating a CH sequence with a modulo operations or random operations: AHW modulo strategy (mod), AHW semi random strategy (semi) and AHW full random strategy (tot). The ATTR results can be reduced from 4 or 3.5T to 2.5T and the probability of rendezvous under jamming attack goes from 45% to between 80% and 100%. The hybrid AHW algorithms are AHWJS and AHWEJ, they do not change the ATTR but the probability to rendezvous is a bit better than the three enhanced AHW algorithms, so they are more robust. The best is the AHWEJS 98% probability to rendezvous under jamming attack.

Interleaved Sequences based on Available Channel set (ISAC) [14] generates CH sequences only based on the available channel instead of the whole network to ensure better performance. The first SU who initiate the rendezvous is the sender and the second is a receiver. ISAC guarantee rendezvous with a MTTR of O(M) for symmetric models and O(M*N) under asymmetric mode, with M and N are the number of available channels of two users.

Role-Based Channel Rendezvous (RCR) [15] is a blind role-based algorithm which works under asynchronous and asymmetric scenarios. An SU_1 lines sequences of M channels and an SU_2 stays randomly on a channel during 2M time-slots. RCR vastly outperform the JS algorithm when there are security concerns about a channel detecting jammer. Especially, the effectiveness of CDJA is negligible for the FR and RCR schemes but their expected time to rendezvous (TTR) is close to the JS's expected TTR[4]. RCR is based on random, like REJS. In fact, the first user generates a random sequence swap. In the same way, the second user remains on a random channel for two time-slots. The jammer cannot detect any CH sequence and unable to find step-length since it changes every time. More recently periodic jump rendezvous (PJR) [12] and enhanced PJR algorithms for role-based and nonrole-based cases were introduced in order to reduce TTR.

Disjoint Relaxed Difference Set (DRDS)[13] works well with asynchronous, asymmetric situations without additional information and ensure rendezvous on every channel. Rendezvous is achieved in O(M) for symmetric model and $O(M^2)$ for asymmetric model. A study was conducted to improve this algorithm under heterogeneous jamming, the interference are different on each channels. The result is the Interference based DRDS (I-DRDS), it ensures rendezvous under jamming using normalization and mapping of interference. A comparison against other recent algorithms showed that I-DRDS has the best rendezvous performance on less interfered channels, with slightly larger rendezvous time in January 2020.

4. Summary

<Table 2> Characteristics of recent algorithms

Algorithms	Guarantee rendezvous	Resistant to jamming (rendezvous under jamming attack)	MTTR (asym)	ATTR (asym)	Further information
FR	No	all of them	infinite	variable	No
FDCH-RB	Yes	No (10% under 1 antenna channel detecting)	$O(M^2)$	$O(M^2)$	Role-based
FDCH-CS	Yes	No (50% under 1antenna channel detecting)	$O(M^2)$	$O(M^2)$	Two antennas per SUs
FDCH+FR	No	Yes (>90%)	infinite	variable	No
JS	Yes	No (20% under CDJA)	$O(MP^2)$	$O(P^3)$	No
EJS	Yes	No (30% under MRCDJA)	$O(P^2)$	$O(P^2)$	No
REJS	No	Yes	infinite	variable	No
AHW	Yes	No (45% under MRCDJA)	O(MPlogN)		ID of SUs
Enhanced AHW	Yes	Yes (between 80% and 100%)			ID of SUs
Hybrid AHW	Yes	Yes (98% for AHW-EJS)			ID of SUs
ISAC	Yes	No	O(MN)		Role-based, available channels
RCR	Yes	Yes	$O(MP^2)$	$O(P^3)$	No
DRDS	Yes	Yes	$O(M^2)$		No

Table 2 summarizes the characteristics of the various algorithms we have mentioned in the previous chapter. For each algorithm, the worst-case scenario TTR was considered and the MTTR and ATTR values in the asymmetric scenario were indicated. Although every algorithm can be applied in both symmetric and asymmetric situations, and time synchronization is not required, we have shown the MTTR and ATTR values in the asymmetric scenario for comparison under the same conditions. Some of them are new technique like ISAC which scan the network for available channel and are not tested under different jamming attacks. For the jamming resistance, 90% probability of rendezvous under jamming attack is enough to be resistant.

5. Conclusion

Most of the proposed rendezvous algorithms did not consider jamming attacks and did not mention the vulnerabilities of jamming attacks, therefore in this paper we mentioned various methods of jamming attacks, and analyzed and presented the vulnerability of jamming attacks for each algorithm. We analyzed as many rendezvous algorithms under jamming attack as possible. Some jamming attacks are smart, powerful but are too expensive to use for a long time. For now there is no perfect algorithm thus a jamming strategy can be imagined to scramble the liaison for each rendezvous scheme. But recent jammers demand a lot of resource with multiple antennas, listening on several channels at the same. Rendezvous algorithms are rapidly

evolving, for instance in 2004 SSCH only worked for symmetric models with time synchronization and now modern algorithms run under asymmetric and asynchronous scenarios. Many methods were considered, like CCC, centralized algorithms, but the best schemes are decentralized and use randomness to achieve rendezvous under jamming attacks without losing guaranteed rendezvous. Moreover those algorithms are constantly improved to be more resistant and fast, often by combining different algorithms. For example, I-DRDS was proposed in 2020 with high rendezvous speed and new ways of dealing with jammers. The next step in the Rendezvous Algorithm is to develop a fast and powerful adaptive smart algorithm in any situation [16].

References

[1] H. Liu, Z. Lin, X. Chu, and Y.-W. Leung, "Taxonomy and challenges of rendezvous algorithms in cognitive radio networks," in Proc. ICNC, pp. 645-649, 2012.

[2] N. C. Theis, R. W. Thomas, and L. A. DaSilva, "Rendezvous for cognitive radios," IEEE Trans. Mob. Comput., vol. 10, no. 2, pp. 216-227, 2010.

[3] M. M. Buddhikot, P. Kolodzy, S. Miller, K. Ryan and J. Evans, "DIMSUMnet: new directions in wireless networking using coordinated dynamic spectrum," in Proc. of IEEE WoWMoM 2005, pp. 78-85, Jun. 2005.

[4] Y. Oh and D. J. Thuente, "Channel Detecting Jamming Attacks against Jump-Stay Based Channel Hopping Rendezvous Algorithms for Cognitive Radio Networks," 2013 22nd International Conference on Computer Communication and Networks (ICCCN), Nassau, 2013, pp. 1-9, doi: 10.1109/ICCCN.2013.6614113.

[5] Bian, K., J. Park and R. Chen. "A quorum-based framework for establishing control channels in dynamic spectrum access networks." MobiCom '09 (2009).

[6] P. Bahl, R. Chandra, and J. Dunagan, "Ssch: slotted seeded channel hopping for capacity improvement in ieee 802.11 ad-hoc wireless networks," in Proceedings of the 10th Annual International Conference on Mobile Computing and Networking, ser. MobiCom'04, pp. 216 - 230, ACM, New York, NY, USA, 2004.

[7] H. Liu, Z. Lin, X. Chu and Y. Leung, "Jump-Stay Rendezvous Algorithm for Cognitive Radio Networks," in IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1867-1881, Oct. 2012.

[8] N. C. Theis, R. W. Thomas, and L. A. DaSilva, "Rendezvous for cognitive radios," IEEE Trans. Mob. Comput., vol. 10, no. 2, pp. 216-227, 2010.

[9] Y.-H. Oh and D. J. Thuente, "Channel detecting jamming attacks against jump-stay based channel hopping rendezvous algorithms for cognitive radio networks," 2013 IEEE ICCCN, pp. 1-9, Jul.-Aug. 2013.

[10] H. Liu, Z. Lin, X. Chu, and Y. W. Leung, "Ring-walk based channel-hopping algorithms with guaranteed rendezvous for cognitive radio networks," in Green Computing and Communications (GreenCom), 2010 IEEE/ACM Int'l Conference on Int'l Conference on Cyber, Physical and Social Computing (CPSCom), pp. 755 - 760, Hangzhou, China, December 2010.

[11] I. H. Chuang, H. Y. Wu, and Y. H. Kuo, "A fast blind rendezvous method by alternate hop-and-wait channel hopping in cognitive radio networks," IEEE Transactions on Mobile Computing, vol. 13, no. 10, pp. 2171 - 2184, 2014.

[12] S. Salehkaleybar and M. R. Pakravan, "A periodic jump-based rendezvous algorithm in cognitive radio networks," Computer Communications, vol. 79, pp. 66 - 77, 2016.

[13] Z. Gu, T. Shen, Y. Wang and F. C. M. Lau, "Efficient Rendezvous for Heterogeneous Interference in Cognitive Radio Networks," in IEEE Transactions on Wireless Communications, vol. 19, no. 1, pp. 91-105, Jan. 2020, doi: 10.1109/TWC.2019.2942296.

[14] Yu, L., Hai Liu, Y. Leung, Xiaowen Chu and Zhiyong Lin. "Efficient Channel-Hopping

Rendezvous Algorithm Based on Available Channel Set." ArXiv abs/1506.01136 (2015): n. pag.

[15] EO Guerra, VA Reguera, RD Souza, G Brante, EMG Fernandez, Simple role-based rendezvous algorithm for cognitive ad hoc radio networks. Electron. Lett. 50(3), 182 - 184 (2014).

[16] R. Gandhi, C. Wang and Y. C. Hu, "Fast rendezvous for multiple clients for cognitive radios using coordinated channel hopping," 2012 9th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON), Seoul, 2012, pp. 434-442.

[17] Y.-H. Oh and D. J. Thuente, "Jamming and advanced modular-based blind rendezvous algorithms for cognitive radio networks," 2016 IEEE WoWMoM, pp. 1-10, Jun. 2016.

〔저자소개〕

마틴로빈 (Martin Robin)
2021년 2월 : 프랑스 사관학교 전자공학과 석사
email : martin.robin71@gmail.com

김 용 철 (Yongchul Kim)
1998년 2월 : 육군사관학교 전자공학과 학사
2001년 11월 : University of Surrey 전자공학과 석사
2012년 1월 : North Carolina State University 전자공학과 박사
2012년 6월 ~ 현재 : 육군사관학교 전자공학과 교수
email : kyc6454@mnd.go.kr