https://doi.org/10.7840/kics.2023.48.1.47

인지 무선 네트워크 환경에서의 전파방해 공격방법에 관한 연구

가이 스켈쳐•, 루도빅 포지*, 김 용 철°

A Survey on Jamming Attack Methods in a Cognitive Radio Network Environment

Guy Schelcher•, Ludovic Forzy*, Yongchul Kim°

요 약

무선 통신 분야의 기술은 빠르게 발전하고 있으며 많은 연구가 진행되고 있다. 불행하게도 무선통신은 전파를 통해 전송되므로 악의적인 사용자의 간섭이 끊임없이 발생하고 있다. 이러한 간섭은 재밍 공격의 한 형태로서 군 전자전 상황에서도 사용될 수 있다. 한편, 무선통신 서비스의 수요가 급증함에 따라 주파수 부족 현상이 발생하고 있으며, 더욱이 주파수 스펙트럼 대역의 남용은 점점 더 우려되는 현상이 되었다. 이러한 문제를 해결하기 위하여 인지 무선 네트워크 기술이 많은 관심을 받고 있으며 군에서도 활용 방안을 고민하고 있다. 인지 무선 네트워크에서는 2차 사용자들이 일반적으로 합법적인 가입자인 1차 사용자들이 사용하지 않는 채널을 사용하게 된다. 이 논문은 인지 무선 네트워크 환경에서 가장 단순한 성능의 재밍으로부터 가장 정교한 성능의 재밍방법까지 다양한 종류의 방해 전파 방법에 대하여 분석하고 특히 군 작전상황에서 활용될 수 있는 인지 무선 네트워크 시나리오와 그에 대응할 수 있는 재밍 방법을 제안하고자 한다.

Key Words : Jamming Attack, Cognitive Radio, Channel-Hopping, Rendezvous Algorithm, Military Communications

ABSTRACT

Start after striking The technologies in the wireless telecommunication field are rapidly developing and a lot of research is being conducted. Unfortunately, as communications are transmitted through electromagnetic waves, any malicious user can provoke interferences. These interferences, therefore, represent a jamming attack and can be used in military electronic warfare. On the other hand, as the demand for wireless communication services has rapidly increased, a frequency shortage has occurred, and overuse of the spectrum bands has become an increasingly concerning phenomenon. To solve this problem, the use of Cognitive Radio Networks (CRN) is receiving a lot of attention, and the military is also planning to use it. The CRN secondary users typically use channels that legitimate primary users are not using. This article presents a study of different kinds of jamming, from the simplest to the most sophisticated, in the context of CRN. In particular, we propose CRN scenarios that can be used in military operational situations and jamming methods that can respond to them.

※ 본 논문은 육군사관학교 화랑대연구소의 2022년도 연구활동비 지원을 받아 연구되었음.
◆ First Author : Korea Military Academy Department of Electrical Engineering, guy.schelcher73@gmail.com, 학생회원
° Corresponding Author : Korea Military Academy Department of Electrical Engineering, kyc6454@kma.ac.kr, 종신회원
* Korea Military Academy Department of Electrical Engineering, l.forzy@outlook.fr
논문번호 : 202211-270-B-RU, Received November 2, 2022; Revised November 15, 2022; Accepted November 21, 2022

Ⅰ. Introduction

Cognitive Radio Network (CRN) is a new wireless communication technology providing an answer to the lack of channels available in unlicensed spectrum bands. Indeed, the latter are overused whereas the licensed spectrum bands, which are reserved for specific users, remain unused most of the time. This technology relies on the fact that cognitive radios can sense the licensed spectrum bands and use the free channels as secondary users (SU). The legitimate users of the licensed spectrum bands are the primary users (PU), which have priority access to the channels compared to SUs[1].

To scan the available channels and the presence of other SUs to communicate with, SUs use the channel hopping (CH) mechanism, namely their ability to hop from channel to channel. When two or more SUs meet on the same channel, there is a rendezvous and the transmission begins.

There are two metrics used to analyze a rendezvous algorithm. First, the Average Time To Rendezvous (AVTTR) refers to the average time for two SUs to rendezvous. Secondly, the Max Time To Rendezvous (MTTR) is the time when two SUs have a rendezvous in the most complicated case: if it is infinite, the algorithm does not guarantee a rendezvous to occur. Furthermore, rendezvous algorithms can be divided into two categories, centralized and decentralized.

The present document consists of a comparison of jamming abilities against CRN. It is organized as follows: first, the rendezvous algorithms will be presented. Then, in the second part, a classification of the jamming capabilities will be established. Finally, some military scenarios, involving CRNs, where jamming abilities would be useful, will be provided.

Ⅱ. Rendezvous Algorithms

Rendezvous Algorithms refer to the different processes that can be used in a CRN to ensure two SUs to have a rendezvous with each other, as depicted in Figure 1, there are two main categories

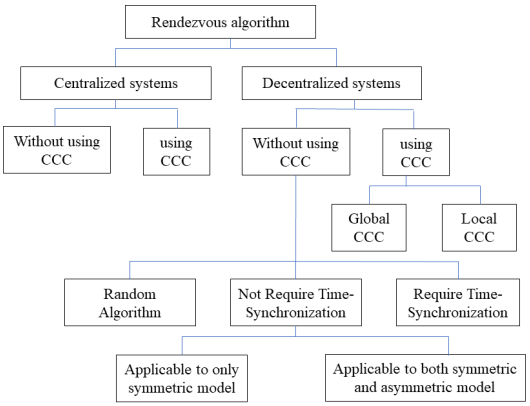


Fig. 1. Diagram of the different types of rendezvous algorithms [1].

of rendezvous algorithms, centralized and decentralized. The centralized one will be depicted first, then the decentralized one, which is more interesting for our study, will be exposed.

Centralized CRN is a type of network in which a dedicated user (the server) assists the other SUs to rendezvous. For instance, the server can collect the sensing data of the SUs to know the global spectrum environment and help SUs in rendezvous. A centralized CRN can be used with or without a Common Control Channel (CCC). A CCC refers to preselected channels, which remain available for all users to assist with the rendezvous protocol and can help SUs with synchronization, for example. In centralized CRN, the CCC is commonly occupied by the server as it is mentioned in [2]. These types of networks are not realistic in a military context. Moreover, given their weakness against most of the jammers, such networks will be put aside for the rest of our study, to focus on more robust solutions against jamming attacks.

Decentralized CRN is a more realistic type of network, where all SUs need to find rendezvous on their own. As well as the centralized case, it can work with a CCC, which will be available to all SUs to facilitate their rendezvous. In our study, the focus will be made on decentralized systems which do not use CCC. As said before, CCCs represent a weakness against a jamming attack and can compromise the entire network. SUs have to proceed with blind rendezvous: this term refers to all the CH

algorithms in a decentralized network without CCC. The primary interest of the blind rendezvous is the use of the CH technique. Indeed, the key lies in the generation of a hopping sequence, to guide two SUs toward a common chain and establish rendezvous in the same time slot as soon as possible. Among these technical blind rendezvous, many algorithms exist. The most straightforward, random algorithm is based on the generation of a perfect random CH sequence. The Adaptive Multiple Rendezvous Control Channel (AMRCC), in [3], improves on this concept by increasing the chances of appearing in the CH sequence on channels with the least interference with PUs. Although the randomness of CH sequences makes them less vulnerable to jamming attacks, random algorithms do not guarantee a rendezvous in a finite time, which is its biggest flaw. Some decentralized algorithms work based on time synchronization. The SUs of the network use the same time slot. In addition, they try to establish a rendezvous at a common start. Therefore, the probability of getting a connection between two SUs is increases, but this case is not realistic. Then, there are the rendezvous algorithms that do not require time synchronization. In that case, the algorithms are adjusted so that the SUs can meet even if they do not start their sequences simultaneously, or if they do not have the same time base. Among them, we can mention the Generated Orthogonal Sequence (GOS) in [4], where users use the same channel hopping sequence to find each other, or the Asynchronous Efficient Channel Hopping algorithm (ASYNC-ECH), which distributes the load and the rate of use of the channels, in addition to lowering the TTR. Furthermore, these asynchronous algorithms can be used in a symmetrical or asymmetrical case. The symmetric case refers to networks where all SUs share the same available channels, which is not always the case especially when two SUs are geographically distant. We nevertheless consider them in this survey, to schematize a geographically isolated network, for example. The probability to get a rendezvous is higher compared to an asymmetric case.

SU_1	1	2	3	4	5	1	**3**	5	4	2
SU_2	3	6	8	7	4	8	**3**	4	6	7

Fig. 2. Asymmetric case

SU1 = {1, 2, 3, 4, 5}
SU2 = {3, 4, 6, 7, 8}

Indeed, the most studied and interesting case is the asymmetrical case, where the SUs wishing to communicate with each other do not necessarily have the same number of available channels, and the same length of time slot. Figure 2 and the paper in [1] illustrate the asymmetric case. One can see that, in the two random CH sequences of SU1 and SU2, the only common channels between the two SUs are SU1 ∩ SU2 = {3, 4}. The two SUs only rendezvous on channel 3. The crossed-out channels indicate time slots on which a common channel is used by one of the two SUs, without getting a rendezvous. This emphasizes that the TTR is often higher in an asymmetric case than in a symmetric one. The algorithms under study are numerous. To provide a detailed analysis of the performance of certain jamming processes, we will return to the various decentralized and asymmetrical algorithms later on.

Ⅲ. Jamming attack methods

In this survey, jamming methods that can be used against a cognitive radio network are presented. As mentioned above, the jamming methods are considered in the framework of a decentralized network, in blind rendezvous, which is the closest to the real scheme. The survey especially focuses on asynchronous and asymmetric algorithms because they are the most effective against jamming attacks. These methods are gathered in three classes of increasingly sophisticated capabilities as shown in Figure 3. The elementary abilities can sense the spectrum bands but simply choose a channel and occupy it actively, to restrict the number of existing channels. The intermediate abilities are the ones that can act on different channels during a period of

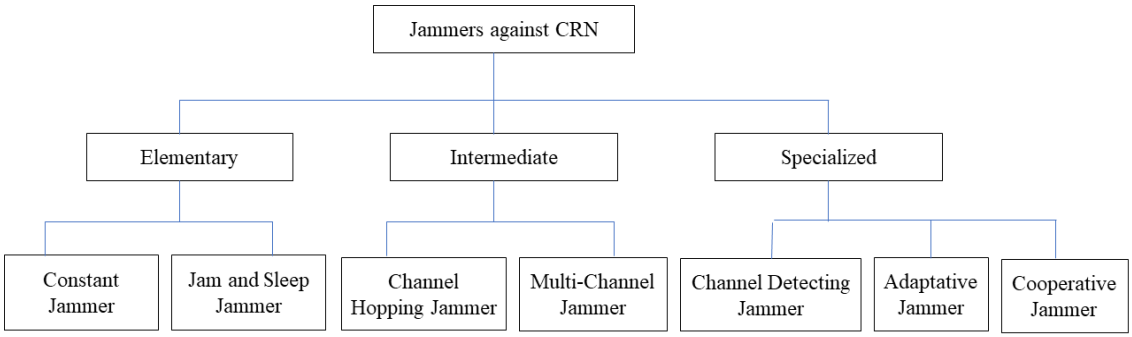


Fig. 3. Diagram of the different Jamming abilities in CRN

several time slots. The specialized jammers are the most suitable for attacking a CRN, they have a high analysis capability and adapt to the algorithm they are attacking.

3.1 Elementary Jammer

The first kind of jamming has been called "elementary abilities''. These jammers are not focused on finding SUs, but they try to attack only a selected and available channel. Thus, the number of available channels in the spectrum is reduced which makes the rendezvous task more complex. These jammers can set up on an available channel and send data, leading to maintaining this channel out of use for SUs, as described in Figure 4. As they are occupying a channel for a long period, this type of jammer is efficient in a network with few channels.

The first one, which is the simplest one, is the constant jammer. When it is set up on a channel, it proceeds to continuously send continuously random bits. As a result, the channel it chooses remains busy and could no longer be used by any users. As depicted in Figure 4, the constant jammer is working on every time slot, however, this could lead to an issue of energy consumption as underlined in [5]. Moreover, because of its constant activity, it is easy to be detected.

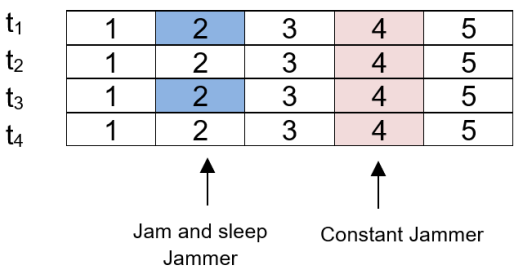


Fig. 4. Jam & Sleep and Constant jammer operating diagram.

The solution found to counter the energy issue is the Jam and Sleep jammer[6]. It works in two phases, a jamming phase, and a sleeping phase. During the jamming phase, it transmits random bits, on a single channel, as well as the constant jammer. The sleeping phases, where the jammer is not acting, are used to save energy, the distribution between the two phases can be random or predefined. Of course, it cannot jam during its sleeping phase, so one has to weigh the jamming efficiency against the energy saving. The process of a JS jammer is illustrated in Figure 4, during time slots 1 and 3, the jammer is working, and it uses the time slots 2 and 4 to sleep.

3.2 Intermediate Jammer

Intermediate capability jammer consists of jammers that can act on several channels. This category contains the jamming abilities which have an impact on many channels during a period of several time slots. However, it cannot organize and adapt itself to the function of the network environment.

Channel Hopping Jammer (CHJ) identifies available channels and jumps over them to jam, as illustrated in Figure 5. It only jams one channel per time slot, which gives it a high power of jamming. If it is detected by a SU, which switches its channel,

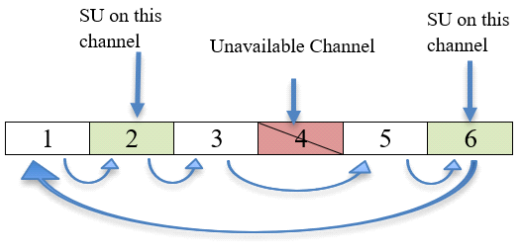


Fig. 5. Channel Hopping Jammer Process

the jammer jumps to another available channel, therefore, even if it is easy to detect, it is difficult to counter. Figure 5 presents the simple process of the CHJ, which is to jump from the nearest channel to the nearest channel. However, this sequence makes it very detectable and predictable. It is better to use a process where its sequence is established, after a sensing phase, pseudo-randomly, as described by Alnifie G, Simon R and in the two papers[7,8].

A Multi-Channel jammer (MCJ) can jam several channels at once, thanks to its number of antennas, it may also change the channels. Figure 6 shows in the two first columns an MCJ jammer fixed at any time slot on channels 5 and 6. While channel 8 is unavailable. Such abilities give it great efficiency. However, when a jammer operates on multiple channels, it must be careful about the power it allocates on each channel. The more channels it focuses on, the less power it will allocate to each one, and the less effective it will be. The power allocation and the efficiency of energy are therefore a prominent issue.

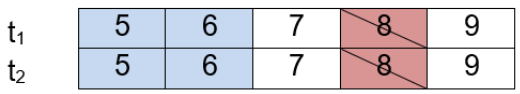


Fig. 6. Multiple Channel Jammer Process

3.3 Specialized Jammer

Specialized jammers have jamming abilities that are very relevant to the specific case of CRN. They often possess an intermediate capability, as mentioned above, but with the help of network activity surveys, they can adapt to the network and become more versatile.

Channel Detecting Jammer attacks (CDJA) are based on sensing multiple channels with its antennas. Thanks to its various readings, it may be able to recognize some recurring CH algorithm sequences. Then, it can compute parts of the SU's sequence thanks to the sensing process. During its missing parts of the CH sequence, it might well attack randomly the undetected channels as mentioned in [9]. In [10], Young-Hyun and Thuent developed a Symmetric Channel Detecting Jamming (SCDJ) attack and Asymmetric Channel Detecting Jamming (ACDJ) attack. These two jammers are CDJA that work in the special context of a Jump Stay algorithm. They have proven to be very effective, even reducing the probability of an appointment from 100% to less than 30% for the ACDJ, in the case of an Enhanced Jump Stay algorithm.

The Adaptive Jammer (AJ) can use all intermediate or elementary capabilities. Its purpose is to seek out the most effective process, depending on the state of its environment, while looking for efficient use of its energy. For instance, if the number of available channels is very small, AJ would choose an elementary jammer's ability to occupy a channel and reduce the number of available channels. In this case, this is the best way for it to be energy.

Cooperative jammers are a potential kind of jamming attack using a network of jammers. There are two ways of using multiple jammers, the simple one is only to use all of them together, but they do not share any information. However, by using the first option, the attacks are not organized, and two jammers could jam the same channel, for instance. When using multiple jammers, the better way is to use a cooperative way to gain efficiency in the jammers' attack. They cooperate by sharing their information about the network jammed. By using them cooperatively, energy can be saved. This cooperative jammer network can be used with all previous jammers, which gives it a great deal of versatility and a flexible appearance from one network to another.

One of the common capabilities of jammers that

has not been classified here is the deceptive one. The deceptive ability is how a jammer used proper packets to act as a true user. By doing so, a jammer can usurp a SU or a PU. This ability is considered being suitable for all previous jammers mentioned.

Ⅳ. Military application

Possessing the ability to jam enemy telecommunications in a war context can give a significant advantage and is one area of electronic warfare. Indeed, during the Russian invasion of Ukraine, jamming was used extensively to disrupt the Ukrainian army.

CRNs are particularly used in the military environment[11], indeed they are very robust to the variation of the network, because of their rendezvous mechanism and thus can easily reboot after a disconnection, which is often the case in the field. Moreover, there are algorithms such as Random Enhanced Jump Stay and Fast and Robust Asynchronous Rendezvous Scheme (REJS and FRARS) that seemed to be very efficient against jammers[10,12].

The first case considered is the communication used when attacking with a Remote Improvised Explosive Device. For example, it was observed during the Afghan war, but also during the fight against Jihadism in the Sahel, that many Improvised Explosive Devices IEDs were detonated with the help of remote devices. The communication between the bomb and the attacker is established using two mobile phones. In our context, the two devices are linked via mobile operators using CRN technology. The enemy sends a signal when an allied troop is deployed near the explosive, to scramble a convoy or to damage vehicles. As shown in Figure 7, armoured vehicles could therefore be equipped with jammers, which would prevent a link between the trigger and the explosive in order to be protected from the IED.

One jammer that could be used, in the case of CRN utilization in this attack model, would be the MCJ. Indeed, most mobile phones use well-known frequency bands (e.g. 3.5 MHz). The MCJ could

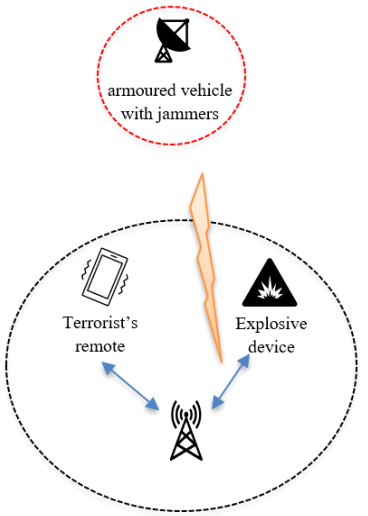


Fig. 7. Application of a jammer on the battlefield

therefore focus on bands that are likely to contain a phone signal. This could reduce the likelihood of an attack.

In a symmetrical conflict between two forces of equal size, the use of CRNs could be considered in a joint battle group structure. For example, the information gathered by fighter jets is transmitted through wireless communications. The latter need to communicate with each other, as well as with the troops on the ground. In addition, the combat helicopters must also be in contact with the men on the ground, with the base, but also with the fighter aircraft, as shown by Figure 8. The military forces could as well do without CRN technology, however, they can be useful in a conflict area where a civilian network is already developed and crowded (e.g.

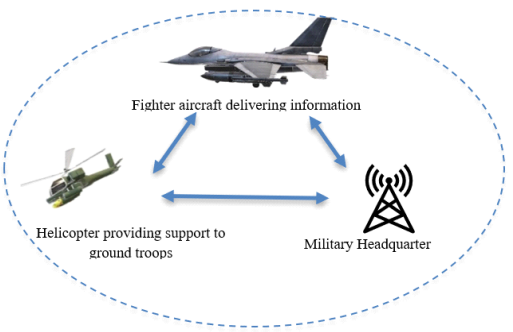


Fig. 8. Use of CRNs by an armed force

telephone operators). Indeed, using CRNs would allow the forces present to establish communication even when the spectrum is already saturated. A large-scale electronic attack on a base using telecommunications jamming could slow down enemy action by removing the monitoring capability of drones. The use of a variety of adaptive jammers would be complicated to set up, but extremely disruptive to the enemy.

Ⅴ. Conclusion

Based on a general study of CRN schemes, we have, with the help of documentation on the different jammers and blind rendezvous algorithms, proceeded to a classification of the different jamming techniques that can be used against these algorithms. They were classified between elementary, intermediate, and specialized according to their main characteristics and major defects. Today, specialized jammers are the best equipped to deal with CRNs. A great revolution for our jamming capabilities would be to develop a jammer that can identify the used algorithm to act more efficiently against it.

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] Y. Kondareddy, P. Agrawal, and K. Sivalingam, "Cognitive radio network setup without a common control channel," in *Proc. IEEE MILCOM*, pp. 1-6, Nov. 2008.

[3] C. Cormio and K. R. Chowdhury, "Common control channel design for cognitive radio wireless ad hoc networks using adaptive frequency hopping," *Ad Hoc Networks*, vol. 8, pp. 430-438, 2010.

[4] N. C. Theis, R. W. Thomas, and L. A. DaSilva, "Rendezvous for cognitive radios," *IEEE Trans. Mob. Comput.*, vol. 10, pp. 216-227, 2011.

[5] K Grover, "Jamming and anti-jamming techniques in wireless networks: A survey," *Int. J. Ad Hoc and Ubiquitous Comput.*, vol. 17, no. 4, pp 197-215, 2014.

[6] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. 6th ACM Int. Symp. Mob. Ad Hoc Netw. and Comput.*, pp. 46-57, 2005.

[7] G. Alnifie and R. Simon, "A multi-channel defence against jamming attacks in wireless sensor networks," in *Proc. 3rd ACM Wkshp. QoS and Secur. Wirel. and Mob. Netw.*, pp. 95-104, 2007.

[8] G. Alnifie and R. Simon "MULEPRO: A multi-channel response to jamming attacks in wireless sensor networks," *Wireless Commun. and Mob. Comput.*, vol. 10, no. 5, pp. 704-721, 2010.

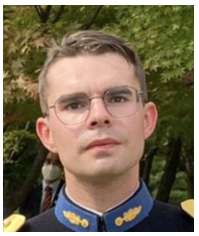
[9] Y.-H. Oh and D. J. Thuente, "Channel detecting jamming attacks against jump-stay based channel hopping rendezvous algorithms for cognitive radio networks," in *Proc. ICCCN*, pp. 1-9, 2013.

[10] Y.-H. Oh and D. J. Thuent, "Jamming and advanced modular-based blind rendezvous algorithms for cognitive radio networks," in *Proc. WoWMoM*, pp. 1-10, 2016.

[11] B. Bharti, P. Thakur, and G. Singh, "A framework for spectrum sharing in cognitive radio network for military applications," in *IEEE Potentials*, vol. 40, no. 5, pp. 39-47, Sep.-Oct. 2021.

[12] Y. Kim, "Fast and robust asynchronous rendezvous scheme for cognitive radio networks," *Applied Sci.*, vol. 9, no. 12, 2481, 2019. (https://doi.org/10.3390/app9122481)

가이 스켈쳐 (Guy Schelcher)



Guy Schelcher was born in Saint Julien en Genevois, Rhone-Alps, France, in 2000. He is specialized in electronic engineering and currently pursuing a master degree.

루도빅 포지 (Ludovic Forzy)

Ludovic Forzy was born in Suresnes, le-de-France, France, in 1999. He is specialized in electronic engineering and currently pursuing a master degree.

김 용 철 (Yongchul Kim)

1998년 3월 : 육군사관학교 전자공학과 학사

2001년 11월 : University of Surrey, UK 전자공학과 석사

2011년 12월 : North Carolina State University, USA 전기컴퓨터 공학과 박사

2012년 2월~현재 : 육군사관학교 전자공학과 부교수

<관심분야> WiMAX, Relay Networks, Ad-hoc Networks, Wireless Jamming.