A Study on How to Attack Secondary Users in Blind Rendezvous Cognitive Radio Networks

Guy Schelcher, Ludovic Forzy, Yongchul Kim

Korea Military Academy

l.forzy@outlook.fr, guy.schelcher73@gmail.com, kyc6454@kma.ac.kr

Abstract

Technologies in the field of wireless telecommunications have fueled active research during the last few years. Unfortunately, as communications are transmitted through electromagnetic waves, any malicious user can provoke interferences. Therefore, these interferences represent a jamming attack, which can be used within the electronic warfare framework. Indeed, a jammer trying to block a communication between two or several users represents a threat. Additionally, the spectrum bands overuse has become a growing cause for concern. Thus, the use of Cognitive Radio Networks (CRN) has become key: with these networks, users are redirected to available channels usually booked by subscribers. This study focuses on the different kinds of jamming attacks, from the simplest to the most sophisticated ones, in the context of CRN.

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 are able to sense the licensed spectrum bands and use the free channels as secondary users (SU). The legitim 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 begin. Furthermore, rendezvous algorithms can be divided into two categories, centralized and decentralized. We will work with decentralized rendezvous algorithms, based on the asynchronous operation of the channel hopping sequence. Many algorithms exist to guarantee a rendezvous.

In this paper, jamming methods that can be used against a cognitive radio network are presented. They are all represented in the figure 2. 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.

II – Jamming attack

One of the common capabilities of jammers is to deceive an SU by sending data, they make the SUs believe they are primary users. The first kind of jamming has been called “elementary abilities". These jammers are not focused on finding SUs by sensing the spectrum bandwidths, but they try to attack only on a selected channel. Thus, the number of available channels in the spectrum is reduced which makes the rendezvous task more complex. The two kinds of jammer are illustrated in figure 1.

These jammers have the capability to set up on an available channel and to send data, leading to maintaining this channel out of use for SUs, as described in figure 2. They can be effective because they only transmit on one channel and therefore have a high transmission power.[2]

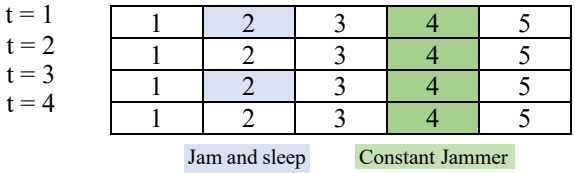

Figure 1. Elementary jammer operating diagram.

The first elementary jammer is the constant jammer. When it is set up on a channel, it proceeds to continuously send random bits. So that it does not respect any communication protocol. Moreover, it prevents all other users from transmitting as the channel is overloaded. So that the channel chosen remains busy. Then, we can mention the elementary jam and sleep jammer. That one counter the energy issue as it works in two phases: a jamming period and an inactivity period. The distribution between the two phases can be random or predefined.

Intermediate capability jammer consists of jammers that can act on several channels. It works in two simultaneous phases, a scanning phase, when the jammer identifies the available channels, and a jamming session. However, even if the jammer can jam the whole network, it does not have the capacity to understand how the algorithm behind the network works.

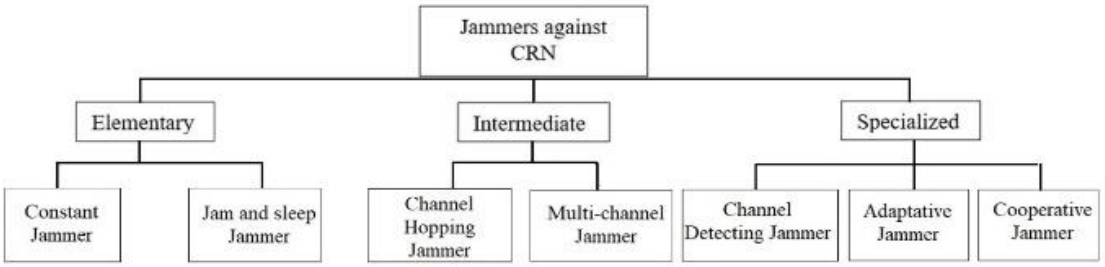

Figure 2. Diagram of the different Jamming abilities in CRN.

Channel Hopping Jammer (CHJ) identifies available channels and jump proactively over them, as illustrated in figure 3. It only jams one channel at a time for a very short time, which gives another angle of attack different from the constant jammer.

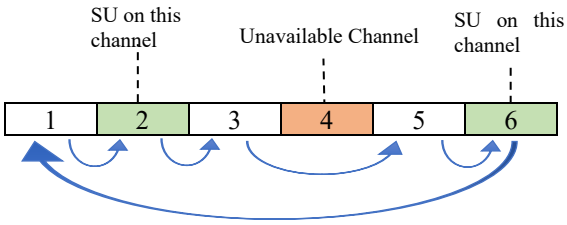

Figure 3. Channel Hopping Jammer Process scheme.

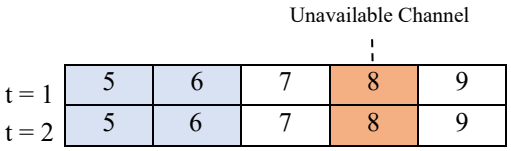

Figure 4. Multiple-Channel Jammer Process scheme.

Multi-Channel jammer (MCJ) can jam several channels at once, thanks to its very large number of antennas, it mays also change the channels. Figure 4 shows in blue a jammer fixed at any time on channels 5 and 6. While channel 8 is unavailable. Such abilities give it a great efficiency. However, when a jammer operates on multiple channels, it must be careful about the power it allocates in 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 is therefore a great issue.

Specialized jammers gather jamming abilities that are very relevant in the specific case of CRN's attacks. Channel Detecting Jammer attacks (CDJA) is 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.[3]

The Adaptive Jammer (AJ) is a jammer able to 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 an efficient use of its energy. For instance, if the number of available channels is very small compared to the number of SUs, AJ will choose an elementary jammer 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 efficient while remaining annoying.

Cooperative jammer is a potential kind of jamming attack. When multiple jammers are used, they can be considered as single jammers. However, by doing so, they lose efficiency. Different jammers can cooperate by giving each other additional information about the network to be jammed. This can prevent, for instance, two jammers working together from ending up on the same channel. By using them cooperatively, efficiency increase.

III - Conclusion

The non-exhaustive list of jamming ability against CRNs has been depicted. They were classified between elementary, intermediate, and specialised according to their main characteristics and major defects. Today, specialised jammers are the best equipped to deal with CRNs, but they are not able of computing the CRN algorithm CH sequences. A great revolution for our jamming capabilities would be to develop a jammer which can identify the used algorithm in order to act more efficiently against it.

References

[1] Hai Liu, Zhiyong Lin, Xiaowen Chu, Yiu-Wing Leung, Taxonomy and Challenges of Rendezvous Algorithms in Cognitive Radio Networks.

[2] Kanika Grover, Alvin Lim and Qing Yang, Jamming and Anti-jamming Techniques in Wireless Networks: A Survey.

[3] Enguerrand Negrello and Yongchul Kim, Enhanced FDCH Rendezvous Algorithm against Jamming Attack in Cognitive Radio Networks.