# On The Impact of Jamming Attacks on Cooperative Spectrum Sensing in Cognitive Radio Networks

V. Balogun
Computer Science Department
University of Idaho
Moscow, ID 83844-1010
balo8072@vandals.uidaho.edu

A. Krings
Computer Science Department
University of Idaho
Moscow, ID 83844-1010
krings@uidaho.edu

## ABSTRACT

*Cognitive Radio* (CR) Networks have been identified in recent literature as having great potential in realizing distributed shared communications, especially the ability to ensure broadband access of limited resources by opportunistically sharing spectrum with the incumbent users. Since the CR uses wireless communication and inherits all of its associated security threats, it is of paramount importance to fully investigate the impact of malicious faults like jamming attacks on CR networks under different fault scenarios. This research investigates CR Networks in the presence of Jamming attacks based on fault-model classification. A hybrid Jamming mitigating approach is proposed to better handle the affect of malicious jamming nodes under consideration of hybrid fault models.

**Keywords**: Cognitive Radio, Jamming, Fault Models, Spectrum Sensing

## 1. INTRODUCTION

Cognitive Radio (CR) [1], has been proposed as the solution to the Spectrum shortage/underutilization problem [14]. In an Overlay CR approach, the general idea is to allow incumbent users to share the spectrum with unlicensed users during their OFF period in a non-interference manner. The Cognitive Radio Network Standard does not allow any level of interference to the Incumbents and does not permit any modification to the Incumbent Networks. The need to sense the spectrum for the presence of an incumbent is a challenging one. Accurate detection of the presence of a primary user could be significantly affected by impairments like shadowing and multipath fading. *Cooperative Spectrum Sensing* (CSS) [2], either in a centralized or distributed architecture, have been found to be effective in countering these impairments. Despite the expected success and potential of CSS as reiterated by its proponents, security consideration of CSS operating in the presence of malicious users is of great importance.

The flexibility and adaptable features of CRs make them vulnerable to security threats like jamming attacks, *Primary User Emulation* (PUE) attacks, masquerading of CR, *Spectrum Sensing Data Falsification* (SSDF) attacks and many more that are either specific to CRs or inherited from traditional wireless networks. Jamming, which is the main focus of this paper, has been addressed by different authors [9, 15, 21, 24] with respect to traditional wireless networks and different anti-jamming techniques have been proposed. There is a need to investigate the performance of CRs in the presence of jammers since CR networks differ significantly from traditional wireless networks. Though several authors [3, 7, 8, 23] have published work on Jamming in CR Networks, to the best of our knowledge none have studied jamming in the context of fault model classifications (including value faults) and their respective fault handling.

**Contributions**: Jamming and its impact on CR are presented in the context of hybrid fault models and a classification is given that considers transmissive and omissive value faults. Traditional approaches and the faults they can deal with are put into context and a hybrid forward error correction (FEC) code is proposed for mitigating Jamming in Fault-Model-Classified CRNs considering value faults.

## 2. BACKGROUND

**Traditional Jamming**

In traditional wireless communications, a jammer can cause *Denial of Service* (DoS) at either the transmitter or the receiver if it adequately injects interfering signals into the same spectral region [9]. Different forms of jamming, which can even interfere with signals of interest by preying on signal characteristics like modulation type or error control coding, have been identified by [7]. These include Broadband Noise Jamming, Narrowband Continuous Wave Jamming, Swept Continuous Wave Jamming and Pulsed Jamming. Jammers use several techniques to carry out their malicious act. A jammer might target a specific frequency (spot jamming), sweeps across available frequencies (sweep jamming) or jam a range of frequencies at once (barrage jamming). Jamming could even be done in a coordinated way [20] such that several jammers collaborate to gain the knowledge of the network with the intent of efficiently reducing the throughput of the network.

Different classes of jammers have also been identified by [15, 24]. These include: *Constant/Static Jammer*, which emits jamming signals continuously on a specific channel, *Random Jammer*, which alternates between jamming and sleeping, *Deceptive Jammer*, which continuously transmits jamming signals but in this case the pulses seem similar to regular data packets from a legitimate user, *Reactive Jam-*

*mer*, which unlike all the previous jamming types transmits jamming pulses only when it finds the channel to be busy so as to cause collision to an on-going transmission, and *Intelligent Jammer*, which is not a physical layer attack like other jammers but targets upper layers for specific control messages like CTS, RTS, and ACK. Intelligent jammers are more efficient with respect to power usage and they are very difficult to detect.

**CSS Architecture in CR Networks**

Isolated/non-cooperative spectrum sensing of Cognitive Radios has been found to be ineffective as CR nodes try to share the spectrum with the incumbent in a non-interference manner. Channel impairments like deep shadowing, which can lead to the so-called "hidden node problem", and multipath fading are some of the reasons why a secondary user might not be able to sense the presence of an incumbent without assistance from other CRs operating in its neighborhood. Cooperative Spectrum Sensing [2] has been proposed and investigated to be effective in handling these impairments. In [2] three different CSS architectures for CR Networks based on the way that cooperating CRs share the sensing information among themselves in the network are identified. The classifications are briefly discussed below:

*Centralized Cooperative Sensing CR Networks*: This is an architecture where the Cooperating CR nodes share their sensing information via a centralized infrastructure known as the Base Station or Fusion Center. The Fusion Center is responsible for aggregating the sensed data from all the cooperating node and making the final decision about the presence of an incumbent. Centralized CSS is illustrated in Figure 1 as indicated by the interaction between CR1, CR2 and CR3.

*Distributed Cooperative Sensing CR Networks*: Here the Cooperating CR nodes, e.g., CR4, CR2 and CR5 in Figure 1, share their sensing information without a centralized infrastructure/base station. A CR node might be designated as a Fusion Center where sensing information is collected and the final decision is communicated to the cooperating nodes. Similarly, each of the nodes might take turn in acting as the Fusion Center and then a distributed agreement algorithm can be used to make a final decision. The latter design removes the workload on a single node especially where power consumption is a factor.

*Relay-Assisted Cooperative Sensing CRNs*: Spectrum Sensing information and decisions are communicated to CR nodes that are more than one hop from the designated Fusion Center through multi-hop relays. Figure 1 illustrates the general form of this classification as the interaction between CR4, CR2, CR5 and CR6. It is assumed here that CR2 is the Fusion Center (FC) and hence sensing decisions from the FC are relayed by CR5 to CR6.

*Combined CSS Architectural Model for CRNs*: Here one considers the combination of all three CSS types earlier mentioned into a single architecture. This presents the CR with the flexibility of being part of any of the three types depending on its location in the network. The complete scenario represented by Figure 1 is the formulation of the Combined CSS Architectural Model for CRNs.

**Fault Models**

Different jamming scenarios can result in different fault types, classified by fault models. A fault model [4, 11] captures the behavior of faults and isolates levels of redundancy needed to tolerate a single fault type or combinations of fault types.

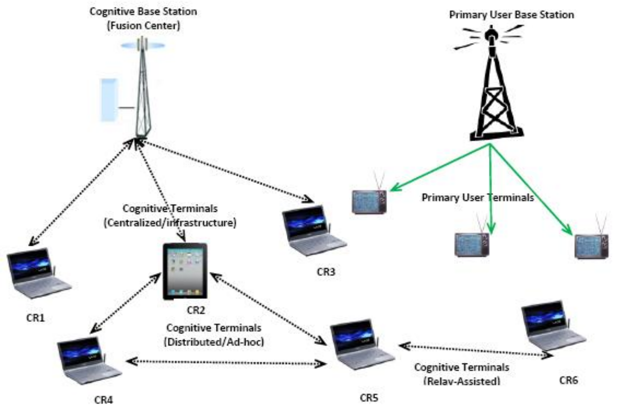


**Figure 1: Combined Architectural Model for CSS in CR Networks**

The simplest fault model considers only one fault type, e.g., only benign faults or malicious faults, as shown in [12]. Combinations of fault types have been addressed using hybrid fault models, e.g., [22] considers benign, symmetric and asymmetric fault behavior. Further refinement of faults was presented in the hybrid fault model of [4], where symmetric to asymmetric faults were considered with transmissive and omissive behavior. It is this latter model by [4] that is the basis for the research presented here.

# 3. JAMMING IN CSS CR NETWORKS

Depending on its location and power, a Cognitive Radio operating as a jammer is able to cause Denial of Service to all the CSS Architectural types earlier discussed.

## 3.1 Security Requirements of CR Networks

Some security requirements are specifically pertinent to the success of CR Networks. The following requirements are adapted from the Telecommunication Networks Security Requirements ITU-T: E.408 to suit cognitive radios: *Controlled access to resources* - Secondary Users (SUs) should only have access to those resources that they are authorized to access and no more. *Robustness* - CRN should be robust against any threat from malicious users. *Protection of confidentiality* - CRN must ensure the confidentiality of communicated (sensed) data. *Protection of data integrity* - CRN must guarantee the integrity of communicated data. *Compliance to regulatory framework* - CRN must comply to non-interference to Incumbent regulatory requirement. *Accountability/Non-repudiation* - CRN must ensure that the SUs cannot deny responsibility of any of their activities. *Verification of identities* - CRN must be able to verify the identity of SUs.

## 3.2 Impact of Jamming attack in CRNs

It is desirable to identify the impact of different classes of jammers operating in a CRN environment. These jammers are potentially CRs themselves and are capable of utilizing their flexible and adaptable capacity to cause serious DoS in a CRN. Table 1 presents a summary of these comparisons with a rating of their impact. As the table is intended to give the reader a feeling for the impact as depicted in cited literature, the simple values low (L), medium (M) or high (H) are used in the Network metrics. A similar approach based on five different values was used in [15]. The impact is considered from two perspectives, i.e., (a) the Jammers point of view and (b) the Defenders point of view. The table should give a feeling for what to expect as the result of mitigating specific attacks. In the table columns are Constant Jamming (Con), Random Jamming (Ran), Deceptive Jamming (Dec), Reactive Jamming (Rec), and Intelligent Jamming (Int).

**Table 1: Impact of Jamming Attacks**

| Metric | Con | Ran | Dec | Rec | Int |
|---|---|---|---|---|---|
| Power usage (a) | H | M | M | M | L |
| Throughput (a) | L | M | L | L | L |
| SNR (a) | H | M | H | M | L |
| Cost (a) | L | M | M | M | H |
| Cost (b) | L | M | M | M | H |
| Scalability (a) | H | H | H | H | H |
| Scalability (b) | H | H | H | H | L |
| Level of DoS (a) | L | M | L | L | M |
| Tech. Complexity (a) | L | M | M | M | H |
| Probability of detection (b) | H | M | L | M | L |
| Intelligence Required (a) | L | M | M | M | H |
| Intelligence Required (b) | L | M | M | M | H |

# 4. FAULT MODEL BASED CRN VIEW

We now classify jamming in CR networks based on hybrid fault models. Since in real-life systems fault scenarios are less likely to exhibit worst-case behavior it makes sense to use hybrid fault models. This helps avoid treating every fault as pathological, which would lead to overly conservative estimates of fault tolerance and reliability [4, 22]. Thus faults of different severities may coexist in the same system. The 3-fault model of [22] (benign, symmetric and asymmetric) was extended to a 5-fault model in [4] by considering transmissive and omissive versions of non-benign faults. A transmissive fault results from delivery of erroneous value(s) to one or more receivers. An omissive fault results from failure to deliver any value to one or more receiver. The distinction between the two is that an omissive fault does not deliver an erroneous value to any receiver. The following cases were identified for CSS in CRNs under this model:

*Total jamming of Cognitive Control Channel (CCC):* This is a situation where all the channels used as CCC in a Infrastructure-based (Centralized) CR Networks are jammed. The faults here are (a) *Benign Fault* if the fault is globally diagnosed, and (b) *Omissive Symmetric Fault* if it has not been globally diagnosed. (c) *Transmissive Symmetric Fault* if erroneous values are delivered at the receiver.

*Partial Jamming of CCC:* This is a scenario where only some of the channels used as CCC in Infrastructure-based (Centralized) CR Networks are jammed. The fault here is either *Strictly Omissive Asymmetric Fault* or *Transmissive Asymmetric Fault.*

*Entire jamming of Distributed CRN:* This is when a jammer causes a DoS to all the nodes in an Ad-hoc (Distributed) CR spectrum sensing and sharing Network. The faults identified here are: (a) *Benign Fault* if the fault is globally diagnosed, and (b) *Omissive Symmetric Fault* if the fault is not globally diagnosed. (c) *Transmissive Symmetric Fault* if erroneous values are delivered at the receiver.

*Partial Jamming of Distributed CRN:* This is the jamming of some of the nodes in an Ad-hoc (Distributed) CR Spectrum Sensing and Sharing Network. The fault here is either *Strictly Omissive Asymmetric Fault* or *Transmissive Asymmetric Fault.*

*Total Jamming of Relay-Assisted CRN:* This is the jamming of all the nodes involved in relaying and sharing sensed spectrum in a Relay-Assisted CSS Cognitive Radio Network. The faults identified here are: (a) Benign Fault if fault is globally diagnosed, and (b) Omissive Symmetric Fault if it has not been globally diagnosed. (c) *Transmissive Symmetric Fault* if erroneous values are delivered at the receiver.

*Partial Jamming of Relay-Assisted CRN:* Here some of the nodes involved in relaying and sharing sensed spectrum in a Relay-Assisted Cognitive Radio CSS architecture are jammed. The fault here is either *Strictly Omissive Asymmetric Fault* or *Transmissive Asymmetric Fault.*

# 5. DEALING WITH JAMMING

Spread Spectrum [16] (Frequency Hopping (FH) and Direct Sequence Spread Spectrum (DSSS)) have been used to alleviate jamming attacks in Wireless Networks. The signal is spread over a large bandwidth thereby making it costly for jammers to hinder an on-going transmission. The combination of Spread Spectrum and Orthogonal Frequency Division Multiplexing [9] can also be used to efficiently mitigate jamming attacks in wireless networks.

In CRNs, based on the Spread Spectrum approach, the available spectrum is divided into several pieces of non-overlapping channels in which only a small portion of the channels is used for transmission at a time. The malicious jammer either jams a large number of the channels with negligible jamming effect in each channel or jam few channels which might not be in use by the Cognitive Radios. If channels used by a CR is under jamming, the CR built on the concept of Software Define Radio has the flexibility to dynamically switch to another channel free of jamming [3, 9]. The problem here is if a jammer is a CR, it could lead to a jamming attack known as *Chaser Jamming* [6] in which the jammer chases the CR nodes as it switches from channel to channel. Another problem arises when one or more of the portion of channels used by CR is jammed, any data being transmitted at that instance is either lost or corrupted.

*Forward Error Correction* (FEC) schemes like LT-code [13], Raptor code [18] and Low Density Parity-Check Codes (LDPC) [17], can be used to regain lost data due to jamming attacks in a CRN through data redundancy. We here discuss only the Raptor code because it is the most widely investigated FEC code for communication. The Raptor code is a type of Fountain code [17] in which a message made up of a number of $k$ symbols is encoded into an infinite series of symbols in such a way that if during transmission some part of the data is lost, e.g., due to jamming, the lost data can be recovered with a probability that increases as the number of the received symbols increase beyond $k$ [18].

The previous approaches are suitable only to deal with benign and omission faults. However, they are not effective if jamming is done in such a way that it changes values, i.e., a value fault arises. To overcome this limitation we propose a hybrid FEC code, defined by the concatenation of *Raptor codes* and *SHA-2* [19]. The Raptor code part of the code is used to recover any data loss due to Omissive fault (symmetric/Asymmetric) as a result of jamming. The SHA-2 hash function will be used to handle transmissive (value) fault due to jamming. Any value fault due to malicious jamming/bad channel could be detected with SHA-2 if the

Message Digest generated at the receiver is different from the message digest generated at the sender. Detection can result in different actions, e.g., a) the receiver could request retransmission, or b) the Raptor part of the Code could be used to iteratively correct suspected bits of the message as if it is omitted and then regenerate the message digest each time with SHA-2 to verify the data received, or c) the erroneous message be discarded and the system be suspected to be under famming attack, requiring reaction, e.g., to move the node away from the jamming source, d) if the message jammed is a control message, it may be migrated to another channel not under jamming attack for transmission.

The effectiveness of the combined approach is bound by the thresholds of the Raptor code and SHA-2. For the Raptor code this is for example the minimum amount of symbols that make the decoding successful. Any manipulation by jamming beyond what these schemes can tolerate will of course also render the combined approach ineffective.

The performance of the combined approach is defined by the combined overhead of the Raptor code and SHA-2. For example, the Raptor code's performance [18] depends on a) Space: Storage requirement of the codes, b) Overhead: This is a function of the decoding algorithm c) Cost: The cost of encoding and decoding the code.

# 6. CONCLUSIONS

In this paper, we discussed jamming in CR Networks in the context of hybrid fault models and identified fault types for different jamming strategies. The investigations of fault potential of a combined architectural model for CSS in CR Networks was extended to fault types to include transmissive and omissive value faults. We discovered that existing FEC codes are not sufficient to handle jamming attacks for these fault types and proposed a hybrid FEC code capable of mitigating the entire class of faults identified in Jamming adversarial model.

# 7. REFERENCES


[1] I. F. Akyildiz, et al., *NeXt generation/ dynamic spectrum access / cognitive radio wireless networks:A survey*, Computer Networks 50 (13) (2006) 2127-2159.

[2] I. F. Akyildiz, B. F. Lo, and R. Balakrishnan, *Cooperative Spectrum Sensing in Cognitive Radio Networks: A Survey*, Physical Communication (Elsevier) Journal, vol. 4, no. 1, pp. 40-62, March 2011.

[3] Asterjadhi, M. Zorzi, *JENNA: A Jamming Evasive Network coding Neighbor discovery Algorithm for Cognitive Radio Networks*, In IEEE ICC Workshop on Cooperative and Cognitive Mobile Networks (CoCoNet3), Cape Town, South Africa, May, 2010

[4] M.H. Azadmanesh, and R.M. Kieckhafer, *Exploiting Omissive Faults in Synchronous Approximate Agreement*, IEEE Trans. Computers, 49(10), pp. 1031-1042, Oct. 2000.

[5] Baldini, G., et al., *Security Aspects in Software Defined Radio and Cognitive Radio Networks : A Survey and A Way Ahead*, Spectrum, (99), 1-25 (2011).

[6] J. Burbank, *Security in Cognitive Radio Networks: The Required Evolution in Approaches to Wireless Network Security*, Third International Conference on Cognitive Radio Oriented Wireless Networks and Communications (CrownCom), 15-17 May, 2008.

[7] J. L. Burbank, et al., *A common lexicon and design issues surrounding cognitive radio networks operating in the presence of jamming*, IEEE MILCOM 2008; 1-7.

[8] W. Cadeau and X. Li, *Anti-jamming performance of cognitive radio networks under multiple uncoordinated jammers in fading environment*, Proc. of the 46th Annual CISS, Princeton Univ., NJ, March 2012.

[9] Qi Dong and Donggang Liu *Adaptive Jamming-Resistant Broadcast Systems with Partial Channel Sharing*, Proc. 2010 International Conference on Distributed Computing Systems, Genova, Italy.

[10] Philipp M. Eittenberger, Todor Mladenov, and Todor Mladenov, *Raptor Codes for P2P Streaming*, 20th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP), 2012

[11] Axel Krings, *Design for Survivability: A Tradeoff Space*, Proc. 4th Cyber Security and Information Intelligence Research Workshop, CSIIRW 2008, Oak Ridge National Laboratory, May 12-14, 2008.

[12] L. Lamport, et.al., *The Byzantine Generals Problem*, ACM Transactions on Programming Languages and Systems, Vol. 4, No. 3, pp. 382-401, July 1982.

[13] M. Luby, *LT-codes*, in Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS), pp. 271âĂŞ280, 2002.

[14] J. Mitola III, *Cognitive Radio: An Integrated Agent Architecture for Software Defined Radio*, Doctor of Technology dissertation, Royal Inst. Technol. (KTH), Stockholm, Sweden, 2000.

[15] K.Pelechrinis, M.Iliofotou and S.V.Krishnamurthy, *Denial of Service Attacks in Wireless Networks: The case of Jammers*, In IEEE Communication Surveys and Tutorials, pp(99):113, April 2011.

[16] R.A. Poisel. *Modern Communications Jamming Principles and Techniques.* Artech House Publ., 2003.

[17] Shokrollahi, A. *LDPC Codes: An introduction*, www.ipm.ac.ir/IPM/homepage/Amin2.pdf. [2003]

[18] A. Shokrollahi, *Raptor codes*, IEEE/ACM Trans. Netw., 14(SI):25512567, 2006.

[19] N. Sklavos and O. Koufopavlou, *Implementation of the SHA-2 Hash Family Standard Using FPGAs*, J. of Supercomputing, Vol. 31, No 3, pp. 227-248, 2005.

[20] P. Tague, D. Slater, G. Noubir, and R. Poovendran, *Quantifying the impact of efficient cross-layer jamming attacks via network traffic flows*, Network Security Lab (NSL), University of Washington, Tech. Rep., 2009, www.ee.washington.edu/research/nsl/papers/TR005.pdf

[21] P. Tague, *Improving anti-jamming capability and increasing jamming impact with mobility control*, In 6th IEEE International Workshop on Wireless and Sensor Networks Security (WSNS), Nov. 2010.

[22] P. Thambidurai, and Y.-K. Park, *Interactive Consistency with Multiple Failure Modes*, Proc. 7th Symp. on Reliable Distributed Systems, Columbus, OH, pp. 93-100, Oct. 1988.

[23] Yongle Wu, Beibei Wang, K. J. Ray Liu, and T. Charles Clancy, *Anti-Jamming Games in Multi-Channel Cognitive Radio Networks* IEEE Journal on Selected Areas in Communications, Vol. 30, NO. 1, January 2012

[24] Wenyuan Xu, et al. *The feasibility of launching and detecting jamming attacks in wireless networks*, Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing, May 25-27, 2005, Urbana-Champaign, IL, USA