AFRL-RV-PS-
TR-2013-0142

AFRL-RV-PS-
TR-2013-0142

# RENDEZVOUS PROTOCOLS AND DYNAMIC FREQUENCY HOPPING INTERFERENCE DESIGN FOR ANTI-JAMMING SATELLITE COMMUNICATION

**Marwan Krunz and Ricardo G. Sanfelice**

**University of Arizona
P.O. Box 210158
Tucson, AZ 85721-0158**

**25 Nov 2013**

**Final Report**

**APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.**

**AIR FORCE RESEARCH LABORATORY
Space Vehicles Directorate
3550 Aberdeen Ave SE
AIR FORCE MATERIEL COMMAND
KIRTLAND AIR FORCE BASE, NM 87117-5776**

# DTIC COPY
# NOTICE AND SIGNATURE PAGE

This report is the result of contracted fundamental research deemed exempt from public affairs security and policy review in accordance with SAF/AQR memorandum dated 10 Dec 08 and AFRL/CA policy clarification memorandum dated 16 Jan 09. This report is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RV-PS-TR-2013-0142 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT

//SIGNED//
R.SCOTT ERWIN
Program Manager

//SIGNED//
PAUL HAUSGEN
Technical Advisor, Spacecraft Component Technology Branch

//SIGNED//
BENJAMIN M. COOK, Lt Col, USAF
Deputy Chief, Spacecraft Technology Division
Space Vehicles Directorate

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government’s approval or disapproval of its ideas or findings.

# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

|  |  |  |
|---|---|---|
| **1. REPORT DATE** *(DD-MM-YYYY)*<br>25-11-2013 | **2. REPORT TYPE**<br>Final Report | **3. DATES COVERED** *(From - To)*<br>26 May 2012-30 Sep 2013 |

**4. TITLE AND SUBTITLE**
Rendezvous Protocols and Dynamic Frequency Hopping
Interference Design for Anti-Jamming Satellite Communication

**5a. CONTRACT NUMBER**
FA9453-12-1-0216

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**
63401F

**6. AUTHOR(S)**
Marwan Krunz and Ricardo G. Sanfelice

**5d. PROJECT NUMBER**
2181

**5e. TASK NUMBER**
PPM00011812

**5f. WORK UNIT NUMBER**
EF007887

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
University of Arizona
P.O. Box 210158
Tucson, AZ 85721-0158

**8. PERFORMING ORGANIZATION REPORT NUMBER**

**9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
Air Force Research Laboratory
Space Vehicles Directorate
3550 Aberdeen Ave. SE
Kirtland AFB, NM 87117-5776

**10. SPONSOR/MONITOR'S ACRONYM(S)**
AFRL/RVSV

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**
AFRL-RV-PS-TR-2013-0142

**12. DISTRIBUTION / AVAILABILITY STATEMENT**
Approved for public release; distribution is unlimited.

**13. SUPPLEMENTARY NOTES**

**14. ABSTRACT**

Cognitive radio technology combines high re-configurability with intelligent spectrum management and adaptation, which materializes into a highly agile and spectrally efficient platform for communications. In fact, cognitive radio technology enables the use of opportunistic spectrum access of the underutilized portions of the assigned spectrum. The benefit of such technology and capabilities for military satellite communications is not well understood. This project studies the properties of new algorithms for frequency hopping, a key component in cognitive radio technology. Methods from game theory and hybrid systems theory are employed for the analytical study, while computer simulations are used to validate these findings.

**15. SUBJECT TERMS**
Cognitive Radio Networks, Frequency Hopping, Game Theory, Hybrid Systems

| **16. SECURITY CLASSIFICATION OF:** |  |  | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON**<br>Richard S. Erwin |
|---|---|---|---|---|---|
| **a. REPORT**<br>Unclassified | **b. ABSTRACT**<br>Unclassified | **c. THIS PAGE**<br>Unclassified | Unlimited | 32 | **19b. TELEPHONE NUMBER** *(include area code)* |

(This page intentionally left blank)

## TABLE OF CONTENTS

## LIST OF FIGURES

**Figure** **Page**

## ACKNOWLEDGEMENT

This material is based on research sponsored by Air Force Research Laboratory under agreement number FA9453-12-1-0216. The U.S. Government is authorized to reproduce and distribute reprints for Governmental purposes notwithstanding any copyright notation thereon.

## DISCLAIMER

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of Air Force Research Laboratory or the U.S. Government.

## 1.0 SUMMARY

Cognitive radio technology combines high re-configurability with intelligent spectrum management and adaptation, which materializes into a highly agile and spectrally efficient platform for communications. In fact, cognitive radio technology enables the use of opportunistic spectrum access of the underutilized portions of the assigned spectrum. The benefit of such technology and capabilities for military satellite communications is not well understood. This project studies the properties of proposed new algorithms for frequency hopping, a key component in cognitive radio technology. Methods from game theory and hybrid systems theory are employed for the analytical study, while computer simulations are used to validate the findings.

## 2.0 INTRODUCTION

Military Satellite Communications (SATCOM) supports a diverse range of services, which vary in their performance objectives (vis-à-vis, throughput and latency metrics) and security requirements (anti-jamming, probability of interception, etc.). Enabling such services in a unified yet cost-effective manner requires a highly agile, spectrally efficient platform based on the Cognitive Radio (CR) technology. The CR concept has recently been at the forefront of wireless research. With a Software Defined Radio (SDR) engine at its core, a CR combines high re-configurability with intelligent spectrum management and adaptation. While still in its infancy, the CR technology has already attracted significant attention from government agencies and private corporations, which have been pushing for accelerating Research and Development (R&D) efforts in this area. A key driving force behind the CR technology is Opportunistic Spectrum Access (OSA) of the underutilized portions of the assigned spectrum, especially in the International Telecommunications Union (ITU) Ultra High Frequency (UHF) band (300 MHz to 3 GHz). This applies both to commercial spectrum (e.g., "TV white spaces") as well as military spectrum, where the demand for higher spectral efficiency continues to rise. A fundamental principle in Opportunistic Spectrum Access (OSA), be it in military or civilian contexts, is to support Secondary Transmissions/Users (SUs) without degrading the performance of Primary Users (PUs), i.e., users with priority access to the given channel.

While CRs have been extensively researched for terrestrial wireless systems, particularly as a means of enabling Wireless Regional Area Networks (WRANs) [1] and opportunistic in-home media streaming [2], their use in SATCOM has just started to receive attention [3]. One main motivation for considering CRs in SATCOM is to mitigate interference and/or jamming. Satellite systems are prone to both unintentional and intentional interference (jamming). Unintentional interference may be caused by human error (e.g., accessing the wrong satellite, channel frequency, or polarization) or equipment malfunction. The latter source of interference has been particularly on the rise due to a global increase in the number of low-cost, transmit-capable antennas Very Small Aperture Terminal (VSAT Terminals). Interference is also attributed to the over-crowdedness of the frequency spectrum and the intense competition among many terrestrial and satellite services to access this spectrum.

As a line of defense against interference/jamming, SATCOM can employ spreading techniques, including Direct Sequence Spread Spectrum (DSSS) and Frequency Hopping Spread Spectrum (FHSS). DSSS exhibits a threshold behavior to interference, whereby an interfering signal is rejected as long as its power remains below the jamming margin. However, the throughput becomes practically zero if this margin is surpassed [4, 5]. On the other hand, FHSS exhibits a graceful degradation in performance with higher interference. Due to this dual behavior, DSSS and FHSS find applications in different domains. The former is typical in the commercial domain, where moderate interference levels are caused by users operating on the same spectrum, while the latter finds applications in adversarial settings where the interference is likely caused by a powerful jammer. In military SATCOM, DSSS has been suggested for the Air Force Satellite Control Network (AFSCN), primarily to support ranging for beyond-Global Positioning System (GPS) satellites, and secondarily as a means of interference rejection. In this project, we argue that with the availability of a spectrum-agile Cognitive Radio/Software Defined Radio (CR/SDR) platform, FHSS is quite feasible to implement, and should be considered as a preferred method for anti-jam SATCOM. However, in contrast with classic FHSS, which relies on a fixed FH sequence, in our proposed design we allow for dynamic adjustment of the hopping sequence, depending on interference and jamming conditions.

Applying dynamic FHSS Dynamic Frequency Hopping (DFH) to military satellite systems comes with technical challenges, stemming from the peculiarities of satellite communications. First, because of the long propagation delay between a ground station and a satellite (hundreds of milliseconds and higher), *reactive* anti-jamming and interference mitigation measures (e.g., using the observed signal strength at the receiver) are often ineffective. A smart jammer who keeps changing its targeted frequencies will prevent any meaningful action by a reactive network operator. Another challenge relates to the highly dynamic nature of Low Earth Orbit (LEO) satellite. A typical LEO satellite travels several kilometers in one second. In the short period (tens of minutes) while the satellite is still in sight, the uplink/downlink signal strength can vary significantly due to distance and atmospheric variations. To maintain a target rate demand during the lifetime of a traffic flow (~ a few minutes), one may allocate a conservative link margin, leading to unnecessary energy consumption. Alternatively, a transmission waveform can be dynamically selected from an available set of waveforms so as to minimize the required power while meeting the target rate demand. While satellite trajectories (and hence, distance to the ground station) are generally known in advance, random channel conditions and unpredictable interference/jamming factors preclude the possibility of adaptively selecting the optimal waveform in a deterministic fashion. A third challenge relates to the possible loss of time-frequency synchronization between the transmitter and receiver of a SATCOM link (e.g., a bent pipe), operating according to FHSS. Even when DFH is used, it requires updating the FH sequence on the fly, and conveying the frequency-time updates to the transmitter on time. The update messages themselves may get corrupted or lost due to interference, resulting in a loss of synchronization. In this case, the transmitter and receiver will have to rendezvous again to re-establish communications. The Time-To-Rendezvous (TTR) becomes a critical metric in the overall performance of the system.

To address the aforementioned challenges, we advocate a novel DFH approach for SATCOM, which relies on *proactive* sensing of upcoming frequency channels in an FH sequence using an auxiliary CR/SDR module that resides within the satellite (for uplink transmissions) or the receiving ground station (for downlink transmissions). Depending on the observed interference, the CR module decides whether the predefined FH sequence is to be modified or not. If there is a need to adjust the FH sequence, the module will also search for appropriate replacement frequencies. The CR may also recommend boosting the transmission powers over certain frequencies to combat relatively mild forms of interference. The spectrum sensing results are then reported back to the transmitter over the reverse link. The time difference between the current frequency hop and the sensed frequency hops should be long enough to allow for the feedback to arrive at the transmitter. By focusing on "future" frequencies in the FH sequence, our approach prevents (rather than reacts to) transmissions over channels with high interference. We have previously considered this proactive approach to combat unintentional, persistent (non-reactive) interference. In this project, we plan on extending our treatment to reactive, intelligent jammers. We will rely on game theory as a basis to analyze the behavior of smart, reactive jammers and devise appropriate "optimal" DFH mechanisms for combating such type of jammers. We will also employ hybrid systems theory to gain a deep understanding of the stability properties of frequency hopping algorithms.

## 3.0 METHODS, ASSUMPTIONS, AND PROCEDURES

Establishing communications in a multi-channel satellite system requires the communicating devices to "rendezvous" on a common channel before carrying out normal data transmissions. The rendezvous process enables the exchange and negotiation of critical information, including transmission parameters (e.g., transmission powers, transmission rates, etc.), timing information, etc. This process takes place following the loss of connectivity between the transmitter and receiver (e.g., due to jamming and/or fading conditions). Clock drifts make it difficult for the communicating parties to maintain a common time reference, so the rendezvous process needs to be robust to misalignment and asynchronous operation.

A simple approach to rendezvous is to rely on a predetermined, statically assigned frequency channel (or a common spreading code). However, this approach is vulnerable to *selective jamming attacks*, in which a smart adversary specifically targets the rendezvous process in hope of creating a *Denial Of Communication (DOC)* attack. The adversary may discover the "rendezvous channel" (or code) by chance, through public knowledge of the underlying protocol semantics, or by compromising one of the network devices. An alternative approach for rendezvous is to use random frequency hopping (FH). In this case, the communicating parties hop independently until they meet each other. While this approach is robust to insider attacks, it suffers from a long time-to-rendezvous (TTR).

Recently, researchers have considered a structured approach for designing FH-based rendezvous sequences based on the concept of *quorums*. In plain terms, a quorum system is a collection of nonempty sets (called quorums) that pairwise overlap by one or more elements. For example, Q ={{3,4},{2,3},{2,4}} is a system of three quorums: {3,4}, {2,3}, and {2,4}. One important advantage of quorum-based FH designs is their robustness to synchronization errors. In particular, certain quorum systems enjoy the *rotation k-closure property*, whereby any misalignment between any *k* quorums of the underlying quorum system results in *k* rotated quorums that also pairwise overlap.

**Figure 1** shows the rotation 2-closure property for a 4-by-4 grid quorum system. In a grid quorum system, each FH sequence is divided into frames, each frame consisting of several time slots. The slots in a frame are arranged into a square grid (e.g., a 4-by-4 grid in **Figure 1**). Each node selects a column and a row from the grid, representing the quorum of that node (the blue cells in **Figure 1**). The slots that correspond to the selected quorum are assigned a channel called the *rendezvous channel* and the remaining slots are assigned a random channel. The two nodes rendezvous during the common quorum slots, indicated by the letter *I* in the two left DOC most subfigures. Rotating either of both quorums still results in common quorum slots (indicated by the letter *I'* in the two rightmost subfigures). The *k*-closure property is a key to achieving rendezvous despite clock misalignment among the communicating devices.

On the other hand, due to their systematic design, quorum-based schemes are inherently vulnerable to jamming attacks, particularly when the attack is launched by an insider node, e.g., when a trusted node has been compromised and its secrets have been partially or completely revealed to the attacker. In this case, the attacker can exploit his knowledge of the underlying quorum system to launch a DOC attack.

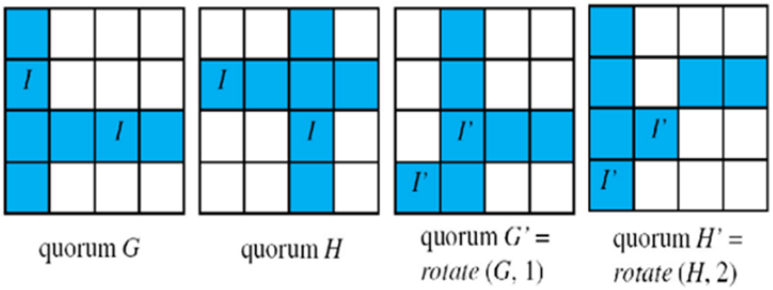


**Figure 1. Rotation 2-closure Property of Grid Quorum Systems**

The methods, assumptions, and procedures employed in this research are summarized in the next subsections.

### 3.1 Quorum-based FH Designs and Rendezvous Protocols for Re-establishing Communications Following the Loss of Synchronization

Quorum systems are used to design the FH sequences of the two nodes. One approach that we have developed relies on *nested grid quorums*, whereby multiple grid quorums of different sizes are used in each FH sequence. The objective of this nested design is twofold. First, it expedites the rendezvous process, i.e., reduces the time-to-rendezvous (TTR) which is also called the Evasion Delay (ED). This is achieved by: (i) increasing the number of overlapping slots in a frame, and (ii) implementing multiple rendezvous channels. The second goal of our nested design is to provide higher resiliency to insider attacks. More specifically, in the nested design, each FH sequence involves multiple quorums of different sizes, which makes it harder for an insider adversary to infer the FH sequence by only knowing the general structure of the underlying grid quorum system. This resiliency is characterized by the Hamming Distance (HD).

The following example illustrates the general idea of the nested quorum design. Consider the construction of one FH sequence. Suppose that this sequence is composed of successive frames, each of length m=9 slots. This frame length corresponds to a 3-by-3 grid quorum system. It results in a nesting degree of two (i.e., two rendezvous channels per frame). Let $Z_n$ denote the set {0,2,…,n-1} for any positive integer n. Then, each FH sequence is obtained as follows:

Step 1: Construct a grid quorum system Q under $Z_9$. Q has 9 different quorums, each containing 2 $\sqrt{9}$ – 1 = 5 slots that comprise one row and one column of the 3 × 3 grid (see **Figure 2**).

Step 2: For each frame j in the FH sequence, j=1, 2, …,:

- Select the outermost quorum $G_1^{(j)}$ of frame j from Q (e.g., $G_1^{(j)}$ = {1, 3, 4, 5, 7}, where each element represents the index of a time slot in a 9-slot frame).
- Assign a rendezvous channel $h_1^{(j)}$ to the slots that correspond to $G_1^{(j)}$. This $h_1^{(j)}$ is called the outermost rendezvous channel.
- Prune quorum $G_1^{(j)}$ from the original 3 × 3 grid and select the next outermost quorum $G_2^{(j)}$ from the resulting 2 × 2 grid (e.g., $G_2^{(j)}$ = {2, 6, 8}). Then, assign another rendezvous frequency $h_2^{(j)}$ to the slots that correspond to $G_2^{(j)}$.
- Assign a random frequency $h_x^{(j)}$ to each of the remaining unassigned slots in the frame.

The above procedure is applied independently to other FH sequences (one per node). We call this algorithm Nested Unicast Rendezvous Algorithm for Denial-of-Service Attacks (NUDoS).

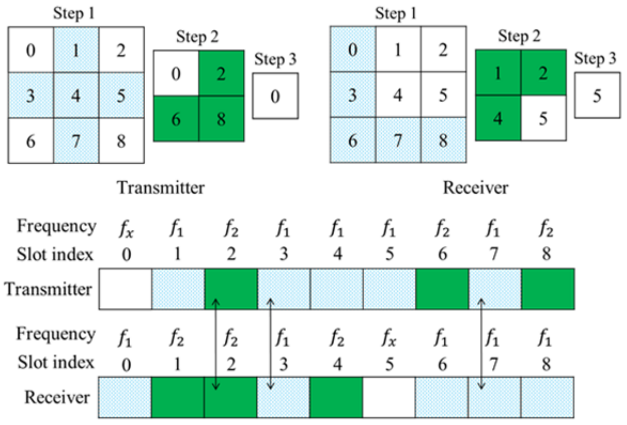

Step 1
0 1 2
3 4 5
6 7 8
Step 2
0 2
6 8
Step 3
0
Transmitter
Step 1
0 1 2
3 4 5
6 7 8
Step 2
1 2
4 5
Step 3
5
Receiver
Frequency $f_x$ $f_1$ $f_2$ $f_1$ $f_1$ $f_1$ $f_2$ $f_1$ $f_2$
Slot index 0 1 2 3 4 5 6 7 8
Transmitter
Frequency $f_1$ $f_2$ $f_2$ $f_1$ $f_2$ $f_x$ $f_1$ $f_1$ $f_1$
Slot index 0 1 2 3 4 5 6 7 8
Receiver

**Figure 2. Example of Nested Grid-Quorum-Based Rendezvous When M = 9.**

The following issues are currently being considered:

- Selection of rendezvous channels: We have developed mechanisms for selecting the rendezvous channels (e.g., channels $h_1^{(j)}$ and $h_2^{(j)}$ in **Figure 2**) depending on the expected adversarial behavior.
- Quorum selection**:** We have investigated mechanisms for selecting the quorums in Q (e.g., $G_1^{(j)}$ and $G_2^{(j)}$ in **Figure 2**) given that the rendezvous channels have already been selected. This selection is done based on the expected behavior of jammers in the next frame.
- Studying other quorum systems: We are considering other types of quorum systems as candidates for FH-based rendezvous. These include torus and cyclic quorum systems.
- Implementation and experimental evaluation: Besides analysis and simulation-based studies, we also plan to implement several of the developed rendezvous protocols using NI/USRP experimental radios and evaluate their performance experimentally.

### 3.2 Game Theory Formulation of FH Strategies under an Intelligent, Reactive Jammer

By means of game theoretical tools, the parameters of a quorum-based rendezvous protocol can be adapted to cope with adversarial jamming. In general, we consider a setup in which multiple adversaries attempt to disrupt the rendezvous process. Different types of adversarial attacks have been investigated, including active/passive, insider/outsider, and reactive (adaptive)/non-reactive. These adversaries are assumed to have different levels of knowledge about the semantics of the rendezvous protocol. Moreover, the rendezvous problem is studied under various network models: homogeneous/heterogeneous and synchronous/asynchronous. In here, by *homogeneous* means that all network nodes experience the same adversarial conditions on various frequency channels. Our aim is to design different algorithms for each setup, analyze the proposed algorithms, and evaluate them by means of simulations and/or experimentations. So far, we have studied the following problems:

**(i)** **Rendezvous Under Non-reactive External Jamming Attacks:** In here, we have considered non-reactive jamming attacks, whereby adversaries do not adapt their strategies in response to actions taken by the rendezvousing nodes. The adversaries are assumed to be external devices that are not aware of any specific information about the semantics of the rendezvous protocol. We plan to consider different types of non-reactive jamming attacks. One type that we have considered is the *Markovian jamming attack*, where the jamming signal follows a two-state Markov model.

To formalize the rendezvous problem, we have formulated it as an optimization problem. This formulation can be customized for any system/type of jamming where the channel state under such system/jamming can be modeled mathematically. Moreover, we have designed a centralized FH construction algorithm that achieves the minimum TTR while keeping the HD greater than a certain threshold. This algorithm will be used as a benchmark for distributed algorithms that we plan to develop. As a first step, we have customized the rendezvous algorithm in the previous section to work in the presence of Markovian jamming attacks. We have evaluated these algorithms under different jamming probabilities (denoted by $\rho$) and different characteristics of the jamming signal.

We have also been investigating the following issues:

- *Optimizing various parameters of the rendezvous algorithm to reduce the performance gap between these algorithms and the centralized one.*
- *Studying other types of non-reactive outsider attacks, such as random jamming attacks, sweep jamming attacks, etc.*

**(ii)** **Rendezvous Under Reactive Insider Jamming Attacks:** In this part, we address the rendezvous problem in the presence of a reactive insider jammer who is aware of the quorum-based FH design used by various nodes to rendezvous. The attacker adaptively selects its action based on the observed actions of the legitimate nodes in the network. The attacker aim is to prevent nodes from rendezvousing, by maximizing the number of jammed rendezvous instances while minimizing the number of successful rendezvous instances. We study the rendezvous problem using different types of quorum systems, including grid, torus, and cyclic quorum systems. **Figure 3** shows an example of a satellite link operating in the presence of a reactive jammer. All nodes (i.e., transmitter, receiver, and jammer) operate using a grid quorum-based FH approach. A successful rendezvous instance refers to a time slot where the transmitter and receiver are tuned to a rendezvous channel (channel f in **Figure 3**), while the jammer is tuned to a different channel. If the transmitter, receiver, and jammer are tuned to a common channel during the same slot, then this slot is called a *jammed rendezvous slot*. We have formulated the interactions between the transmitter, receiver, and jammer as a three-player game. The formulation depends on the type of quorum system that is used for rendezvous. The transmitter and receiver try to maximize the number of successful rendezvous slots, while minimizing the number of jammed rendezvous slots. The jammer has the opposite objective. First, we have investigated the synchronous rendezvous game on a single channel (i.e., we assume that all players know the rendezvous channel). In this case, the game is to select the best quorum from the standpoint of each player. Next, we plan to investigate the case of synchronous and asynchronous rendezvous when various players do not know the rendezvous channels.

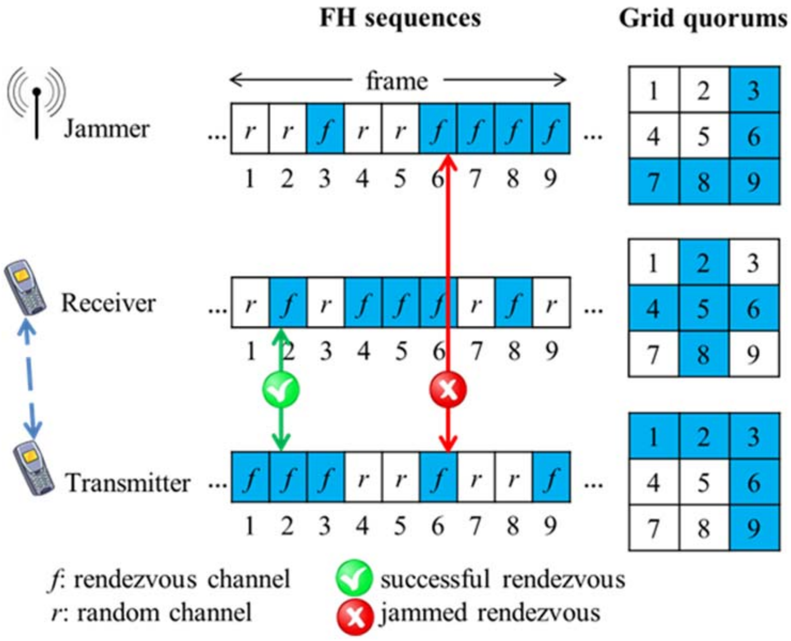


**Figure 3. Two Nodes Try to Rendezvous in the Presence of a Jammer. All Nodes Follow a Grid-Quorum-based FH Approach**

The following issues are currently being considered:

- *Studying the existence and uniqueness of the Nash Equilibrium (NE) for the formulated games.*
- *Investigating the `best response' for each player that results in convergence to a NE (if one exists), and studying the convergence speed of the best-response update mechanisms (sequential/parallel) under the formulated games.*
- *Explore incentive-based (pricing) mechanisms for improving the efficiency of the resulting NEs.*

### 3.3 Hybrid Systems Formulation of Cognitive Radio Strategies

Event-based adaptation of parameters of frequency hopping algorithms, like the one outlined in Section 3.1 using the nested quorum design approach, can also be performed within a framework of hybrid systems [6]. Hybrid systems are dynamical systems with state variables that can evolve both continuously and discretely (or impulsively). In the context of the algorithm in Section 3.1, the variables determining the channel to use change discretely according to the rules embedded in the quorum-based algorithm, while in between changes they remain constant. A hybrid system model for such an algorithm would provide a concise mathematical description that can be analyzed using control theoretical tools. More interestingly, due to their event-based nature, hybrid system models can be used to capture the dynamics of different algorithms used in CR systems, such as those for automatic waveform adaptation and output power selection.

To illustrate the hybrid systems approach, consider one ground station and one satellite with parameters $\mathrm{p}_1$ and $\mathrm{q}_1$ denoting their current communication channel selection, respectively. Let the channel options for both nodes be $\mathrm{f}_1, \mathrm{f}_2, \ldots, \mathrm{f}_K$, in which both $\mathrm{p}_1$ and $\mathrm{q}_1$ take their values from. For the case when the ground station operates as a transmitter and the satellite operates as a receiver, a simple control strategy that selects a transmission channel, transmits in it, and switches to the next channel after T seconds, will require a continuous state $\xi_1$ acting as a timer to trigger the channel changes. In this way, the dynamics of $\xi_1$ and $\mathrm{p}_1$ for the ground station are given by

$$\dot{\xi}_1 = 1 \tag{1}$$

and

$$\mathrm{p}_1^+ = \mathrm{g}_1(\mathrm{p}_1) \tag{2}$$

when

$$\xi_1 \geq \mathrm{T} \tag{3}$$

where $\mathrm{g}_1$ is a function that defines how $\mathrm{p}_1$ is updated. The continuous evolution of $\xi_1$ and $\mathrm{p}_1$ can be written as a differential equation with right-hand side

$$\dot{\xi}_1 = \mathrm{F}_1(\xi_1, \mathrm{p}_1) = 1 \tag{4}$$

while the instantaneous changes of $\xi_1$ and $\mathrm{p}_1$ can be written as a different equation with triggering condition (3) by defining

$$\mathrm{p}_1^+ = \mathrm{g}_1(\mathrm{p}_1) := \mathrm{next}\,(\mathrm{p}_1) \tag{5}$$

where the function next is defined as $\mathrm{next}\,(\mathrm{f}_\ell) = \mathrm{f}_{\ell+1}$ for $\ell \in \{1,2,\ldots,\mathrm{K}-1\}$ and $\mathrm{next}\,(\mathrm{f}_\mathrm{K}) = \mathrm{f}_1$. The updates of $\mathrm{p}_1$ are triggered when $(\zeta_1, \mathrm{p}_1) \in \mathrm{D}_1^\mathrm{u} := \{(\xi_1, \mathrm{p}_1) \,:\, \xi_1 \geq \mathrm{T}\,\}$. A similar hybrid model can be derived for the satellite's end.

Our aim is to develop a hybrid systems framework for the study of CR systems and exercise it in frequency hopping algorithms. Our efforts on this task include the following:

**(i)** **Rendezvous as an Optimization Problem with Hybrid Dynamics:** An initial problem of study under the proposed hybrid framework is the problem of coordinating the selection of channels by the ground stations and satellites so as to establish a communication link. This problem is referred to as the *rendezvous problem*. For the scenario in which a ground station $i \in \mathrm{U} := \{1,2,\ldots,\mathrm{N}\}$ is to establish a communication link with satellite $j \in \mathrm{V}:=\{1,2,\ldots,\mathrm{M}\}$, the goal is to design a control policy that makes the channel selection parameters $p_\mathrm{i}$ (ground station) and $q_\mathrm{j}$ (satellite). This problem is formulated as an optimization problem with hybrid dynamics.

**(ii) Rendezvous with Adversarial Behavior as an Optimization Problem with Hybrid Dynamics:** In this part, an additional player, a jammer, is introduced to the rendezvous problem above. Namely, we also consider the scenario in which a ground station is to establish a communication link with a satellite, but, now, under the presence of a jammer. In this scenerio, the goal is to design a control policy that makes the channel selection parameters $p_{\mathrm{i}}$ and $q_{\mathrm{j}}$ (associated to the ground station and satellite) equal and, simultaneously, different from the channel selection made by the jammer. This problem is formulated as an optimization problem with hybrid dynamics.

The following issues are currently under investigation:

- *Studying the existence and uniqueness of the Nash Equilibrium (NE) for the formulated games within the hybrid system framework.*
- *Studying the stability and its robustness of the Nash Equilibrium.*
- *Developing a method to systematically construct the `best response' for each player that results in convergence to a NE (if one exists).*

## 4.0 RESULTS AND DISCUSSION

### 4.1 Quorum-based FH Designs and Rendezvous Protocols for Re-establishing Communications Following the Loss of Synchronization

In this section, we present simulation results for the NUDoS algorithm and compare it with the proposed centralized algorithm. The proposed algorithm is studied under different frame lengths (n) and jamming probabilities ($\rho(m)$). Our evaluation metrics are the ED and the HD. NUDoS is simulated under a realistic setting of no synchronization (the misalignment between FH sequences is randomly selected in each experiment). The 95% confidence intervals are indicated. When these intervals are very tight, they are not drawn to prevent cluttering the graph. In the centralized algorithm, because of the minimum required HD, nodes may not rendezvous if $n$ is sufficiently small because all the slots in the frame will be assigned differently for different nodes, and hence some ED points are missing from the plot.

### 4.1.1 Evasion Delay

In **Figure 4** and **Figure 5**, we depict the ED of NUDoS and compare it with the centralized algorithm (denoted by C in the legend). The ED for both NUDoS and the centralized algorithm increases with n because of the reduction in the overlap ratio, as shown in **Figure 4**. The ED also increases with ρ(m). NUDoS achieves less ED for less fluctuating channels, under medium to high values of $\rho(m)$ (recall that quorums and channels are selected in NUDoS based on the expected channel's). While achieving comparable HD value to the centralized algorithm, the speed of NUDoS is comparable to the centralized algorithm for small to moderate values of $\rho(m)$. The ED of NUDoS increases with $pth$.

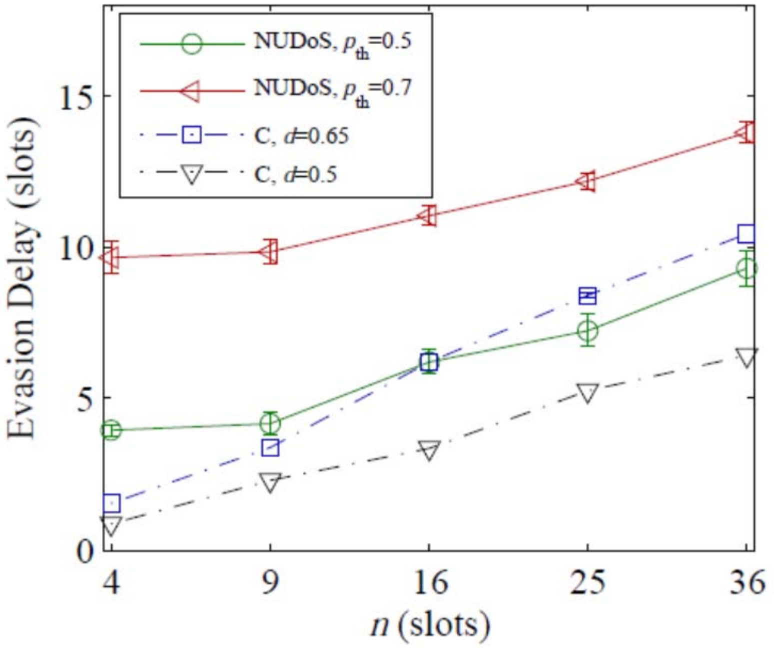


**Figure 4. ED vs. n for NUDoS**

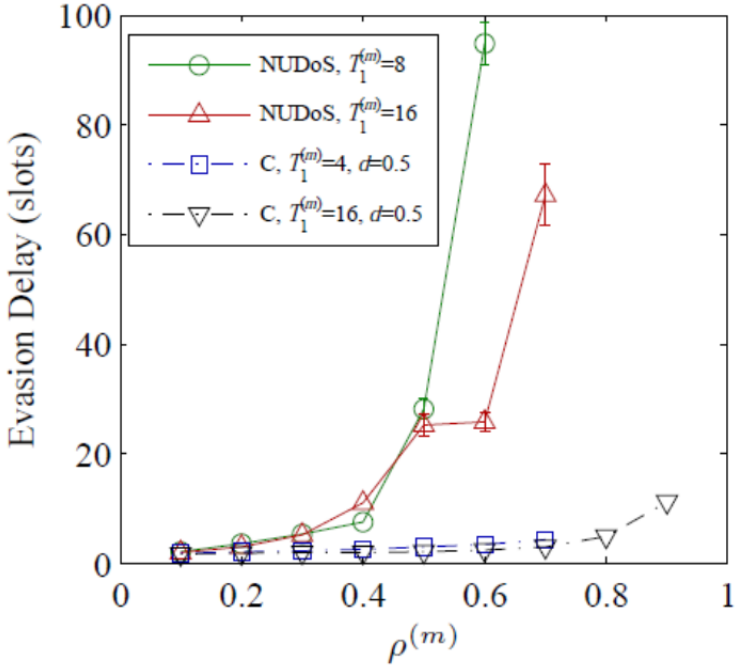


**Figure 5. ED vs. ρ(m) for NUDoS**

### 4.1.2 Hamming Distance

The HD for NUDoS and *C* is plotted in **Figure 6** and **Figure7**. The HD of NUDoS increases with *n* because of the reduction in the overlap ratio. It also increases with both *pth* and $\rho(m)$ because of the increase in the number of unassigned slots (in our simulations, each unassigned slot increments the HD by $1/n$). For small values of $\rho(m)$, less fluctuating channels result in larger HD, and the opposite is true for large values of $\rho(m)$.

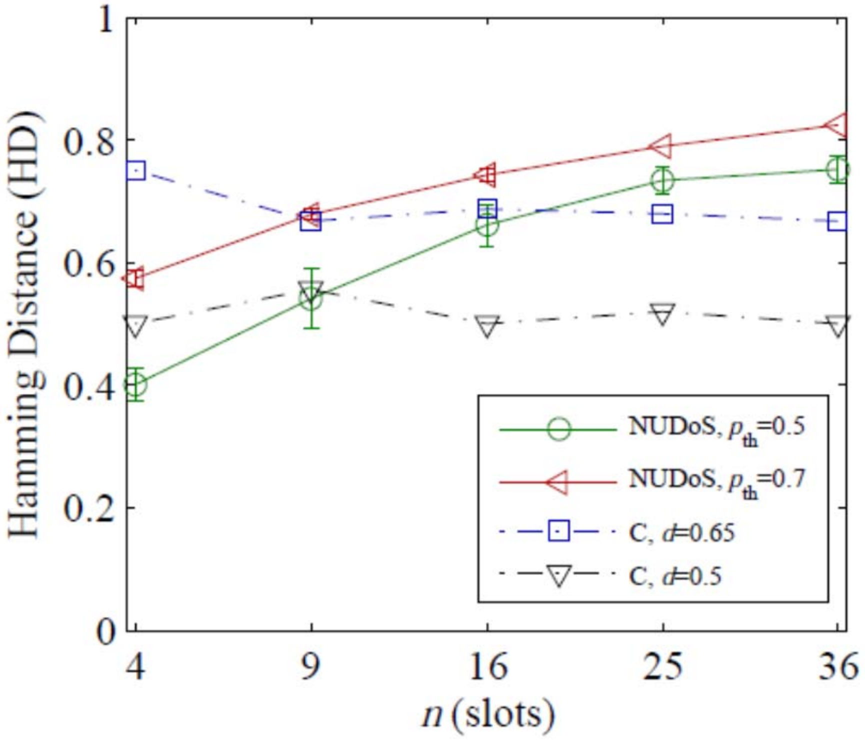


**Figure 6. HD vs. n for NUDoS**

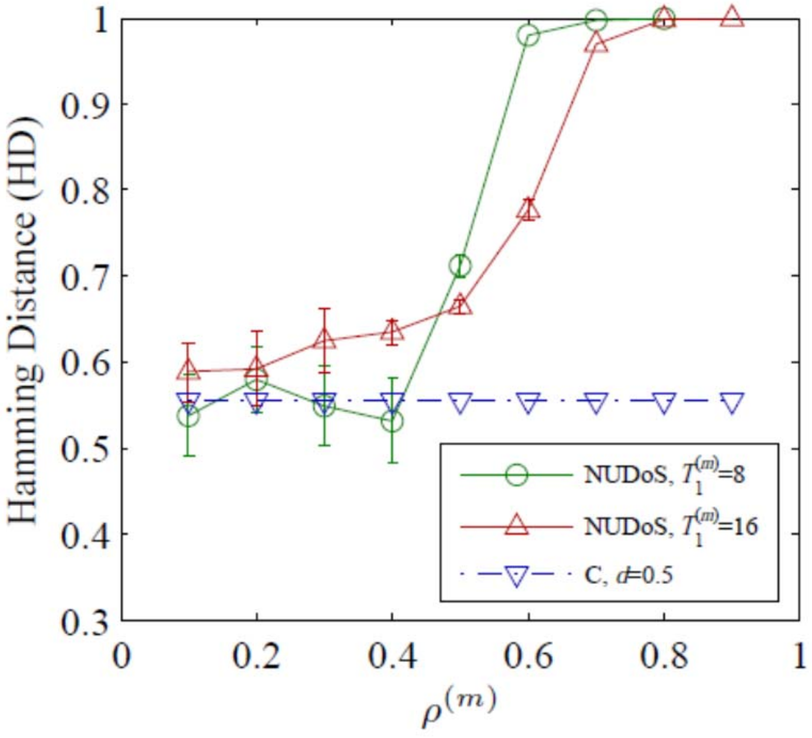


**Figure 7. HD vs. ρ(m) for NUDoS**

### 4.2 Game Theory Formulation of FH Strategies under an Intelligent, Reactive Jammer

In this section, we study our formulated games numerically under different values of the system parameters. We implement our games in MATLAB. The 95% confidence intervals are indicated in the figures. We have simulated the synchronous rendezvous game between the receiver (*R*) and jammer (*J*), assuming a uniformly random strategy for transmitter. **Figure 8** plots the expected utilities of *R* and *J* vs. the frame length (*m*). It also shows the utilities of *R* and *J* at the NE.

**Result:** *R benefits from being, along with J, unaware of the transmitter strategy. Furthermore, the benefits of R increase with m.*

As shown in **Figure 8**, the utility of *R* when *the transmitter strategy* is unknown is always better than his NE utility when *the transmitter strategy* is known. On the other hand, being unaware of *the transmitter strategy* always harms *J*. As *m* increases, the randomness about *the transmitter strategy* increases (recall that the strategy space of *T* is of dimension *m*), and the expected utility of *R* increases while the expected utility of *J* decreases.

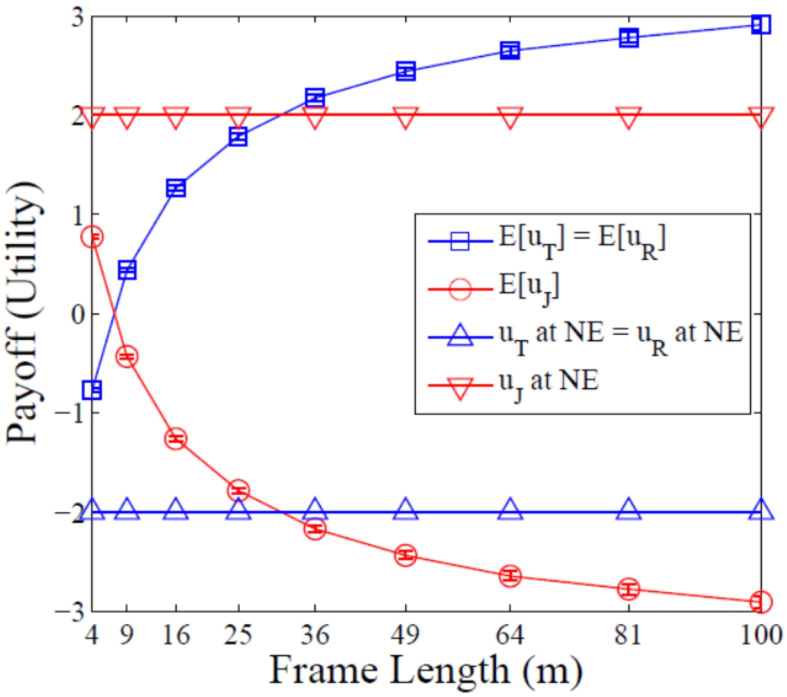


**Figure 8. Effect of the Frame Length on the Expected Utilities of Transmitter, Receiver, and Jammer**

### 4.3 Hybrid Systems Formulation of FH Strategies

**(i)** The modeling outlined in Section 3.3 falls in a general framework for hybrid systems [6] as the events triggering the changes of parameters are impulsive and do not necessarily follow a discretization of time, i.e., parameter changes can occur at any time instant $t$. An initial problem of study under this framework is the problem of coordinating the selection of channels by the ground stations and satellites so as to establish a communication link. This problem is referred to as the *rendezvous problem*. For the scenario in which a ground station $i \in \mathrm{U}$ is to establish a communication link with satellite $j \in \mathrm{V}$, the goal is to design a control policy that makes the channel selection parameters $p_\mathrm{i}$ and $q_\mathrm{j}$ (associated to the ground station and satellite) equal and, simultaneously, different from the channel selection made by the jammer. This problem is formulated as an optimization problem with hybrid dynamics. This can be formulated as an optimization problem with hybrid dynamics as presented below.

For the case of one ground station and one satellite, we define the indicator function

$$C(s_1, s_2) := \begin{cases} 1 & if \quad s_1 = s_2 \\ 0 & otherwise \end{cases} \tag{6}$$

Solutions to the following dynamic optimization problem lead to rendezvous between the ground station and the satellite:

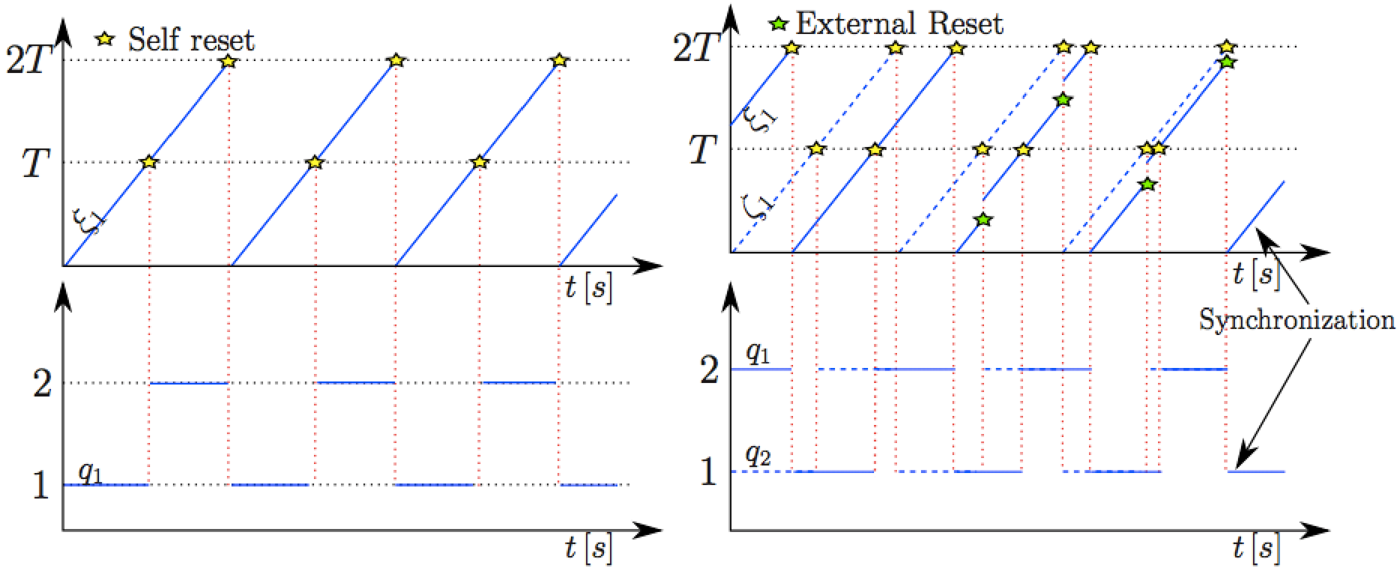
$$\begin{aligned} & \max C(p_1, q_1) \\ & subject\ to \\ & C1: \quad \dot{\xi}_1 = f_1(\xi_1, p_1), \dot{\zeta}_1 = h_1(\zeta_1, q_1) \\ & C2: \quad p_1^+ = g_1(p_1) \qquad (\xi_1, p_1) \in D_1^u \\ & C3: \quad q_1^+ = \kappa_1(q_1) \qquad (\zeta_1, q_1) \in D_1^v \end{aligned} \tag{7}$$

where $h_1, \kappa_1$ and $D_1^v$ are defined as $f_1, g_1$ and $D_1^u$ in Section 3.3, respectively. Maximization of $C$ will be attained when its arguments coincide, which corresponds to $p_1 = q_1$, i.e., same channel selection for ground station and satellite. Constraint C1 enforces that the variables evolve continuously according to the differential equations therein. Constraints C2 and C3 guarantee that the updates of the parameters $p_1$ and $q_1$ are:

The dynamic optimization problem above has the functions $f_1$, $h_1$, $g_1$, $\kappa_1$ and the sets $D_1^v$ and $D_1^u$ left unassigned. A particular initial selection of these functions and computation of the associated solutions to this problem were performed. For this purpose, the state $\xi_1$ of the ground station and the state $\zeta_1$ of the satellite are by timers and their parameters, $p_1$ and $q_1$, denote their current channel selection, respectively. These states and parameters are discretely updated when the timers reach a threshold ($T$) and are externally reset when information is received from each other. Information arrives to each agent from the pre-defined sub-band frequency channels. Both the ground station and satellite are considered as individual agents and are restricted to listen to a single channel at a time. The following mechanism is implemented according to the following rules:

- Each agent listens on the currently selected channel until its timer expires (reaches threshold $T$). Under such an event, the agent transmits a signal (or packet) on the current channel, resets its timer to zero, and switches to the other channel. **Figure 9** shows that situation for a single pulse-coupled oscillator.

- If an agent receives a packet while listening on the currently chosen channel, its timer is reset via an update law that reduces the listening time on that channel for the receiving agent. The reduction of the listening time is governed by a parameter denoted as $\varepsilon$. **Figure 9** demonstrates the interaction between two agents operating over two channels ($K = 2$).



(a) A single pulse-coupled oscillator.

(b) Two pulse-coupled oscillators.

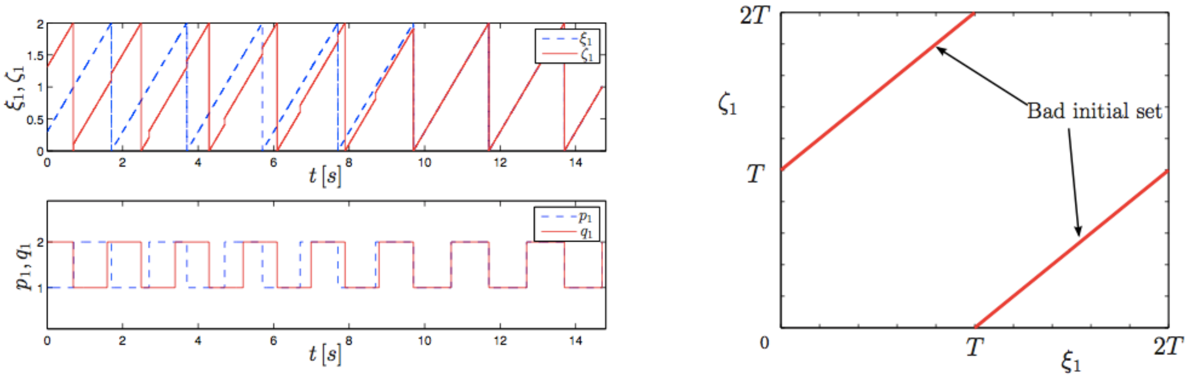
**Figure 9. (a) Trajectories $(\xi_1, p_1)$ of an Agent Over Two Channels**
**(b) Trajectories $(\xi_1, p_1)$ and $(\zeta_1, q_1)$ of Two Agents Over Two Channels**

This mechanism can be thought as a control algorithm. It is inspired by synchronization of biological systems in [7], where agents can “listen" all the time. In fact, the main difference between the mechanism above and the synchronization mechanism studied in [7] is that here there is a constraint on data reception, which depends on the channel currently chosen by the agents and does not guarantee that information sent is always received. In the case of a common channel and no information loss, the agents will synchronize as in the work of [7].

**Figure 10** shows a simulation of two agents synchronizing their internal timers and channel states until they are equal and evolving simultaneously over time. Using Lyapunov stability tools for hybrid systems, we have shown that the two agents are globally asymptotically stable to the set

$$\mathcal{A} := \{(\xi_1, p_1, \zeta_1, q_1) \ : \ \xi_1 = \zeta_1, p_1 = q_1\} \tag{8}$$

for every point not in the set depicted in red in **Figure 9**. Every other point not in red characterizes the basin of attraction of the solutions to the game stated above.



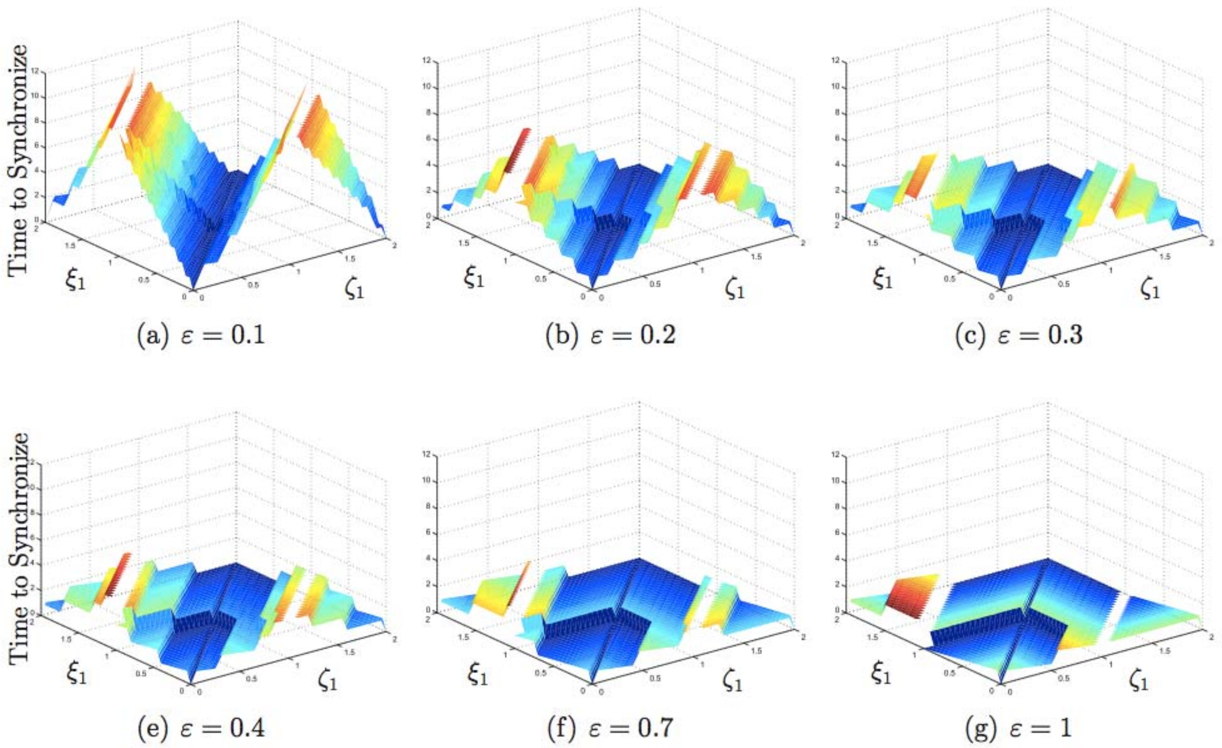
(a) Two agents covering two channels showing synchronization

(b) Region of attraction for 2 agents on 2 channels, the red lines are the points where the 2 agents will not rendezvous

**Figure 10. Two Agents Attempting Communication Between Two Channels and Region of Attraction**

The timer advance constant, $\varepsilon$, affects the rate at which the agents synchronize. In fact, the amount that the timers advance when a packet is received is governed by $\varepsilon$. If $\varepsilon \ll T$, when a packet is received, the algorithm increments the timers by a small amount. If $\varepsilon \geq T$ and a packet is received, the algorithm will automatically switch channels.

**Figure 11** shows the time for convergence to synchronization with respect to the timer advance constant, $\varepsilon$, and as a function of the initial conditions (away from the set of bad initial conditions in **Figure 9**).



(a) $\varepsilon = 0.1$ (b) $\varepsilon = 0.2$ (c) $\varepsilon = 0.3$

(e) $\varepsilon = 0.4$ (f) $\varepsilon = 0.7$ (g) $\varepsilon = 1$

**Figure 11. Time to Converge to $\mathcal{A}$, i.e., Time to Synchronize Timers and Channel Selections, for Parameter Values $\boldsymbol{\varepsilon = 0.1, 0.2, 0.3, 0.4, 0.7, 1}$**

A plot of the time to converge to synchronization with respect to the timer advance constant, $\varepsilon$, can be determined by choosing a potential worse case scenario. **Figure 12** shows the time to synchronization as a function of $\varepsilon$ with initial condition away from the synchronization set $\mathcal{A}$. The decreasing trend present in **Figure 12** indicates that as the timer advance constant is increased the time to convergence is decreased.

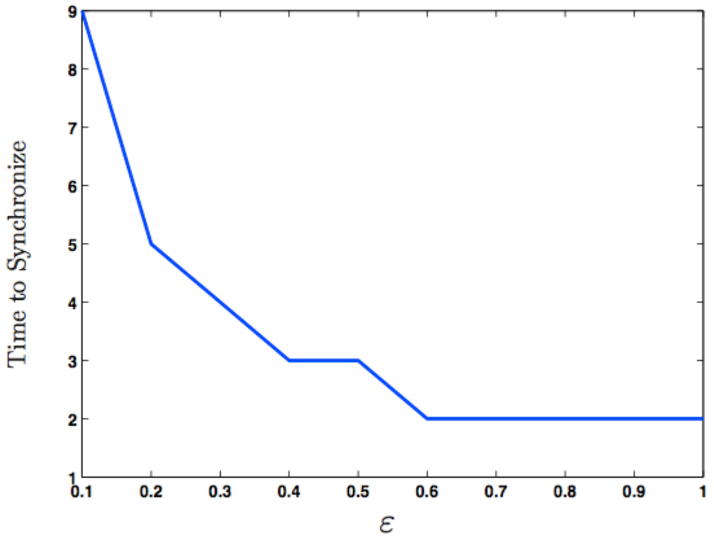


**Figure 12. Time to Synchronize as a Function of the Timer Advance Constant, $\varepsilon$ with Initial Condition Away from $\mathcal{A}$**

The performance analysis above suggests that the larger $\varepsilon$, the faster the trajectories will approach $\mathcal{A}$. However, a choice of the parameter $\varepsilon$ large may compromise the robustness to adversarial attack or environmental interference. To determine the robustness of the algorithm, two sets of simulations were performed. To model environmental interference, pseudo-random times for injection of interfering packets were generated. At these time instances, a packet was injected into agent 2's correct channel, forcing it to reset and advance its timer by $\varepsilon$. **Figure 13** also shows the number of injected packets versus the percentage of time on the same channel with the parameter $\varepsilon$ equal to 0.3 and 1. Polynomial curve fittings were numerically generated to express the downward trend as the number of packets increase. The figure shows that the effect of the interfering packets is more significant for large $\varepsilon$. In fact, the agents stay on the same channel longer (for the same number of interfering packets) when $\varepsilon$ is smaller.

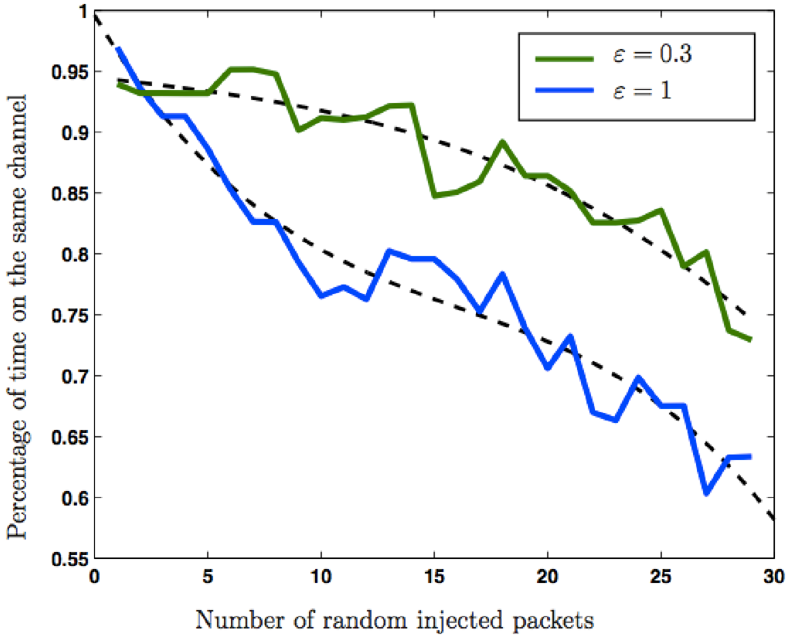


**Figure 13. Percentage of Time on the Same Channel Versus Number of Interfering Packets**

Regarding the case of more than two channels, initial efforts suggest that a minor tweak allowing randomized jumps leads to rendezvous over multiple channels with a large basin of attraction. **Figure 14** has two agents with $K = 20$. The agents reach the same channels at approximately 15 seconds. After that time, they continue to change channel together as they can communicate their decisions.

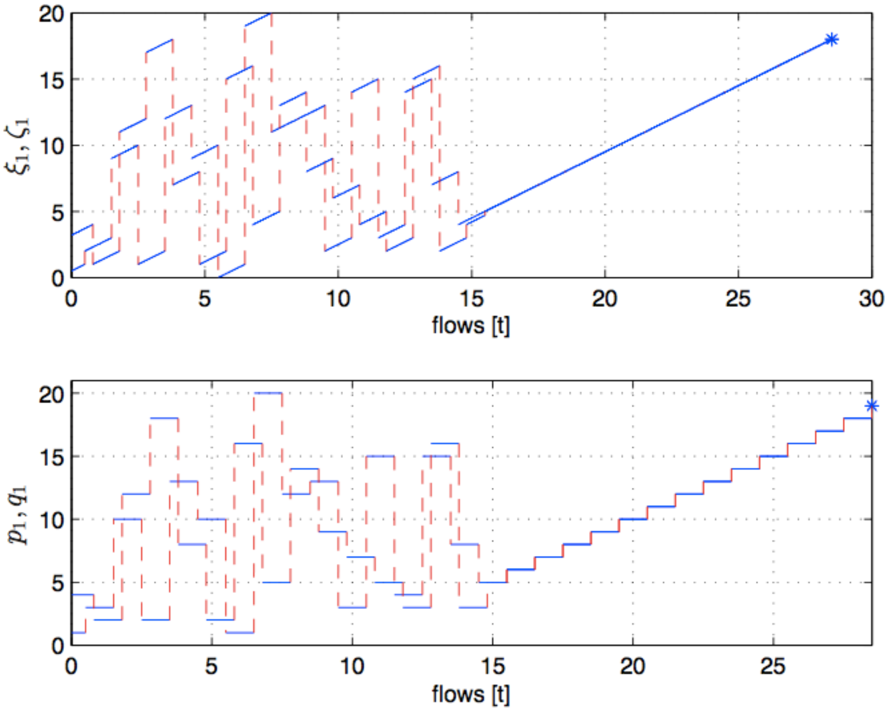


**Figure 14. Two Agents Attempting Communication Across 20 Channels**

Regarding the case of a jammer, an optimization problem with added jammer dynamics has been formulated. In the case where the rate of reaction of the jammer is not infinitely fast, namely, there is an uniform positive lower bound on the time elapsed between consecutive changes of the jammer's decision, the solutions to the optimization problem indicate that the choices made by the ground station and the satellite lead to rendezvous over the time window when the jammer choices is fixed. A limitation of this result is that the mentioned lower bound needs to be known to the other agents so that they can tune their timer threshold *T* appropriately. Currently, research efforts on this problem focus on the property of stabilizing the rendezvous condition under arbitrary changes of the jammer decisions. The approach currently being explored uses recent results on stabilization of hybrid systems under certain classes of switching signals [8].

## 5.0 CONCLUSIONS

In this project, we have designed a frequency hopping algorithm for rendezvous in satellite systems (NUDoS) in the presence of a jamming attack. Our algorithms are distributed, do not incur additional message exchange overhead, and work in the absence of synchronization. We simulated our algorithms under a realistic setting of no synchronization. Also, we have studied the rendezvous problem in the presence of an insider attack using a game-theoretic framework. Our numerical results revealed that being unaware of the transmitter strategy benefits the receiver. Hybrid systems theory was employed to model event-based algorithms in CR. In particular, optimization problems with hybrid dynamics have been formulated and solved numerically for the rendezvous problem.

## REFERENCES

[1] C. Cordeiro, K. Challapali, D. Birru, and S. Shankar. “IEEE 802.22: The first worldwide wireless standard based on cognitive radios.” *Proceedings of the IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks (DySPAN)*, November 2005, pp. 328-337.

[2] J. Wang, M. S. Song, S. Santhiveeran, K. Lim, G. Ko, K. Kim, S. Hwang, H. Sung, M. Ghosh, V. Gaddam, R. Vasanth, and K. Challapali. “First Cognitive Radio Networking Standard for Personal/Portable Devices in TV White Spaces.” *Proceedings of the IEEE DySPAN Conference*, April 2010, pp. 1-12.

[3] AFRL 2nd Workshop on Cognitive & Software-Defined RF Technology: Achieving Spectral Dominance for the AF of the Future, Dayton, Ohio, September 2011.

[4] R. Poisel. “Modern communications jamming principles and techniques.” *Artech House on Demand*, 2004.

[5] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. **Spread Spectrum Communications Handbook**. McGraw-Hill, 2001.

[6] R. Goebel, R.G. Sanfelice, and A. R. Teel. **Hybrid Dynamical Systems: Modeling, Stability, and Robustness**, *Princeton University Press*, 2012.

[7] R. E. Mirollo and S.H. Strogatz. “Synchronization of Pulse-Coupled Biological Oscillators.” *SIAM Journal on Applied Mathematics*, 1990, 50, pp. 1645-1662.

[8] P. Nanez and R. G. Sanfelice. “An Invariance Principle for Differential-Algebraic Equations with Jumps.” *Submitted to the 2014 American Control Conference*, June 4th - 6th 2014, Portland, OR, USA.

# LIST OF SYMBOLS, ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| AFSCN | Air Force Satellite Control Network |
| CR | Cognitive Radio |
| DFH | Dynamic Frequency Hopping |
| DOC | Denial of Communication |
| DSSS | Direct Sequence Spread Spectrum |
| ED | Evasion Delay |
| FH | Frequency Hopping |
| FHSS | Frequency Hopping Spread Spectrum |
| GPS | Global Positioning System |
| HD | Hamming Distance |
| ITU | International Telecommunication Union |
| LEO | Low Earth Orbit |
| NUDoS | Nested Unicast Rendezvous Algorithm for Denial-of-Service Attacks |
| OSA | Opportunistic Spectrum Access |
| PU | Primary User |
| R&D | Research and Development |
| SATCOM | Satellite Communications |
| SDR | Software Defined Radio |
| SU | Secondary User |
| TTR | Time-to-Rendezvous |
| UHF | Ultra High Frequency |
| VSAT | Very Small Aperture Terminal |
| WRAN | Wireless Regional Area Network |

# DISTRIBUTION LIST

DTIC/OCP
8725 John J. Kingman Rd, Suite 0944
Ft Belvoir, VA 22060-6218 1 cy

AFRL/RVIL
Kirtland AFB, NM 87117-5776 2 cys

Official Record Copy
AFRL/RVSV/Richard S. Erwin 1 cy