Living with Boisterous Neighbors: Studying the Interaction of Adaptive Jamming and Anti-Jamming

Bruce DeBruhl and Patrick Tague
Carnegie Mellon University
Electrical and Computer Engineering
{debruhl, tague}@cmu.edu

***Abstract*—Jamming has long been a problem in wireless communications, but with recent advances in adaptive jamming, adaptive anti-jamming, and other advanced physical layer security techniques, it is hard to understand whether we can keep the jammer at bay. In this work, we consider this problem and introduce a game-theoretic framework which gives us a tool to analyze the complex adaptive jamming and anti-jamming space. To illustrate the strengths and weaknesses in intelligent jamming and anti-jamming techniques, we present a straightforward two-player instance and analyze a number of possible jamming and anti-jamming techniques.**

I. Introduction

Susceptibility to interference is one of the major vulnerabilities in wireless communications. The process of maliciously sending a signal to interfere with or degrade wireless communications is known as jamming [1]. One way that jamming can be mitigated is by spreading the signal over a wider frequency band in a process known as spread spectrum [2]. One of the implementations of spread spectrum communications is known as direct sequence spread spectrum (DSSS). DSSS hides the legitimate signal by mapping each bit to many chips and sending them at a higher rate. This diversity allows for a higher probability of properly recovering a bit and makes the radio less succseptible to jamming.

Because of the additional energy needed to jam spread spectrum techniques, intelligent jamming techniques have been proposed [3], [4], [5], [6]. These include reactive jamming [4], in which the attacker listens to the channel and jams only when a signal of interest is detected. This also can be done in a targeted manner, jamming only when particular nodes are broadcasting [7]. Another type of effective and efficient jamming attack is periodic jamming [4], in which the attacker alternates its radio between jamming and sleeping states. If the jamming pulses are sufficiently high power, the attacker can set the jamming period to around the inter-packet duration, and the resulting duty cycle can be as low as a few percent of this inter-packet duration without significant loss of effectiveness. Other jamming attacks use higher layer information to mount even more efficient jamming attacks [5], [6].

Recently, classes of adaptive jamming and anti-jamming techniques have been proposed [8], [9], [10]. These attacks and defense mechanisms allow for a more intelligent approach to optimizing the interaction a radio has with its neighbors. These attacks have been proposed for online optimization [8], [10] and defense mechanisms [9].

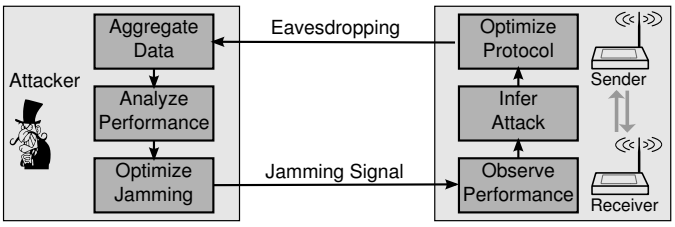

Fig. 1: We show the interaction of an adaptive jammer and a communication system employing anti-jamming techniques. It is difficult to predict the equilibrium state of these two dynamic systems because of their complex interactions.

As more adaptive jamming and anti-jamming techniques are designed, we must consider how they interact. In this work, we thus introduce a game-theoretic model to explore the interaction of adaptive jamming and anti-jamming strategies. The major contributions of our work include the following.

- We introduce a dynamic asynchronous 3-player game to analyze the performance of adaptive jamming and anti-jamming technology.
- We introduce a simplified 2-player single round asynchronous game to analyze basic performance of adaptive jamming and anti-jamming receivers.
- We present an empirical test for the 3-player game.
- We present preliminary empirical results for the 2-player single round game where a jammer and receiver both have complete freedom to choose there strategy.

II. 3-Player Asynchronous Game Framework

In this section we introduce a high-level model of the communication system that we consider. We then introduce the complete 3-player game that is used to analyze our jamming and anti-jamming systems.

A. System Model

We assume a system model consisting of an attacker, a receiver, and a transmitter. All of these devices have similar energy capabilities. These devices are also assumed to be software-defined radios with the ability to adapt their radio configuration. However, we constrain them to all use the same channel.

We refer to the receiver and transmitter as the legitimate node's and define their main goal as transferring data from

the transmitter to the receiver with the minimal amount of work, as seen in the right half of Figure 1. We allow for the legitimate nodes to use direct observations about the channel as well as meta-data about its performance to decide on the communication protocol and parameters that it uses. The legitimate nodes' data are assumed to be encrypted, and they operate with high fidelity in benign conditions.

The attacker in our system is able to observe the legitimate communications as well as jam the channel, as shown in the left half of Figure 1. This allows for an attacker to change its strategy when its current attack is ineffective or inefficient. In this work, we focus on an attacker using periodic jamming, though this framework can be generalized to a large number of network attacks. The jammer's observations only aim to observe meta-data, like packet delivery ratio between the two nodes, because the encryption makes decoding packets prohibitively expensive.

B. Game Participants

The game participants can be divided into two teams. The defending team consists of the transmitter and receiver, while the attacking team consists of only the jammer. In this section, we discuss each team, their goals, and their operation.

1) Defenders: The receiver and transmitter in our system choose from a set of protocols that we call strategies and denote as S_r and S_t, respectively. We also define a set of free-parameters for each strategy denoted as $\mathbf{p}_r$ and $\mathbf{p}_t$ for the receiver and transmitter, respectively. At any given time step the legitimate nodes also are given feedback

Remembering that the legitimate nodes goal is to effectively communicate with a minimal amount of work, we define vectors $\mathbf{u}_r$ and $\mathbf{u}_t$, which are a collection of parameters indicating the goals for both the receiver and transmitter. We can define elements of $\mathbf{u}_r$ or $\mathbf{u}_t$ to include goals like energy consumption, throughput, goodput, or many other network statistics.

We also define $\mathbf{q}_r$ and $\mathbf{q}_t$ as vectors of information that has been inferred about the attack being mounted against the legitimate nodes from the receiver and transmitter, respectively. Thus the goal of a receiver is to choose a strategy S_r and parameters $\mathbf{p}_r$ to optimize its utility function $\mathbf{u}_r$ given the knowledge of the jammer $\mathbf{q}_r$. A similar statement can be made for the transmitter.

The defending team must co-operate and collaborate. If a transmitter is using a protocol that the receiver is unable to decipher, they are not able to communicate. Working collaboratively also allows for common goals for the two nodes. This allows us to define a utility function for the defending team as $\mathbf{u}_d = \frac{1}{2}(\mathbf{u}_r + \mathbf{u}_t)$. Having collaboration between the receiver and transmitter allows for collusion to infer information about the attacker's location. The need and benefits of the sender and receiver collaborating is an interesting research problem that we leave as future work.

2) Attacker: The attacker in this game both observes the legitimate system and jams the communication channel. Like above, we define a strategy parameter S_j, a parameter vector $\mathbf{p}_j$, a utility function vector $\mathbf{u}_j$, and a knowledge vector about the legitimate system $\mathbf{q}_j$.

One Player Turn	
Given:	$\xi_{k-1}, \mathbf{u}, \mathbf{q}_{k-1}$
Update knowledgebase:	$\mathbf{q}_k = append(\mathbf{q}_{k-1}, \xi_{k-1})$
Optimize:	$(S_k,\ \mathbf{p}_k) = \underset{S,\mathbf{p}}{\arg\max}\ \mathbf{u}$ given $\mathbf{q}_k$

Fig. 2: This algorithm shows the operations performed for every turn of the multiplayer asynchronous game.

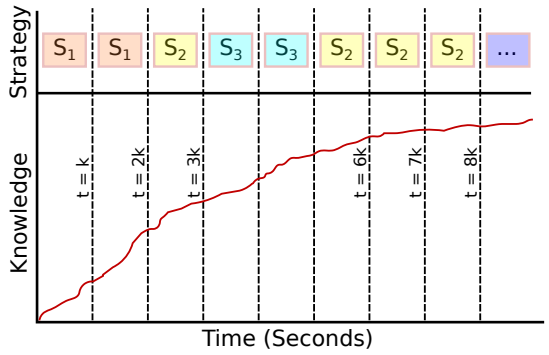

Fig. 3: We present one dynamic player in a game against two static players. As time continues the amount of knowledge the player has continually increases allowing for increasingly intelligent strategies.

C. Game Play

To explain the game play we show how play works with one dynamic player and two static players. We then continue our explanation for the case of three dynamic players.

D. One player

We first discuss game play from the perspective of one player, while the two other players are static in strategy. Examples of this include a receiver trying to optimize reception for particular transmitter and attacker or a jammer trying to optimize its attack against a particular transmitter and receiver. We assume that the game is played such that a player can select a new strategy at each time multiple of k, but can select new parameters for their strategy at any time. Thus in Figure 3 we see the player change its strategy after time $t = 2k$, $t = 3k$, $t = 5k$ and so on. But the player could have adapted its parameters many times before time $t = 2k$. We also show an example of the amount of knowledge gained as time goes on. Since we assume all other players have static locations, strategies, etc in this example the knowledge gained always increases. In the next section we discuss a case when this is not true.

The basic round for a player is as follows. To begin, they update their knowledge base using current information, $\mathbf{q}_k = append(\mathbf{q}_{k-1}, \xi)$ where *append* combines two vectors: $\mathbf{q}_{k-1}$ is the vector from the previous time step and ξ is

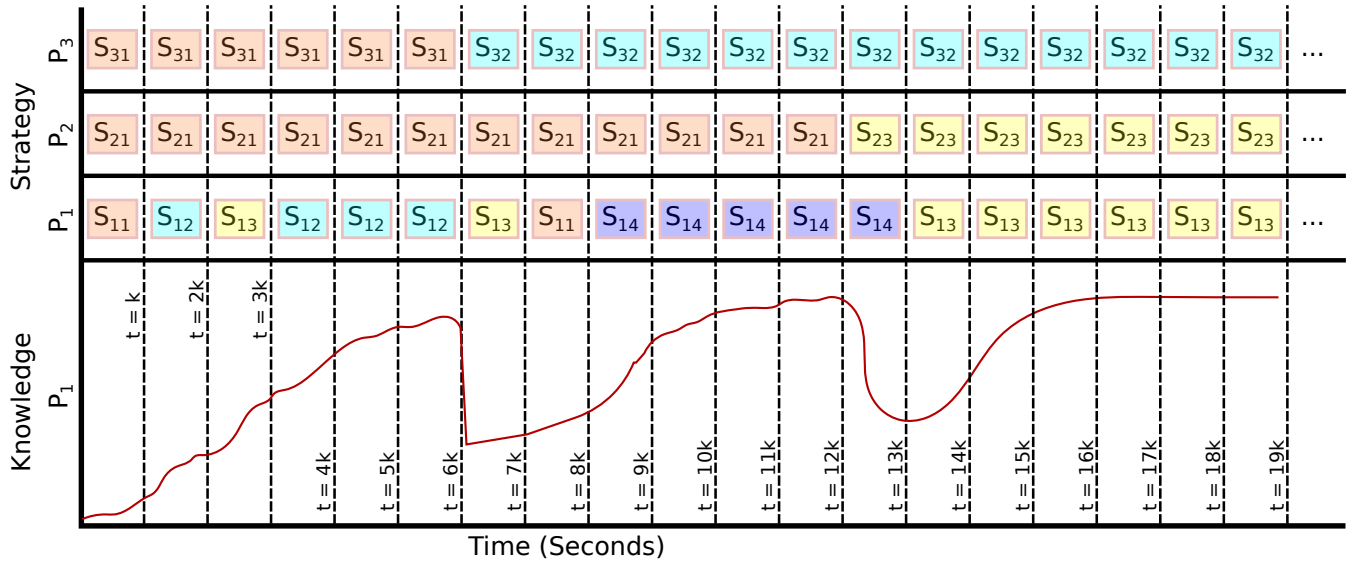

Fig. 4: We present a game with three players adapting their strategies dynamically. At each time multiple of k a player can continue using its current strategy or select a new strategy. Here we also show a example of the curve for knowledge gained about the other players from player ones perspective. When another player's strategy changes the knowledge gained drops because some information no longer holds. At the end of the graph all three players converge to a strategy showing the end state.

new observations. The player than chooses a strategy and parameters to optimize $\mathbf{u}$ given $\mathbf{q}_k$.

E. Three Players

We now discuss the game played by three nodes with dynamic strategies as shown in Figure 4. The game play for any one player in this game is the same as above but the gained knowledge is not monotonically increasing as in the one-dynamic player case. The reason this happens is that a player builds a knowledgebase which becomes a liability when one of the other players switch strategies. This can be seen to happen after time $t = 6k$ and $t = 12k$. To counteract the effect of bad data being a liability a node that is learning about a system needs to use a forgetting factor. The rest of the learning and game parameters carry over from the basic case.

III. 2-Player Single Round Game Framework

In this section, we introduce a simplified game that allows us to do preliminary analysis of the interactions of 2-players. The 2-players analyzed are the attacker and receiver, while the transmitter is static in strategy and parameters. In this game both the receiver and jammer secretly select a strategy. This is done with no previous knowledge or assumptions about what the other player will do. The 2-players then implement their strategy in the physical system and measure their utility. Figure 5 summarizes the single round 2-player game.

It may be helpful to describe the game from one of the player's, we thus describe the game from the jammer's perspective. Prior to the start of the game the jammer chooses a strategy S_j and the necessary parameters $\mathbf{p}_j$ for S_j. At the start of the game the receiver and jammer reveals their strategy S_R and parameters $\mathbf{p}_R$. The jammer and receiver than attempt their strategy on the system and observe their desired

2-Player Game		
	Jammer	Receiver
Choose Secret Strategy:		
Reveal:		
Evaluate Objective Function:	$u_J = .902$	$u_R = .124$

Fig. 5: In this figure, we show a simplification of the three player asynchronous multi-round game as a single round 2-player game. This allows us to do preliminary analysis of strategies and strategy parameter spaces.

utility function. Thus the jammer now has a measurement for $\mathbf{u}(\mathbf{p}_j, S_j, \mathbf{p}_R, S_R)$. For this game, we assume that each player has a single-objective utility function. This can be accomplished by only choosing one parameter or by averaging multiple parameters.

The main goal of introducing the 2-player game is to allow for ease in analysis of steady state responses of an attacking and defending strategy. This is an important results for choosing an attack or protocol as well as being the necessary predecessor to the full 3-player game. In the 3-player case it is important that a player understand the space enough

to be able to perturb the network, or purposely try things to test the state of other players in the network. Thus we introduce preliminary analysis of the 2-player game in Section IV.

IV. Empirical Results of 2-player Game

In this section we introduce empirical results for the game presented in this paper. We first introduce an instantiation of the game, then discuss the hardware setup used to analyze the game, and finally introduce interesting results from a preliminary test of the single round 2-player game.

A. Instantiation

We build a preliminary test of our 2-player game using the IEEE 802.15.4 protocol [11] as a testing platform. We implement a generic IEEE 802.15.4 protocol which is a direct sequence spread spectrum protocol (DSSS). We also implement a modified DSSS which adds a single filter [12] and another implementing an adaptive set of filters [9]. We can thus define the vector $S_R = \{\text{DSSS, Single Filter, Adaptive Filter}\}$. We do not consider adaptation of the parameters of the receiver, though this would expand the search space of the receiver considerably and be an interesting extension to our game.

We design a short form periodic jammer that can be used in multiple ways. The most basic attack uses it as a periodic jammer with free parameters for offset from channel center frequency, signal amplitude, and duty cycle. Thus $S_{j1} = \{\text{Periodic Jammer}\}$ with corresponding parameters $\mathbf{p}_{j1} = \{\text{Amplitude, Duty Cycle, Center Frequency Offset}\}$. The second strategy we use is Self-Tuned, Inference-based, Real-Time jamming or STIR-jamming [10]. We can then define $S_{j2} = \{\text{STIR-jamming}\}$ with corresponding parameters $\mathbf{p}_{j2} = \{W_I, W_E, W_D\}$, where W_I, W_E, W_D are the importance the jammer ascribes to having a high impact, minimizing energy usage, and not being detected. Lastly we include a random center jammer [9], where the jammer changes its offset of its center frequency to different points in the channel every τ seconds. We define $S_{j3} = \{\text{Random Center Jamming}\}$ and corresponding parameters $\mathbf{p}_{j3} = \{\text{Amplitude, Duty Cycle, } \tau\}$

1) Hardware Set-Up: We implement this game on USRP2 software defined radio [13] using GnuRadio [14] and a previous IEEE 802.15.4 [15] implementation. For our implementation we connect three radios, a receiver, transmitter, and a jammer, to one laptop which allows for control of, and feedback from, all the radios, allowing us to analyze the utility of both the transmitter and the receiver. We explore the attacks effect only on the physical layer and do not consider the effect of jamming on a carrier sensing system.

We define the utility function for the receiver as packet delivery ratio (PDR). This is a straight forward parameter to measure since we are using a constant packet rate from our radios. For the jammer's utility function we are concerned with energy usage and performance. We thus define the jamming utility function in terms of PDR and normalized instantaneous power usage P as $\mathbf{u}_j = \frac{P+PDR}{2}$.

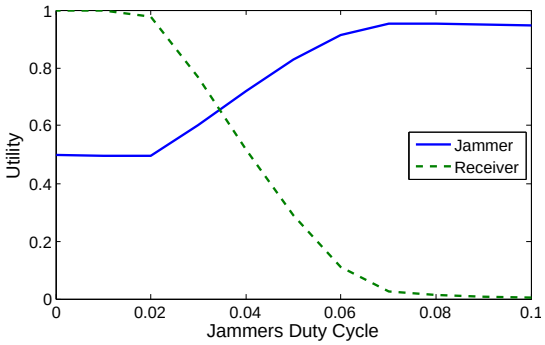

Fig. 6: We show the results of a periodic jamming attack against a DSSS system. It is interesting to note that an attacker only has to be on 8% of the time to effectively deny all packets from transmitting to the receiver. This does not consider the effect of MAC layer jamming either, if CSMA is used the effect would likely be greater.

B. Results

In this section we introduce four type of results. The first is from a basic DSSS radio and periodic attacker. The second is from a receiver with a single filter and an attacker that can offset the center of its modulation frequency while the third allows for a receiver with adaptive filtering and an attacker which can change the center of its modulation frequency every τ seconds. Lastly we present preliminary analysis of STIR-jamming's effectiveness against a basic DSSS receiver and a single filter receiver.

1) Basic Attacker and Receiver: The first experiment is to test the basic attacker and receiver. One free parameter that we explore is duty cycle because we desire to know at which duty cycle does a jammer effectively deny service to the legitimate node.

We show the results for a periodic jammer against the DSSS attack in Figure 6. This figure shows an interesting result that almost all traffic can be stopped by jamming only 8% of the time. A considerable amount, around 20% of packets can also be stopped by attacking as little as 3% of the time. This shows the main advantage of periodic jamming, it is able to have a high impact with little cost.

2) Single Filter: To mitigate the effect of periodic jamming it was proposed to use a single filter to eliminate the attacker's spectrum. This filter is inserted in the receiver's architecture at base band and eliminates a very narrow spectrum. If the attacker is using the channel then its narrow band is weakened while the legitimate node still has enough bandwidth to recover information.

To experiment on a single filter receiver we are interested in seeing which attacks can effectively degrade its performance. To do this we again use a periodic jammer. We first attempt to find a parameter set that degrades performance by adjusting power and duty cycle. When we increase both of these to maximum it is still unable to effect the single filter receiver. This is due to our jammer having a maximum allowed power, if it had a larger upper bound a solution to jam the receiver would be found.

In Figure 7 we show an attack that is effective against the

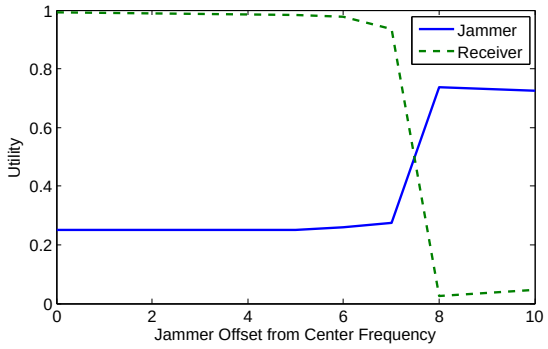

Fig. 7: In this figure, we show the effect of a periodic jammer against a receiver with a single filter. The jammer holds a constant normalized power level and duty cycle but varies its modulation center frequency. It can be seen that by varying the center frequency 8 kHz the jammer can effectively attack the legitimate system.

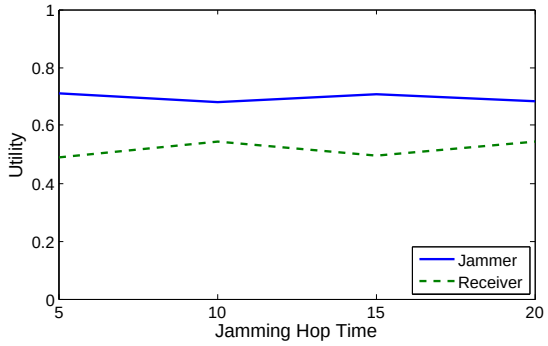

Fig. 8: In this experiment we explore the effect of random transition of a random center jammer on the utility of a jammer and receiver. Surprisingly, the effect of changing τ seems negligible in these preliminary tests.

single filter. In this attack we use a normalized power of .5 and a duty cycle of 10% but vary the offset of the jammer modulation center frequency. It can be seen that by varying only 8 kHz the jammer can effectively deny service to the receiver. This is an important result that shows the limitations of using a single filter to mitigate the effect of jamming.

3) Adaptive Filtering: The third experiment we consider is when an attacker randomly changes its modulation center frequency every τ seconds and a receiver adaptively tries to find a filter from a filter bank. The adaptive filter receiver tries a new solution every .5 seconds when its performance is below a threshold.

In Figure 8 we show the results for different values of τ for the jammer. These results are counterintuitive, at first glance one would expect the legitimate systems performance to be best when the attacker switches slowly and worse when it switches quickly. This does not hold because some attacking frequencies are very difficult to find and thus a good solution may never be found on a round. With the attacker with a larger τ this means that if it finds a solution without a good filter it degrades communications for a full 20 seconds. Further testing should be done on this problem to determine if there exists an optimal set of filters such that this problem does not persist.

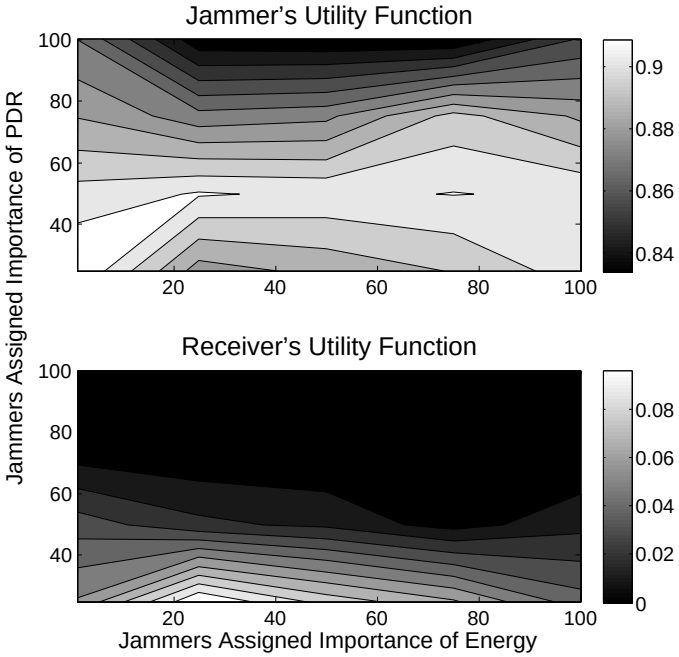

Fig. 9: In the first STIR-jamming experiment we show the results of varying two of STIR-jamming's weights. Along the x-axis we vary W_E and along the y-axis we vary W_I. The effect of these two parameters on the utility function is limited as can be seen in these contour plots.

4) STIR-Jamming: Lastly we explore the effectiveness of STIR-jamming. STIR-jamming tries to design effective attacks by observing the legitimate system, modeling its effect on the system, and optimizing given this information. There are two primary questions that we explore for a STIR-jammer. First, how effective is a STIR-jammer at meeting its goals given a set of weights. Secondly, does a STIR-jammer know when to quit.

We present Figure 9 to explore the effect of STIR-jamming weights on the utility of the attacker. This figure shows that there is limited differentiation between the effect of the Impact and Energy parameters W_I and W_E for the STIR-jammer. In our run of the various parameter combinations we saw a range of from only .82 to .94 utility. For the receiver we similarly saw a utility range from 0 to .12. It is important to note that these results should only be used as suggestions, to conclusively state the effectiveness of various parameters of STIR-jamming a much mode detailed analysis would have to be completed.

We then present Figure 10 to explore if there is a set of parameter for which STIR-jamming quits attacking. To do this we use STIR-jamming against a single filter receiver, which is effective at mitigating the effects of STIR-jamming given the attacker's power constraints. To test this we set the importance of impact to the maximum value $W_I = 100$ and decreased the values for the other two weights W_E and W_D at the same rate. What we found was that given that $W_E = W_D \leq 8$ that the attacker would attempt to degrade the legitimate systems service even if it was having no effect. Thus its utility approaches zero. On the other hand if $W_E = W_D > 8$

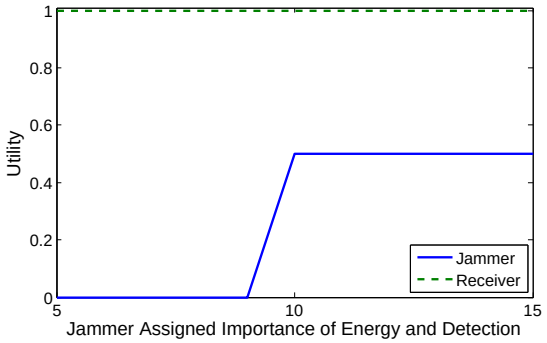

Fig. 10: In the second STIR-jamming experiment we show the effect of varying parameters on STIR-jamming retreating. If a strong imbalance in parameters is present $W_I >> W_E = W_D$ than STIR-jamming wastes energy when it is having no effect.

then we find that the STIR-jammer knows to quit attempting to degrade service and turns off. Since we define utility as an average dependant on power usage and degradation of service this give a much better utility score.

5) Aggregation: As we learn more about the system and the interaction of our legitimate receiver and attacker it is important to explore how the two can adapt. The aggregation of information about system performance has many nuances that are interesting but particularly interesting in this case is how one perturbs the system and how to forget data that is no longer true. The first problem can be solved by incorporating a simulated annealing like mechanism where it is possible to "heat" a search space and leave a good solution to look for better. The second problem requires a player to wager how quickly opponents change there strategy. If they assume they change too quick then they will not use their full information. If they assume they change to slow they use bad information.

Both of these problems are interesting research problems in this game theoretic framework that we leave as future work.

V. Conclusion

In this work, we have presented a game-theoretic framework to characterize and analyze the complex interactions between adaptive jamming and anti-jamming. Based on the general framework, we presented a two-player instance and described a number of jamming and anti-jamming strategies with the corresponding attack and defense parameters. We showed how the framework can be used to analyze the performance of the adaptive jamming protocols and reach interesting and valuable conclusions about the attacks and corresponding defenses. We believe this framework provides a firm basis for evaluating future jamming and anti-jamming techniques in a practical setting, allowing for analysis of steady-state performance between two interacting non-linear systems.

References

[1] K. Pelechrinis, M. Iliofotou, and S. Krishnamurthy, "Denial of service attacks in wireless networks: the case of jammers," *IEEE Comm Surveys and Tutorials*, 2011.

[2] D. J. Torrieri, *Principles of Secure Communication Systems*, 2nd ed. Boston: Artech House, 1992.

[3] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the performance of IEEE 802.11 under jamming," *INFOCOM 2008*, Apr. 2008.

[4] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[5] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control channel jamming: Resilience and identification of traitors," in *Proc. IEEE International Symposium on Information Theory (ISIT'07)*, Nice, France, Jun. 2007.

[6] P. Tague, M. Li, and R. Poovendran, "Mitigation of control channel jamming under node capture attacks," *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, Sep. 2009.

[7] W. M, I. Martinovic, J. Shmitt, and V. Lenders, "Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. 4th ACM Conf. on Wireless Network Security*, Hamburg, Germany, 2011.

[8] B. Awerbuch, A. Richa, and C. Scheideler, "A jamming-resistant mac protocol for single-hop wireless networks," in *Proceedings of ACM Symposium on Principles of Distributed Computing*, Toronto, CA, 2008.

[9] B. DeBruhl and P. Tague, "Adaptive filtering techniques for jamming mitigation," in *PECCS'12 (Special Session)*, Feb. 2012.

[10] B. DeBruhl, Y. Kim, Z. Weinberg, and P. Tague, "Stir-ing the wireless ether with self-tuned, inference-based, real-time jamming," Wireless Network and System Security Lab, CMU, Tech. Rep., 2012, available at http://wnss.sv.cmu.edu/papers/TR-STIR.pdf.

[11] "IEEE 802.15.4-2006," 2006, http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf.

[12] B. DeBruhl and P. Tague, "Digital filter design for jamming mitigation in 802.15.4 communication," in *ICCCN'11*, Aug. 2011.

[13] "Ettus research LLC," 2011, http://www.ettus.com/.

[14] "GNU radio," 2011, http://gnuradio.org/.

[15] T. Schmid, O. Sekkat, and M. Srivastava, "An experimental study of network performance impact of increased latency in software defined radios," in *WiNTECH'07*, Montreal, Quebec, Canada, 2007.