A Toolbox to Explore the Interaction of Adaptive Jamming and Anti-Jamming

Bruce DeBruhl, Yu Seung Kim, and Patrick Tague
Carnegie Mellon University
{debruhl, yuseungk, tague}@cmu.edu

***Abstract*—Jamming has long been a problem in wireless communications. Recently, adaptive jamming and anti-jamming techniques have been proposed which aim to use feedback to better perform their task. For an anti-jamming receiver this means detecting jamming and adapting its protocol appropriately. For a jammer this means using feedback from the legitimate system to design a high-impact, low-power, hard-to-detect attack. In this work we introduce a toolbox to allow users to tests the performance of adaptive jamming and anti-jamming on the USRP2 radio platform. These test provide an important function by letting developers understand how well new protocols work against evolving jamming technologies.**

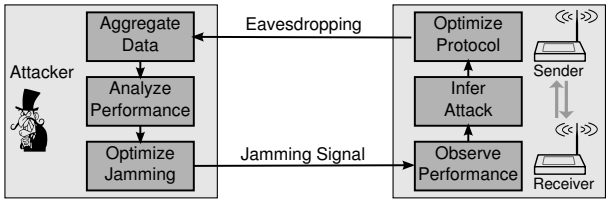

Fig. 1: We show the interaction of an adaptive jammer and a communication system employing anti-jamming techniques. It is difficult to predict the equilibrium state of these two dynamic systems because of their complex interactions.

I. Introduction

Wireless communications allows for transferring data without expensive wires but this open nature also increases susceptibility to malicious users. An attack known as jamming [1] degrades wireless communications by purposely broadcasting interference onto the wireless medium. One defense to mitigate jamming [1] is direct sequence spread spectrum (DSSS), where radios maps bit or symbols to many chips which are sent at greater rates than the data rate. DSSS makes the legitimate signal hard to detect, allows for more robust bit recovery, and makes a jammer use more energy to mount equally effective attacks. Another approach to deter jamming is to use detection techniques and retreat from jammers. At the MAC layer, jamming detection can be done by monitoring the packet delivery ratio (PDR) and flagging unexpected changes [2].

To overcome the additional cost of jamming a spread spectrum system and avoid detection, intelligent jamming techniques have been proposed [1]. One intelligent jamming attack is periodic jamming, where the attacker alternates between a sleeping and attacking state. In previous work, we explore the use adaptation for jamming and defending the IEEE 802.15.4 protocol [3]. To defend against jamming, we introduced adaptive filtering [4] which looks to mitigate the effects of periodic jamming by adapting band-stop filters to eliminate the attackers. We have also introduced an adaptive jamming attack we call Self-Tuned, Inference-based, Real-time jamming or STIR-jamming [5]. STIR-jamming uses feedback inferred from the legitimate communication system to optimize an attack with high impact, low power, and low probability of detection.

As more adaptive jamming and anti-jamming techniques are designed it is important to consider how they interact. Thus we introduce a toolbox to explore the interaction of Adaptive Jamming and Anti-Jamming strategies. The major contributions of our work include the following.

- We develop a toolbox of basic and adaptive jammers which also allows parameter selection.
- We develop a toolbox of static and adaptive anti-jamming techniques.
- Our system allows for real-time visualization of the performance of adaptive jammers and receivers.

II. Toolbox Features

In this section, we introduce our toolbox. This includes static and adaptive jammers as well as various receiver architectures. We also consider the benefit of seeing the complex interaction of adaptive jamming and anti-jamming receivers.

A. Jammers

We include static strategy and adaptive jammers in out toolbox for robust testing of anti-jamming techniques. We include a **constant tone jammer**, which continually modulates a tone onto the channel. In our demo we allow the user to adjust the constant tone jammers power level and modulation center frequency. We also implement a **periodic jammer**, which alternates between attacking and sleeping states. For the periodic jammer in our demo the user can adjust power level, percentage of time attacking, and modulation center frequency.

We include two jammers with moving modulation center frequencies. These jammers use periodic jamming that changes modulation frequencies occasionally. The first moving center technique is **random center jamming** which randomly selects a new center frequency every time step. The second moving center technique is **decremental jamming** which decreases its center frequency by a constant frequency every time step.

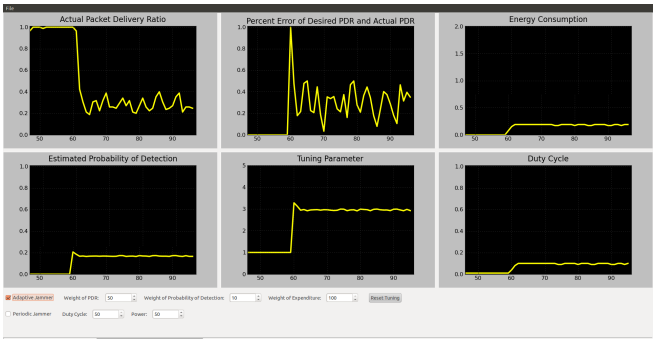

Fig. 2: We show a screen-shot of our demo with STIR-jamming against a DSSS receiver. The top left graph shows the receiver's PDR and the top right graph shows the jammers energy consumption.

For these attacks, the user selects parameters including power, duty cycle and time step for changing center frequencies.

Finally, we include **STIR-jamming** [5] which is an adaptive jamming technique. STIR-jamming aims to use information inferred about the performance of the system-under-attack to optimize a high-impact, low-power, hard-to-detect attack. To do this STIR-jamming monitors the packet delivery ratio (PDR) of the system-under-attack and uses this information to develop a model of the jammer's impact. When this model is trained STIR-jamming can optimize the tradeoffs between impact, power consumption, and detectability. In this attack, the user assigns weights indicating the importance of impact, power consumption, and detectability.

B. Anti-jamming Techniques

We include two anti-jamming receivers in our toolbox. The first is a **DSSS** receiver architecture modeled after the IEEE 802.15.4 2.4 GHz physical layer standard [3].

The second receiver employs **adaptive filtering** [4] which adds a digital filter and filter-tuner to the DSSS architecture to mitigate the effect of periodic jamming. Adaptive filtering is accomplished by first monitoring the receivers performance by calculating the PDR. Adaptive filtering then selects a jamming mitigation filter if an attack is inferred from a low PDR. We do this by selecting a filter from a filter-bank and testing if the receivers performance is improved. This process is repeated until a proper filter is found in the filter-bank.

C. Interaction

One of the interesting applications of this toolbox is to assess the strength of adaptive jamming and anti-jamming techniques when used against each other. Adaptive jamming and anti-jamming interact as shown in Figure 1. This figure shows the complexity of two dynamically changing systems. This toolbox allows for real-time comparisons of new jamming and anti-jamming technologies as jamming technology continue to advance. Such comparisons is important for the designing vital communication technologies of the future.

III. Demo Setup

This demo will highlight adaptive jamming and anti-jamming techniques as well as the interaction between these technologies. It is implemented on the USRP2 hardware platform [6] using GnuRadio [7] and a previous IEEE 802.15.4 [8] implementation. For the demo we connect three radios, a receiver, transmitter, and a jammer, to one laptop which allows for control of, and feedback from, all the radios.

This demo aims to be interactive, allowing the user to select a jamming attack, a receiver architecture and relevant parameters. The user has the option of selecting a wide range of static jammers (tone jamming, periodic jamming, random center jamming), dynamic jammers (random center jamming, STIR-jamming), and receivers (DSSS, adaptive filtering) to show a diversity of results. Once the user has selected the receiver, jammer, and appropriate parameters performance results are shown graphically in real time. An example of the graphical output of our system running STIR-jamming and a DSSS receiver is shown in Figure 2.

Some interesting test cases that are demonstrated with our toolbox include STIR-jamming's performance, adaptive-filtering against periodic jamming, and the interaction of STIR-jamming with adaptive filtering. Demonstrating STIR-jamming's performance allows a user to see the protocol tune to a optimal solution, using minimal power to cause high level of packet degradation. This demo is interesting because using real time system feedback to adapt a jamming attack is a new concept. Showing adaptive-filtering for jamming mitigation is able to demonstrate signal processing technique that can be used to mitigate the effects of a particular class of jammers, mitigating their effect by over 90% when a solution is found.

IV. Conclusion

This work introduces a toolbox to explore the interaction of state-of-the-art adaptive jamming and anti-jamming techniques. The toolbox includes STIR-jamming which uses information inferred from legitimate communication to design a high-impact, low-power, hard-to-detect attack. We also include adaptive filtering in the toolbox to demonstrate the use of adaptive filtering. The main goal of our toolbox is to give users tools to be able to asses new communication protocols against evolving jamming attacks.

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] M. Çakıroğlu and A. T. Özcerit, "Jamming detection mechanisms for wireless sensor networks," in *InfoScale'08*, Vico Equense, Italy, 2008.

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

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

[5] 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.

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

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

[8] 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.