Digital Filter Design for Jamming Mitigation in 802.15.4 Communication

Bruce DeBruhl and Patrick Tague
Carnegie Mellon University
NASA Research Park, Building 23 (MS-11), Moffett Field, CA 94035
Email: {bruce.debruhl, patrick.tague}@sv.cmu.edu

***Abstract*—Jamming attackers can dramatically increase attack efficiency and stealth by randomly or periodically cycling the jamming transmission on and off, attacks respectively known as random and periodic jamming. In this paper, we analyze the impact of such attacks on the IEEE 802.15.4 communication protocol, commonly used in wireless sensor networking applications, and show that the cycling behavior introduces a narrow spectral component into the received signal. We propose the inclusion of a digital filter at the receiver side to effectively eliminate this spectral component, and we discuss the benefits involved in this filter design. We evaluate the impacts of random and periodic jamming with and without the proposed filter, through implementation in software defined radios. Through our evaluation, we observe over 90% reduction in packet error rate with the proposed digital filter.**

***Index Terms*—Wireless security; Jamming; Receiver filter design; IEEE 802.15.4**

I. Introduction

Wireless communications operate over a shared medium and are thus vulnerable to denial of service attacks since the availability of the medium can be diminished by a misbehaving user [1]. When a user broadcasts a signal maliciously or unfairly over a wireless medium to intentionally diminish the availability of the wireless channel, this is referred to as jamming. In the simplest form of a jamming attack known as constant jamming, the attacker broadcasts a constant narrow-band signal at the carrier frequency.

To defend against basic jamming attacks, spreading techniques can be used to decrease the attack impact or increase the cost of an equally effective attack [1]. These techniques often incur additional usage of resources, typically in the form of increased bandwidth. Two such spreading techniques are commonly used. The first is direct sequence spread spectrum (DSSS) which looks to convert each bit to many chips and send these chips at an increased rate resulting in a wider-band signal, that is more difficult to detect and more costly to jam [2]. This also allows for error correction coding at the chip level to improve recovery of the original bits in the presence of jamming or other forms of interference. The second spreading technique is frequency hopping spread spectrum (FHSS) in which the sender and receiver synchronously hop between channels, making it difficult for a narrow-band jammer to completely deny communications as long as the hopping sequence is private [2]. In either case, a jammer must resort to wide-band jamming to achieve the same attack goals, incurring additional energy expenditure and possibly requiring specialized hardware. Anti-jamming techniques have also been proposed at the MAC layer [3], but such approaches require modification of the MAC protocol which is impractical or infeasible in existing platforms. Other anti-jamming protocols focus on detecting the attacker [4] and using evasion techniques to avoid further jamming impact [5].

To effectively attack communication channels employing spread spectrum techniques, more advanced jamming techniques can be used, aiming to minimize both energy expenditure and likelihood of detection. Advanced jamming techniques fall into multiple categories ranging from using more complex signals to using the knowledge of higher level attack protocols [6, 7]. For example, attackers can target control channels to reduce energy expenditure by serveral orders of magnitude over jamming data channels [8, 9]. To increase attack efficiency, a jammer can also alternate between jamming and sleeping, either with a constant period and duty cycle in a periodic jamming attack, or using randomized jamming and sleeping durations in a random jamming attack [10]. An illustration of random jamming is shown in Figure 1.

Since the use of finely tuned periodic or random jamming counter-acts the defense benefits of spread spectrum, alternative methods of jamming mitigation are required. In this work we show that *the cycling behavior of periodic and random jamming introduces a spectral component into the received signal that can be effectively eliminated using a digital filter.* This filtering technique can be implemented with low resource overhead using a low-order digital high-pass filter.

The major contributions of our work include the following.

- We analyze the effect of periodic and random jamming on 802.15.4 communications.
- We propose a method to mitigate jamming attacks with filtering.
- We evaluate the effect of the jamming mitigation filter through implementation in software defined radio (SDR).

The rest of this paper is organized as follows. In Section II, we present the communication and attack models. In Section III, we introduce our filtering techniques and our

This research was supported by CyLab at Carnegie Mellon under grant DAAD19-02-1-0389 from the Army Research Office. The views and conclusions contained here are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either express or implied, of ARO, CMU, or the U.S. Government or any of its agencies.

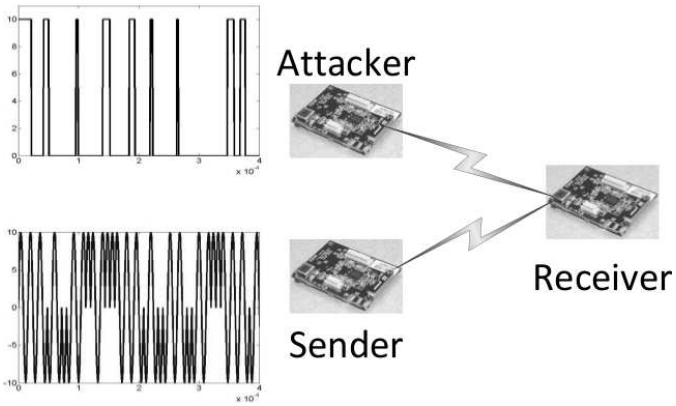

Fig. 1. Random Jamming Attack

filter design. In Section IV, we validate our filter through implementation in SDR, and Section V concludes the paper.

II. Models

In this section, we introduce models for both communication and jamming. We first introduce the IEEE 802.15.4 2450 MHz physical layer protocol. We then introduce models for random and periodic jamming, which includes constant jamming as a special case.

A. 802.15.4 Communication Protocol

The physical layer protocol of interest is based on the IEEE 802.15.4 standard under the 2450 MHz PHY specification [11]. This protocol maps 4 bits into a 32 chip sequence to allow for DSSS. Each of these chips is represented by a half sine pulse shape. Half of these chips are then sent on the inphase channel and half on the quadrature channel. Thus the portion of the symbol on the inphase channel is expressed as a sum of pulses

$$s_I(t) = \sum_{i=0}^{15} a_i s_i(t), \tag{1}$$

where a_i is ± 1 depending on the chip and s_i is modeled as

$$s_i(t) = \begin{cases} P_t \sin\left(\pi \frac{t}{2T_c}\right) & \text{if } 2iT_c \le t \le (2i+2)T_c \\ 0 & \text{else.} \end{cases} \tag{2}$$

In (2), T_c is the chip time and P_t is the transmit power. The signal quadrature channel is expressed as

$$s_Q(t) = \sum_{i=16}^{31} a_i s_i(t). \tag{3}$$

where a_i is ± 1 depending on the chip and s_i is modeled as

$$s_i(t) = \begin{cases} P_t \sin\left(\pi \frac{t}{2T_c}\right) & \text{if } (2i+1)T_c \le t \le (2i+3)T_c \\ 0 & \text{else.} \end{cases} \tag{4}$$

This is then sent using orthogonal quadrature phase shift keying. The receiver for the O-QPSK spread signal receives the signal and uses a low pass filter to receive the 5MHz bandwidth for a given channel. The receiver estimates the received symbols using maximum likelihood estimation [12], mapping the 32 received chips into the most likely original symbol. This spreading allows for robust performance requiring many incorrect chips to cause a symbol error. The packet recovery mechanism used by *IEEE* 802.15.4 is a 2 byte CRC code [11], which requires all symbols to be received to recover a packet. The fact that *IEEE* 802.15.4 has not built in error correction above the sybol level is important to note for our work because it motivates the fact that *corruption of one symbol per packet with high probability is sufficient to deny availability of the 802.15.4 communication channel*. We assume independence of the channels in our model and thus consider only the inphase channel, noting that the quadrature channel is similarly handled.

B. Attack Models

We focus on the case of advanced jamming attacks in which the jammer randomly or periodically cycles its radio on and off to reduce energy expenditure or increase attack stealth. In a random jamming attack, the attack and sleep durations are both randomized, and in a periodic jamming attack the jammer uses a fixed period and duty cycle [10]. These attacks are most effective if information is known to the attacker about the error correction and error checks used by the legitimate communication. If the number of chips, bits or symbols that must be corrupted to make a packet corrupt is known, the jammer can use the minimum attack cycle length and transmit power to have a high probability of success.

1) Random Jamming: A random jamming attack alternates between durations of attacking and sleeping. We let T_k denote the duration of the k^{th} cycle in which the attacker both sleeps and attacks. We define α_k as the fraction of τ_k that the attacker is jamming, which is chosen at random. In this case, we let b_k as either ± 1 and P_J as the attack power. We can then define the random jamming signal as

$$s_{jam}(t) = P_J \sum_{k=1}^{\infty} b_k \text{rect}\left(\frac{t - T_k - \frac{\tau_k \alpha_k}{2}}{\tau_k \alpha_k}\right) \tag{5}$$

$$T_k = \sum_{n=1}^{k} \tau_n. \tag{6}$$

For this model the attacker chooses the power P_J and the distributions of random variables τ_k and α_k. The attacker will then broadcast a similar signal on both the inphase and quadrature channel.

2) Periodic Jamming: The periodic jamming model is effectively a special deterministic case of the random jamming model. We define $B = \tau_k$ and $\alpha = \alpha_k$ for all values of $k > 0$. We then find T_k to be

$$T_k = \sum_{n=1}^{k} B = kB. \tag{7}$$

This allows us to write the periodic jammeig attack signal as

$$s_{jam}(t) = P_J \sum_{k=1}^{\infty} b_k \text{rect}\left(\frac{t}{\alpha B} - \frac{2k+\alpha}{2\alpha}\right). \tag{8}$$

Thus an attacker will be able to choose the attack power P_J, the duty cycle α, and the period B. The attacker then broadcasts this signal on both the inphase and quadrature channels. It is also useful to note that this encompasses the constant jammer as the case when $\alpha = 1$.

III. Filtering for Jamming Mitigation

Jamming mitigation has been approached in numerous ways, namely through the use of DSSS and FHSS and through higher-level methods, as discussed earlier. In this work, we propose to mitigate jamming by adding a second filter in the receiver design.

The traditional receiver uses a low pass filter to get rid of side channel interference and minimize the amount of noise that effects a channel [12]. This approach is not intended to thwart jamming but to simply minimize the effect of the noise floor and interference from other legitimant users on adjacent channels for communication. We propose to mitigate the effect of the two jamming models presented in Section II-B at the baseband by adding a second high pass filter as shown in Figure 2. In this section, we consider the motivation for our method, the theoretical basis, the filter design, and finally the trade-offs involved.

A. Motivation

Protocols like IEEE 802.15.4 are designed in such a way that they depend on direct sequence spread spectrum technique to mitigate jamming. This defense mechanism assumes that the jammer is not willing to spend large amounts of power to interfere with the wider-band signals. While this is certainly a good practice, it does not protect against intelligent attack strategies. With knowledge of the upper layer protocols of 802.15.4, an attacker can choose to corrupt a small fraction of symbols and still effectively destroy packets. This is an attractive attack because the energy required to mount it is low and the effect is catastrophic to communications with the current CRC error checks. Even if the protocol was redesigned to allow for stronger error correction, it would likely still only correct for a small fraction of symbol errors.

This higher layer knowledge allows a jammer to attack not using constant noise but rather symbol length bursts of noise. Based on the protocol structure, an attacker can limit the jamming duration to only a few symbols, where increasing the jamming duration will increase the expected number of jammed packets. However, as we show, this cycling behavior in the jamming attack has a narrower spectrum than the legitimate signal, thus allowing for a filter to eliminate much of the jamming signal while retaining the original signal. This filtering method is attractive because of its ease of implementation for a radio designer compared to tradition jamming defense mechanisms. DSSS requires more bandwidth and different radio equipment and can still be susceptible to attacks. FHSS requires multiple channels and advanced channel scheduling which is difficult to implement in a dense wireless sensor network. Our method allows for mitigation of the jamming attack described without the complex scheduling required by FHSS.

TABLE I
Cases for Jamming Attack analysis

Case	Cycle Width (symbols)	B	α
1	64	$32\mu s$	.25
2	32	$16\mu s$	.75
3	32	$16\mu s$	.5
4	8	$4\mu s$	.5

B. Analysis

The analytical support for our filtering approach is based on frequency-domain analysis of the IEEE 802.15.4 protocol and the random and periodic jamming attacks. The frequency domain of the signal can be derived from (1) using Fourier Transform analysis as

$$S_I(\omega) = 2P_t T_c j \sum_{i=0}^{15} a_i \pi \left[\gamma_i(\omega) - \eta_i(\omega)\right], \tag{9}$$

where γ and η are defined as

$$\gamma_i(\omega) = \mathrm{sinc}(\omega T_c + \frac{\pi}{2}) \exp^{-j(\omega T_c + \frac{\pi}{2})(2i+1)}, \tag{10}$$

$$\eta_i(\omega) = \mathrm{sinc}(\omega T_c - \frac{\pi}{2}) \exp^{-j(\omega T_c - \frac{\pi}{2})(2i+1)}. \tag{11}$$

The transmitter will filter between -2.5 MHz and 2.5 MHZ [11] and then modulate to the 2.425 GHz carrier frequency. The attacker's frequency domain response is similarly derived from (8) as

$$S_{jam}(\omega) = P_J \alpha B \sum_{k=1}^{\infty} b_k \mathrm{sinc}\left(\omega \alpha B\right) \exp^{-j\omega \frac{2kB + \alpha B}{2}}. \tag{12}$$

The question thus becomes, what the attackers frequency response looks like on the 5 MHz frequency where the valid communication occurs. We consider four cases for our attacker summarized in Table I.

The resulting waveforms are shown from -1 MHz to 1 MHz in Figure 3 and Figure 4 where most of the signal occurs. It is clear in this model that the bandwidth of these attackers are much smaller than that of the spread 802.15.4 signal. It is thus possible to add the high-pass filter motivated above to mitigate the jamming attack. The case of the random jammer is similar in analysis to that of the periodic jammer, but it would be a summation of various periodic waves. This would end up with very similar performance to that of the periodic jammer, and thus it can also be mitigated with our periodic filtering technique. Figure 3 looks to explore the effect of varying duty cycle and shows both attacking waveforms are in a low frequency area. Figure 4 shows the effect of varying the attackers period. This again suggests that a range of attack parameters can be mitigated with our proposed filtering method.

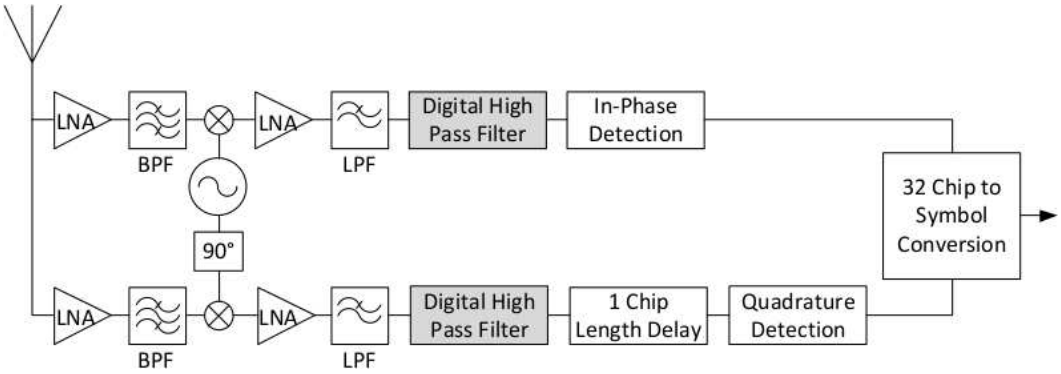

Fig. 2. Our proposed approach incorporates a digital high-pass filter to eliminate the spectral component introduced by random and periodic jamming.

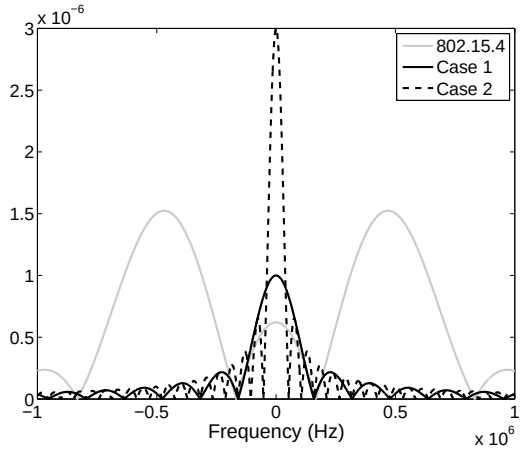

Fig. 3. Frequency Response of Attackers with Varying Duty Cycles

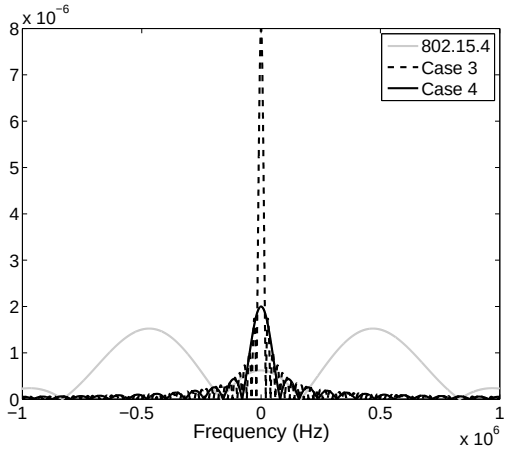

Fig. 4. Frequency Response of Attackers with Varying Periods

C. Filter Design

We completed our filter design using a simple FIR filter with empirical tuning. Figure 5 shows the ideal filter that we attempted to emulate overlaid on the IEEE 802.15.4 spectrum and case 2 from Section III-B. The filter was empirically tuned, resulting in a center frequency of 90 kHz with a transition

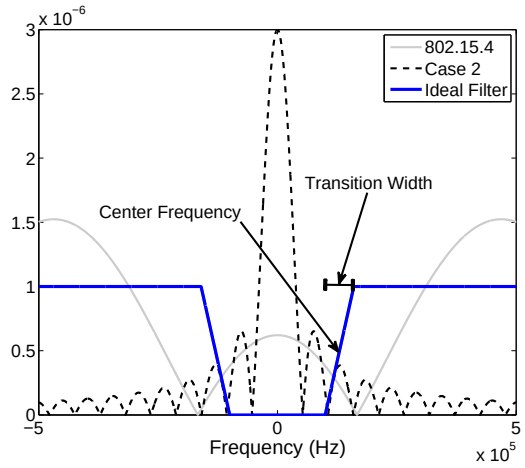

Fig. 5. Ideal filter design with both attacker and 802.15.4 frequency response

width of 80 kHz and a Hamming window [13]. This filter was again selected for its simple software implementation and low complexity allowing it to be implemented in software on basic radio modules.

D. Trade-offs

With any jamming mitigation technique, trade-offs are going to be present. The major cost of this defense is that it degrades the legitimate received signal and makes it more susceptible to random noise of the communication channel. This results in higher error rates in non attack scenarios. This trade-off allows a radio designer to choose whether they will face a high enough probability of malicious jamming to justify the technology. In applications where jamming is probable, the loss of performance could likely be justified as this filter eliminates a wide range of random and periodic jamming attacks that could give a malicious user a lower-power denial-of-service attack against legitimate nodes. In our future work, we will explore implementing this technique in an adaptive fashion. This could allow for the receiver to add the filter when an attack is detected and use normal communications when there is no attack.

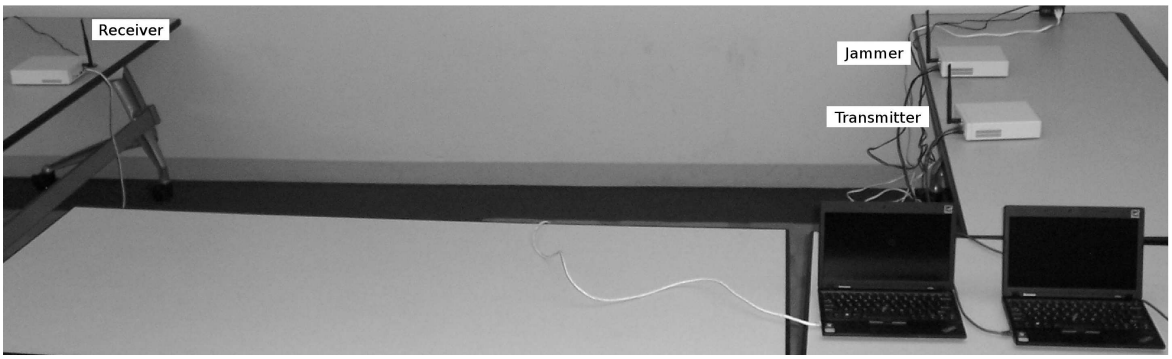

Fig. 6. Jamming Test Setup

IV. Implementation

To verify our theory, we implemented our receiver architecture in an SDR. This allowed for analysis of high numbers of packets in the traditional receiver and the receiver with the added filter. We will first introduce our test setup and then we present our experiments and results.

A. Experimental Test Setup

We implemented our system using Ettus USRP2 SDR [14] with the GNU Radio [15] software version 3.3. We used the UCLA Zigbee physical layer implementation [16] with modification to allow for operations with the USRP2 and the most recent GNU Radio package. We set one SDR which is used for the receiver on a table. Fifteen feet away we placed two more SDRs 12 inches apart. These two SDRs will be used as a transmitter and jammer. The test setup is shown in Figure 6.

For each test point, we sent 6000 packets in 2000 packet bursts. We then recorded how many packets out of 6000 where received correctly. We simply checked the CRC on the packets and did not check the packet content, since the probability of the CRC being matched while the packet is corrupted is negligible. We ran our tests during late night hours which allowed for fairly low usage of the ISM band compared to the daytime hours when WiFi is actively used. We calculated the packet error rate and used this as a parameter to determine the effectiveness of communication.

The jamming attack is also implemented in the SDR. The jammer simply reads and plays a binary file. The binary file is generated using discrete versions of (5) and (8). For the periodic attacks, the file is 20 periods in length, and for the random attacker, the file is 1000 periods in length. Replay of these files is repeated as necessary.

B. Results

The first experiment we ran looked to explore the effect of the attacker's period with a low duty cycle. To explore this we looked at attackers that have 10% and 20% duty cycle. The attacker with 10% duty cycle was able to deny over 90% of packets with a period of 13 symbols or greater as seen in Figure 7. This shows that an attack can be very effective with only 10% of the effort. When we apply the filtering technique, the error rate decreases to less than 4% on average.

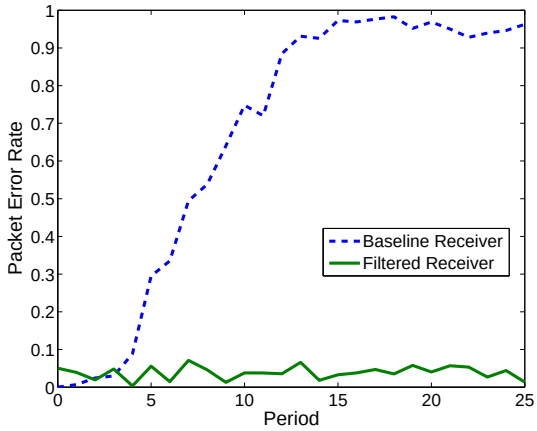

Fig. 7. Periodic Jamming Attack with a 10% Duty Cycle

The attacker with a 20% duty cycle is able to deny over 90% of packets with a period from 6 symbols to 25 symbols as seen in Figure 8. Furthermore with a period from 7 to 25 symbols the packet error rate is over 99% on average. When the filtering techniques proposed are implemented, the packet error rate again drops to below 4% on average.

The results for an attacker with a period of 22 symbols are shown in Figure 9. The attacker is able to deny over 90% of packets when the duty cycle is over 15%. When the proposed filtering technique is applied, the packet error rate drops under 1%. This shows that the defense is effective at mitigating the proposed periodic attacks. One special case to consider is when the duty cycle is equal to 100%. This case is a constant jammer, the most basic jammer. It is able to effectively destroy over 99% of packets. The filtering method proposed mitigates this attack also to under 1% packet error rate.

The random jammer is generated with each period's length selected uniformly between half a symbol and 32 symbols in length. The duty cycle for each period is selected using a beta distribution [17] with the variance defined as the average duty cycle divided by twelve. The results for the random jammer are

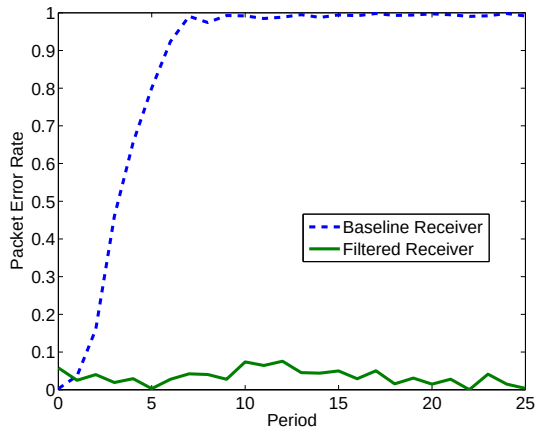

Fig. 8. Periodic Jamming Attack with a 20% Duty Cycle

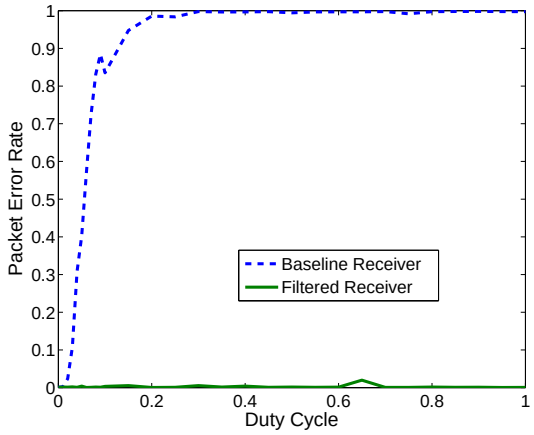

Fig. 9. Periodic Jamming Attack with a Period of 22 Symbols

shown in Figure 10. The proposed filtering method is shown to mitigate the effective jamming attack to less than 1% packet error rate.

V. Conclusion

In this paper we proposed a filtering technique to effectively mitigate periodic and random jamming attacks on 802.15.4 communications. We have shown the technique to be analytically feasible. We implemented the filtering technique for jamming mitigation and demonstrated empirical results to show that the technique is effective. By adding a high-pass filter at the base band into the receiver architecture, we can reduce the resulting packet error rate under random and periodic jamming from over 95% to less than 5%. Furthermore, our filtering approach incurs only the small overhead of a simple FIR filter, requiring little computational overhead. In future work, we will look to detect jamming and apply the jamming mitigation filter only when necessary. We will also explore how this filtering technique can adapt to an intelligent attacker that shifts frequencies.

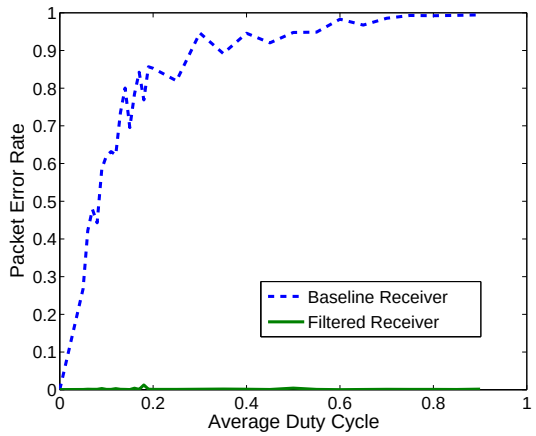

Fig. 10. Random Jamming Attack

References

[1] D. J. Torrieri, *Principles of Secure Communication Systems*, 2nd ed. Boston: Artech House, 1992.
[2] A. Molisch, *Wireless Communications*. John Wiley & Sons, Inc., 2005.
[3] A. D. Wood, J. A. Stankovic, and G. Zhou, "DEEJAM: Defeating energy-efficient jamming in IEEE 802.15.4-based wireless networks," in *Proc. 4th Annual IEEE Conference on Sensor, Mesh and Ad Hoc Communication Networks (SECON'07)*, San Diego, CA, USA, Jun. 2007.
[4] M. Çakıroğlu and A. T. Özcerit, "Jamming detection mechanisms for wireless sensor networks," in *Proc. 3rd International Conference on Scalable Information Systems (InfoScale'08)*, Vico Equense, Italy, 2008, pp. 1–8.
[5] 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.
[6] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. 25th IEEE Communications Society Military Communications Conference (MILCOM'06)*, Washington, DC, Oct. 2006, pp. 1–7.
[7] Y. W. Law, M. Palaniswami, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network MAC protocols," *ACM Transactions on Sensor Networks*, vol. 5, no. 1, pp. 1–38, 2009.
[8] 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.
[9] 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.
[10] A. Fragkiadakis, V. Siris, and N. Petroulakis, "Anomaly-based intrusion detection algorithms for wireless networks," in *Wired/Wireless Internet Communications*. Springer, 2010.
[11] "IEEE 802.15.4-2006," http://standards.ieee.org/getieee802/download/802.15.4-2006.pdf.
[12] B. Lathi, *Modern Digital and Analog Communication Systems*. Oxford University Press, 1998.
[13] L. Tan, *Digital Signal Processing: Fundamentals and Applications*. Academic Press, 2007.
[14] "Ettus research LLC," http://www.ettus.com/.
[15] "GNU radio," http://gnuradio.org/.
[16] T. Schmid, O. Sekkat, and M. Srivastava, "An experimental study of network performance impact of increased latency in software defined radios," in *Proc. 2nd ACM workshop on Wireless network testbeds, experimental evaluation and characterization*, Montreal, Quebec, Canada, 2007.
[17] D. J. C. MacKay, *Information Theory, Inference, and Learning Algorithms*. Cambridge: Cambridge University Press, 2003.