Counter-Jamming Using Mixed Mechanical and Software Interference Cancellation

Triet D. Vo-Huu Erik-Oliver Blass Guevara Noubir
College of Computer and Information Science
Northeastern University, Boston, MA
{vohuudtr|blass|noubir}@ccs.neu.edu

ABSTRACT

Wireless networks are an integral part of today's cyber-physical infrastructure. Their resiliency to jamming is critical not only for military applications, but also for civilian and commercial applications. In this paper, we design, prototype, and evaluate a system for cancelling jammers that are significantly more powerful than the transmitting node. Our system combines a novel mechanical beam-forming design with a fast auto-configuration algorithm and a software radio digital interference cancellation algorithm. Our mechanical beam-forming uses a custom-designed two-elements architecture and an iterative algorithm for jammer signal identification and cancellation. We have built a fully functional prototype (using 3D printers, servos, USRP-SDR) and demonstrate a robust communication in the presence of jammers operating at five orders of magnitude stronger power than the transmitting node. Similar performance in traditional phased arrays and radar systems requires tens to hundreds of elements, high cost and size.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Wireless communication

General Terms

Design, Experimentation, Security

Keywords

anti-jamming; beam forming; software radio

1. INTRODUCTION

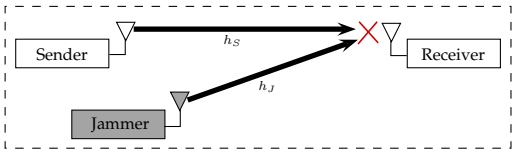
Over the last decades, wireless communication proved to be an enabling technology for an increasingly large number of applications. The convenience of wireless and its support of mobility has revolutionized the way we access data, information services, and interact with the physical world. Beyond enabling mobile devices to access information and data services ubiquitously, it is today widely used in cyber-physical systems such as air-traffic control [42], power plants synchronization, transportation systems, and human body implantable devices [13]. For example, the United States Congress recently passed an FAA bill that speeds up the switching to GPS-based air traffic control [24]. The trend of wireless communication utilization in the electricity grid is already visible with over 20 millions smart meters already installed in the US and over 70 million worldwide [26]. Wireless Remote Terminal Units (W-RTU) with long-range wireless communication capabilities have been used for many years and several companies are increasingly switching to Wireless RTUs, e.g., vMonitor [38], Industrial Control Links [14], Synetcom [34], and Semaphore [29].

This pervasiveness elevated wireless communication systems to the level of critical infrastructure. Jamming is a prominent security threat as it cannot only lead to denial of service attacks, but can also be the prelude to sophisticated spoofing attacks against cellular, WiFi, and GPS system [6]. While basic jamming hardware against GPS, Cellular Systems, and WiFi are already a commodity that can be found on Internet online websites for few tens of dollars, more powerful jammers can also easily be made given that they do not necessitate to generate precise, clean RF signals. A $7 magnetron generates a 1KWatt interfering signal (covering hundreds of meters) and can be tuned to a wide range of frequencies by slightly modifying its resonant cavity [4]. Various websites have online and YouTube tutorials to re-purpose the magnetron of a $50 microwave oven and build High Energy RF guns (HERF). In addition to its use in war zones, jamming recently caused sufficient concerns to trigger an FCC campaign to enforce anti-jamming laws as stated by the chief of the FCC's Enforcement Bureau on February 2011 [10, 23].

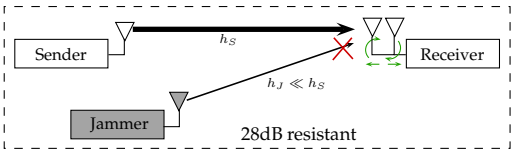
We consider a setup of jamming where the spread spectrum and coding gain are not sufficient to counter the jammer. This paper focusses on the case of a single jammer/antenna adversary. We assume a fairly narrowband signal (few MHz) and that mechanical steering components are possible as is the case on many military vehicles or as widely used around the world in motorized dish antennas. Our system operates in two stages (Figure 1):

- **First stage – Antenna Auto-Configuration:** We introduce a novel two-element antenna that dynamically reconfigures to track the jammer and to weaken its signal by up to 28 dB (Fig. 1b). Our design with two moving elements is *simple*, *low-cost*, and has unique characteristics unexplored in mechanically steerable an-

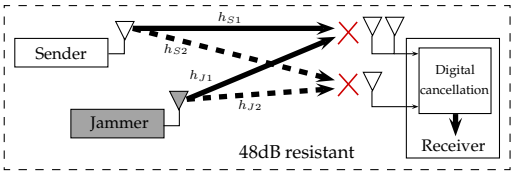
WiSec'13, April 17–19, 2013, Budapest, Hungary.



(a) Without anti-jamming



(b) Our system with 2-element antenna (1st stage)



(c) Our system, digital cancellation (2nd stage)

Figure 1: Jamming and its effect in a traditional system and in our system with two stages of anti-jamming.

tennas. Our configuration algorithm allows to converge on elements separation/rotation that maximizes the signal-to-jamming ratio (SJR) within 20 seconds.

- **Second stage – Digital Jamming Cancellation:** To further eliminate the jammer's signal, we also use a single-element antenna to get an additional copy of the jamming signal and develop a MIMO-like interference cancellation techniques tailored for anti-jamming. Unlike traditional MIMO and beam-forming techniques we do not rely on training sequences. We demonstrate a reliable communication equivalent to reducing the impact of a jammer by 48 dB.

Our contributions are:

- *Anti-jamming adversaries with significantly more power than transmitting nodes:* We are able to efficiently remove unknown jamming signals up to almost five orders of power higher than legitimate user's signals and recover the user data with an acceptable bit error rate.
- *Zero-knowledge anti-jamming:* We neither require knowledge about the legitimate signals (no additional preamble, no training sequence), nor knowledge about the jammer (unknown location, variable jamming power).
- *Environment adaptiveness:* The system works efficiently in both outdoor as well as indoor environments and can handle multipath jamming.

While the techniques used in this system are rooted in techniques developed for MIMO communication [36] and phased array antenna [22, 35], fields that have been extensively studied over several decades, the characteristics of our setup and design require new algorithms and techniques. Our digital jamming cancellation algorithms target *powerful unknown jammers*, unlike traditional MIMO techniques that operate over user-designed transmission signals of similar powers, allowing adequate channel estimation through training sequences.

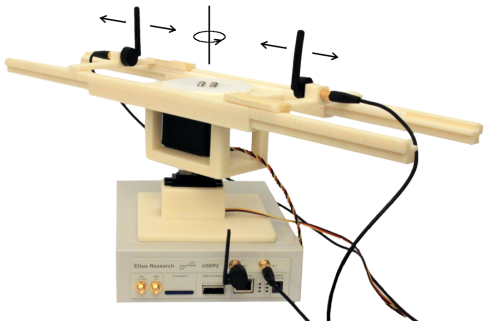


Figure 2: System prototype.

Previous work on *phased array antennas* uses fixed elements and primarily aims at producing a directed beam that can be repositioned electronically/digitally. Adaptive beamforming with algorithms such as MVDR and MMSE beamformers aims at minimizing the impact of the sidelobe and considered to be more adequate for radar systems. Phased array systems used in radar systems achieving our jamming cancellation gain use a large number of elements and size (sometimes hundreds [3, 4]). In contrast, our design allows the formation of a large number of beam patterns that are impossible for an electronically steerable fixed two-element antenna [18, 35] and is combined with a MIMO-like digital interference cancellation.

One starting point for our approach is that increasing the distance between the antenna elements increases the number of beams and reduces their width. A traditional two-element electronically steerable antenna can only *rotate* the beam patterns [18]. With our setup, the large number of controlled "nulls" allows to potentially cancel even several simultaneous jammers and their multipaths. In addition, the large number of beams allows the creation of connected networks.

2. MODELS AND APPROACH

2.1 Communication and adversarial models

We consider a communication setup (Figure 1a) with two legitimate communicating nodes and one jamming node.

2.1.1 Communication nodes

The two communicating nodes operate over an open, fairly narrowband channel (few MHz), using a pre-agreed modulation scheme. The sender transmits data at a constant power via a single-element antenna. The receiver uses a two-element antenna and a single-element antenna for signal reception. Both nodes are unaware of each other's location and their own location, also the presence of jammer. During the communication, the users remain in fixed locations.

2.1.2 Adversary

The jammer is equipped with a single transmit antenna that can emit a powerful jamming signal to interfere with the communication between the users. The jamming signal can be either noise or a modulated signal. The jammer can purposely start or stop jamming at any time, or adjust the transmit power to variable levels during the jamming period. The jammer does not change its location while jamming.

2.1.3 Communication channel

The users' communication channel is assumed to be narrowband with slow-fading. Typically the channel is few MHz wide at the 2.4GHz band and the modulation is BPSK or QPSK. We consider both outdoor and indoor environments in this setup.

2.2 Approach

In a traditional system, where the receiver R has only a single antenna, the simultaneous transmission of both sender and jammer causes interference at the receiver: $R = h_S S + h_J J$, where h_S and h_J are the channel gains from sender S and jammer J to the receiver, respectively. If the jammer interference is strong, the signal-to-jamming ratio (SJR) at the receiver is low (equivalently h_S/h_J is small), the signal S is undecodable.

In our system, the receiver has an additional two-element antenna. To decode the data, the receiver operates in two stages to increase the SJR. In the *first stage* (Figure 1b), the two-element antenna is used for signal reception. The configuration algorithm adjusts the two-element antenna (Figure 2) such that the distance between the two elements (*element separation*) and the rotational direction (*angle*) of the antenna increases the received legitimate's signal power, while, at the same time, reducing the received jammer's signal power. As a result, the SJR is increased, allowing successful data decoding.

As the antenna angle and element separation are adjustable, the receive pattern is dynamically configurable. In fact, we can construct a *large* number of different receive patterns (shown in Section 3), in comparison with fixed-position electronically steerable arrays. Our experiments show that our system can cope with a jammer with up to 28dB stronger power than legitimate users. At the heart of the first stage, we introduce an algorithm that dynamically configures the angle and the element separation of the antenna to maximize the received SJR. The flexibility of our custom-designed antenna allows the auto-configurability of the system to work effectively in both outdoor and indoor environments, where the latter often incurs problems to electronically steerable antenna arrays and results in poor performance. We also show that our configuration algorithm significantly outperforms a brute-force configuration in speed and converges within 20 seconds.

However, our purpose is to allow communication in the presence of jammers *beyond* the 28dB limit. In the *second stage*, we extend our model by using digital interference cancellation techniques (Figure 1c) to eliminate the jamming signal. Equation (1) illustrates the idea of the jamming cancellation techniques applied to the received signals at the two-element antenna and the single-element antenna. We obtain two different copies of the transmitted signal at the receiver: R_1 from the two-element antenna and R_2 from the single-element antenna.

$$\begin{aligned} R_1 &= h_{S1} S + h_{J1} J \\ R_2 &= h_{S2} S + h_{J2} J \end{aligned} \tag{1}$$

One major difference between our setup and MIMO systems is that MIMO systems use training sequences to estimate the channel gains. This is not possible in our setup since we do not have control over the jamming signal. Instead, we propose a technique specific to this model to estimate the channel gain ratio $a = h_{J2}/h_{J1}$ in order to recover the legitimate signal, as shown in the following equation:

$$bS = aR_1 - R_2, \tag{2}$$

where $b = ah_{S1} - h_{S2}$. Knowing a, we can decode S. The ratio a depends on the channel characteristics such as attenuation, multipath and the power of the jamming signal. The factor b is considered as a new channel gain of the residual signal after eliminating the jamming signal, and does not introduce any difficulty for the decoder, thus requires no estimation.

In summary, the high-level idea of our approach is to build a hybrid system consisting of two levels of anti-jamming techniques: analog signal cancellation by mechanical means of our custom-designed antenna and digital interference cancellation by software-based signal processing techniques. The robustness of our system highly depends on the performance of the configuration algorithm and digital interference cancellation algorithm. In the next sections, we will discuss the following problems:

- What is the optimal antenna configuration (separation, angle) that maximizes the SJR?
- How to estimate the channel characteristics to optimize the performance of the digital jamming cancellation technique against unknown jamming signals?

3. ANTENNA CONFIGURATION

Increasing the SJR at the receiver is a key goal of our system. We will now present a new, efficient algorithm for reconfiguring the two-element antenna, such that the receiver is able to reduce a significant portion of the jammer's power. For ease of understanding, we first introduce our notation:

DEFINITION 1. *A* configuration *of the two-element antenna, denoted as* (L, ϕ)*, consists of element* separation L *and a rotational* angle ϕ*.*

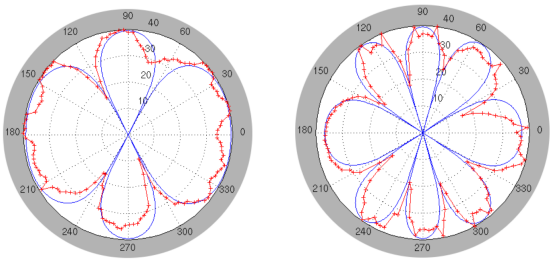
A configuration specifies the angular position of the two-element antenna and the physical separation of its elements. The antenna is able to rotate within a range $[\phi_{\min}, \phi_{\max}]$, and adjust the separation between the limits $[L_{\min}, L_{\max}]$. In practice, depending on the mechanical devices' capabilities, the number of possible configurations, L and ϕ for given ranges, is finite. We denote $P(L, \phi)$ as the received signal's power at the two-element antenna with configuration (L, ϕ).

DEFINITION 2. (L, ϕ) *is a* minimizing *(or* maximizing*)* configuration*, if* $P(L, \phi) \leq P(L', \phi')$ *(or* $P(L, \phi) \geq P(L', \phi')$*) for all other configurations* (L', ϕ')*.*

DEFINITION 3. L_ϕ *is called a* minimizing separation *for an angle* ϕ*, if* $P(L_\phi, \phi) \leq P(L, \phi)$ *for all* $L \in [L_{\min}, L_{\max}]$*. Similarly,* L_ϕ *is a* maximizing separation *for an angle* ϕ*, if* $P(L_\phi, \phi) \geq P(L, \phi)$ *for all* $L \in [L_{\min}, L_{\max}]$*.*

DEFINITION 4. ϕ_L *is called a* minimizing angle *for a separation* L*, if* $P(L, \phi_L) \leq P(L, \phi)$ *for all* $\phi \in [\phi_L - \theta, \phi_L + \theta]$*. The parameter* θ *denotes the desired search range for the antenna control algorithm. Similarly,* ϕ_L *is a* maximizing angle *for a separation* L*, if* $P(L, \phi_L) \geq P(L, \phi)$ *for all* $\phi \in [\phi_L - \theta, \phi_L + \theta]$*.*

Intuitively, minimizing angles are directions inside the nulls where the received power is minimized, and maximizing angles are directions inside the lobes where the received power is maximized.



(a) $L = \lambda$ (b) $L = 2\lambda$

Figure 3: Outdoor receive patterns of the two-element antenna. Experimental gains (lines with plus signs) are compared to theoretical values.

3.1 Pattern analysis

We first study the basic characteristics of the two-element antenna. Signals received at two elements can be added constructively or destructively depending on their phase difference when arriving at the elements. When the signals add up together, we have lobes in the receive pattern. When the signals eliminate each other, we have nulls. In free-space communications, the phase difference between arriving signals can be determined based only on the element separation L. The following two theorems give the locations and number of lobes and nulls in the receive pattern of the two-element antenna.

THEOREM 1. *The receive pattern of the two-element antenna in a free-space communication has maximizing angle at ϕ_k and minimizing angle at ϕ_m, which satisfies*

$$\begin{array}{ll} \cos\phi_k = \frac{k}{K} & k \in \mathbb{Z} \\ \cos\phi_m = \frac{2m+1}{2K} & m \in \mathbb{Z}, \end{array}$$

where $K = L/\lambda$ is the ratio between the separation and the carrier wavelength, k and m are integers. Besides, if $\{K\} \geq \frac{1}{2}$, where $\{K\}$ denotes the fractional part of K, 0 and π are 2 additional maximizing angles; otherwise, they are 2 additional minimizing angles.

THEOREM 2. *The number of maximizing angles of the two-element antenna in a free-space communication is equal to the number of minimizing angles and equal to*

$$\begin{array}{ll} 4K, & \text{if } K \in \mathbb{Z} \\ 2\lfloor 2K \rfloor + 2, & \text{if } K \notin \mathbb{Z} \end{array}$$

where $K = L/\lambda$, and $\lfloor K \rfloor$ is the largest integer not greater than K.

3.1.1 Outdoor Experiment

We conducted an experiment to measure the received power at the two-element antenna. The transmitter is placed at distance 10m to the receiver. Figure 3 shows the measured receive patterns for separation $L = \lambda = 12.5$cm and $L = 2\lambda = 25$cm ($f = 2.4$GHz). The results show that the outdoor environments have very similar characteristics to the theoretical patterns in free-space communications. Our antenna design is featured with the capability of adjusting the element separation, by which the two-element antenna can change the *locations* and the *number* of lobes and nulls in the receive pattern (according to Theorem 1 and Theorem 2).

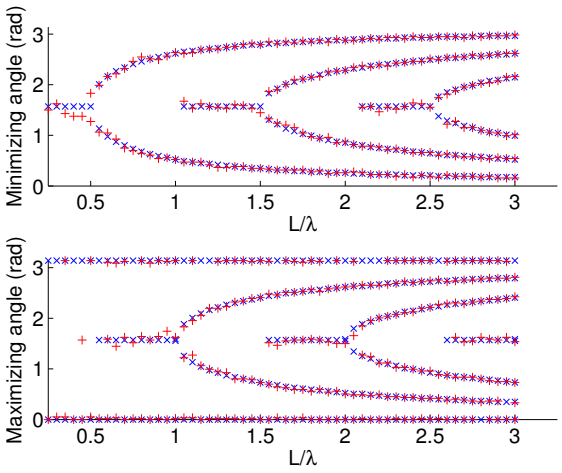
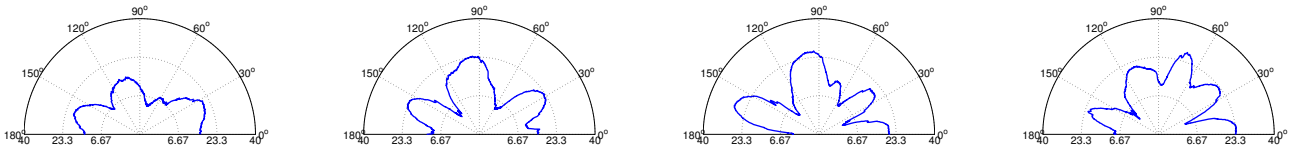


Figure 4: Locations of minimizing and maximizing angles for separations between $\lambda/4$ and 3λ in an outdoor environment. Plus (+) indicates experimental results, and cross (X) indicates theoretical predictions.

To study the *change* of locations of lobes and nulls when adjusting the separation, we conducted another experiment, in which the separation is adjusted from minimum value $L_{\min} = \lambda/4 = 3.1$cm to maximum value $L_{\max} = 3\lambda = 37.5$cm. Figure 4 shows the locations of maximizing and minimizing angles for each separation value found in both experimental and theoretical cases. Note that, since the pattern is almost symmetric, only the maximizing and minimizing angles found in one half $[0, \pi]$ of the pattern are shown. As an example, the receive pattern for separation $L = \lambda$ has 4 minimizing angles at $\pm\pi/3$, $\pm 2\pi/3$ and 4 maximizing angles at 0, $\pi/2$, π, and $3\pi/2$, which imply 4 nulls and 4 lobes in Figure 3a. When the separation is increased by a small value to $L' = L + \Delta L$ with $\Delta L \approx 0.6$cm, 2 more minimizing angles and 2 more maximizing angles appear in the pattern (in Figure 4 we see 1 more minimizing angle and 1 more maximizing angle in $[0, \pi]$), which comply with the results of Theorem 2. In addition, Theorem 1 implies that if $K' \approx K$, $\cos\phi' \approx \cos\phi$, then $\phi' \approx \phi$, i.e., the locations of the maximizing and minimizing angles deviate *slightly* from the previous locations. We call this the *continuity* property of the receive pattern. This property is important for the antenna configuration algorithm described later.

3.1.2 Indoor Experiment

In an indoor environment, the receive patterns become more unpredictable due to reflecting and blocking objects. Figure 5 shows that the indoor receive patterns (at different separation values) highly depend on the indoor environment. The locations and the number of lobes and nulls do not always comply with the results of Theorem 1 and Theorem 2. However, similarly to the outdoor scenario, the indoor receive patterns also have the *continuity* property of maximizing angles and minimizing angles, which can be observed from Figure 6: a small adjustment of separation results in a small change of maximizing angles and minimizing angles; in other words, the maximizing angles (or minimiz-



(a) $L = 3\lambda/2$ (b) $L = 2\lambda$ (c) $L = 5\lambda/2$ (d) $L = 3\lambda$

Figure 5: Experimental indoor receive patterns.

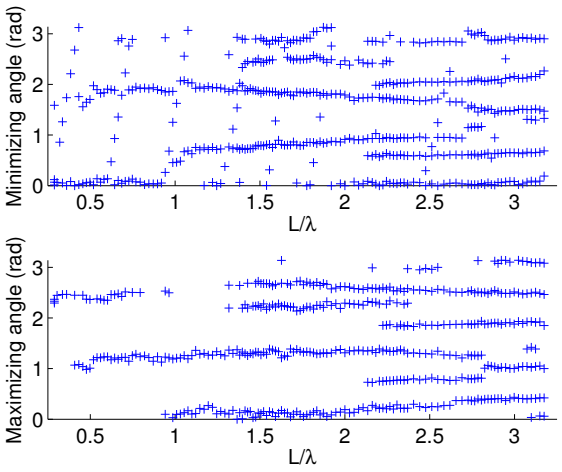


Figure 6: Locations of minimizing and maximizing angles for separation values between 0.25λ and 3.25λ measured in an indoor experiment.

ing angles) of two close values of separation are likely not to deviate much from each other.

3.2 Antenna configuration algorithm

In this section, we derive the algorithm for controlling the two-element antenna to maximize the SJR at the receiver. We note that if both jammer and sender are in the same (or tiny range of) angles relatively to the receiver, Theorem 1 implies that there is no configuration resulting in significantly changing the portion of jamming power in the received signal, as the gains to the transmitters are always (almost) the same. We consider a situation in which the jammer is located in a different direction with respect to the sender.

3.2.1 *Outdoor and known locations*

In an outdoor environment, if the locations of the communicating and jamming nodes are known, we can maximize the SJR by determining the maximizing angles according to the relative locations between sender and receiver in order to maximize the received power from the sender, and at the same time, determining the minimizing angles according to the relative locations between jammer and receiver in order to minimize the received power from the jammer. Based on the results of Theorem 1, the maximizing and minimizing angles can be precomputed, cf. Algorithm 1.

Algorithm 1 Precomputable configuration for outdoor and known locations

```
for L ∈ [L_min, L_max] do
  A_J ← minimizing_angles_to_jammer(L)
  A_S ← maximizing_angles_to_sender(L)
  for φ ∈ A_J ∩ A_S do
    if SJR(L, φ) > SJR(L_opt, φ_opt) then
      (L_opt, φ_opt) ← (L, φ)
    end if
  end for
end for
return (L_opt, φ_opt)
```

In Algorithm 1, minimizing angles and maximizing angles are computed based on the element separation L and relative locations of the nodes and returned as two sets: $A_J = [\phi_{m_1} - \theta, \phi_{m_1} + \theta] \cup \ldots \cup [\phi_{m_k} - \theta, \phi_{m_k} + \theta]$ for minimizing jammer's power and $A_S = [\phi_{k_1} - \theta, \phi_{k_1} + \theta] \cup \ldots \cup [\phi_{k_n} - \theta, \phi_{k_n} + \theta]$ for maximizing sender's power, where k and n are the number of minimizing and maximizing angles found by above theorems, respectively. As for each separation L, there are multiple positions that maximize the SJR, the SJR corresponding to each angle in the intersection of A_J and A_S are compared to find the best configuration. The advantage of Algorithm 1 is that the computations can be done offline, therefore requiring minimal setup time in a real-world deployment.

3.2.2 *Unknown locations*

For outdoor environments and unknown locations of nodes, Algorithm 1 is not applicable. For indoor environments, even if the locations of nodes are known, the channel highly depends on the specific environment and results in unpredictable patterns. In this section, we present the antenna configuration algorithms that work for both outdoor and indoor environments.

Our goal is to maximize the SJR at the receiver. According to Theorem 1, changing separation results in new locations of maximizing and minimizing angles, therefore yielding different gains for the jammer and the sender (as they are not in the same direction). Consider a powerful jammer whose power dominates the received signal. Changing the antenna configuration to null the jammer, we would reduce the received signal's power. Thus, *maximizing* the SJR implies *minimizing* the total received power at the receiver. For low-power jammer, this implication is not applied, however the algorithms described below are still useful when combining with the digital cancellation technique to recover the user data.

Brute-force algorithm.

To minimize the total received power, a "brute-force" search would yield the best configuration: this search would measure the received power at the two-element antenna for all possible configurations and select the one corresponding to the minimum power.

Algorithm 2 Brute-force for unknown node locations

function bruteforce($L_{\min}, L_{\max}, \phi_{\min}, \phi_{\max}$)
  for $\phi_{\min} \le \phi \le \phi_{\max}$ **do**
    for $L_{\min} \le L \le L_{\max}$ **do**
      if $P(L, \phi) < P(L_{\text{opt}}, \phi_{\text{opt}})$ **then**
        $(L_{\text{opt}}, \phi_{\text{opt}}) \leftarrow (L, \phi)$
      end if
    end for
  end for
  return $(L_{\text{opt}}, \phi_{\text{opt}})$

Without knowledge of node locations, we cannot rely on Theorem 1 to compute the optimal configuration. Instead, the brute-force approach tries each configuration by varying the rotational angle and the element separation within the physical limits and measuring the received power. Given the large number of separation values and angle values, such approach would take a significant amount of time to find the best configuration.

Fast algorithm.

Recall the continuity property of the receive pattern: continuously changing the separation results in new locations of maximizing angles and minimizing angles in the small vicinity of the previous ones. Based on this property, we propose the *fast algorithm*, cf. Algorithm 3.

Algorithm 3 Fast algorithm for unknown node locations

function fast($L_0, L_1, L_2, \phi_0, \phi_1, \phi_2$)
  $L_{\text{opt}} \leftarrow L_0$, $\phi_{\text{opt}} \leftarrow \phi_0$
  repeat
    for $\phi_1 \le \phi \le \phi_2$ **do**
      if $P(L_{\text{opt}}, \phi) < P(L_{\text{opt}}, \phi_{\text{opt}})$ **then**
        $\phi_{\text{opt}} \leftarrow \phi$
      end if
    end for
    for $L_1 \le L \le L_2$ **do**
      if $P(L, \phi_{\text{opt}}) < P(L_{\text{opt}}, \phi_{\text{opt}})$ **then**
        $L_{\text{opt}} \leftarrow L$
      end if
    end for
    $L_1 \leftarrow L_{\text{opt}} - \Delta L$; $L_2 \leftarrow L_{\text{opt}} + \Delta L$
    $\phi_1 \leftarrow \phi_{\text{opt}} - \theta$; $\phi_2 \leftarrow \phi_{\text{opt}} + \theta$
  until $(L_{\text{opt}}, \phi_{\text{opt}})$ unchanged
  return $(L_{\text{opt}}, \phi_{\text{opt}})$

To find the optimal configuration, Algorithm 3 is run with $L_1 = L_{\min}$, $L_2 = L_{\max}$, $\phi_1 = \phi_{\min}$, $\phi_2 = \phi_{\max}$, and the current configuration (L_0, ϕ_0). The configuration search is, first, started by rotating the antenna between the given range while fixing the separation at the given separation value L_0. By measuring the received power at each angular position, we locate the angle ϕ_{opt} that gives the minimum received power for the current separation value L_0. We know that ϕ_{opt} found in this step is not necessarily the best one for other separation values. Therefore, in the next step, different separations within the given range $[L_1, L_2]$ are tried to improve the configuration. The configuration search in these two steps relies on the continuity property: if there is a better configuration, it is likely to be found in small vicinity of the most recently optimal configuration. We repeat these steps until no better configuration is found. We note that, before repeating the search, we reduce the search range by setting new values for L_1, L_2, ϕ_1, ϕ_2.

Algorithm 3 is much faster than brute-force, as it probes the optimal angle and separation values separately. We emphasize that the configuration returned by the fast algorithm is not essentially the best configuration, however as shown in Section 6, is comparable to brute-force.

To have a hybrid anti-jamming system, we use the fast algorithm to control the two-element antenna in parallel with digital processing. The fast algorithm is performed to reduce the received to such power levels that the signal received at the two-element antenna can be directly decoded.

4. DIGITAL JAMMING CANCELLATION

The digital jamming cancellation improves the system, in the case that the *first stage* cannot completely remove the jamming signal when the jammer power is extremely high (over 28 dB). The *second stage* comprises digital processing components as shown in Figure 7. The main idea of digital jamming cancellation is to eliminate the jamming signal from equation (1) to obtain the decodable user signal by equation (2). Therefore, the most important component in this stage is the *gain ratio estimation* component, which estimates the gain ratio a. In MIMO systems [36], the channel characteristics are usually estimated by training sequences. This technique is not applicable in our scenario, as the jamming signal is unknown to the receiver. Consequently we derive our own estimate technique described as follows.

4.1 Gain ratio estimation

In general, the channel gains affected by the communication medium are represented as complex numbers which introduce magnitude and phase change in the received signals. Our digital processing techniques are applied to sequences of samples taken from the analog input at discrete time $t = t_0, t_0 + \tau, t_0 + 2\tau, \ldots$ where τ is the sampling period and t_0 is the time when the signals arrive at the receiver input. Equation (1) can be rewritten in the time domain:

$$R_1(t) = h_{S1}(t)S(t) + h_{J1}(t)J(t)$$
$$R_2(t) = h_{S2}(t)S(t) + h_{J2}(t)J(t)$$

Removing the jamming signal involves the estimation of $a(t) = \frac{h_{J2}(t)}{h_{J1}(t)}$.

4.1.1 Magnitude estimation

The received power at the two-element antenna in the sampling time range $[t_0 - (n-1)\tau, t_0]$ of the past n samples before t_0 is

$$P_1(t_0) = \frac{1}{n} \sum_{t=t_0-(n-1)\tau}^{t_0} |h_{S1}(t)S(t) + h_{J1}(t)J(t)|^2$$

Since the jammer's signal and user's signal are highly uncorrelated, i.e. $\sum h_{S1}(t)h_{J1}(t)S(t)J(t) = 0$, the received

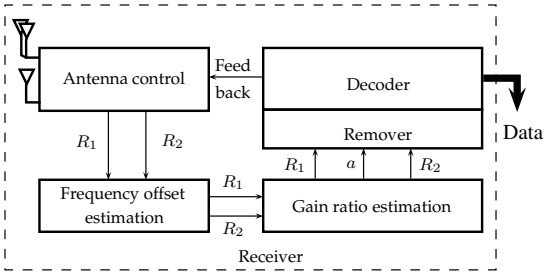


Figure 7: Receiver components.

power at the two-element antenna is rewritten as:

$$\begin{aligned} P_1(t_0) &= \frac{1}{n}\left(\sum_{t_0}|h_{S1}(t)S(t)|^2 + \sum_{t_0}|h_{J1}(t)J(t)|^2\right) \\ &= \frac{1}{n}\left(|h_{S1}|^2\sum_{t_0}|S(t)|^2 + |h_{J1}|^2\sum_{t_0}|J(t)|^2\right) \end{aligned}$$

where the second equality comes from the fact that the channel gains are considered constant during the period $[t_0 - (n-1)\tau, t_0]$, due to slow-fading characteristics in a narrowband communication [36], i.e., $h_{S1}(t) = h_{S1}$, $h_{S2}(t) = h_{S2}$, $h_{J1}(t) = h_{J1}$, $h_{J2}(t) = h_{J2}$. Similarly, the power received at the single-element antenna can be represented as $P_2(t_0) = \frac{1}{n}\left(|h_{S2}|^2\sum_{t_0}|S(t)|^2 + |h_{J2}|^2\sum_{t_0}|J(t)|^2\right)$.

If the portion of jamming power in $P_1(t_0)$ and $P_2(t_0)$ were significantly greater than that of the sender, one could estimate $|a| = \left|\frac{h_{J2}}{h_{J1}}\right| = \frac{P_2(t_0)}{P_1(t_0)}$. In order to estimate $|a|$ in more general cases, we apply another approach, in which the receiver is assumed to be able to determine at a specific time instant whether there is a data transmission or whether there is an interference, and therefore, can record the signals level in those periods. We note that in simple scenarios, where the jammer only emits noise, the jammer can be identified when the received signal is undecodable. In complex scenarios, if the jammer is capable of transmitting "user-like" data (e.g., the jammer is a compromised user), the system needs more sophisticated methods to identify whether the received signal is the jammer's signal. By rate adaptation algorithm, the sender can transmit the signal at different levels of power at different time, which also affects the accuracy of the jammer identification process. We leave those complex scenarios for future work. In this work, we consider a sender with basic constant-power modulation scheme (BPSK, QPSK) and a "dump" with unknown signal jammer in the following two cases:

Sender transmitted before collision.

If the sender transmitted before the jammer causes interference, the receiver estimates $|a|$ by the following steps:

- Measures $P_i(t_0)$ in the period t_0, which contains only the power of the sender's signal received at both (two-element and single-element) antennas, $P_{Si}(t_0) = P_i(t_0) = \frac{1}{n}|h_{Si}|^2\sum_{t_0}|S(t)|^2$ ($i = 1$ denotes the two-element antenna, and $i = 2$ denotes the single-element antenna). As the sender's power is constant, we obtain $P_{Si}(t) = P_{Si}(t_0) = P_{Si}$ for any other period $t > t_0$.
- Measures $P_i(t_1)$ in the interference period t_1, $|a|$ can be computed: $|a| = \left|\frac{h_{J2}}{h_{J1}}\right| = \sqrt{\frac{P_2(t_1)-P_{S2}}{P_1(t_1)-P_{S1}}}$.

Jammer transmitted before collision.

If the jammer is known to jam before the collision time t_0, the receiver measures the power at both (two-element and single-element) antennas before the collision, $P_i(t_0) = \frac{1}{n}|h_{Ji}|^2\sum_{t_0}|J(t)|^2$. In the collision period t_1, the receiver measures $P_i(t_1)$. Since the time period immediately before and after the collision is short, the jammer's power remains almost constant, i.e., $P_{Ji}(t_1) \approx P_{Ji}(t_0)$. This allows the sender's power at each antenna to be found by $P_{Si} = P_i(t_1) - P_i(t_0)$. Knowing P_{Si}, $|a|$ can be estimated by the last step described in the first case.

4.1.2 Phase estimation

The phase difference ϕ between $R_1(t)$ and $R_2(t)$ is determined by $\phi = \tan^{-1}\left(-\frac{\sum_t[I_1(t)Q_2(t)-I_2(t)Q_1(t)]}{\sum_t[I_1(t)I_2(t)+Q_1(t)Q_2(t)]}\right)$, where $I_1(t) = \mathrm{Re}[R_1(t)]$, $Q_1(t) = \mathrm{Im}[R_1(t)]$, $I_2(t) = \mathrm{Re}[R_2(t)]$, $Q_2(t) = \mathrm{Im}[R_2(t)]$ represent the real and imaginary parts of the received signals. Similarly to the approach used in estimating the magnitude, we derive ϕ based on the phase difference ϕ in the periods before and after the collision. In software-defined radio, for both magnitude and phase estimation, the signal processing operations are done for chunks of n samples taken from the analog input.

4.2 Removing and Decoding

When the gain ratio a is estimated correctly, the jamming signal can be removed completely from the received signals by solving equation (2). The residual signal $b \cdot S$ is sent to the decoder to decode the data. The gain b of the residual signal is considered as a new channel gain of the signal after removing the jamming signal. Therefore, the data can be decoded by the decoder with well-known decoding techniques [12, 27] in software-defined radio. Consequently, estimation of b is not required.

4.3 Practical issues

In practice, we need to address the issue of frequency offset between the received signals which are unavoidable in real devices. Moreover, the multipath problem is always an interesting part of systems working indoor.

Frequency offset estimation.

With the goal of providing a zero-knowledge anti-jamming system, manual calibration for compensating the frequency offset is not desired in our system. The frequency offset between the received signals is estimated in real-time by $\Delta f^* = \mathrm{argmax}_{\Delta f}|\mathscr{F}\{R_1(t)R_2^*(t)\}|$, for which the performance is optimized when the chunk size is a power of 2.

Dealing with multipath.

Our system also works efficiently in indoor environments (see Section 6). Due to space limits, we will now only provide a short, intuitive justification. In an indoor environment, due to reflection, multiple copies of the transmitted signals arrive at the receive antennas

$$\begin{aligned} R_1 &= \left(\sum_k h_{S1}^{(k)}\right)S + \left(\sum_k h_{J1}^{(k)}\right)J \\ R_2 &= \left(\sum_k h_{S2}^{(k)}\right)S + \left(\sum_k h_{J2}^{(k)}\right)J \end{aligned} \quad (3)$$

where $h_{Si}^{(k)}$, $h_{Ji}^{(k)}$ denote the channel gain of the k-th path from the sender and the jammer to the receiver, respectively.

By letting $h_{Si} = \sum_k h_{Si}^{(k)}$ and $h_{Ji} = \sum_k h_{Ji}^{(k)}$, equation (3) becomes equivalent to equation (1). Thus, sums R_1 and R_2 are now considered as line-of-sight signals transmitted from a different location. Recall that Algorithm 3 is designed to deal with unknown location transmitters, so it is applicable in this scenario in an attempt to reduce the multipath jamming signal.

Low-power jammer

As mentioned in Section 3, the antenna control algorithms rely on the implication of minimum received power. In case of low-power jammer, minimizing total received power does not necessarily maximizes the SJR at the two-element antenna. However, the antenna algorithms result in the change in portion of jammer power in the total received power at the two-element antenna compared to that at the single-element antenna, i.e., $h_{J1}/h_{S1} \neq h_{J2}/h_{S2}$, which allows obtaining the residual signal in equation (2). Therefore, when combining with the digital stage, the antenna algorithms help eliminating the jamming signal. Although the first stage does not necessarily reduce the jamming power, it helps the second stage to derive the residual signal for successful decoding, thus is useful even for low-power jammers.

Variable-power jammer

Recall the estimation of the gain ratio; as soon as the sender's power portion is determined, it can be used to derive the jammer's power portion (and hence their ratio a). Therefore, as long as the antenna remains in the same configuration, the power of the signal received from the sender is constant during the collision period, allowing the system to remove the variable-power jamming signal.

5. PROTOTYPE AND IMPLEMENTATION

Our system consists of one receiver node and two transmitter nodes. We use a software-defined radio [12] to deploy our testbed. The digital signal processing is done by a host computer connected to the receiver.

Nodes: Each node is deployed on an Ettus USRP device [28] with RFX2400 daughterboards. The jammer and sender use a single-element antenna for transmission. The receiver has a single-element and a two-element antenna for signal reception. All antenna elements are Titanis 2.4 GHz dipole Swivel SMA antennas.The receiver transfers digital samples to the host computer through an Ethernet link.

Two-element antenna: Our two-element antenna (Figure 2) comprises two Titanis antennas. Signals received from two elements are added together through a HyperLink Technologies SCW02 combiner, which is then connected to one input of the receiver (the other input is connected to the single-element antenna). To build the antenna frame, we used Autodesk Inventor 2012 to design it and built it using a uPrint Plus 3D printer [37]. The mechanical movement of the two-element antenna is controlled by two servos.

- **Rotation:** To rotate the antenna frame, we use a Hitec HS-485HB servo and attach the antenna frame to its rotating shaft. The HS-485HB servo is capable of rotating up to 200 degrees. However, we only need 180 degrees for half-circle rotation of the antenna, as two elements of the antenna are attached into the frame symmetrically with respect to the shaft. We set $\phi_{\min} = 0$ and $\phi_{\max} = \pi$ for the configuration algorithms.

Table 1: Comparison of brute-force and fast algorithm

	Brute-force	Fast
Reduction of power	15-30dB	15-28dB
Reduction compared to brute-force in each experiment	–	<6dB
Running time	> 5mins	5-18s

- **Separation:** We use a Hitec HS-785HB servo (capable of rotating up to 3.5 circles) to transform the rotation movement to element separation by using a combination of gears and racks adjustable on the antenna frame. The frame allows the separation adjusted from $L_{\min} = 3.1$cm to $L_{\max} = 37.5$cm.

The servos operate based on pulse-width modulation signals given to their input. To generate those signals from the host computer, we use a Crossbow TelosB mote for receiving commands from the host and generating signals with appropriate pulse-width.

6. EVALUATION

In this section, we evaluate our system for indoor environments using three nodes: jammer, sender, and receiver. In our testbed environment, there are usual blocking objects and reflectors, such as walls, desks, metallic cabinets, and office space separators. We run the testbed at a fixed frequency of 2.4GHz ($\lambda \approx 12.5$cm).

6.1 Antenna configuration

Basic operations

Two basic operations of the two-element antenna are the rotation and the separation adjustment. We measure the performance of those operations in terms of running time. The half-circle rotation takes roughly 1 second to rotate the antenna frame from 0 to π. The rotation servo is capable of rotating in sub-degree step. The separation adjustment takes about 2 seconds to increase the separation from 3.1cm to 37.5cm. The minimal separation step is ≈ 3.5 mm.

Brute-force algorithm

The brute-force algorithm is evaluated in terms of running time and capability of reducing jamming power. We deploy three nodes in a typical indoor environment. The jammer is set to transmit at 30dB higher power than the sender. Figure 8 shows the running time versus the power received at the two-element antenna relatively to the minimum value during the brute-force search. In this specific setup, using brute-force can eliminate up to almost 30dB of the jammer's power. Depending on the environment, the optimal configuration can be found at different time and the capability of reducing jamming power may vary. The total time to complete the brute-force search is more than 5 minutes as it tries all possible configurations.

Fast algorithm

In order to evaluate the performance of the fast algorithm, we run the fast algorithm with the same setup (same node locations and same settings of transmit power). The capability of reducing jamming power is shown explicitly in two steps in Figure 9. While the first step (rotation only)

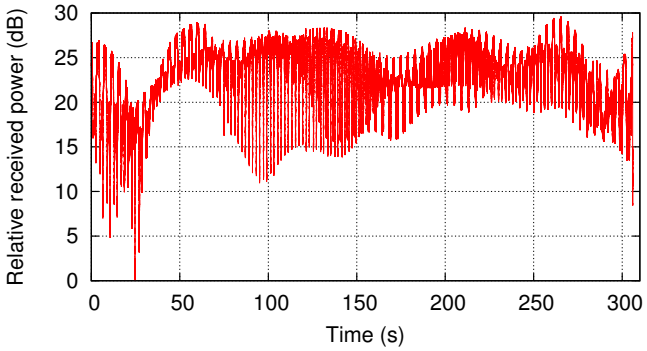


Figure 8: Brute-force: total received power relative to total received power's minimum value during search.

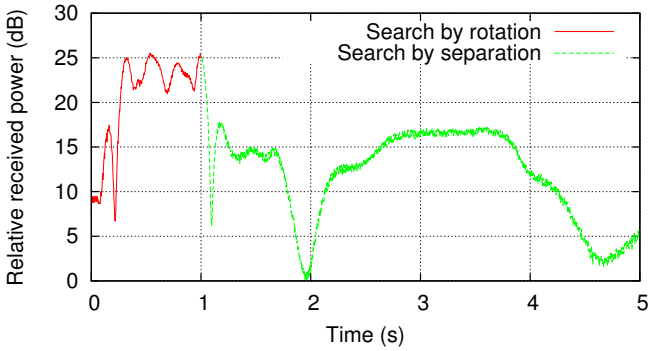


Figure 9: Fast: total received power relative to total received power's minimum value during search.

can find a configuration that reduces the received power to more than 15dB, the second step (separation adjustment only) helps improving the power reduction of the jammer to roughly 25dB, which is not far compared to the performance of the brute-force algorithm. The running time of the fast algorithm in this experiment takes only 5 seconds to complete. We note that the running time of the fast algorithms depend on the environment. Table 1 summarizes the performance of the brute-force and fast algorithms in various experiments with different setups.

6.2 Anti-jamming performance

We investigate the performance of our system by examining the probability of bit error of the decoded data after removing the jamming signal. In this experiment, we use basic DBPSK modulation for data transmission between sender and receiver and for generating the jamming signal of the jammer. The bit rate used by sender is 500kbps. The receiver runs continuously during the experiment. In order to investigate the probability of bit error, sent and received signals are recorded at each node and later transferred to the host computer to compare and count the error bits. In the experiment, we keep the power of the sender constant and increase the power of the jammer gradually after each run to a threshold that the data becomes undecodable.

To evaluate our system's performance, we compare three cases: (a) decode the received signal directly from the receiver's single-element antenna, i.e. without any anti-jamming technique, (b) decode the received signal from the receiver's two-element antenna, and (c) decode the residual signal after applying the digital jamming cancellation. The average probability of bit error is presented in Figure 10a. We visualize the BER in absolute (not log-scale) to make it easier to show the relative gain between combinations of techniques. Without the antenna auto-configuration capability (AA) and digital jamming cancellation (DC), the probability of bit error at the single-element antenna increases quickly when the jamming-to-signal ratio is greater than 3dB. Using the antenna auto-configuration with fast algorithm, the receiver can resist the jammer up to 28dB. The overall anti-jamming performance of the system is around 48dB when we combine two stages. The results demonstrate that our system is able to work efficiently in indoor environments.

DQPSK modulation

To study the effects of a higher-rate modulation on the performance of our system, we repeat the above experiments with DQPSK modulation at a doubled bit rate of 1Mbps.

Figure 10a compares the probability of bit error between DBPSK and DQPSK modulation. The performance of the system, when using DQPSK modulation, is around 42dB. Compared to the case of DBPSK modulation, the efficiency of the anti-jamming capability drops around 4 to 5dB. This is not surprising, since the constellation of the DQPSK modulation has a smaller minimum distance which results in higher probability of bit error [27]. Considering only the performance of the digital jamming cancellation, there is no significant difference in the capability of jamming cancellation between the two cases. This shows the efficiency of the estimation techniques applied in the second stage.

Variable power jammer

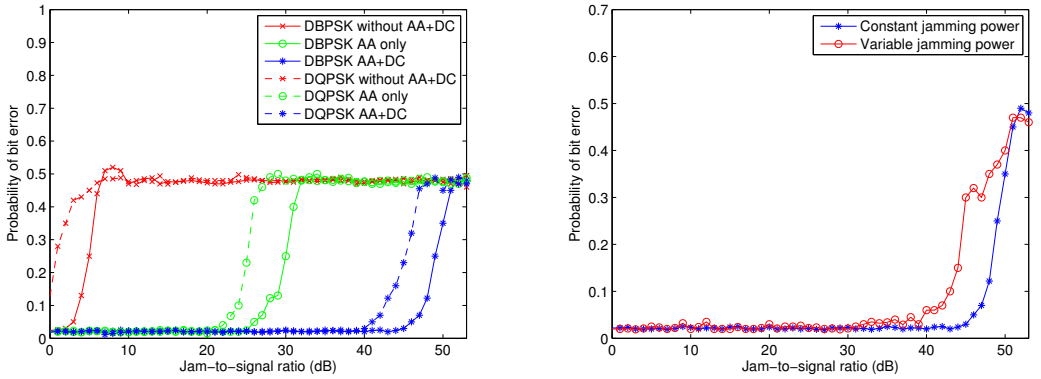
In the above experiments, the jammer transmitted at constant transmission power. To evaluate our system against a variable-power jammer, we modify the jammer such that after every 40 bytes it changes the transmit power to a random level within the range of 10 dB compared to the specified average power in each run. For this experiment, we use DBPSK modulation. We note that during the experiment, the antenna configuration does not change and is capable of removing a portion of about 28 dB in jamming power. Figure 10b shows the comparison between variable and constant jamming power cases in probability of bit error versus the average power in each run. The results show a performance degradation of 5-6 dB, demonstrating that the gain estimation is adaptive to the change of jamming power as long as the sender's power and the antenna remain unchanged.

7. DISCUSSION AND RELATED WORK

Based on our hybrid system, one can envision nodes with the two-element antenna that are capable of simultaneous signal transmission and reception. For example, in previous work [15], a design based on a balanced/unbalanced transformer could completely eliminate the self-signal. Similar components can augment our system, therewith enabling *full duplex* wireless communication.

In the context of *multi-hop wireless networks*, the two-element antennas open new opportunities for communicating nodes to enable selective transmission to desired destinations while at the same time avoiding jamming from concurrent or malicious nodes. This allows multiple simultaneous senders and increases the network's total throughput.

Anti-jamming has been an active area of research for decades. Techniques developed at the physical layer [30] in-



(a) DBPSK and DQPSK modulation

(b) Variable vs. constant power jamming

Figure 10: Bit error measurements.

clude directional antennas [18], spread spectrum communication, and power, modulation, and coding control. More recently, research has also addressed higher layers [1, 2, 7, 9, 11, 16, 17, 20, 21, 25, 31–33, 39–41]. However, given the ease of building *high power* jamming devices, there is still a strong need for efficient and flexible techniques operating at the physical layer. There is a demand for low-cost solutions mitigating the effects of jammers that are orders of power stronger than legitimate communication.

While spread spectrum has been a solution of choice for anti-jamming, it suffers from a need for pre-shared secrets between the communicating nodes. Several solutions were recently proposed for alleviating the need for pre-shared secrets [5, 11, 16, 19, 21, 32, 33]. However, they are not designed to tackle powerful jammers (meaning jammer with power 4-5 orders of magnitude higher than the transmitting node).

Other recent work has demonstrated mechanisms for cancelling interference. This work has found applications in protecting the confidentiality of communication [8, 13]. However cancelling *powerful*, *unknown* jammers results in several challenging problems such as jammer signal identification and channel estimation.

The closest related work to our system consists of phased array antennas and MIMO systems. Phased array antennas were very well studied since the 1950s [3, 4, 18, 35]. Likewise, multiple input multiple output systems (MIMO) were also very well studied since the 90s [36]. Our design and approach have unique characteristics that distinguishes them from prior work. Similar performance phased array antennas consist of a fairly large number of *fixed*-position elements aiming at creating a directed beam that can be electronically and digitally repositioned. A major goal is to minimize the impact of side lobes. Adaptive beamforming with algorithms such as MVDR and MMSE beamformers aims at minimizing the impact of the sidelobe, using a fairly large number of antennas and are considered to be more adequate for radar systems. In contrast, our system's goal is to create one or multiple nulls to minimize the jammer's impact while maximizing the legitimate user signal power and preparing the signal for a digital MIMO-like second stage of interference cancellation. To the best of our knowledge, our two-elements mechanical beam-forming design is new and is supplemented with an automatic configuration algorithm that achieves 28dB jammer cancellation in less than 20 seconds – both in indoor and outdoor environments. The system reaches 48dB cancellation when combined with our second-stage digital jamming cancellation. Existing phased array antennas achieving a gain of 48dB require hundreds of elements even with high-end, expensive 7-bit phase shifters [3, 22]. Our two-elements mechanical steering can be controlled with low-cost micro controllers instead of requiring expensive DSP boards. Our second-stage digital jamming cancellation is in principle similar to MIMO. However, existing algorithms assume that the incoming signals are of similar power, transmitted by a cooperating node, with the possibility to embed training sequences for the channel estimation.

8. CONCLUSION AND FUTURE WORK

The availability of software radios and commodity jammers are making jamming of wireless communication a problem of increasing importance for many cyber-physical applications. To mitigate the problem of jammers that are significantly more powerful than the transmitting nodes, we have designed, physically built, and evaluated a hybrid system of mechanical beam/null-forming and MIMO-like digital interference cancellation. Our novel antenna design and algorithms have several important characteristics and advantages compared to phased array antennas and MIMO techniques e.g., simplicity, low-cost, convergence speed. It allows a flexible creation of multiple nulls to cancel the effects of multi-path jamming. We have developed several techniques to effectively cancel the remaining interference digitally and verified their effectiveness in practice. To the best of our knowledge, this is the first academically published low-cost system that reduces the effects of powerful unknown jammers by almost five orders of power. As future work, we plan to extend our techniques from BPSK/QPSK modulation to multi-carrier BPSK/QPSK OFDM and higher order modulation. We plan to extend our antenna configuration algorithm and analytically quantify the worst-case gain loss as a function of speed in comparison with the brute-force configuration. We also believe that the unique beam-forming characteristics of our system results in new research problems in the context of multi-hop wireless network topology control in the presence of malicious interference.

References

[1] B. Awerbuch, A. Richa, and C. Scheideler. A jamming-resistant mac protocol for single-hop wireless networks. In *PODC*, pages 45–54, 2008.

[2] M. Bender, M. Farach-Colton, S. He, B. Kuszmaul, and C. Leiserson. Adversarial contention resolution for simple channels. In *SPAA*, pages 325–332, 2005.

[3] E. Brookner. Phased arrays and radars – past, present and future. *Microwave Journal*, 49(1):24–46, 2006. ISSN 01926225.

[4] E. Brookner. Phased-array radar: Past, astounding breakthroughs, and future trends. *Microwave Journal*, 51(1):30–50, 2008. ISSN 01926225.

[5] A. Cassola, T. Jin, G. Noubir, and B. Thapa. Efficient spread spectrum communication without pre-shared secrets. *IEEE Transactions on Mobile Computing*, to appear.

[6] A. Cassola, W. Robertson, E. Kirda, and G. Noubir. A practical, targeted, and stealthy attack against wpa enterprise authentication. In *Proceedings of NDSS*, 2013.

[7] J. Chiang and Y.-C. Hu. Dynamic jamming mitigation for wireless broadcast networks. In *INFOCOM*, pages 1211–1219, 2008.

[8] J. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti. Achieving single channel, full duplex wireless communication. In *MOBICOM*, pages 1–12, 2010.

[9] J. Dong, R. Curtmola, and C. Nita-Rotaru. Practical defenses against pollution attacks in intra-flow network coding for wireless mesh networks. In *In Proceedings of WiSec*, pages 111–122, 2009.

[10] FCC. Jammer enforcement, 2012. `http://www.fcc.gov/encyclopedia/jammer-enforcement`, `http://transition.fcc.gov/eb/News_Releases/DOC-304575A1.html`.

[11] S. Gilbert, R. Guerraoui, and C. Newport. Of malicious motes and suspicious sensors: On the efficiency of malicious interference in wireless networks. In *OPODIS*, 2006.

[12] GNU. Gnu radio. `http://www.gnuradio.org`.

[13] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: Non-invasive security for implantable medical devices. In *SIGCOMM*, pages 2–13, 2011.

[14] iClinks. Scada and industrial automation, ethernet scada and ethernet i/o. `http://www.iclinks.com/`.

[15] M. Jain, J. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha. Practical, real-time, full duplex wireless. In *Proceedings of international conference on Mobile computing and networking*, pages 301–312, Las Vegas, USA, 2011.

[16] T. Jin, G. Noubir, and B. Thapa. Zero pre-shared secret key establishment in the presence of jammers. In *In Proceedings of ACM MobiHoc*, pages 219–228, 2009.

[17] C. Koo, V. Bhandari, J. Katz, and N. Vaidya. Reliable broadcast in radio networks: The bounded collision case. In *PODC*, pages 258–264, 2006.

[18] J.-D. Kraus. *Antennas*. Mcgraw Hill Higher Education; 3rd edition, 2001.

[19] A. Liu, P. Ning, H. Dai, Y. Liu, and C. Wang. Defending dsss-based broadcast communication against insider jammers via delayed seed-disclosure. In *Proceedings of ACSAC'2010*, 2010.

[20] S. Liu, L. Lazos, and M. Krunz. Thwarting inside jamming attacks on wireless broadcast communications. In *In Proceedings of ACM WiSec*, pages 29–40, 2011.

[21] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential dsss: jamming-resistant wireless broadcast communication. In *INFOCOM*, pages 695–703, 2010.

[22] R. Mailloux. *Phased Array Antenna Handbook*. Artech Print on Demand, 2005.

[23] R. Miller. FCC steps up crackdown on cell jammers, 2012. `http://www.securitysystemsnews.com/article/fcc-steps-crackdown-cell-jammers`.

[24] NPR. Congress passes FAA bill that speeds switch to GPS, 2012. `http://www.npr.org/`.

[25] K. Pelechrinis, S. V. Krishnamurthy, C. Gkantsidis, and I. Broustis. Ares: An anti-jamming reinforcement system for 802.11 networks. *CoNEXT*, pages 181–192, 2009.

[26] PG & E. Smart meters by the numbers, 2011. `http://www.pge.com/myhome/customerservice/smartmeter/deployment/`.

[27] J. G. Proakis and M. Salehi. *Digital Communications*. McGraw-Hill, 5 edition, 2007.

[28] E. Research. Universal software radio peripheral. `http://www.ettus.com/`.

[29] SEMAPHORE. Integrated scada, control, and communication solutions. `http://www.cse-semaphore.com/`, 2011.

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

[31] D. Slater, P. Tague, R. Poovendran, and B. J. Matt. A coding-theoretic approach for efficient message verification over insecure channels. In *Proceeding of ACM WiSec*, 2009.

[32] M. Strasser, C. Popper, and S. Capkun. Efficient uncoordinated FHSS anti-jamming communication. In *Proceedings of ACM MobiHoc*, 2009.

[33] M. Strasser, C. Popper, S. Capkun, and M. Cagalj. Jamming-resistant key establishment using uncoordinated frequency hopping. In *Proceedings of IEEE Symposium on Security and Privacy*, 2008.

[34] Synetcom. Synetcom industrial wireless systems. `http://www.synetcom.com/`.

[35] H. V. Trees. *Detection, Estimation, and Modulation Theory, Part I*. Wiley & Sons, 2001.

[36] D. Tse and P. Viswanath. *Fundamentals of wireless communication*. Cambridge University Press, New York, NY, USA, 2005.

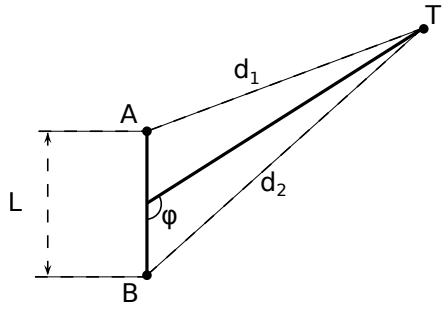


Figure 11: The two-element antenna in a free-space communication with one transmitter.

[37] uPrint. Uprint plus. `http://www.uprint3dprinting.com/`.

[38] vMonitor. Scada wireless systems. `http://www.vmonitor.com/`, 2011.

[39] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders. Short paper: reactive jamming in wireless networks: how realistic is the threat? In *Proceedings of ACM WiSec*, 2011.

[40] W. Xu, K. Ma, W. Trappe, and Y. Zhang. Jamming sensor networks: attack and defense strategies. *IEEE Network*, 20(3):41–47, 2006.

[41] W. Xu, W. Trappe, and Y. Zhang. Channel surfing: defending wireless sensor networks from interference. In *Proceedings of IPSN*, 2007.

[42] W. Zhang, M. Kamgarpour, D. Sun, and C. Tomlin. A hierarchical flight planning framework for air traffic management. *Proceedings of the IEEE*, 100(1), 2012.

APPENDIX

A. PROOFS

PROOF. [Theorem 1] In Figure 11, we consider the antenna configuration (L, ϕ) and the signals transmitted from T and received at antenna elements A and B. We assume a narrowband slow fading communication channel, therefore the signal received at A and B does not significantly differ in frequency offset, channel attenuation, fading, etc. The received signals at the two elements are represented by $r_A(t) = g(x)\cos(2\pi ft + 2\pi\frac{d_1}{\lambda})$, $r_B(t) = g(x)\cos(2\pi ft + 2\pi\frac{d_2}{\lambda})$, where $g(x)$ contains the transmitted data, f is the carrier frequency, λ is the carrier wavelength, and t denotes the receiving time. The sum of two signals at the output of the combiner, $r(t) = r_A(t) + r_B(t) = 2g(x)\cos(\pi\frac{d_1-d_2}{\lambda})\cos(2\pi ft + \pi\frac{d_1+d_2}{\lambda})$, is a signal of amplitude $|2g(x)\cos(\pi\frac{d_1-d_2}{\lambda})|$. Regardless of the transmitted data, the amplitude of $r(t)$ depends on the value of $|\cos(\pi\frac{d_1-d_2}{\lambda})|$. Since the distances between the transmitter and the receiver elements are much larger than the element separation, i.e., $d_1 \gg L$, $d_2 \gg L$, we have $d_1 - d_2 \approx L\cos\phi$. Let $h(\phi) = \cos^2(\pi K\cos\phi)$, $K = L/\lambda$. We investigate the amplitude of $r(t)$ indirectly by investigating $h(\phi)$. Note that by definition of maximizing angles and minimizing angles, the maximum and minimum values of $|r(t)|$ are not necessarily equal to 0 or 1. In fact, they are the roots of $h'(\phi) = 0$, where $h'(\phi) = 2\pi K\sin\phi\sin(2\pi K\cos\phi)$ is the derivative of $h(\phi)$. Roots of $h'(\phi) = 0$ satisfy the following conditions:

$$\sin\phi = 0 \tag{4}$$

$$\text{or} \quad \sin(2\pi K\cos\phi) = 0 \tag{5}$$

Letting $h_1(\phi) = 4\pi^2K^2\sin^2\phi\cos(\pi K\cos\phi)$ and $h_2(\phi) = 2\pi K\cos\phi\sin(\pi K\cos\phi)$, we have $h''(\phi) = h_2(\phi) - h_1(\phi)$.

First, we consider the equation (4). Let ϕ_1 be a root of (4), i.e., $\sin(\phi_1) = 0$, then $\cos(\phi_1) = \pm 1$, and $\phi_1 = 0$ or $\phi_1 = \pi$. As a result, $h_1(\phi_1) = 0$, and $h_2(\phi_1) = \pm 2\pi K\sin(\pm 2\pi K) = 2\pi K\sin(2\pi K)$ (the last equality is due to x having same sign as $\sin x$). Now that $h''(\phi_1) = h_2(\phi_1) = 2\pi K\sin(2\pi K)$.

- If $\{K\} \le \frac{1}{2}$, $h''(\phi_1) \ge 0$, then ϕ_1 is a minimizing angle.
- If $\{K\} \ge \frac{1}{2}$, $h''(\phi_1) \le 0$, ϕ_1 is a maximizing angle.

Now consider the equation (5). Let ϕ_2 be a root of (5), i.e., $\sin(2\pi K\cos\phi_2) = 0$, then we have $h_2(\phi_2) = 0$, and $h''(\phi_2) = -h_1(\phi_2) = -4\pi^2K^2\sin^2(\phi)\cos(\pi K\cos\phi)$. Note that $\cos(2\pi K\cos\phi_2) = \pm 1$.

- If $\cos(2\pi K\cos\phi_2) = 1$, or $\cos\phi_2 = k/K$, then $h''(\phi_2) < 0$, and ϕ_2 is a maximizing angle.
- If $\cos(2\pi K\cos\phi_2) = -1$, or $\cos\phi_2 = (k+\frac{1}{2})/K$, then $h''(\phi_2) > 0$, and ϕ_2 is a minimizing angle.

In conclusion, ϕ is a maximizing angle, if $\cos\phi = k/K$, or a minimizing angle, if $\cos\phi = (k+\frac{1}{2})/K$, $k \in \mathbb{Z}$. In addition, if $\{K\} \ge \frac{1}{2}$, we have two more maximizing angles at 0 and π; otherwise, they are two additional minimizing angles. □

PROOF. [Theorem 2] First, we observe that there is always one null between two lobes, and one lobe between two nulls, that is the number of minimizing angles equals the number maximizing angles. Therefore, it is enough to only determine the number of maximizing angles of the receive pattern given ratio K between the separation and the carrier wavelength. We prove the theorem by counting the number of maximizing angles.

If K is integer, according to Theorem 1, we have maximizing angles at ϕ, $\cos\phi = \frac{k}{K}$, $k = -K, \ldots, 0, \ldots, K$, $k \in \mathbb{Z}$.

- For $k = \pm K$, we have maximizing angles at 0 and π.
- For each $k \in S_1 = \{-K+1, \ldots, 0, \ldots, K-1\}$, $|S_1| = 2K-1$, there are two maximizing angles at $\phi = \arccos\frac{k}{K}$ and $\phi = \pi - \arccos\frac{k}{K}$.

In total, we have $2 + 2|S_1| = 4K$ maximizing angles.

If K is a non-integer, for each $k \in S_2 = \{-\lfloor K\rfloor, \ldots, 0, \ldots, \lfloor K\rfloor\}$, $|S_2| = 2\lfloor K\rfloor + 1$, we have 2 maximizing angles at $\phi = \arccos\frac{k}{K}$ and $\phi = \pi - \arccos\frac{k}{K}$. The number of those maximizing angles is $2|S_2|$.

- If $\{K\} \le \frac{1}{2}$, we have no more maximizing angles (Theorem 1), so the total number of maximizing angles is $2|S_2| = 2\cdot(2\lfloor K\rfloor + 1) = 2\lfloor 2K\rfloor + 2$.
- If $\{K\} \ge \frac{1}{2}$, we have two additional maximizing angles at 0 and π (Theorem 1), which increase the total number of maximizing angles to $2|S_2|+2 = 2\cdot(2\lfloor K\rfloor + 1) + 2 = 4\lfloor K\rfloor + 4 = 2\lfloor 2K\rfloor + 2$.

Therefore, the total of maximizing angles for the case of non-integer K is $2\lfloor 2K\rfloor + 2$. Note that the above formulas are established based on the following claim: *"for any number x, if $\{x\} < \frac{1}{2}$, then $\lfloor 2x\rfloor = 2\lfloor x\rfloor$; otherwise $\lfloor 2x\rfloor = 2\lfloor x\rfloor + 1$"*. □