Ph.D. Thesis Proposal

Robust Wireless Communication for Multi-Antenna, Multi-Rate, Multi-Carrier Systems

Triet Dang Vo-Huu

College of Computer and Information Science
Northeastern University

Ph.D. Committee

Guevara Noubir	Advisor, Northeastern University
Erik-Oliver Blass	Airbus Group Innovations / Northeastern University
Rajmohan Rajaraman	Northeastern University
Srdjan Capkun	External member, ETH Zurich
David Starobinski	External member, Boston University

October 2014

Abstract

Today's trend of migrating radio devices from hardware to software provides potential to create flexible applications for both commercial and military use. However, this raises security concerns, as malicious attackers can also be generated easily to break legitimate communications. In this research work, our goal is to design a robust anti-jamming radio framework. We particularly investigate three different aspects of jamming threats: high-power jammers, link attacks on rate adaptation, and jamming in multicarrier systems.

The threats of high-power jamming to wireless communications today are realistic due to the ease of access to powerful jamming sources such as the availability of commercial GPS/WiFi/cellular devices on the market, or RF guns built from microwave ovens' magnetron. To counter high-power jamming attacks, we develop SAIM which is a hybrid system capable of resisting jammers of up to 100,000 times higher power than legitimate communication nodes. The system robustness relies on our own antenna structure specially designed for anti-jamming purpose. We develop an efficient algorithm for auto-configuring the antenna adaptively to dynamic environments. We also devise a software-based jamming cancellation technique for appropriately extracting original signals, which is more robust than traditional MIMO approaches, as pilot signals are not required in SAIM.

In spite of the robustness of SAIM, our design is more appropriate for malicious environments with powerful jammers, where mechanical steering is feasible, e.g., military applications. Residential and commercial wireless communication systems are still vulnerable to even limited-power jamming, as in today's standard wireless protocols, rate information is exposed to adversaries. Rate-based attacks have been demonstrated to severely degrade the networks at very low cost. To mitigate rate-based attacks, we develop CBM, a system capable of hiding rate and – at the same time – increasing resiliency against jammers up to seven times higher than regular systems, where rate is exposed. We achieve the resiliency boost by generalizing Trellis Coded Modulation to allow non-uniform codeword mapping. We develop an efficient algorithm for finding good non-uniform codes for all modulations in {BPSK, QPSK, 8-PSK, 16-QAM, 64-QAM}. To conceal rate information, we devise an efficient method for generating cryptographic interleaving functions.

In recently deployed communication networks such as WiFi and LTE systems, MIMO and OFDM are the two main techniques for increasing bandwidth efficiency. While MIMO increases the channel capacity by spatial processing on multiple received signals, OFDM mitigates impacts of dynamic variations in wide-band channels and allows frequency reuse with overlapping carriers. Synchronization is a key for high-throughput performance in MIMO and OFDM systems. In this work, we study impacts of jamming attacks specifically targeting to control channels in WiFi and LTE networks. Our study focuses on efficient techniques for both jamming and anti-jamming in multicarrier systems.

Contents

1 Introduction **1**

2 SAIM: Countering High-power Jammer **2**
2.1 Approach . . . 2
2.2 Related work . . . 3
2.3 First stage – Antenna Auto-Configuration . . . 3
2.3.1 Pattern analysis . . . 3
2.3.2 Antenna configuration algorithm . . . 5
2.4 Second stage – Digital Jamming Cancellation . . . 6
2.4.1 Channel gain ratio estimation . . . 6
2.4.2 Practical issues . . . 7
2.5 Evaluation results . . . 7
2.5.1 Antenna configuration performance . . . 7
2.5.2 Anti-jamming performance of the whole system . . . 7

3 CBM: Concealing Rate Information and Boosting Resiliency for Link Adaptivity **8**
3.1 Challenges . . . 8
3.2 Approach . . . 9
3.3 Related work . . . 10
3.4 General Trellis Coded Modulation Codes . . . 11
3.5 Cryptographic Interleaving . . . 12
3.6 Evaluation results . . . 14

4 Enhancing Multicarrier Multiantenna Systems **14**
4.1 OFDM system . . . 14
4.2 OFDM in IEEE 802.11 . . . 15
4.3 Vulnerabilities in IEEE 802.11 OFDM . . . 16
4.4 Challenges . . . 16

5 Future work and research plan **17**

1 Introduction

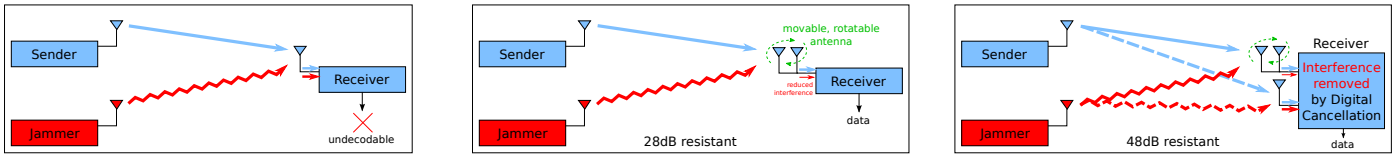
Over the last decades, wireless communication proved to be an enabling technology for an increasingly large number of applications. The convenience of wireless and its support of mobility has revolutionized the way we access data, information services, and interact with the physical world. Beyond enabling mobile devices to access information and data services ubiquitously, it is today widely used in cyber-physical systems such as air-traffic control [70], power plants synchronization, transportation systems, and human body implantable devices [22]. For example, the United States Congress recently passed an FAA bill that speeds up the switching to GPS-based air traffic control [40]. 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 [46]. 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 [64], Industrial Control Links [23], Synetcom [57], and Semaphore [51]. 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 [30, 12]. For example, an adversary can make a cellular network disappear and spoof it by a rogue network (usually a downgraded 2G network that does not have the appropriate mutual-authentication mechanisms but is still accepted by today's deployed devices). Another example consists of jamming the GPS signals and replacing them with a stronger replayed version. Beyond corrupting the location information, which can have severe impact on air traffic control, this can also stealthily corrupt time synchronization, which is critical for controlling electricity flow in power grids [52, 69, 71]. This jamming/replay attack applies not only to commercial grade GPS but also military ones.

With the fast growth of hardware and software-defined radio platforms along with the spectrum becoming a scarce resource, jamming has recently regained interest in the wireless security community. In this research work, we are particularly interested in three different aspects of jamming attacks.

- *High-power jamming:* Jamming with high power is today realistic with jamming hardware against GPS, Cellular Systems, and WiFi already available on the Internet 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. For example, High Energy RF (HREF) guns can be built from a $7 magnetron that 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 [10, 44]. This type of jamming can completely take down the whole communication network within a large area.
- *Rate-based jamming:* Even in limited-power jamming scenarios, today's standardized wireless systems are still vulnerable, as in most of communication protocols, control information is exposed to adversaries. In particular, jamming based on rate information leakage has proved to be a highly efficient attack. For example, Noubir et al. [39] showed that knowledge of the rate used in a transmission enables selective jamming of packets resulting in link degradation from 54 Mbps to 1 Mbps, and it also blocks other devices and causes high collisions provoking a long-lasting network-wide congestion collapse. One of the key reasons why such attacks are possible is because the rate information is either explicit (e.g., PSF field of the IEEE 802.11 PLCP header) or implicit (analysis of I/Q modulation).
- *Multicarrier jamming:* Due to quick adoption of MIMO (Multiple Input Multiple Output) and OFDM (Orthogonal Frequency Division Multiplexing) in recent communication networks (e.g., WiFi, 3G, LTE), the robustness and resiliency against jamming of those multicarrier networks raise new challenges for network operators. For example in LTE networks, a jammer can generate interference in a very short time to destroy the PCFICH, which carries the number of allocated symbols, to eliminate subsequent transmitted data frames [25]. This attack is very energy-efficient. As another example, pilot channels, which serve as a synchronization mechanism between transmitter and receiver, have been shown to be sensitive to interference [18]. This implies that jamming attacks focused on control channels can efficiently destroy transmissions in multicarrier systems.

Our goal is to develop an efficient and practical system to mitigate jamming attacks belonging to three classes described above. For the high-power jamming and rate-based jamming problems, we have developed concrete efficient solutions and our preliminary results show that significant jamming impact can be reduced with our system. Our study on multicarrier jamming, however, is still at the preliminary stage of investigating the possible threats. Our work is summarized below.

SAIM – Countering High-power Jammer We develop SAIM (Steerable-separable Antenna for Interference Mitigation) system which operates in two stages: Antenna Auto-Configuration and Digital Jamming Cancellation. The high-power anti-jamming capability of the system relies on our novel two-element antenna structure controlled by a fast auto-configuration algorithm and an efficient adaptive jamming canceling technique. Our two-element mechanical beam-forming design is new and can mitigate jamming power up to almost three orders of magnitude (28 dB). Overall, SAIM can reduce the impact



(a) Traditional system without anti-jamming. **(b)** SAIM's 1st stage: Two-element Antenna Control. **(c)** SAIM's 2nd stage: Digital Cancellation.

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

of jamming by up to give orders of magnitude (48 dB) and can work efficiently in both indoor and outdoor environments without the need of pilot channels or training sequences as with traditional MIMO techniques.

CBM – Concealing Rate Information and Boosting Resiliency We introduce CBM (Conceal and Boost Modulation), an integrated solution to conceal the rate information of wireless transmissions while simultaneously boosting the communication resiliency against interference. The proposed solution is based on a generalization of Trellis Coded Modulation combined with Cryptographic Interleaving. We developed efficient algorithms for discovering and validating new trellis codes capable of upgrading any modulation constellation in {BPSK, QPSK, 8-PSK, 16-QAM, 64-QAM} to any higher order modulation. We relax the uniformity and devise explicit codes with higher coding gain than traditional codes conforming to uniformity. We demonstrate that in most cases this modulation hiding scheme has the side effect of boosting resiliency by up to seven times in comparison to regular systems (with rate exposed) and up to ten times to prior work [48]. By Cryptographic Interleaving, CBM also helps mitigating passive attacks against users traffic analysis [2].

Enhancing Multicarrier Systems Our study of jamming problem in multicarrier systems includes the study of jamming techniques and practical efficient anti-jamming mechanisms. We particularly focus on the effectiveness of pilot carriers, cyclic prefix, and preamble used for synchronization and channel estimation in currently deployed WiFi and LTE systems.

2 SAIM: Countering High-power Jammer

We consider a setup of jamming where the spread spectrum and coding gain are not sufficient to counter the jammer. In this preliminary work, we focus 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.

2.1 Approach

In a traditional system (Figure 1a), where the receiver has only a single antenna, the simultaneous transmission of both sender and jammer causes collisions at the receiver. If the jammer interference is strong, the data becomes undecodable due to low SJR (Signal-to-Jamming Ratio) at the receiver. Our SAIM system operates in two stages (Figures 1b and 1c):

- **First stage – Antenna Auto-Configuration:** We introduce a novel two-element antenna (Figure 2a) that dynamically reconfigures to track the jammer and to weaken its signal by up to 28 dB (nearly 640 times). Our design with two moving elements is *simple*, *low-cost*, and has unique characteristics unexplored in mechanically steerable antennas. Our configuration algorithm allows to converge on element separation/rotation that maximizes the SJR within 20 seconds.
- **Second stage – Digital Jamming Cancellation:** To further mitigate the inteference, we also use a single-element antenna to get an additional copy of the jamming signal and develop a MIMO-like interference cancellation technique 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 jamming impact by 48 dB (nearly 64,000 times).

Our main 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.

2.2 Related work

Anti-jamming has been an active area of research for decades. Techniques developed at the physical layer [53] include directional antennas [28], spread spectrum communication, and power, modulation, and coding control. More recently, research has also addressed higher layers [67, 56, 55, 24, 35, 36, 16, 45, 3, 21, 6, 27, 66, 19, 65, 54]. 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 [56, 55, 24, 36, 21, 34, 11, 1]. 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 [22, 17, 60]. However cancelling *powerful*, *unknown* jammers results in several challenging problems such as jammer signal identification and channel estimation.

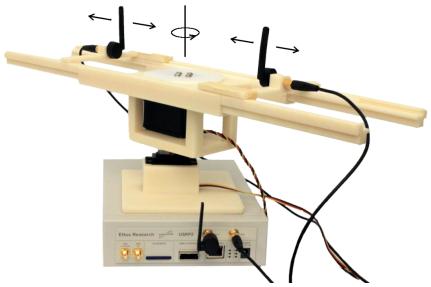
The closest related work to our approach consists of phased array antennas and MIMO systems. Phased array antennas were very well studied since the 1950s [61, 28, 9, 10]. Likewise, MIMO systems were also very well studied since the mid 90s [62]. Our design and approach have unique characteristics that 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. Various adaptive beamforming algorithms have been studied with the goal of minimizing the impact of sidelobes. For example, MMSE (Minimum Mean Squared Error) approaches aim to adjust weights on array elements such that the error with respect to a referenced signal is minimized. Alternatively, approaches based on MVDR (Minimum Variance Distortionless Response) mitigate interference by minimizing the received signal given the knowledge of propagating channel. The effectiveness of these approaches heavily rely on the training phase, and they use 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. Existing phased array antennas achieving a gain of 48dB require hundreds of elements even with high-end, expensive 7-bit phase shifters [37, 9]. 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. Furthermore, MIMO-like digital beam-forming is not efficient against powerful jammers because of the limited dynamic-range of RF front-ends and ADCs (which are typically 12 to 14 bits).

2.3 First stage – Antenna Auto-Configuration

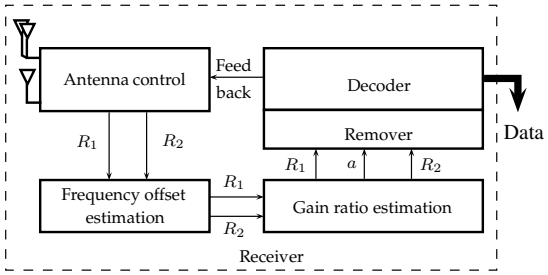
In SAIM, the first stage employs a special design of antenna used for the receiver (Figure 2a). Specifically, two single antennas are connected together through a combiner to create a composite antenna. In this work, we use the term *two-element antenna* to indicate the cardinality of the composition. We design the antenna structure such that not only the antenna orientation, but also the distance between two elements can be adjusted, resulting in dynamic receive patterns. We will show that a *large* number of different receive patterns can be constructed, in comparison with fixed-position electronically steerable arrays. Later in this section, we present our efficient algorithm for auto-configuring the antenna adaptively to dynamic environments such that the received legitimate signal is enhanced, while – at the same time – the received jammer's signal is mitigated. In other words, we aim to maximize the received SJR. The auto-configuration algorithm is implemented in the "Antenna control" component shown in Figure 2b.

2.3.1 Pattern analysis

We first study the basic characteristics of our two-element antenna. As the antenna structure can rotate around the vertical axis and two elements can move along the holding frame, signals received at two elements can be added constructively or destructively depending on the difference between phases arriving at two elements, which in turn depend on orientation

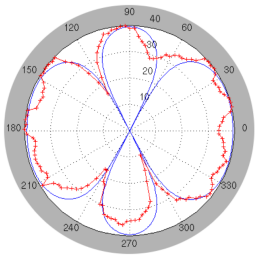


(a) Two-element antenna prototype.

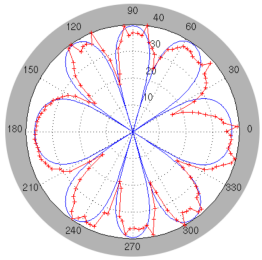


(b) Receiver's building components.

Figure 2: Two-element antenna prototype and receiver's building components.



(a) Element separation $L = \lambda$



(b) Element separation $L = 2\lambda$

Figure 3: Two-element antenna's theoretical (line without plus signs) and experimental (line with plus signs) receive patterns.

and separation of elements. When two signals have the same phase, they add up together. When phases are opposite, signals eliminate each other. In the following, we characterize the receive pattern[1] of the antenna. Specifically, we are interested in the locations of lobes (where signals add up) and nulls (where signals eliminate). For ease of presentation, we introduce our notation:

Definition 2.1. *The antenna is said to be in a configuration (L, ϕ), if the element separation is equal to L and the frame position creates an angle ϕ with a referenced frame position. We assume that $L_{\min} \leq L \leq L_{\max}$ and $\phi_{\min} \leq \phi \leq \phi_{\max}$ for some system parameters $L_{\min}, L_{\max}, \phi_{\min}, \phi_{\max}$ depending on design and implementation constraints. We denote $P(L, \phi)$ as the signal power received with the corresponding configuration.*

Aiming to reducing interference, we are interested in such antenna configurations that result in minimum and maximum received power. Those special configurations are defined accordingly as follows.

Definition 2.2. *(L, ϕ) is a minimizing (resp. maximizing) configuration, if $P(L, \phi) \leq P(L', \phi')$ (resp. $P(L, \phi) \geq P(L', \phi')$) for all (L', ϕ'), $L' \in [L_{\min}, L_{\max}]$,$\phi' \in [\phi_{\min}, \phi_{\max}]$.*

Definition 2.3. *L_ϕ is called ϕ-minimizing separation, if $P(L_\phi, \phi) \leq P(L, \phi)$ for all $L \in [L_{\min}, L_{\max}]$. Similarly, L_ϕ is called ϕ-maximizing separation, if $P(L_\phi, \phi) \geq P(L, \phi)$ for all $L \in [L_{\min}, L_{\max}]$.*

Definition 2.4. *ϕ_L is called L-minimizing angle, if $P(L, \phi_L) \leq P(L, \phi)$ for all $\phi \in [\phi_L - \theta, \phi_L + \theta]$. The parameter θ denotes the local search range, which will be discussed later. Similarly, ϕ_L is called L-maximizing angle, if $P(L, \phi_L) \geq P(L, \phi)$ for all $\phi \in [\phi_L - \theta, \phi_L + \theta]$.*

Analytical pattern – light-of-sight model In light-of-sight propagation model, phases of signals received at two antenna elements only depend on the antenna configuration and the distance to transmitter. When distance to transmitter is significantly far in comparison to element separation, Theorems 2.1 and 2.2 give the locations and number of lobes and nulls as functions of the relative ratio $K = L/\lambda$ between element separation L and signal wavelength λ. Theorem 2.1 precisely determines the locations of lobes and nulls. It is interestingly noted that the angles 0 and π become nulls when the ratio's fractional part $\{K\} = K - \lfloor K \rfloor$ is less than half; otherwise, they become lobes. Theorem 2.2 determines the number of lobes and nulls expected for a configuration, which is useful for optimizing the antenna control algorithm shown later.

[1]Receive pattern of an antenna shows the power of signal received at the antenna from a specific direction. We use polar coordinate system to depict the pattern, where the angle represents the incoming signal's direction, while the distance to origin indicates the level of signal power (dB scale).

Theorem 2.1 (Locations of lobes and nulls). *For a free-space communication at carrier wavelength λ with a receiver's two-element antenna configured at separation L, letting $\mathcal{M} = \{\phi, \cos\phi = k/K, |k| < K, k \in \mathbb{Z}\}$, where $K = L/\lambda$, the maximizing angles are located at*

$$\phi_L \in \mathcal{M}, \text{ if } \{K\} < \tfrac{1}{2} \qquad \phi_L \in \{0, \pi\} \cup \mathcal{M}, \text{ if } \{K\} \geq \tfrac{1}{2}.$$

Similarly, letting $\mathcal{N} = \{\phi, \cos\phi = \frac{k+1/2}{K}, |k + 1/2| < K, k \in \mathbb{Z}\}$, the minimizing angles are located at

$$\phi_L \in \{0, \pi\} \cup \mathcal{N}, \text{ if } \{K\} < \tfrac{1}{2} \qquad \phi_L \in \mathcal{N}, \text{ if } \{K\} \geq \tfrac{1}{2}.$$

Theorem 2.2 (Number of lobes and nulls). *The number of maximizing angles of the two-element antenna in a free-space communication is equal to the number of minimizing angles, which is*

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

Experimental pattern – Continuity property We conducted extensive experiments in both outdoor and indoor environments, and we verified that the results given by Theorems 2.1 and 2.2 can apply to outdoor scenarios (Figures 3a and 3b). Unfortunately, they are not applicable to indoor scenarios due to unpredictable propagation paths. However, we observe that similarly to light-of-sight model and outdoor environments, the locations of maximizing and minimizing angles in indoor scenarios also deviate slightly if there is only a small change in either antenna orientation or element separation. We call this the *continuity property* of the antenna pattern.

2.3.2 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 2.1 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.

We exploit the pattern's *continuity property* to develop our fast antenna control algorithm using heuristic approach, cf. FastAntennaControl. In our preliminary results, our antenna control algorithm can quickly find a configuration within 20 seconds and reduce the jamming impact by up to 28 dB (nearly 640 times).

FastAntennaControl$(L_0, L_1, L_2, \phi_0, \phi_1, \phi_2)$

```
1  L* = L_0,   φ* = φ_0                    // initial configuration
2  repeat
3      for φ = φ_1 to φ_2                  // rotating search while fixing separation
4          if P(L*, φ) < P(L*, φ*)
5              φ* = φ
6      for L = L_1 to L_2                  // separating search while fixing orientation
7          if P(L, φ*) < P(L*, φ*)
8              L* = L
9      // update search range
10     L_1 = L* − ΔL,   L_2 = L* + ΔL
11     φ_1 = φ* − θ,    φ_2 = φ* + θ
12 until (L*, φ*) unchanged
13 return (L*, φ*)
```

Main idea: Our algorithm is a local optimum search based on online measurement of received power at the receiver. The algorithm is initialized with a full search range $L_1 = L_{\min}$, $L_2 = L_{\max}$, $\phi_1 = \phi_{\min}$, $\phi_2 = \phi_{\max}$, which are determined by the antenna implementation constraints. The initial configuration (L_0, ϕ_0) are given as parameters. The configuration is iteratively improve in a series of steps, each comprises searching in only one dimension, either rotation or separation change. Due to the continuity property of the receive pattern, the algorithm converges in a local optimum point which corresponds to a good configuration, in which the SJR is maximized. The search range $(L_1, L_2, \phi_1, \phi_2)$ is updated after each iteration with system parameters ΔL and θ.

2.4 Second stage – Digital Jamming Cancellation

In the second stage (Figure 1c), we extend our model by using digital interference cancellation to eliminate the jamming signal. Our cancellation technique requires an additional signal provided to the receiver. We use a single-element antenna for the additional signal reception. As a result, SAIM's receiver uses totally three single antennas, two of which are joined to construct the composite two-element antenna. In our simplified model, eq. (1) illustrates the idea of the jamming cancellation technique applied to the received signals at the single-element antenna (ANT-1) and the two-element antenna (ANT-2). We obtain two different copies R_1, R_2 of the transmitted signal at the receiver:

$$\begin{aligned} R_1 &= h_{S1}S + h_{J1}J, \qquad h_{S1}, h_{J1} : \text{channel gain of sender, jammer to ANT-1} \\ R_2 &= h_{S2}S + h_{J2}J, \qquad h_{S2}, h_{J2} : \text{channel gain of sender, jammer to ANT-2} \end{aligned} \tag{1}$$

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: $bS = aR_1 - R_2$, where $b = ah_{S1} - h_{S2}$. Knowing a, we can decode S. The channel gain 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. While the techniques used in this system are rooted in techniques developed for MIMO communication [62] and phased array antenna [61, 37], 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 and unknown jammers*, unlike traditional MIMO techniques that operate over user-designed transmission signals of similar powers, allowing adequate channel estimation through training sequences. In the following, we discuss our channel gain ratio estimation, the key challenge in our cancellation technique.

2.4.1 Channel 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 explicitly rewritten in the time domain as follows:

$$\begin{aligned} R_1(t) &= h_{S1}(t)S(t) + h_{J1}(t)J(t) \\ R_2(t) &= h_{S2}(t)S(t) + h_{J2}(t)J(t) \end{aligned}$$

where the channel gains are complex functions of time t. Removing jamming signal involves the estimation of $a(t) = \frac{h_{J2}(t)}{h_{J1}(t)}$. We estimate $a(t)$ by separately computing its magnitude and phase over a small number of n samples. Since the jamming signal is unknown (i.e., $h_{J1}(t), h_{J2}(t)$ are unknown), our approach is to exploit the independence of stochastic processes.

Magnitude estimation The received power at ANT-1 in the past n samples before time t_0 is:

$$P_1(t_0) \triangleq \frac{1}{n}\sum^{t_0} |h_{S1}(t)S(t) + h_{J1}(t)J(t)|^2 = \frac{1}{n}\left(\sum^{t_0} |h_{S1}(t)S(t)|^2 + \sum^{t_0} |h_{J1}(t)J(t)|^2\right) = \frac{1}{n}\left(|h_{S1}|^2 \sum^{t_0} |S(t)|^2 + |h_{J1}|^2 \sum^{t_0} |J(t)|^2\right)$$

where the second equality is due to the independence between jamming signal and sender's signal, i.e., $\sum h_{S1}(t)h_{J1}(t)S(t)J(t) = 0$, while the third equality comes from the slow-fading characteristics in a narrowband communication [62], 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 ANT-2 can be represented as $P_2(t_0) = \frac{1}{n}\left(|h_{S2}|^2 \sum^{t_0} |S(t)|^2 + |h_{J2}|^2 \sum^{t_0} |J(t)|^2\right)$.

In order to estimate $|a|$, our approach is to measure the received power before and after the collision, and compare the recorded power in these two short periods to determine the ratio's magnitude. The correctness of our method relies on the slow-fading assumption, by which the user/jammer's signal is considered to have constant average power across the collision time.

Detect collision: To detect the collision, we monitor the average received power in a short period (several symbols) and seek for the abrupt change in magnitude. The collision is reported when the average received power suddenly increases by at least twice in a period of 1 or 2 symbols.

Sender transmitted before collision: If only the sender transmitted before the jammer generates interference at time t_0, the receiver estimates $|a| = \left|\frac{h_{J2}}{h_{J1}}\right| = \sqrt{\frac{P_2(t_0+n\tau) - P_2(t_0)}{P_1(t_0+n\tau) - P_1(t_0)}}$, where $P_i(t_0 + n\tau)$, $P_i(t_0)$ are the measured power in collision period and prior-collision period, respectively.

Jammer transmitted before collision: If the jammer generates interference before the collision time t_0, the receiver first computes the portion of sender in collision period: $P_{Si}(t_0 + n\tau) = P_i(t_0 + n\tau) - P_i(t_0)$. Since the sender is assumed to always transmit at constant average power, $P_{Si}(t)$ is considered as constant: $P_{Si}(t) = P_{Si}$. Thus, $|a|$ is estimated by $|a| = \left|\frac{h_{J2}}{h_{J1}}\right| = \sqrt{\frac{P_2(t_0+n\tau)-P_{S2}}{P_1(t_0+n\tau)-P_{S1}}}$.

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.

2.4.2 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 $\Delta f^* = \mathrm{argmax}_{\Delta f} |\mathscr{F}\{R_1(t)R_2^*(t)\}|$, where $\mathscr{F}$ denotes the Fourier transform.

Dealing with multipath: In this paragraph, we demonstrate that our estimation approach also works efficiently in indoor environments, where multipaths can occur. Intuitively, due to reflection, multiple copies of the transmitted signals arrive at the receive antennas:

$$\begin{aligned} R_1 &= \left(\textstyle\sum_k h_{S1}^{(k)}\right) S + \left(\textstyle\sum_k h_{J1}^{(k)}\right) J \\ R_2 &= \left(\textstyle\sum_k h_{S2}^{(k)}\right) S + \left(\textstyle\sum_k h_{J2}^{(k)}\right) J \end{aligned} \tag{2}$$

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 (2) becomes equivalent to equation (1). Thus, the sums R_1 and R_2 are now considered as line-of-sight signals transmitted from a different location. As a result, FastAntennaControl algorithm and our jamming cancellation technique are still applicable. Our experimental results for indoor environments (Section 2.5) confirm this conclusion.

2.5 Evaluation results

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 (carrier wavelength $\lambda \approx 12.5$cm).

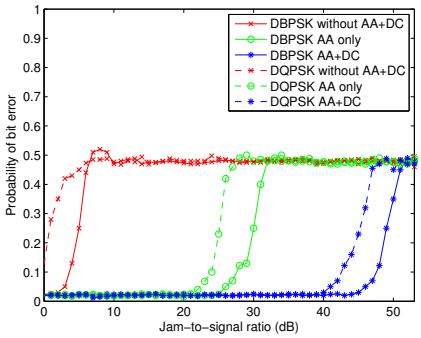
2.5.1 Antenna configuration performance

Basic operations Two basic operations of the two-element antenna are rotation and 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 antenna 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.

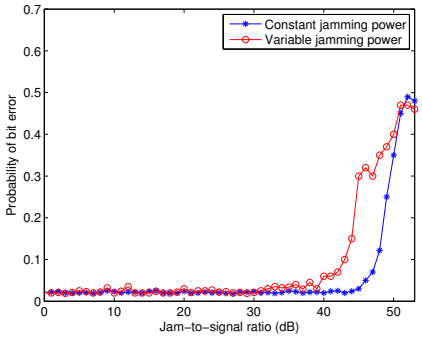
Configuration algorithm's performance In order to evaluate the auto-configuration ability, we run the algorithm under the presence of jammer with 30dB higher power. We observe that the algorithm takes only 5 seconds in the best case and roughly 20 seconds in the worst case to find the best configuration. The power reduction of jammer due to reconfiguration is roughly 25dB, leaving a gap of only 5dB difference between the sender's signal and jammer's signal, which can be resolved by the digital cancellation stage.

2.5.2 Anti-jamming performance of the whole system

We investigate the performance of our system by examining the probability of bit error of the decoded data after removing the jamming signal. 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



(a) Impact on different modulations.



(b) Impact by variable vs. constant power jamming.

Figure 4: Anti-jamming performance comparison.

experiment. In order to investigate the probability of bit error, sent and received signals are recorded at each node for later comparison and bit-error counting. 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 4a. 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 4a 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 [47]. 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 4b 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.

3 CBM: Concealing Rate Information and Boosting Resiliency for Link Adaptivity

3.1 Challenges

Knowing the rate being used by the communication link can lead to a very efficient attack for the adversary, because most of wireless systems can only operate reliably at a bit error rate of 10^{-6} or below. For instance, a TCP packet of typical size 1440 bytes can only be transmitted at a success probability of 99% if the bit error rate of the channel is under 10^{-6}. At the bit error rate 10^{-6}, a communication using 64-QAM modulation requires the transmitter to transmit at a power

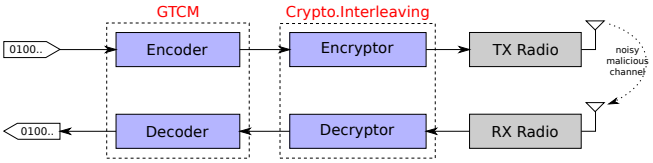


Figure 5: Our CBM system comprises General Trellis Coded Modulation and Cryptographic Interleaving modules.

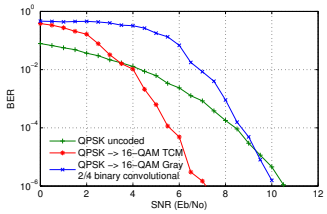


Figure 6: Performance comparison: (1) our TCM code with standard 16-QAM, and (2) best traditional binary code (from [14]) of rate 2/4 with Gray coded 16-QAM.

18dB (60 times) higher than the noise level. This implies that an adversary only needs to use a jamming power of about 60 times lower than the transmitter's power to make the communication unreliable. In contrast, a BPSK communication requires a stronger adversary to achieve the same jamming impact. Smart adversaries have been built to efficiently jam the wireless link based on the knowledge of the transmission rate (see [39] for an example of adaptive jamming in IEEE 802.11 networks). Therefore, concealing the rate information is crucial for the robustness of practical wireless systems, and is the focus of this work. In the following, we show that the rate information can be detected by various techniques ordered by their complexity.

Explicit rate information In many communication protocols, the rate information of a transmission is unprotected. For instance in IEEE 802.11 networks, the rate is explicitly specified in the PLCP Signaling Field (PSF) of the physical layer's frames. Similarly in LTE cellular systems, the transmission rate is specified in the Modulation and Coding Scheme (MCS) field within the Downlink Control Information (DCI), which is itself encoded using a publicly known fixed rate 1/3 convolutional code and QPSK modulation. An adversary can easily synchronize with the communication between two parties, analyze the data frames and extract the rate. This attack is very practical as demonstrated by [39].

Modulation guessing Even if the rate information is not explicitly provided within the packet header, the adversary can analyze the received signal in complex I/Q form. After performing the carrier synchronization, frequency and phase offset correction, the adversary can trace the received constellation pattern and determine the modulation in use. A practical rate-aware jammer can easily be built on a software-defined radio (e.g., USRP [50]) by processing the received samples of the transmitted signal, obtaining the rate, and jamming in real time [65, 39].

Code guessing Also based on constellation patterns, a more complicated method which traces the symbol sequences can determine the codes in used given that most communication standards specify a limited set of coding schemes.

Modulation and code guessing techniques fall into a category of *constellation-based guessing attacks*, which does not require the knowledge of the protocol's frame structure. In the following paragraphs, we show that without specific techniques by design, an adversary can easily identify the rate information and launch efficient attacks. Note that straightforward solutions do not work, e.g., encryption cannot be done before the channel coding, and straightforward modulation upgrade with coding compensation is not efficient.

3.2 Approach

In this section, we discuss the main ideas and mechanisms of our integrated solution that can not only hide the rate information, but also increase the robustness of the communication against interference. Our CBM scheme is depicted in Figure 5. The General Trellis Coded Modulation (GTCM) module's functionalities are two-fold. First, it makes the constellation pattern indistinguishable to the adversary, therewith countering the *modulation guessing*. Second, it boosts the system resiliency against interference. The Cryptographic Interleaving (CI) module conceals the rate information from explicit *exposing* and implicit *code guessing*.

Counter modulation guessing Our idea for hiding the modulation is to always use a *single unifying* modulation (the highest order) to transmit data in order to create the same constellation observed by the adversary. To be precise, let's consider a system that supports a set of $\mathcal{N}$ different modulations ordered by the number of bits per symbol $b_1 \leq \ldots \leq b_{\mathcal{N}}$. Assume that the transmission is carried at a bit rate $k = b_{\mathcal{K}}$ bits per symbol for some modulation $\mathcal{K}$. In order to conceal the modulation, we transmit using the highest-order modulation $\mathcal{N}$ of bit rate $n = b_{\mathcal{N}}$ as the target modulation, then

encode the data using an adequate code of rate k/n and transmit the encoded data using modulation $\mathcal{N}$. It is important to understand the implications of rate hiding. On one hand, the highest-order modulation creates redundancy by the constellation expansion. On the other hand, the constellation points' pair-wise distances are closer than in the original constellation. Without good design specifically targeting to the upgraded modulation's constellation, the system can become less resilient against interference. For example, the modulation unification technique used in [48] results in the system robustness 1-2dB less than regular rate-exposing systems. The reduced resiliency is because no coding is used in their system. However, even using good traditional binary codes cannot guarantee the robustness of the system because they maximize the Hamming distance between codewords and are not designed for coded modulation (see example in Figure 6). In our approach, since the adversary will always observe the same constellation, the GTCM module hides the actual rate from *modulation guessing* attacks. Moreover, with our coding scheme, the system's robustness can also be improved.

In the literature, finding good TCM codes is a challenging problem, for which only heuristic solutions have been studied such as the set partitioning rules established in [63]. Unfortunately, a full theoretical analysis is not yet known for good TCM code construction. In this work, we introduce a new heuristic approach for upgrading arbitrary modulations. Our heuristic solution is not based on the conventional set partitioning concept. Instead, we generate the code based on the general structure of a convolutional code, which allows us to discover better non-uniform TCM codes.

Counter code guessing To counter the *code guessing*, we harden the system using the CI module, which interleaves the modulated symbols before transmission. We emphasize that the interleaving process is performed at the baseband samples level, i.e., complex symbols produced by the GTCM module are interleaved per block of transmitted symbols. We note that straightforward encryption of data before the GTCM processing does not conceal the rate information. For example, the adversary can try to decode the data iterating over all the possible codes. During the decoding phase, the likelihood of decoding each possible sequence is recorded and evaluated. The code corresponding to the maximum likelihood will be the one used by the transmission. The attack is based on the fact that output sequences of different codes are not identically distributed in the output stream. This requires that we design an interleaving mechanism based on cryptographic functions in order to make the interleaved symbol sequence indistinguishable to the adversary. We derive a specific method to efficiently generate interleaving functions used for permuting the output symbols from the GTCM module in such a way that the transmit stream does not leak the rate information.

Our work is summarized in the following main points:

- We develop a set of new algorithms that efficiently discovers good modulation codes of general rate k/n. Such codes are not restricted to be uniform as in previous work. Such algorithms include a new technique to efficiently compute the free distance of non-uniform codes.
- We explicitly constructed 85 efficient codes of constraint length up to 10 used for any pair of modulations in {BPSK, QPSK, 8-PSK, 16-QAM, 64-QAM}. For the case of the rate $k/(k+1)$ considered by traditional TCM, we found codes that perform better than the ones introduced in [63].
- We design a generating method that can efficiently produce fast interleaving functions used for concealing the rate information.
- We evaluate the performance of each constructed code demonstrating a robustness boosting up to 8.5dB (seven times) and an improvement over related rate hiding techniques of up to 10dB (ten times).

3.3 Related work

Although specifically crafted attacks and counter-measures have been studied for packetized wireless data networks [32, 31, 65], multiple access resolution [7, 5, 4], multi-hop networks [66, 58, 31], MIMO systems [26], broadcast and control communication [27, 15, 13, 59, 29, 36, 35], cross-layer resiliency [32], spatial jamming [8], and wireless sensor networks [66, 67, 68], spread-spectrum without shared secrets [56, 24, 34], navigation information broadcast systems [49], limited work has been done on strengthening rate adaptation algorithms [42, 43, 45, 20]. An unresolved challenge remained to prevent an adversary from guessing the rate (Modulation, Coding information) during the transmission and therefore from selectively interfering with packet. More recently, Rahbari and Krunz proposed a modulation level encryption to hide the rate of communications [48]. While this scheme conceals the rate information, it does so at the cost of degrading the robustness of the communication by 1-2dB.

The idea of increasing the system's robustness in our work is related to the problem of designing good codes to increase the communication's jamming-resiliency without sacrificing the transmission rate, which requires the codes finding algorithms to take into account the system's constellation mapping. This problem was first studied by Ungerboeck [63], where the concept of set partitioning was proposed to simplify the good codes search. Despite of extensive study and extension

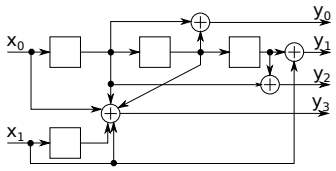


Figure 7: Our TCM code $(4,2,4)$ for QPSK $\rightarrow$ 16-QAM upgrading with coding gain 3.8dB (2.4 times).

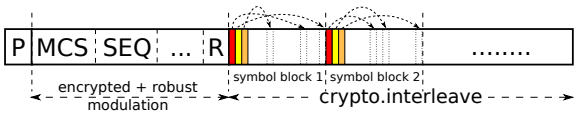


Figure 8: CBM system's frame format.

of TCM codes, our work is distinguished in that we do not rely on set partitioning concept, yet our results show that we found better codes for some cases.

Our rate concealing technique is realized by Cryptographic Interleaving mechanism, which, in our knowledge, has not yet been studied in the literature. Different from the regular encryption concept, which aims to hide the content of data sequences, our work targets to hide only the order of items in the sequences while the items' content must be left intact for the system's robustness.

3.4 General Trellis Coded Modulation Codes

In this section, we describe the searching procedure for general TCM codes of rate k/n, which are used to encode data originally modulated by a modulation $\mathcal{K}$ of order 2^k to the highest-order modulation $\mathcal{N}$ of order 2^n. The evaluation results (Section 3.6) show that there are codes such that in addition to modulation hiding, the resiliency of the system can be boosted up to 8.5dB over uncoded systems, resulting an improvement of up to 10dB compared to recent work [48].

For convenience, we give a brief overview on TCM codes. A TCM code is a convolutional code (n,k,v) of rate k/n that can be generated by finite state machine, in which k input bits are stored in a set of k shift registers whose total length is $v = \sum_{i=1}^{k} v_i$ (v is called the constraint length, v_i is the i-th shift register's length), and an input-output map produces n output bits (e.g., Figure 7). The longer the shift registers are, the more redundancy the codes can have. Thus, we classify the codes by their constraint length v. In our work, we only consider the feed-forward construction of convolutional codes, because any construction with feedback can be transformed into a feedback-free construction that produces equivalent codewords [33]. To represent a code, we use the conventional generator polynomial form $G(D) = \{g_{ij}(D), i = 0 \ldots k-1, j = 0 \ldots n-1\}$, where $g_{ij}(D) = \sum_{l=0}^{v_i} a_l D^l$ is a univariate polynomial, and the indeterminate D represents the delay of the input bit in the corresponding shift register. If $a_l = 1$, the i-th input's current value (for $l = 0$) and past values (for $l > 0$) are mod-2 added (exclusive-or) to the j-th output. For example, the convolutional code $(4,2,4)$ in Figure 7 has the generator polynomial $G = \begin{bmatrix} D+D^2 & D^3 & D+D^3 & 1+D+D^2 \\ 0 & 1 & 0 & 1+D \end{bmatrix}$. Different than binary convolutional codes whose performance depends on the Hamming distance of the binary output symbols, TCM codes' performance is determined by the free *Euclidean* distance d^{∞}, which is the minimum Euclidean distance of any two complex symbol sequences produced by the code and modulation $\mathcal{N}$. Since binary codes are not designed for coded modulation, they do not take into account the constellation mapping. The best binary code with optimized Hamming distance can have arbitrarily small Euclidean distance between transmitted complex symbols and result in low performance when combined with a specific modulation (e.g., Figure 6). Therefore, the metrics for a good TCM code is the asymptotic coding gain ratio measured by $\beta = d^{\infty}_{\mathcal{N}}/\Delta_{\mathcal{K}}$, where $\Delta_{\mathcal{K}}$ is the minimum Euclidean distance between constellation points in the original modulation $\mathcal{K}$. Good TCM codes have high β ratio.

Search algorithm for good General TCM codes We introduce a new heuristic approach for searching for good general TCM codes. The idea of the algorithm is that for a given code specification $(n,k,\{v_i\})$, the coefficients of the generator polynomials g_{ij} are randomized between values 0 and 1. Since each coefficient change corresponds to a new code construction, we check the generated code for the free Euclidean distance. The search is performed for a fixed number of trials independent of the code specification, thus it is extremely faster than a full search which evaluates all possible code constructions. Nevertheless, our randomization approach can achieve the same results as a full search. The RandomCodeSearch algorithm randomly generates T code constructions. The algorithm verifies that each generated code is *non-catastrophic*, i.e., there exist no non-zero input sequences that can produce all-zero output sequence resulting in mistaken decoding at the receiver. Moreover, each generated code is also checked for *equiprobable* property, i.e., the probability of every codeword produced by the code is all equal. The equiprobability ensures the adversary cannot distinguish the code by observing *individual* output symbols. We emphasize that equiprobability is a necessary, but not a sufficient condition for concealing the rate information, which requires the CI module.

RandomCodeSearch$(k, n, \{v_i\}, \mathcal{M}, T)$

1 $d^\infty = 0$ // free distance of current best code
2 **for** $i = 1$ **to** T
3 $C =$ generateCode$(k, n, \{v_i\})$
4 **if** valid(C) // non-catastrophic and equiprobable
5 $d =$ ComputeDistance$(C, \mathcal{M}, d^\infty)$
6 **if** $d > d^\infty$
7 $d^\infty = d$ // update free distance
8 $C^* = C$ // store new best code
9 **return** (C^*, d^∞)

ComputeDistance$(C, \mathcal{M}, d^\infty_{best})$

1 $D[S, \tilde{S}] = \infty$ for all $(S, \tilde{S}) \in V^2$ // state-distances
2 $d^\infty = \infty$ // free distance
3 **for each** $S \in \Lambda$, $(x, \tilde{x}) \in I^2$, $x \neq \tilde{x}$
4 UpdateDistance$(S, x, S, \tilde{x})$
5 **repeat**
6 **for each** $(S, \tilde{S}) \in \Lambda^2, S \neq \tilde{S}, D[S, \tilde{S}] < d^\infty$
7 **for each** $(x, \tilde{x}) \in I^2$
8 UpdateDistance$(S, x, \tilde{S}, \tilde{x})$
9 **if** $d^\infty \leq d^\infty_{best}$
10 **return** d^∞
11 **until** $(S, \tilde{S})$ not found in line 6
12 **return** d^∞

Free distance computing algorithm The computational bottlneck of the code search is computing the Euclidean free distance, since it is performed for every generated code. We devise an efficient algorithm – ComputeDistance – whose running time is on average less than 2ms on a 3GHz CPU computer for the modulations and depths we consider. The main idea of ComputeDistance is based on traversing the trellis of the code and appropriately updating the *state-distances*, which we define shortly below.

First, we introduce some convenient notations. Let $I = \{0, \ldots, 2^{C.k} - 1\}$ be the set of inputs, $O = \{0, \ldots, 2^{C.n} - 1\}$ the set of output symbols, and $\Lambda = \{0, \ldots, 2^{C.v} - 1\}$ the set of possible states corresponding to a code C. A path P of length L is defined as a sequence of 3-tuples $P = \{(S_i, x_i, y_i), i = 0 \ldots L-1\}$, where $S_i \in \Lambda, x_i \in I$ are respectively the state and input of the code at time i, and $y_i \in O$ is the output symbol due to S_i and x_i. The distance between two paths P and $\tilde{P}$ of length L is computed by $\text{dist}(P, \tilde{P}) = \sum_{i=0}^{L-1} \mathcal{M}.ed(P.y, \tilde{P}.y)$, where $\mathcal{M}.ed(a, b)$ gives the Euclidean distance between two points a and b on the target coded modulation $\mathcal{M}$'s constellation. Now we define the state-distance $D[S, \tilde{S}] \triangleq \min\{\text{dist}(P, \tilde{P})\}$ of two states S and $\tilde{S}$ as the minimum Euclidean distance between all possible paths of the same length that end at state S and $\tilde{S}$, respectively.

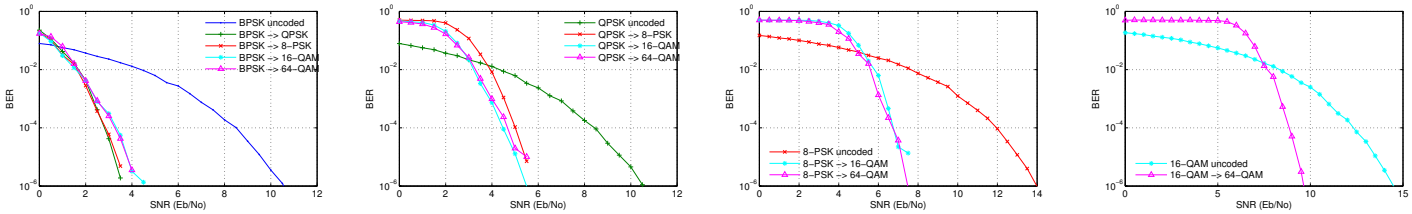
The algorithm ComputeDistance starts by initializing the state-distances to the distance between any path P and $\tilde{P}$ starting from any *same* state S (line 1–4). We make the paths diverge from the same state (line 3), then compute the distance between them (line 4). In the main loop (line 5–11), the state-distances are repeatedly updated for each new segment added (line 7) to the paths until there exist no more state pairs $(S, \tilde{S})$ whose state-distance $D[S, \tilde{S}]$ is less than d^∞ (line 11). The maintenance and update of state-distances in both the initialization and the main loop are performed by UpdateDistance, which keeps records of $D[S, \tilde{S}]$ for all $S, \tilde{S}$. Whenever two paths P and $\tilde{P}$ merge at a state S, i.e., $P.S_{L-1} = S = \tilde{S} = \tilde{P}.S_{L-1}$, the corresponding state-distance $D[S, S]$ is checked to update d^∞ with $D[S, \tilde{S}]$. Recall the random search procedure discussed previously where each generated code is computed for the free distance, we speed up the search by storing the best free distance d^∞_{best} associated to the best code C^* discovered so far in order to quickly eliminate the code of free distance shorter than d^∞_{best} (line 9 in ComputeDistance).

The time complexity of ComputeDistance is $O(2^{2(v+k)}L)$, where L depends on the code specification $(n, k, \{v_i\})$. In our experimental search results, we observe that the value of L can be bounded by $L \leq 3v$ for any code. The running time of the algorithm on our 3GHz CPU computer is less than 2ms.

3.5 Cryptographic Interleaving

Although good TCM codes can improve the system robustness and hide the modulation, an adversary capable of tracing symbol sequences (not just observing individual symbols) can still discover the rate information, because the uniqueness of every code relies on not only the codewords, but also transitions between them. In this section, we propose "Cryptographic Interleaving" as a solution for the code concealing problem. Different from conventional data encryption, cryptographic operations are performed on the baseband symbols (otherwise it is vulnerable to constellation-based modulation guessing attacks). We devise an efficient method for generating fast cryptographic interleaving functions.

Interleaving process The interleaving process is performed on coded symbols produced by the GTCM module before radio transmission. The interleaved symbols must be indistinguishable to the adversary. Specifically, the following requirements should be met: (1) interleaved symbols look like a sequence produced by a random code, (2) symbols belonging to different packets are differently permuted, and (3) the user identity is not revealed. For compactness, we assume the



(a) Concealing BPSK. **(b)** Concealing QPSK. **(c)** Concealing 8-PSK. **(d)** Concealing 16-QAM.

Figure 9: Rate exposing (uncoded) vs. Concealed and Boosted Higher-order Modulation.

existence of a shared secret key associated to the undergoing communication session between the transmitter and receiver. The symbol interleaving map is randomly selected based on the session's secret key and the transmitted packet number.

For convenience, we assume that the coded symbols produced by the GTCM module are divided into multiple blocks, each has m symbols, and a fixed number of blocks are packed into a transmitted frame. To randomly interleave the symbols, the basic idea is to pre-build a set of interleaving tables and select one to use based on the tuple information (user key K, packet number s, block i). The mapping from the tuple (K, s, i) to the interleaving table index can be created by a hash function (e.g., SHA2). For example, let $\{I_0, \ldots, I_{N-1}\}$ be the set of N predefined interleaving tables, and h denote the hash function. The interleaving table I_j is selected by $j = h(|K|s|i|) \bmod N$ and used to interleave the block i of packet s. As a result, the block i's coded symbols $y_0, \ldots, y_{m-1}$ are permuted into $y_{I_j(0)}, \ldots, y_{I_j(m-1)}$ for transmission.

Although the precomputed tables approach is conceptually simple, it is hard to implement in practice as one needs to precompute a large number of interleaving functions so that the adversary cannot guess. This, however, requires significant computation and storage resources. In the following, we propose a practical and efficient solution based on a cryptographic linear construction of permutation/interleaving functions.

Cryptographic linear interleaving To eliminate the cost of precomputing interleaving tables, we assume the number of symbols per block, m, is a prime, and define the interleaving functions as linear functions: $I_{A,B}(x) = Ax + B \bmod m$, where $A \in \{1..m-1\}, B \in \{0..m-1\}$. It is clear from the construction above that any pair (A, B) will produce a bijective function $I_{A,B}(x)$ with respect to x, i.e., $I_{A,B}(x)$ is an interleaving function. To randomly generate A, B such that the requirements for indistinguishability are met, we apply a hash function h on the tuple information (K, s, i) and compute

$$A = (h(|K|s|i|0) \bmod (m-1)) + 1, \quad B = h(|K|s|i|1) \bmod m.$$

The coded symbols $y_0, \ldots, y_{m-1}$ of block i are now permuted into $y_{I_{A,B}(0)}, \ldots, y_{I_{A,B}(m-1)}$ for transmission.

Frame format Since the interleaving processing on the coded symbols of the user data involves using not only the secret key K, but also the packet number s and block index i, the transmitter needs to embed those information along with the rate information into the transmitted frame. In the following, we describe the structure of the physical layer's frame and also discuss the encoding procedure for the frame header.

In the transmitted frame, the preamble P is a publicly known bit sequence (typically 64 bits) used for frame synchronization at the receiver. The MCS (modulation and coding scheme) field stores the TCM code's identifier used to encode the data. The SEQ field specifies the packet number required for the interleaving process. The R field stores a random number generated per packet by the transmitter. The frame header is encrypted by $E_K(MCS|SEQ|\ldots|R)$ using AES encryption E with the shared secret key K. The header is encoded by a public robust coding scheme and along with the preamble is modulated by a public robust modulation. Note that since header and preamble are short, TCM codes are not beneficial as Viterbi decoder is only applied for long sequences.

Security and robustness Since the interleaving functions are generated based on the cryptographic hash function with a secret key K applied on varying packet number s and block i, the coefficients A and B are indistinguishable under chosen plaintext attacks (semantically secure), thus the interleaved symbol sequences are also indistinguishable. As the hash function is lightweight, the computation of $I_{A,B}$ is extremely fast. The header is also semantically secure due to the use of random R with AES encryption. It is also robust as lost synchronization does not propagate to next frames.

3.6 Evaluation results

In this section, we report on the evaluation of the codes found in Section 3.4, in comparison with their corresponding uncoded modulations. The evaluation is performed through simulations in MatLab. For each pair of the original uncoded modulation $\mathcal{K}$ and the target coded modulation $\mathcal{N}$, a transmission of 1Gbits is carried in an additive white Gaussian noise channel. We start the simulation at the normalized signal-to-noise ratio $E_b/N_0 = 0$ and increase it by 0.5dB after every run. The bit error rates corresponding to each SNR level are recorded. The simulation stops when all data is done transmitted or 1000 bit errors are reached.

Performances of codes of constraint length $v = 10$ are shown in Figures 9a to 9d. At BER $= 10^{-6}$, in addition to hiding the rate, the coding gain (boosting) provided by the coded modulations ranges from about 5dB to more than 6.5dB when 64-QAM modulation is used for rate concealing. Compared to the modulation unification technique proposed in recent related work [48] whose performance degrades by about 1.2dB for hiding BPSK modulation in 64-QAM modulation, we gain up to 8dB. If the system only supports QPSK as the highest-order modulation, an upgrading BPSK $\rightarrow$ QPSK can give an advantage of 7.5dB over uncoded BPSK, while the modulation unification loses about 2dB, resulting in our improvement of up to 9.5dB. In scenarios where the adversary is weak (i.e., high SNR), the coding gain is close to the asymptotic gain about 8.5dB presented in Section 3.4, resulting in an improvement of up to 10dB.

The evaluation results also show that the performance boost is similar across different target modulations. For example in Figure 9b, using 8-PSK as the target modulation is within 1dB of using target modulation 16-QAM or 64-QAM. This leads to a key lesson that the rate concealing technique based on coded modulations can be flexibly used in various systems, where different modulations are supported. One can imagine that in future wireless communication systems always use the highest modulation possible for the RF Front End ADC and AGC, and adapt to the channel conditions only by changing the code.

4 Enhancing Multicarrier Multiantenna Systems

Advances in digital signal processing techniques such as efficient implementation of Fast Fourier Transform (FFT) have popularized Orthogonal Frequency Division Multiplexing (OFDM) in recent wireless systems. The power of OFDM is its ability to combat dynamic variations in the wireless medium without the need of complicated signal processing methods in comparison with wide-band single-carrier systems. The robustness of OFDM, however, significantly relies on the orthogonality of carriers, which can be distorted by frequency offset between communication nodes. In this section, we give a brief overview of OFDM technique and study vulnerabilities in IEEE 802.11 OFDM systems.

4.1 OFDM system

The principle of OFDM is to split the wide-band channel into multiple *orthogonal* narrowband carriers[2] and use them for transmissions. Two main advantages of OFDM are bandwidth efficiency and robustness in dynamic environments.

- *Bandwidth efficiency:* By orthogonality, carriers in OFDM can overlap, resulting in efficient frequency reuse (Figure 10), while in non-orthogonal FDM, carriers are separated with significantly large gaps to avoid ICI (Inter-Carrier Interference) issue, leading to bandwidth-inefficiency.
- *Robustness:* As carriers in OFDM are narrowbands, they are relatively flat (frequency-nonselective), allowing a simpler implementation of the receiver in comparison with single-carrier systems, where frequency-selective channel requires complex equalization techniques to deal with ISI (Inter-Symbol Interference) issue.

The advantages of OFDM result from the carriers' orthogonality, which, however, makes OFDM more sensitive to frequency offset issue than single-carrier systems. Therefore, pilot signals and cyclic prefix are usually employed to harden OFDM systems, which are described in the following.

Design and operation Design of a simple OFDM system is shown in Figure 11. The transmit and receive chains in OFDM operate on groups of N data symbols $(S_1, \ldots, S_N)$.

Transmit chain: The data symbols are first split into N parallel streams, each corresponds to one carrier. Before transmission, a number of P additional pilot carriers are added, where each pilot signal carries a predefined fixed sequence known by both transmitter and receiver. The pilot carriers help the receiver estimate frequency offset on each data carrier. More pilots improve the estimation accuracy, but reduce the bandwidth efficiency. The resulted set of $(N + P)$ carriers is transformed by the Inverse FFT block into a discrete time signal consisted of complex numbers $(s_1, \ldots, s_{N+P})$, which

[2] In the literature, the terms *carrier*, *subcarrier*, and *sub-channel* are equivalent and used interchangeably.

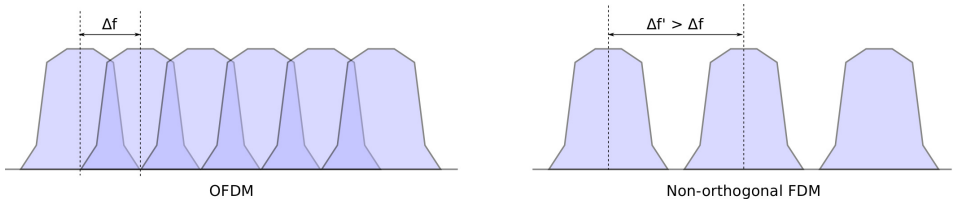


Figure 10: OFDM and non-orthogonal FDM signals in frequency domain.

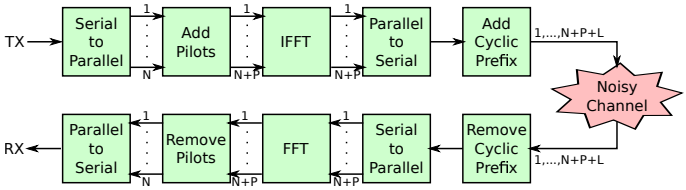


Figure 11: General design of an OFDM system.

is then prepended by a cyclic prefix (CP) of length L, which is set to be identical to the last portion of the signal, i.e., $\text{CP} = (s_{N+P-L+1}, \ldots, s_{N+P})$. The embedding of CP in transmitted signal creates a guard interval (GI), by which the ISI can be eliminated assumed that the length of channel impulse response vector is shorter than the CP length.

Receive chain: The received time-domain signal is processed on group of $(N + P + L)$ complex numbers. First, since the cyclic prefix is a repetition of the last portion of the transmitted signal, the ISI and multipaths issues are automatically eliminated during the signal propagation. Thus, at the receiver, the cyclic prefix is just simply removed. The remaining $(N + P)$ complex numbers are transformed by the FFT block to obtain $(N + P)$ carriers containing both pilot and data signals. Using information in pilot carriers, frequency offset and phase noise in data carriers are estimated to recover their orthogonality, allowing the decoding of original data.

4.2 OFDM in IEEE 802.11

In this section, we give a brief overview of IEEE 802.11's OFDM system. The standard specifies that IEEE 802.11's OFDM system has 64 carriers consisted of $N = 48$ data carriers, $P = 4$ pilot carriers, and the remaining 12 carriers nulled out for interference mitigation between WiFi channels. The cyclic prefix length of $L = 16$ is used, resulting in duration of an OFDM symbol equal to $4\mu s$ for 20MHz channel (312.5kHz per carrier). Along with these basic OFDM mechanisms, a preamble is added for frame detection and synchronization purpose. Figure 12 depicts the transmission of MAC layer's packet (MPDU), which can be separated into two stages: Packet encoding and OFDM modulation.

Packet encoding On request for transmission of a MPDU, the PHY layer prepares a PLCP packet consisted of header and payload. Since OFDM modulation process operates on groups of $N = 48$ symbols, both header and payload are encoded such that their length is a multiple of 48 symbols. The header and payload construction are slightly different as described in the following. The header is created by embedding the requested transmission rate (RATE field) and MPDU's length (LENGTH field) along with a parity bit for error checking and some tail bits set to 0. The resulted 24-bit header is encoded with a convolutional code of rate $1/2$ to make a 48-bit encoded header, which is then interleaved by an interleaver of size 48 and finally mapped to BPSK constellation to obtain a chunk of 48 symbols.

The payload is prepared according to the transmission rate requested by the MAC layer. Specifically, the RATE field determines a Modulation and Coding Scheme (MCS) consisted of the coding rate r and bits-per-symbol b of the constellation

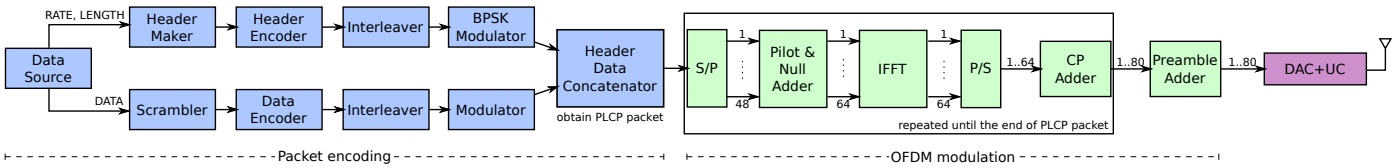


Figure 12: WiFi-OFDM transmitter block diagram.

mapping. Prior to encoding the payload, the MPDU is appropriately prepended and appended with padding bits to obtain its length as a multiple of $48br$ bits. The payload is constructed by first scrambling[3] the padded MPDU, then it is encoded by a convolutional code of rate r. The encoded payload is divided into groups of $48b$ bits, each of which is permuted by the interleaver of size $48b$. Finally, groups of interleaved bits are accordingly mapped to constellation complex points specified by RATE field to obtain groups of 48 symbols. Header and payload's symbols are concatenated and transmitted by the OFDM modulation process.

OFDM modulation OFDM modulation process in IEEE 802.11 is similar to a general OFDM system, except that:

- Pilot carriers are located with equal spacing at carrier indices $(-21, -7, 7, 21)$. In addition to pilots, null carriers are also added to the side and DC carriers in order to avoid interference for adjacent WiFi channels.
- PLCP packet is prepended with a preamble (discussed below) for synchronization and channel estimation purposes.

Preamble Preamble in IEEE 802.11 OFDM systems is a predefined fixed sequence of short symbols and long symbols, which corresponds to a total duration of $16\mu s$. The first half ($8\mu s$) of preamble contains 10 repeated short symbols, and the second half ($8\mu s$) contains 2 repeated long symbols. Besides its main use for frame detection, the preamble can also be used for frequency offset estimation in slow-fading channels (channel is constant in an OFDM symbol duration). However, in practice, where environments are usually dynamic, pilots are used for accurate channel estimation.

4.3 Vulnerabilities in IEEE 802.11 OFDM

The performance of IEEE 802.11 OFDM systems depends on the capability of mitigating ICI and ISI issues, which are treated by the use of preamble, pilots, and cyclic prefix. However, a concrete implementation for synchronization and channel estimation is not specified in IEEE 802.11 standard, thus the robustness of the system depends on its implementation. In this section, we briefly discuss the effectiveness of those mechanisms and possibilities to break the system in the viewpoint of a malicious jammer.

Preamble: Jamming PLCP preamble may appear to be inefficient, because both short and long symbol sequences specified by the standard have good correlation property, resulting in a high jamming-resilient time synchronization mechanism. However, the specific implementation method for time synchronization (e.g., cross-correlation, auto-correlation) can have impact on the synchronization quality [18]. Moreover, as the IEEE 802.11 standard also suggests frequency offset estimation based on preamble, a smart jammer can exploit this to falsify the channel estimation process.

Pilot carriers: In pilot-assisted systems such as IEEE 802.11 OFDM, interference in pilot carriers significantly affects the system's robustness [18, 41]. On the other hand, locations of pilot carriers are known and fixed, which implies that an efficient jamming technique targeted to pilot carriers can potentially degrade the network.

Cyclic prefix: Since the cyclic prefix is just simply removed at the receiver, jamming the cyclic prefix apparently has no impact on the received signal. Moreover, the cyclic prefix is periodically added for each OFDM symbol, a jammer must be able to quickly synchronize with the transmission in order to target to the cyclic prefix part. It is followed that jamming cyclic prefix appears inefficient to the adversary.

4.4 Challenges

Based on the above discussion of vulnerabilities, challenges are present for both jamming and anti-jamming sides. In this work, we are interested in designing an efficient jammer and practical anti-jamming methods for currently deployed WiFi networks.

- **Jamming challenges:** The most difficulty in building an efficient jammer is the responsiveness of the jammer. For example, a WiFi OFDM frame duration of $4\mu s$ for 20MHz channels requires the jammer to act within the order of microseconds. Very recently, authors in [38] were able to build an efficient jammer of response time $80ns$. However, since the jammer was implemented on FPGA, designing more sophisticated jamming techniques is still challenging given the limitations of storage and processing capabilities of FPGA. The second challenge of building jammers is energy efficiency. As discussed above, jamming pilot carriers and preamble appears to be more efficient in terms of energy consumption.
- **Anti-jamming challenges:** The weakness of most communication standards such as IEEE 802.11 is that malicious interference is not taken into account when the protocol is designed. This leads to the ease of developing efficient attacks. For example, since equal spacing of pilot carriers often yields good performance in typical environments

[3]Scrambling creates randomness in transmitted symbols, which assists synchronization process at the receiver.

with unintended noise and interference [41], IEEE 802.11 specifies concrete locations $(-21, -7, 7, 21)$ for pilot carriers. However, this allows an efficient jammer to be constructed which simply targets to the specified pilot carriers' frequencies for jamming. Countering this jamming technique is not straightforward as a solution has to take into account the adaptivity to environments, scalability, and deployability in practice.

5 Future work and research plan

For the completion of this research work, I plan to continue my study on the following specific problems:

1. **SAIM:** Quantification of SAIM's resiliency against multiple jammers.
2. **CBM:** Implementation and experimental evaluation of Conceal and Boost Modulation on real testbed.
3. **Enhancing Multicarrier Systems:**
   - Implement a jammer on USRP/GNURadio platform.
   - Study jamming impacts and countering solutions in WiFi OFDM systems.
   - Extend investigation to LTE systems.
   - Study weaknesses of MIMO techniques.

The following table is the proposed timeline to complete the research:

To-do tasks	Completion Date
Quantification of SAIM's resiliency against multiple jammers scenarios	October 2014
Implementation and experimental evaluation of CBM	November 2014
Investigation of jamming and anti-jamming mechanisms in WiFi and LTE sysems	February 2015
Ph.D. Dissertation Defense	April 2015

References

[1] Naveed Ahmed, Christina Pöpper, and Srdjan Capkun. Enabling short fragments for uncoordinated spread spectrum communication. In Mirosław Kutyłowski and Jaideep Vaidya, editors, *Computer Security - ESORICS 2014*, volume 8712 of *Lecture Notes in Computer Science*, pages 488–507. Springer International Publishing, 2014.

[2] John S. Atkinson, O. Adetoye, Miguel Rio, John E. Mitchell, and George Matich. Your WiFi is leaking: Inferring user behaviour, encryption irrelevant. In *WCNC*, 2013.

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

[4] Baruch Awerbuch, Andréa W. Richa, and Christian Scheideler. A jamming-resistant MAC protocol for single-hop wireless networks. PODC'08, pages 45–54, 2008.

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

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

[7] Michael A. Bender, Martin Farach-Colton, Simai He, Bradley C. Kuszmaul, and Charles E. Leiserson. Adversarial contention resolution for simple channels. In *SPAA*, 2005.

[8] S. Bhattacharya and T. Basar. *Advances in Dynamic Game Theory and Applications*, volume 12 of *Annals of Dynamic Games*, chapter Differential game-theoretic approach to a spatial jamming problem, pages 245–268. Birkhauser, 2012.

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

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

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

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

[13] Agnes Chan, Xin Liu, Guevara Noubir, and Bishal Thapa. Control channel jamming: Resilience and identification of traitors. In *proceedings of the IEEE International Symposium on Information Theory*, 2007.

[14] Jinn-Ja Chang, Der-June Hwang, and Mao-Chao Lin. Some extended results on the search for good convolutional codes. *Information Theory, IEEE Transactions on*, 43(5):1682–1697, Sep 1997.

[15] J.T. Chiang and Y.-C. Hu. Cross-layer jamming detection and mitigation in wireless broadcast networks. In *MobiCom*, 2007.

[16] J.T. Chiang and Yin-Chun Hu. Dynamic jamming mitigation for wireless broadcast networks. In *INFOCOM*, pages 1211–1219, 2008.

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

[18] AJ. Coulson. Narrowband interference in pilot symbol assisted ofdm systems. *Wireless Communications, IEEE Transactions on*, 3(6):2277–2287, Nov 2004.

[19] 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.

[20] Koorosh Firouzbakht, Guevara Noubir, and Masoud Salehi. On the capacity of rate-adaptive packetized wireless communication links under jamming. WISEC '12. ACM, 2012.

[21] 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.

[22] 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.

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

[24] 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.

[25] Jaber Kakar, Kevin McDermott, Vidur Garg, Marc Lichtman, Vuk Marojevic, and Jeffrey Reed. Analysis and Mitigation of Interference to the LTE Physical Control Format Indicator Channel. 2014.

[26] A. Kashyap, T. Basar, and R. Srikant. Correlated jamming on mimo gaussian fading channels. *Information Theory, IEEE Transactions on*, 50(9), 2004.

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

[28] Jean-Daniel Kraus. *Antennas*. Mcgraw Hill Higher Education; 3rd edition, 2001.

[29] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In *In Proceedings of ACM WiSec*, pages 169–180, 2009.

[30] Barry Levine. Who is putting up 'interceptor' cell towers? The mystery deepens. *Venturebeat*, September 2014. `http://venturebeat.com/2014/09/02/who-is-putting-up-interceptor-cell-towers-the-mystery-deepens/`.

[31] Mingyan Li, I. Koutsopoulos, and R. Poovendran. Optimal jamming attacks and network defense policies in wireless sensor networks. In *INFOCOM*, 2007.

[32] Guolong Lin and Guevara Noubir. On link layer denial of service in data wireless lans. *Wiley Journal on Wireless Communications and Mobile Computing*, August 2005.

[33] Shu Lin and Daniel J. Costello. *Error Control Coding, Second Edition*. Prentice-Hall, Inc., 2004.

[34] An Liu, Peng Ning, Huaiyu Dai, Yao Liu, and Cliff Wang. Defending dsss-based broadcast communication against insider jammers via delayed seed-disclosure. In *Proceedings of ACSAC'2010*, 2010.

[35] 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.

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

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

[38] Danh Nguyen, Cem Sahin, Boris Shishkin, Nagarajan Kandasamy, and Kapil R. Dandekar. A real-time and protocol-aware reactive jamming framework built on software-defined radios. In *Proceedings of the 2014 ACM Workshop on Software Radio Implementation Forum*, SRIF '14, pages 15–22, New York, NY, USA, 2014. ACM.

[39] Guevara Noubir, Rajmohan Rajaraman, Bo Sheng, and Bishal Thapa. On the robustness of IEEE 802.11 rate adaptation algorithms against smart jamming. WiSec '11, 2011.

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

[41] Shuichi Ohno, Emmanuel Manasseh, and Masayoshi Nakamoto. Preamble and pilot symbol design for channel estimation in OFDM systems with null subcarriers. *EURASIP Journal on Wireless Communications and Networking*, 2011(1), 2011.

[42] C. Orakcal and D. Starobinski. Jamming-resistant rate control in Wi-Fi networks. In *IEEE GLOBECOM*, 2012.

[43] Cankut Orakcal and David Starobinski. Jamming-resistant rate adaptation in wi-fi networks. *Performance Evaluation*, 75–76(0):50 – 68, 2014.

[44] David Pacholok. ATV Transmitter from a Microwave Oven! Low-cost high-power microwave operation has arrived. *Amateur Radio*, Jul 1989.

[45] 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.

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

[47] John G. Proakis and Masoud Salehi. *Digital Communications*. McGraw-Hill, 5 edition, 2007.

[48] Hanif Rahbari and Marwan Krunz. Friendly CryptoJam: A Mechanism for Securing Physical-layer Attributes. WiSec '14, 2014.

[49] Kasper Bonne Rasmussen, Srdjan Capkun, and Mario Cagalj. Secnav: secure broadcast localization and time synchronization in wireless networks. In *MobiCom*, 2007.

[50] Ettus Research. Universal software radio peripheral. `http://www.ettus.com/`.

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

[52] Daniel P. Shepard, Todd E. Humphreys, and Aaron A. Fansler. Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks. *International Journal of Critical Infrastructure Protection*, 5(3-4):146–153, 2012.

[53] Marvin K. Simon, Jim K. Omura, Robert A. Scholtz, and Barry K. Levitt. *Spread Spectrum Communications Handbook*. McGraw-Hill, 2001.

[54] David Slater, Patrick Tague, Radha Poovendran, and Brian J. Matt. A coding-theoretic approach for efficient message verification over insecure channels. In *Proceeding of ACM WiSec*, 2009.

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

[56] 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.

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

[58] P. Tague, D. Slater, G. Noubir, and R. Poovendran. Linear programming models for jamming attacks on network traffic flows. In *WiOpt*, 2008.

[59] Patrick Tague, Mingyan Li, and Radha Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In *Proceedings of International Symposium on Personal, Indoor and Mobile Radio Communications*, 2007.

[60] N.O. Tippenhauer, L. Malisa, A Ranganathan, and S. Capkun. On limitations of friendly jamming for confidentiality. In *Security and Privacy (SP), 2013 IEEE Symposium on*, pages 160–173, May 2013.

[61] H.L. Van Trees. *Detection, Estimation, and Modulation Theory, Part I*. Wiley & Sons, 2001.

[62] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge University Press, New York, NY, USA, 2005.

[63] G. Ungerboeck. Channel coding with multilevel/phase signals. *Information Theory, IEEE Transactions on*, 28(1):55–67, Jan 1982.

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

[65] 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.

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

[67] Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Channel surfing: defending wireless sensor networks from interference. In *Proceedings of IPSN*, 2007.

[68] Wenyuan Xu, Wade Trappe, and Yanyong Zhang. Defending wireless sensor networks from radio interference through channel adaptation. *ACM Transactions on Sensor Networks*, 4, 2008.

[69] Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher, Srdjan Capkun, and David Basin. Short Paper: Detection of GPS Spoofing Attacks in Power Grids. In *Proceedings of the 2014 ACM Conference on Security and Privacy in Wireless & Mobile Networks*, WiSec '14, pages 99–104, New York, NY, USA, 2014. ACM.

[70] 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.

[71] Zhenghao Zhang, Shuping Gong, AD. Dimitrovski, and Husheng Li. Time Synchronization Attack in Smart Grid: Impact and Analysis. *Smart Grid, IEEE Transactions on*, 4(1):87–98, March 2013.