Redundancy Offset Narrow Spectrum: Countermeasure for Signal-Cancellation Based Jamming

Sang-Yoon Chang[†*] Yih-Chun Hu[†] Jerry T. Chiang[*] Soo-Young Chang[+]
[†]University of Illinois at Urbana-Champaign, Urbana, IL, USA
[*]Advanced Digital Sciences Center, Singapore
[+]S Y Chang & Associates, Davis, CA, USA

ABSTRACT

Correlated jamming, introduced in the 1980's as the optimal interference signal in information theory, aims to cancel the target victim signal in contrast to the more traditional jamming approach of adding noise-like interference. The recent surge of antenna-cancellation based technology with benign intention (including full duplex radio technology and friendly jamming for confidentiality) has reignited interest in correlated jamming attack in wireless security.

Randomization is an effective technique for availability against such attacks; for instance, spread spectrum technology randomizes the channel access to counter jamming. However, spread spectrum technology assumes dividing the medium into multiple orthogonal channels, only one of which is accessed per time, and thus has an inherent spreading cost. Redundancy Offset Narrow Spectrum (RONS) offers a *narrow spectrum* technology that bypasses the spreading cost and effectively counters correlated jamming and further helps ensuring confidentiality.

Categories and Subject Descriptors

C.2.0 [**Computer-Communication Networks**]: General—*Security and protection (e.g., firewalls), Data communications*

Keywords

Wireless; Jamming; Signal cancellation; Physical layer; Redundancy

1. INTRODUCTION

Due to the inherent nature of sharing the medium, wireless communication is vulnerable to signal injection. Correlated jamming is a strong attack against wireless availability that aims to cancel the source transmitter signal at the victim receiver. Successful attack of complete cancellation yields zero information about the source transmission signal to the victim receiver and the optimal receiver strategy of recovering bits reduces into random coin toss with equal weight. The information about the victim transmission that makes correlated jamming possible also yields easy access to the messages that has been relayed from above the physical layer and enables the attacker to compromise the message integrity.

Correlated jamming utilizes antenna-based signal cancellation. In a non-security framework, the field of full duplex with multiple antennas uses such signal cancellation technique; they cancel the signal being transmitted at the receiver location, so that it does not interfere with the receiver reception [1]. In wireless security, others have used the technique in a white-hat approach where *friendly jamming* is used as a defense mechanism for confidentiality against eavesdroppers [2]; correlated jamming, on the other hand, assumes a malicious adversary who injects wireless interference to disrupt communication. As has been demonstrated in the above studies, one of the key challenges for signal cancellation is synchronization between the jammer and the target transmitter. Thus, we study the impact of synchronization offsets and compare correlated jamming, *coded jamming* (that does not need to follow the target transmission at real-time), and Gaussian jamming. However, to devise a secure countermeasure against wireless interference, we assume the Dolev-Yao threat model [3] and consider the strongest threat of correlated jamming (assuming a weaker threat model and underestimating the attacker capability, despite the ongoing incorporation of signal-cancellation techniques in the state-of-the-art wireless schemes, will leave security holes in the countermeasure scheme); Section 4 and Section 5 discusses about the threat.

Typical spread spectrum solutions against jamming assumes dividing the medium into multiple orthogonal channels and involves channel access randomization [4,5], so that the choice of accessed channel (among many channel options) is random against attackers; a reactive attacker that observes the victim's channel access and adjust its strategy accordingly can be thwarted by switching channels and having the access duration on a channel be smaller than the attacker's reaction time. Spread spectrum technology assumes channelization that provides orthogonal channel access by interleaving the channel use either by time, frequency, or code (processing) and can be effective in ensuring both confidentiality and availability by having the random spreading code/key (from which the channel access information is derived) known only between the source-destination pair involved in the communication. However, spread spectrum bears a *spreading cost*. In other words, the wireless users consume more resource than no spreading by a factor that

MobiWac'13, November 3–8, 2013, Barcelona, Spain.

is proportional to the number of channel options that the users have for channel access, because the process of spreading symbols entitles either transmitting redundant information (in case of code-based spreading) or reserving more resource than the user uses at a time (in cases of frequency or time-based spreading), and thus has a negative impact on the throughput rate performance.

We introduce a novel physical-layer technology, Redundancy Offset Narrow Spectrum (RONS), that effectively counters both passive and active wireless attacks. RONS is *narrowband spectrum* since it does not require the spreading cost of consuming wireless resource proportionally to spreading gain; it uses the built-in physical-layer blocks of the communication chain but only adds phase offsets or cyclic delays (which values are only known among the legitimate key holders). Fully implemented at the physical layer, RONS also does not rely on randomization of the physical channel access. In other words, RONS counters threats even when the attacker knows the victim transmission's physical channel location in time and frequency; in fact, we assume that the attacker does not waste its power accessing other channel to model the worst-case impact.

The rest of the paper is organized as following. Section 2 provides physical layer background and the framework that we use throughout the paper, and Section 3 further details our system setup. We discuss the threat model and study the transmission-customized jamming strategies (correlated jamming and coded jamming) and compare them with the more common white Gaussian jamming in Section 4; we study the performances of the three distinct jamming strategies in simulation in Section 5. Afterward, Section 6 introduces RONS (including the motivation and the related schemes), and Section 7 evaluates the scheme in simulations. Lastly, we conclude the paper in Section 8.

2. PHYSICAL LAYER PRIMER

This section provides a primer for wireless communication with focus on the physical layer, where logical data (typically bits in computer applications) get converted into physical signal that is suitable for propagation on the communication medium. It also presents the physical-layer framework and defines the terms that we use throughout the paper.

2.1 Adding Redundancy (in Information-Theoretical Sense)

In coding, communication systems *add redundancy* by generating multiple bits that contain duplicate messages to mitigate the impact of failed delivery on communication reliability. After coding, at the physical layer (where discrete-time communication systems are limited in sampling rate), even though the information theoretically optimal strategy is to have all samples carry discrete, non-overlapping information content[1], system designers further *add redundancy* in real-life communication practice by having redundant samples that carry overlapping information content as opposed to having all samples contain distinct information content.

[1]In a high SINR-regime (where SINR is the signal-to-interference-and-noise ratio), the capacity grows linearly with the transmission rate but grows logarithmically with SINR, and the maximum benefit of adding redundant symbols increases the SINR linearly by the number of samples that the information content spreads across, example of which technique is discussed in Section 6.1.

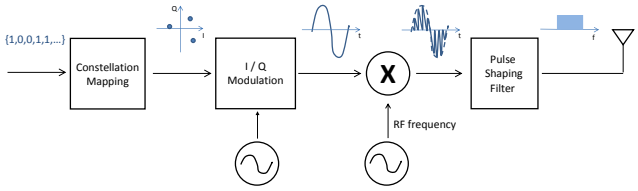


Figure 1: Typical transmitter processing chain at the physical layer

Transmitters add redundancy by spreading symbols over multiple samples via one-to-many mapping; that is, an input symbol entering the physical layer becomes mapped into multiple samples (and eventually to analog continuous signal) when leaving the transmitter chain. Although adding redundancy increases the processing load, it is commonly used to effectively deal with the real-life physical characteristics of the channel medium; specifically, adding redundancy is useful *a*) for combating noise and incorporating error control, *b*) for nullifying the effects of channel fading and synchronization imprecision/error, and *c*) for fitting the transmissions to the channel constraints, e.g., frequency bandwidth. The channel constraints also come from sharing the medium with other communication users and can either be decided at the application layer by legislative enforcement or at the link layer from a medium access control (MAC) protocol. Thus, we extend the notion of *redundancy* beyond coding (with its typical error control and reliability purpose) and use the term in the information-theoretical sense; the extra samples that carry overlapping or duplicate information content are redundant in information theory but may be *necessary* to meet the real-life constraints.

We call the physical-layer processing blocks that perform one-to-many mapping, and thus dilute the amount of information content per sample, *redundancy blocks* and the number of outputs of the redundancy block per input *redundancy rate*. Redundancy blocks perform two operations: oversampling and profile modulation. *Oversampling* maps an input into multiple outputs by repetition, and the block then modulates the signal with a *redundancy profile*, which defines the redundancy block mapping (for example, a heterodyning upconverter block is characterized by the element-by-element multiplication with a sinusoidal profile with the local oscillator frequency). In Section 2.2, we present a typical radio chain design and present examples of redundancy blocks.

2.2 Basic Transmitter Design

Figure 1 shows a typical standard block design[2] of a radio chain that uses phase modulation (PM) and/or amplitude modulation (AM) as the parameter control choice for the modulation scheme. A basic transmitter processing chain consists of blocks that perform the following functionalities (in the typical order of signal conversion): constellation mapping, I/Q modulation (or quadrature modulation), baseband-to-passband mixer, a pulse shaping filter, and a

[2]RF communication system generally agrees with this basic framework, but common practice also involves the variations on the processing chain. For instance, system designers can use multiple filters before and after the mixer, or they can use analog mixer or analog filter (in which case, the blocks' operations occur after the digital-to-analog converter). Our proposed scheme RONS assumes a digital, linear filter.

radio-frequency (RF) frontend. The constellation mapping block performs bit-to-symbol mappings. Called *M-ary modulation*, it takes $\log_2(M)$ number of bits and convert them into M distinct symbols (greater alphabet size of M provides better bit-throughput rate but also increases the symbol susceptibility to error caused by channel/circuit noise). The next block is the quadrature modulation which takes two quadrature carriers for modulation; typically a sine wave generates the in-phase (I) channel while the cosine wave generates the quadrature (Q) channel (sinusoidal carriers are used due to their ease of generation). Afterward, a mixer upconverts the baseband signal to passband by mixing the signal with a sinusoid with RF frequency, adjusting the transmission's center frequency. Then, the signal goes through a pulse shaping filter, which modulates the signal with a pulse that is designed to fit the signal into the given channel bandwidth, before entering the analog domain of RF frontend via digital-to-analog converter (DAC), which converts the signal into electromagnetic form for propagation.

Even though it is theoretically impossible to have a time-constrained signal constrained in frequency and vice versa, the pulse shaping filter is designed to minimize the transmission impact beyond the channel bandwidth (and typically adds redundancy and spreads the symbol in the time domain). Using a filter to control the bandwidth overspill is very typical among legitimate devices, which adhere to the FCC regulations on spectral mask that controls the bandwidth overspill beyond the channel, e.g., by specifying the minimum power attenuation outside the accessed frequency band. Due to its common use, we focus on applying RONS on the redundancy block of pulse shaping filter for the evaluations of RONS in Section 7.

In this standard design of the transmitter chain, there are three redundancy blocks: the quadrature (I/Q) modulation block, the pulse shaping filter, and, optionally (if transmitter hardware sampling can support additional redundancy), the RF mixer. The redundancy profile for the quadrature (I/Q) modulation is the element-by-element multiplication with a local frequency sinusoidal and that for the pulse shaping filter is the convolution with the pulse specified by the transmitter design.

2.3 Receiver Design

We assume linear receiver and treat interference (both self-interference from fading and external interference from other transmitters) as random noise. At a high level, given a bit-to-samples mapping of the transmitter chain, the corresponding correct receiver that results in zero error with certain amount of channel uncertainty (degree of which depends on the redundancy added, for example, for error correction) performs an inverse mapping to the transmitter chain. With the receiver processing blocks operating in the reverse-chronological order as their counterparts on the transmitter chain, the notion of inverse mapping is straightforward for the processing blocks that perform an injective one-to-one mapping (in other words, they are not redundancy blocks). For the inversion of the other redundancy blocks, the receiver uses a soft-decision correlator and minimum mean squared error (MMSE) decision rule for samples-to-symbol mapping. When noise and interference's statistics are invariant of time, MMSE reduces into *matched filter* (the receiver performs the inverse mapping using the same profile that has been used by the transmitter). Matched filter is also SINR-optimal in Gaussian channels and is independent of both channel state (e.g., does not require channel estimation) and the interferers' strategies. Thus, to demodulate and decode the received signal, the receiver needs to know not only the exact transmitter chain/strategy but also the profiles that the transmitter uses for the mapping.

3. SYSTEM MODEL & ASSUMPTIONS

Due to the wide adoption in wireless communication community, we design RONS based on the basic communication design described in Section 2.2 and the receiver strategy in Section 2.3. The transmitter-receiver pair a priori agrees on a secure key [6,7]. However, there is no collision-preventing channel coordination between the simultaneous transmitters at the medium access control (MAC) layer (MAC-layer approach to mitigate interference is an active field [8,9] and its physical layer counterparts for orthogonal medium access are described in Section 6.1).

Assuming additive white Gaussian wireless channel model with numerous noise sources and limited fading with clear line-of-sight channel path (e.g., for evaluation in Section 7, RONS uses filtering that is robust to fading), the source transmitter coexists with $n-1$ other transmitters, consisting of a network of n users, sharing a bandwidth of W. In this framework, the user accesses the entire bandwidth by outputting samples at the rate of W before the RF frontend and transmits at all time with full queue. In contrast, typical channelization schemes discussed in Section 6.1 have an average application-layer goodput rate of $\frac{W}{n}$ at best, which requires correct and orthogonal channelization at MAC-layer and above. The single-channel setting (where the entire bandwidth is accessed) also models the worst-case collision-behavior among multiple coexisting transmitters.

We use the effective signal-to-interference-and-noise ratio (SINR) for the performance metric, since the greater the effective SINR at the receiver the better the reliability and rate performance. For instance, Shannon-Hartley theorem provides the theoretical upper bound on communication rate performance (R) in information theory: $R = W \log(1 + \text{SINR})$. The effective SINR metric both enables us to abstract away from the particulars of the physical layer design such as the modulation and coding scheme and reduces the problem by a degree of freedom, since we no longer need to consider how many transmitters are coexisting but rather what their collective impact on the receiver is (e.g., the transmitted power on the channel); for example, the case of five interfers that have identical channel with equal power budget has the same impact on the receiver as the case of one interfer with five times the power budget.

4. ATTACK MODEL

An attacker's goal is to degrade the victim transmitter's performance as much as possible. We aim for security by design and consider a strong attacker model where the attacker knows not only the transmitter chain strategy but also the physical frequency and time location of the source transmitter's medium access (that is, all of the attacker's emitted power impacts the victim's transmission as interference); our model applies the Dolev-Yao threat model [3] to wireless communication.

In specific, we distinguish three levels of jamming by attackers' capabilities and the information advantage that they have on the victim communication system (while assuming that the adversary has the capability to maximally use the

information advantage for their jamming). The strongest is the *correlated jammer* who knows not only the victim transmitter's physical-layer processing chain information but also the data input that has been relayed from the upper layers (or equivalently, correlated jammer is a processing-powerful reactive jammer with negligible reaction time). If an attacker does not know the data input but only the transmitter's physical-layer strategy, then it becomes a *coded jammer*. Lastly, an attacker who does not have any information injects interference signal that is independent to the victim transmission signal, in which case Gaussian signaling has the most detrimental effect on the victim transmission [10, 11], and thus the attacker is a *Gaussian jammer*. We establish the attacker model in this section, and then analyze and compare the jamming effect of the three jamming strategies in Section 5 (we introduce RONS that effectively counters the strongest attack of correlated jamming afterward).

4.1 Active Attack on Availability

To model the worst-case scenario for interference, we model the interferer to be a malicious jammer, an interferer whose sole goal is to degrade the source transmitter's performance. The optimal jammer strategy, or the interference signal that results in the minimum capacity rate performance, is linearly correlated with the target source signal if the jammer has a power budget comparable to that of the target source transmitter [10–12]. Based on these studies in information theory, we consider such *correlated jamming* attack. A correlated jammer cancels the source signal by injecting the same signal but only inverted (it *cancels* the signal by causing destructive interference, in contrast to the more conventional use of jamming to add noise). If successful, the received signal becomes uncorrelated with the transmitted signal (and the received signal does not contain any information about the transmitted signal) and the capacity becomes zero. A power-constrained attacker needs to only match the transmission power in order to force zero information transfer at the receiver. In fact, inverted transmission that exceeds beyond cancellation leaks information to the victim receiver and may also be helpful in detecting the attacker, as we study in Section 5.1. Therefore, a power-efficient correlated jammer only matches the transmission power.

Correlated jamming is the most dangerous when frequency, phase, and amplitudes are matched with the victim's transmit signal. Natural frequency and phase drift and jitter can be matched by the use of aggressive locking mechanism such as by using phase-locked loop; this attacker model challenges the notion of (natural) indelible marks on transmissions using sinusoidal signals [13]. Such strong attacker needs to precisely know about the transmission and be able to quickly react. Pöpper et al. studies the feasibility and challenges of launching correlated jamming in a system-oriented work and concludes that, even with the current state-of-the-art technology, such attack is feasible in a static environment (such as wireless network in rural areas) [14].

A weaker attack is *coded jamming* where an attacker only knows about the physical-layer transmission strategy (such as the redundancy profiles) and do not actively listen to the transmission. Thus, coded jamming is independent to the data input that has been relayed from the upper layers (it is still dependent on the transmission), whereas correlated jamming is dependent on both the data input and the transmission chain (and thus correlated to the output transmission signal). A coded jammer, which has a much less stringent requirement than a correlated jammer, is much stronger than simple Gaussian jamming in real-world communication practices due to the transmitter's adding redundancy and the corresponding receiver strategy to use the redundancy to decode the symbol (as is explained in Section 2); for instance, the coded jamming threat on integrity, e.g., making the receiver tune into the jamming signal as opposed to the legitimate source transmitter signal, has also been studied in the literature [15]; Section 5.1 studies the impact of coded jamming in more detail. Section 5 studies interference and compares between correlated, coded, and Gaussian jamming.

4.2 Passive Attack on Confidentiality

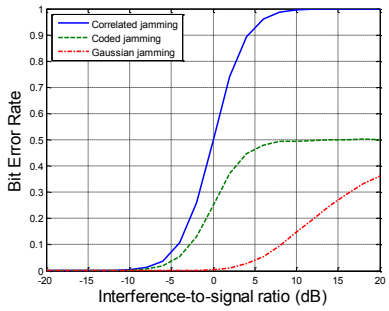
Since they know the victim transmitter's physical-layer strategy, both correlated jammer and coded jammer can correctly decode the message and breach privacy. (Gaussian jammer, on the other hand, does not know the processing chain and can not decode the message.) RONS effectively preserves privacy against attackers who know the victim's modulation and coding schemes, as we study in Section 7.1.

5. JAMMING INTERFERENCE ANALYSIS

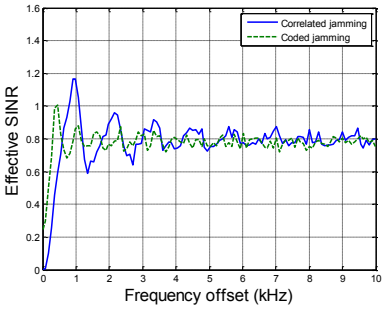
For interference analysis, we perform Monte-Carlo simulations using MATLAB. While assuming the system model in Section 3 and the attack model in Section 4, we use binary phase shift keying (BPSK) modulation and a root raised cosine filter (RRCF) for pulse shaping; the linear FIR (finite impulse response) has a filter order of 256. The natural SNR (without interference) is 10 dB.

5.1 The Usefulness of Information Advantage

In Figure 2(a), we compare the three jamming strategies of correlated, coded, and Gaussian against wireless availability and observe that knowing the victim transmitter strategy gives the jammer advantage and capability to inflict more damage on the network. While varying the attacker power budget with respect to that of the legitimate user and assuming perfect synchronization in phase and frequency, correlated jamming that cancels the signal power has the biggest impact on wireless availability by yielding the highest error rate for the legitimate system; coded jamming also has a more detrimental effect than Gaussian jamming. When the attacker power is matched to the legitimate transmitter's power, correlated jamming results in an error rate of 0.5 (i.e., no information due to complete cancellation of the transmitted signal) while coded jamming results in an error rate of 0.25 (since coded jamming sends random symbols imitating the physical-layer chain of the source transmitter and since the source transmitter uses BPSK with alphabet size of two, there is 0.5 chance of coded jammer sending conflicting symbols and, when that happens, there is a conditional probability of 0.5 for the event that the receiver tunes into and decodes the symbol that coded jammer sent; thus, $0.5 \cdot 0.5 = 0.25$). On the other hand, the legitimate user performs very well against transmission-independent Gaussian jamming since we incorporate redundancy at the physical-layer and the receiver uses soft-decoding to use the information of multiple samples to decode a symbol (as described in Section 2.3) and thus effectively mitigates transmission-independent noise; coded and correlated jamming, on the other hand, knows the MMSE-based receiver strategy and customizes its signal injection accordingly. Bakr and Mudum-



(a) Comparison between correlated, coded, and Gaussian jamming



(b) Correlated jamming becomes like coded jamming when frequency is not synchronized

Figure 2: Interference analysis

bai [16] also suggests that Gaussian jamming is less effective than the transmission-customized jamming (their white-hat approach uses jamming for defense against an eavesdropping attacker).

As the interference power grows, the error rate for correlated jamming converges to 1 and that for coded jamming converges to 0.5 because jamming transmission dominates the channel and the receiver tunes to the jamming symbol (for correlated jamming, the inverted symbol is the other symbol of BPSK and for coded jamming, the random symbol dominates the transmitted symbol). While an error rate of 0.5 effectively reduces into a coin flip and corresponds to no-information, an error rate exceeding 0.5 actually yields information to the legitimate user since the correlated jammer sends an (inversely) correlated symbol to the transmission. If a correlated jammer is concerned about yielding any information (e.g., legitimate user uses high error rate for correlated jammer detection), then the correlated jammer can adjust its transmission power to match that of the legitimate user.

5.2 The Effect of Frequency Offset

We study the case when the jamming signal and the victim's transmission signal are not synchronized. While we vary the power amplitude in Section 5.1, we now vary the frequency offset between the two signals, as hardware oscillators naturally operate at different frequencies and have unique frequency drift and jitter. Figure 2(b) displays the result while the jamming power amplitude is matched to that of the legitimate transmitter (transmission-independent Gaussian jamming has a constant SINR of 0.909 and is not plotted). When perfectly frequency-synchronized, correlated jamming yields zero SINR since it completely cancels the legitimate source signal; coded jamming yields some information about the source transmission and the effective SINR is 0.25. The effect of both jamming strategies substantially decreases within 0.5 kHz of frequency offset and eventually settles at an effective SINR of 0.8, which performance is still better than Gaussian jamming in the attacker's malicious perspective. As the frequency offset grows, correlated jamming converges to coded jamming because the transmission signal does not effectively get cancelled. To accommodate the difference in operating frequencies between hardware oscillators, IEEE 802.11 allows a center frequency error of ± 20 ppm [17]. When operating in GHz-band, such frequency offsets are enough for correlated and coded jamming to reach the steady-state effective SINR of 0.8; for instance, IEEE 802.11a channel 165 at carrier frequency 5.825 GHz tolerates frequency offset of 233 kHz around the center frequency. Although all oscillators operate at their own unique frequencies and it is natural to have frequency offsets, an attacker can use a frequency locking scheme with an aggressive use of phase-locked loops to synchronize frequency and perform the likes of correlated jamming for signal cancellation.

6. PROPOSED SCHEME

6.1 Motivation and Related Schemes

To embrace the coexistence of simultaneously transmitting wireless systems, communication researchers perform channelization and divide the medium into multiple channels. The channels are designed to be orthogonal to each other, so that the transmissions using different channels do not result in collision and interfere with each other. Typically, wireless systems achieve channel orthogonality by interleaving their access by time, frequency, and code (processing). For security, randomization technique can build on such orthogonal channels by accessing one channel (or subset of channels) at a time and having the channel access random to the users who do not hold the key and are not legitimate participants of the communication [4, 5].

Unfortunately, the current approaches implementing orthogonal channelization negatively affect the individual user's data rate performance. By sharing the medium with a network of users (all of which have equal transmission priorities) via orthogonal channelization, in the best-case scenario, the expected individual user's rate performance is inversely proportional to the number of coexisting users, while the overall network performance (the sum aggregation of individual user performances) remains the same. This is because frequency or time-based channelization divides the respective resources by the number of users or more, whereas all the medium resources could have been used by the source transmitter if other transmitters were not present.

On the other hand, code-based channelization introduces additional redundancy and consumes more medium resources than it would have needed if there were no channel division. For instance, a typical realization of code division multiple access (CDMA) involves a redundancy block called direct sequence spread spectrum (DSSS); DSSS temporally spreads the symbol by mapping a sample into multiple chips, and the number of chips per symbol is called *processing gain* or

spreading gain (which is the redundancy rate of the DSSS redundancy block). If the system retains the sampling rate within the block, then it consumes the amount of time that is larger than if there were no DSSS block to transmit the same amount of information (the time increase is proportional to the processing gain). Alternatively, DSSS increases the sampling rate (so that the chip rate is greater than the input symbol rate by the processing gain), which consumes a proportionally larger bandwidth. DSSS increases the SNR by the processing gain and effectively mitigates physical interference by first, carefully choosing the set of DSSS profiles (chip sequences that map the symbol to chips), so that they are orthogonal to each other, and then, having the receiver combine the information of multiple chips to decode the corresponding sample. By sharing the random spreading code only among the participating parties, DSSS can be helpful in both availability (interference, like noise, gets mitigated) confidentiality (correct code is necessary to decode the message). In contrast to the spread spectrum technology which entitles the spreading cost in rate, RONS, described in Section 6.2, minimizes intra-channel interference by emulating orthogonal access without the drawback in rate performance.

A closely related scheme to RONS that does not focus on achieving statistical orthogonality and availability within colliding transmissions is symbol re-mapping, which is the typical physical-layer implementation of cryptographic encryption (plaintext-to-ciphertext conversion and vice versa); by design, the mapping is one-to-one and there is no information loss in the information-theoretical sense. Such mapping adds randomization in the constellation mapping block (described in Section 2.2) where message bits relayed from upper layers get mapped to physical-layer symbols. However, the technique operates on the sample space of the symbol alphabets (the alphabet space consists of the options that the physical-layer symbols can take). On the other hand, RONS provides a much general platform to implement randomization, since the randomization is in samples, which offers the finest resolution in the discrete domain. RONS can emulate encryption by restricting the operating space (e.g., the phase/sample offsets are restricted to be the multiples of M where M is the alphabet size).

6.2 Redundancy Offset Narrow Spectrum

The goal of RONS is to mitigate interference without the spreading cost in data rate. RONS is similar to DSSS in that it is processing based, but it uses the redundancy blocks that are already in place of the transmitter chain, as opposed to introducing a new set of redundancy as DSSS does. Given the profile of a pre-existing redundancy block, RONS creates multiple profiles by adding *cyclic phase offsets* (or *cyclic delay*), which we denote with ϕ[3]. With the offset values chosen so that the generated redundancy profiles have zero correlation with one another (so that they are statistically orthogonal to each other), the use of a profile for signal processing yields statistically independent channel path from using any other profiles. We call the profiles generated using such phase offsets *RONS channels*. In other words, the cross correlation between *any* two signals using discrete RONS channels is very small.

Deciding on RONS channels depends on the processing operation of the redundancy block. The phase offset selection for RONS channel generation is straightforward when the redundancy block only performs oversampling and element-by-element mapping; in such cases, we can observe the correlation between the generated redundancy profiles after adding the cyclic phase offsets. One common use of RONS is the quadrature modulation (I/Q modulation), described in Section 2.2, where one channel (the in-phase channel) uses sine profile and the other channel (the quadrature channel) uses sine with $\phi = \pi/2$. However, in contrast to quadrature modulation and DSSS, there are redundancy blocks that involve more complicated operations than an element-by-element mapping, such as the pulse shaping filter (which involves convolution); for these blocks, the RONS phase offset selection depends not only on the redundancy profiles but also on the input of the redundancy block (the latter of which gets determined by the physical-layer design before the redundancy block).

After deciding on the set of pair-wise mutually uncorrelated RONS channels, the transmitter-receiver pair choose a random RONS channel (which can be derived from the secret key), so that a correlated jammer (and an eavesdropper) can not target the correct RONS channel to compromise the signal. For reactive jammers who sense the channel, we incorporate randomization by fast channel hopping across RONS channels. Since the RONS phase offsets can be added per symbol basis, this requires that the attacker can not respond within a symbol (even against a very processing-powerful attacker, which has negligible delay from victim signal's reception to the transmission of jamming signal, by causality, there is a lower bound on the required symbol length; the signal can not travel faster than the speed of light and there is a triangular distance difference between the path that detours through the attacker location and the direct path between the transmitter-receiver pair).

We also introduce a design parameter τ that controls the tradeoff between the statistical orthogonality between RONS channels and the number of RONS channels that the system can afford, since more RONS channels will make the channel-guessing attacker more difficult to make a correct guess. In other words, we allow that the inter-RONS-channel correlation to be as great as τ when selecting RONS channels.

Furthermore, RONS uses natural binary code when it maps from bits to symbols rather than the more popular Gray code; in natural binary code, the number index of the bits proportionally increases with phase. By having the adjacent symbols only differ by a bit when mapping the bits into symbols, Gray code is also popularly used along with error correction since, if symbol error occurred, it is more likely that the random noise yields closeby symbols than symbols that are further away on the constellation diagram (thus, an error in symbol decoding results in less number of erroneous bits). However, the threat of correlated jamming injects inverted signal with a phase offset of π (on the opposite side of the constellation diagram) and not random noise, and thus, it is more likely that the decoded symbol is further away from the transmitted symbol, especially when correlated jammer transmits with higher power than the legitimate transmission. When the attacker power dominates, the coding scheme (e.g., the decision between Gray code and

[3]If the redundancy profile of the block that RONS is deployed is odd and periodic, then $\phi = \pi$ is equivalent to the signal that a correlated jammer will transmit once the victim transmission is present.

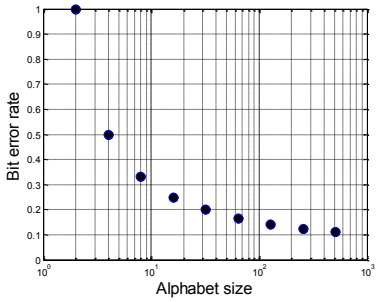


Figure 3: Bit error rate with the bit-to-symbol alphabet size M when correlated jammer dominates

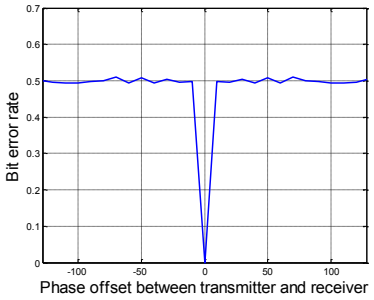


Figure 4: For correct decoding, the transmitter and the receiver needs to be tuned in the same RONS channel.

the natural binary code) does not affect the symbol error rate (there will almost always be errors because the receiver tunes on the attacker signal) but it affects the bit error rate, and RONS uses natural binary coding to lower the bit error rate after the symbol-to-bit mapping on the receiver. Figure 3 displays the bit error rate varying the coding alphabet size while assuming a modulation scheme that, for every symbol representing a message, has another symbol representing distinct message with a phase offset of π; the correlated jammer dominates and the receiver decodes the inverted symbol. With RONS using natural binary code, the bit error rate becomes inversely proportional to the $\log_2 M$ where M is the alphabet size, or the number of bits that gets mapped to the symbol.

7. RONS EVALUATION

For RONS evaluation, we perform Monte-Carlo simulation using MATLAB. We assume Section 3 and, for consistency, use the same set up and parameters as we did in Section 5. Namely, we use binary phase shift keying (BPSK) modulation and a root raised cosine filter (RRCF), and the natural SNR (without interference) is 10 dB.

We apply RONS on the pulse-shaping root raised cosine filter (RRCF), described in Section 2.2. The digital finite impulse response (FIR) filter has an order of 256, and the redundancy rate is 10 barring filter delay (i.e., a symbol gets mapped into 10 samples before being modulated with RRCF pulse). RRCF filter is suitable for RONS because it is a digital filter operating in discrete-time domain (easier to implement, stable, and has a linear phase characteristic) and is robust to fading (and thus agrees with the channel model). We use correlation threshold τ of 0.01 and the number of RONS channels is 8. The correlated jammer guesses a RONS channel and varies its guess for every symbol.

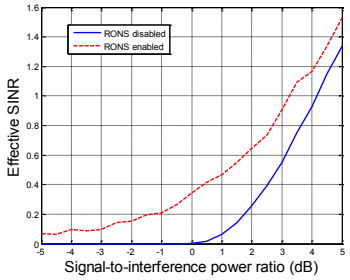
The performance metric of effective SINR (in the data receiver's perspective) is based on the error performance. In BPSK, treating interference as white Gaussian noise, the expected SINR and BER has the following relationship: $\overline{\text{SINR}} = [Q^{-1}(2 \cdot \text{BER})]^2$ where $Q(.)$ is the Q-function of a standard normal function. A more sophisticated physical-layer scheme incorporating the interference structure to further suppress the interference after RONS (as opposed to oversimplifying the artificial interference and treating it like Gaussian noise), will increase the effective SINR and generate better performance, but such development and analysis is beyond the scope of this work.

7.1 RONS for Confidentiality

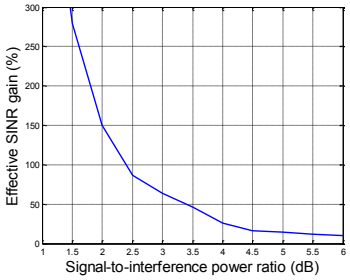
By incorporating randomization in the phase offsets (the RONS channels), RONS can be helpful for protecting confidentiality. Figure 4 shows communication reliability while varying the phase offsets between a transmitter and a (potentially malicious) receiver. Without knowing the correct phase offset, the receiver does not have the capability of decoding the transmission, as the error rate quickly approaches 0.5, which yields no information about the transmission. Therefore, if the source transmitter can keep the RONS channel random and secret, then the receivers failing to tune into the correct RONS channel fails to decode the transmitted data correctly.

7.2 RONS for Availability

We study RONS performance against correlated jamming. In Figure 5(a), we study the expected effective SINR while varying the signal-to-interference ratio (SIR) (where the interference model is the worst-case of correlated jamming). Without RONS, the effective SINR becomes zero when interference power is greater than the signal power meaning that the received signal has zero information about the transmitted signal, since it effectively gets cancelled. Unsurprisingly, the performance monotonically increases as the SIR increases. Enabling RONS prevents the transmitted signal from getting completely cancelled and outperforms the case when RONS is disabled. Figure 5(b) plots the expected effective SINR gain of enabling RONS compared to that when RONS is disabled and the jamming attacker knows the transmission and is synchronized (for example, gain of 100% indicates that the performance of enabling RONS is twice as good as that of disabling RONS). With the gain being ∞ when SIR < 0 dB (since the reference case of disabling RONS yields zero performance), the gain decreases as SIR increases. Even though RONS performance eventually converges to the correlated jamming performance both when SIR grows (as the remaining signal after cancellation is still big) and when SIR shrinks (as interference power simply overwhelms the signal power), RONS performance against correlated jamming is the most effective when they have comparable amount of power, i.e., SIR is close to 0 dB, and thus when correlated jamming has the most detrimental impact on the victim without a countermeasure (as discussed in Section 5.1).



(a) The effect of correlated jamming and RONS's mitigation



(b) RONS's performance gain over no countermeasure

Figure 5: RONS's performance for jamming mitigation

8. CONCLUSION

RONS provides a novel rate-efficient scheme to incorporate randomization for wireless security; the scheme adds cyclic phase offsets on an existing redundancy block at the physical layer without introducing further redundancy. Against the information-theoretically optimal attack of frequency-synchronized correlated jamming (a realization of Dolev-Yao threat model in wireless), RONS provides throughput even when the correlated jammer's power budget exceeds that of the source transmitter (in contrast, with no countermeasure, correlated jammer forces zero capacity). RONS is the most effective when correlated jamming is the most effective (without a countermeasure deployed) with its transmitter power comparable to that of the victim transmitter; when the jammer power exceeds -3 dB of that of the source transmitter, the effective performance gain over disabling RONS is greater than 70%. RONS also provides confidentiality against users who do not know the shared key.

9. ACKNOWLEDGMENTS

This material is based upon work partially supported by USARO under Contract No. W-911-NF-0710287 and by NSF under Contract No. NSF CNS-0953600. We would also like to thank the anonymous reviewers for their feedback.

10. REFERENCES

[1] J. I. Choi, M. Jain, K. Srinivasan, P. Levis, and S. Katti, "Achieving single channel, full duplex wireless communication," in *Proceedings of the sixteenth annual international conference on Mobile computing and networking, MobiCom '10*. New York, NY, USA: ACM, 2010, pp. 1–12.

[2] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM 2011 conference*. New York, NY, USA: ACM, 2011, pp. 2–13.

[3] D. Dolev and A. C. Yao, "On the security of public key protocols," *Information Theory, IEEE Transactions on*, vol. 29, no. 2, pp. 198–208, 1983.

[4] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications–a tutorial," *IEEE Transactions on Communications*, pp. 855–884, May 1982.

[5] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread spectrum communications handbook*. McGraw-Hill: New York, Mar. 1994.

[6] J. Chiang and Y. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in *IEEE INFOCOM*, Phoenix, AZ, USA, Apr. 2008, pp. 1211–1219.

[7] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, Oakland, CA, USA, May 2008, pp. 64–78.

[8] S.-Y. Chang, Y.-C. Hu, and N. Laurenti, "SimpleMAC: a jamming-resilient mac-layer protocol for wireless channel coordination," in *Proceedings of the 18th annual international conference on Mobile computing and networking, MobiCom '12*, Istanbul, Turkey, 2012, pp. 77–88.

[9] B. Awerbuch, A. Richa, and C. Scheideler, "A jamming-resistant MAC protocol for single-hop wireless networks," in *PODC*, Aug. 2008, pp. 45–54.

[10] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Info. Theory*, vol. 29, no. 1, pp. 152–157, Jan. 1983.

[11] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," in *IEEE ICC*, vol. 1, Jun. 2004, pp. 458–462.

[12] M. Medard, "Capacity of correlated jamming channels," in *Allerton Conference on Communications, Computing and Control*, Monticello, IL, USA, 1998.

[13] L. Baird, W. Bahn, M. Collins, M. Carlisle, and S. Butler, "Keyless jam resistance," in *Information Assurance and Security Workshop*, Jun. 2007, pp. 143–150.

[14] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," in *Proceedings of the 16th European conference on Research in computer security, ESORICS '11*. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 40–59.

[15] S. Capkun, M. Cagalj, R. Rengaswamy, I. Tsigkogiannis, J.-P. Hubaux, and M. Srivastava, "Integrity codes: Message integrity protection and authentication over insecure channels," *Dependable and Secure Computing, IEEE Transactions on*, vol. 5, no. 4, pp. 208–223, 2008.

[16] O. Bakr and R. Mudumbai, "A new jamming technique for secrecy in multi-antenna wireless networks," in *IEEE International Symposium on Information Theory Proceedings, ISIT '10*, Austin, TX, USA, 2010, pp. 2513–2517.

[17] "IEEE std 802.11a," *IEEE Std. Association*. [Online]. Available: http://standards.ieee.org/getieee802/download/802.11a-1999.pdf