Implementation of Two Physical Layer Security Techniques in an OTA System

Kevin Ryland KSR3625@VT.EDU
Marc Lichtman MARCLL@VT.EDU
T. Charles Clancy TCC@VT.EDU
Hume Center, Virginia Tech, Arlington, VA, USA

Abstract

Physical Layer Security (PLS) is a classification of security methods that take advantage of physical properties in the waveform or channel to secure communication. These schemes can be used to directly obfuscate the signal from eavesdroppers, or even generate secret keys for traditional encryption methods. This paper discusses the design of two PLS techniques in GNU Radio to facilitate over-the-air experimentation: 1) a 2x1 MIMO system where artificial noise is injected into the receivers nullspace, and 2) a single-carrier Alamouti coding system with pseudo-random phase shifts applied to each transmit antenna, known as Phase-Enciphered Alamouti Coding (PEAC). A brief tutorial of these techniques is provided. Discussion of a GNU Radio based implementation and testbed provide insight into the challenges of incorporating these techniques into real communications systems.

1. Introduction

Confidentiality in modern communication systems is constantly challenged by the broadcast nature of the wireless medium. This problem is traditionally solved by encrypting the message at a high network layer. As new technology appears, new applications emerge that present fundamental problems for traditional encryption. One example is that with the increasing number of power-constrained and computationally-limited devices being incorporated into Internet of Things (IoT) networks, lightweight security methods have become essential (Mukherjee, 2015).

Physical Layer Security (PLS) is a classification of security methods that take advantage of physical properties in the waveform or channel to secure communication. Over the past decade, advancements in Multiple-Input Multiple-Output (MIMO) systems have expanded the potential capabilities of PLS, meanwhile the development of technologies such as the IoT has provided new applications. While PLS has been heavily researched, literature that includes implementation is still developing. (Daly & Bernhard, 2010) analyzes the implementation of a phased array beamformer masked with the Direction Modulation (DM) technique and (Pellegrini et al., 2014) expanded on this implementation with the development of a DM-enabled Digital Video Broadcast transmitter. (Jordan et al., 2016) characterizes the performance of the Out-Phase Array Linearized Signaling technique developed in (Tollefson et al., 2015). (Ngassa et al., 2017) describes the implementation of a system that performs secret key generation using shared channel characteristics tested on both LTE and WiFi signals. The design work covered here attempts to add to this area of developing research by creating an open-source implementation of two PLS techniques that can be used directly with common Software-Defined Radio (SDR) front-end devices to enable easy Over-the-Air (OTA) experimentation and adaptation into new waveforms.

This paper discusses the design of two PLS techniques in GNU Radio to facilitate OTA experimentation. The first design involves a 2×1 Multiple Input Single Output (MISO) system where the transmitter uses Channel State Information (CSI) from the intended receiver to inject Artificial Noise (AN) into the receivers nullspace. The AN is consequently not seen by the intended receiver, however, it will interfere with eavesdroppers in an independent channel realization. The second design involves a single-carrier Alamouti coding system with pseudo-random phase shifts applied to each transmit antenna, referred to as Phase-Enciphered Alamouti Coding (PEAC). The intended receiver has knowledge of the pseudo-random sequence and can undo these phase shifts when performing the Alamouti equalization, while an eavesdropper without knowledge of the sequence will be unable to decode the signal.

The remainder of the paper is organized as follows. Section 2 provides a brief background of PLS. In Section 3, the system models for both the AN and PEAC techniques are introduced. Sections 4 and 5 detail the design process for the PEAC and AN systems, respectively. Section 6 describes the testbed used to evaluate these designs. Section 7 concludes this paper

Proceedings of the 7^{th} GNU Radio Conference, Copyright 2017 by the author(s).

with a discussion of future work. Lastly, Section 8 contains an appendix of several GNU Radio flowgraphs which are referenced throughout Sections 4 and 5.

2. Physical Layer Security Background

PLS, as it applied to confidentiality, is broken up into two main branches. The first branch deals with directly obfuscating the transmission from an eavesdropper. These techniques attempt to degrade the reception for eavesdroppers while simultaneously ensuring that the message is successfully communicated to the intended recipient. This is accomplished by exploiting the unique properties of the channel shared by the transmitter and intended receiver. The second branch of PLS focuses on using the unique characteristics of the channel between the transmitter and intended receiver to generate a private key that can be used to encrypt communication.

(Wyner, 1975) laid the foundation for PLS by introducing the concept of information-theoretic security in the context of a discrete memoryless wiretap channel, modeling the communication of two legitimate parties in the presence of an eavesdropper. Figure 1 shows the general case of the Wyner wiretap channel where the legitimate users communicate over a main channel with transition probabilities $\mathbf{Q}_M$ and are observed by an eavesdropper through an additional wiretap channel with transition probability matrix $\mathbf{Q}_W$. Note that this convention of representing the wiretap channel as in series with the main channel originates from Wyner's problem formulation. The encoder operates on blocks of source bits $S^K = (S_1, S_2, ..., S_K)$ and produces an encoded sequence $X^N = (X_1, X_2, ..., X_N)$. The intended receiver sees the output of the main channel, $Y^N = (Y_1, Y_2, ..., Y_N)$.

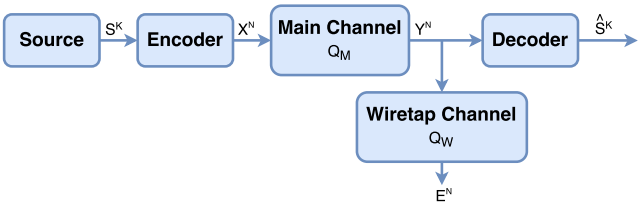

Figure 1. General Case of the Wyner Wiretap Channel.

There are three design metrics in Wyner's wiretap channel: transmission rate, error probability, and equivocation rate. The transmission rate of the channel is defined as the ratio of information sent to the total code length $R = (H_s K)/N$ where H_s is the source entropy. The eavesdropper observes the output $E^N = (E_1, E_2, ..., E_N)$ and the equivocation rate

$$\Delta = \frac{1}{K} H(S^K | E^N)$$

is a measure of the confusion experienced by the eavesdropper where $H(S^K|E^N)$ is the conditional entropy of S^K given E^N.

Wyner characterized a region of achievable rate-equivocation pairs (R, d) for wiretap codes and defined the secrecy capacity for the wiretap channel

$$C_S = \max_{p \in P} (I(X;Y) - I(X;E))$$

where $I(X;Y) = H(X) - H(X|Y)$ is the mutual information of X and Y which is maximized by an input probability p in the set of possible probabilities P. For independent main and eavesdropper channels, the secrecy capacity can be simplified to the difference in the capacity of the main and wiretap channels:

$$C_S = C_M - C_W.$$

Wyner's work proved that when the intended receiver operates in a more favorable channel than the eavesdropper, there is a quantifiable amount of information that can be communicated in perfect secrecy. This is the fundamental concept behind the obfuscation branch of PLS techniques.

The key-generation branch relies on the transmitter and intended receiver mutually measuring a unique quality of their shared channel. Common properties include the Received Signal Strength Indicator (RSSI), complex channel coefficients, and channel phase (Mukherjee et al., 2014). A practical consideration when measuring these properties on both ends of the channel is the accuracy of the measurement and the potential correlation of the measurement with the eavesdropper. In the case of measuring RSSI, the system will round the result to aid the transmitter and receiver in measuring the same value. Additionally, the designer may want to remove one or more of the most significant figures of the measurement if the eavesdropper is likely to measure the same value.

The adoption of MIMO communication in 802.11n and LTE created a resurgence in PLS research over the past decade. MIMO provides more opportunities for enhancing security at the physical layer such as adaptively steering a null towards an eavesdropper or simply beamforming in the direction of the intended receiver. The drawback is that eavesdroppers can now take advantage of multiple antennas in a MIMO Multiple Eavesdropper (MIMOME) channel to reduce the effectiveness of these techniques (Khisti & Wornell, 2010).

Information-theoretic security is claimed to be a stricter level of security than traditional encryption methods taking place at the upper OSI layers (Mukherjee et al., 2014). The rationale behind this assertion is that cryptographic encryption is built on the assumption that it will be computationally infeasible for an eavesdropper to decrypt the ciphertext without the secret key. This assumption is not mathematically rigorous and there are examples of ciphers being broken due to a combination of flaws in implementation and technological advancements. Information theoretic security can provide provably perfect security at data rates under the secrecy rate of a wiretap channel. The catch is that to reliably measure the secrecy rate,

the channel to all eavesdroppers must be known. In the case of a passive eavesdropper, only a probabilistic measure, the ergodic secrecy rate, can be obtained. PLS techniques can be practically applied in conjunction with traditional encryption or to provide lightweight security solutions for massive networks. Cryptographic techniques operate independently from the physical layer, making PLS an easy option to augment existing security systems.

3. System Models

A common security nomenclature used throughout this paper is to refer to the transmitter as Alice, the intended receiver as Bob, and the unintended receiver as Eve. The channel between Alice and Bob is described with $\mathbf{H}$ and the channel between Alice and Eve is described with $\mathbf{G}$.

3.1. Artificial Noise Generation

(Negi & Goel, 2005) proposed an AN Generation scheme where Alice divides her power between transmitting a message to Bob and transmitting Gaussian noise into Bob's nullspace. Assuming Bob and Eve's channels are independently faded, Eve will see some of the AN in her rangespace. This technique's major strength is that the secrecy provided scales well with SNR since an increase in SNR at Eve will increase the received AN power along with the message power.

To construct the AN, Alice must know Bob's CSI. For a Rayleigh channel with flat fading, Bob only needs to relay his channel coefficients to Alice faster than the coherence time of the channel. Another interesting property of this scheme is that the communication's secrecy does not depend on the secrecy of Bob's CSI (Negi & Goel, 2005). This means that Bob can transmit his CSI directly to Alice without fear of it being intercepted by Eve.

Under this scheme, Alice transmits a signal plus AN:

$$\mathbf{x}_k = \mathbf{s}_k + \mathbf{w}_k$$

where $\mathbf{x}_k$ and $\mathbf{w}_k$ are complex Gaussian vectors and $\mathbf{w}_k$ is chosen to lie in the nullspace of $\mathbf{H}_k$ by satisfying $\mathbf{H}_k\mathbf{w}_k = 0$. The AN term, $\mathbf{w}_k$, is generated from $\mathbf{w}_k = \mathbf{Z}_k\mathbf{v}_k$ where $\mathbf{Z_k}$ is a unitary matrix that is the orthonormal basis for the nullspace of $\mathbf{H_k}$. Since Eve may be in a channel realization that aligns her nullspace with Bob's, the best strategy is to make each element of $\mathbf{v_k}$ a Gaussian distributed random variable. By doing this, the AN is generated randomly from the available orthonormal basis vectors for Bob's nullspace. The number of possible basis vectors for Bob's nullspace, N_{null}, is limited by the difference in the array sizes of Alice and Bob:

$$N_{null} = N_{Alice} - N_{Bob} \quad \text{for} \quad N_{Alice} \geq N_{Bob}$$

The signals received by both Bob and Eve are

$$\mathbf{z}_k = \mathbf{H}_k\mathbf{s}_k + \mathbf{n}_k$$

$$\mathbf{y}_k = \mathbf{G}_k\mathbf{s}_k + \mathbf{G}_k\mathbf{w}_k + \mathbf{e}_k$$

where the $\mathbf{G}_k\mathbf{w}_k$ represents the additional noise seen by Eve.

Figure 2 displays an example of a wiretap code being applied to the AN scheme. To encode data with the wiretap code, one of four possible constellation points (one in each quadrant) are chosen for each of the four symbols. In this scenario, Bob can only see the source information and has a SNR large enough to demodulate 16-QAM. Eve sees AN along with the source information and only has a SNR large enough to demodulate QPSK, for example. When Eve receives a transmitted symbol, she can only tell which quadrant it is in and since all of the source symbols can map to points in every quadrant, it is completely ambiguous to Eve which symbol was sent. The wiretap coding adds redundancy by mapping a single symbol to four possible constellation points and therefore the effective transmission rate is reduced by half which agrees with the theoretical calculation of the secrecy rate

$$R_S = R_B - R_E$$

In the example shown in Figure 2, the secrecy rate equates to $R_S = 4$ bits/sym $- 2$ bits/sym $=$ **2 bits/sym**. It is important to emphasize that in this example, Eve's receiver is in an edge case where it can do absolutely no better than QPSK.

3.2. Phase-Enciphered Alamouti Coding

In (Alamouti, 1998), Alamouti proposed a Space-Time Block Code (STBC) to achieve transmitter diversity. Prior to this, diversity techniques were only applied at the receiver using algorithms such as Maximal Ratio Combining (MRC). These techniques require multiple receive antennas and were often impractical to implement on mobile handsets in cellular networks, because the antennas can only be spaced out by so much due to the handsets's small size. As a result, diversity techniques were only used at base stations to improve their reception quality. Alamouti showed that it was possible to achieve the same advantages, or diversity order, with a technique requiring multiple transmit antennas and a single receive antenna. Furthermore, he showed that the transmit data can be separated at the receiver with only linear computational complexity, making the processing requirements comparable to MRC. An additional feature of the Alamouti coding scheme is that it provides diversity gains independent of the degeneracy of the channel.

The Alamouti coding scheme is usually described by the 2×2 matrix

$$\mathbf{C} = \begin{bmatrix} s_1 & -s_2^* \\ s_2 & s_1^* \end{bmatrix}$$

where the columns represent timeslots and the rows represent different transmit antennas.

For many PLS techniques, Alice needs to have an accurate estimate of Bob's CSI. When the CSI estimate Alice uses is inaccurate, these techniques become less reliable and may even

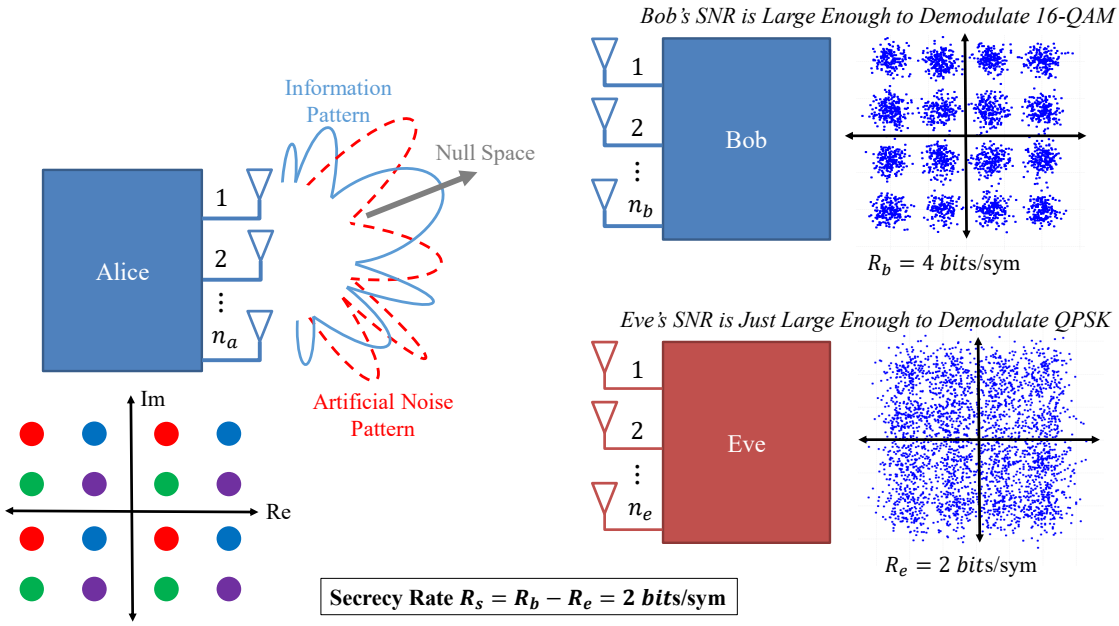

Figure 2. An example wiretap coding scheme applied to the Artificial Noise technique.

ill-condition the environment for Bob. For the AN scheme, the inaccuracy in Alice's knowledge of Bob's CSI directly corresponds to AN leakage into Bob's channel.

The author of (Allen et al., 2014) introduces a technique to achieve a secure STBC without needing to estimate CSI at the transmitter. This technique relies on a mutual RSSI measurement in order to seed a psuedo-random sequence used to secure communication. The psuedo-random sequence will determine phase shifts, θ_1 and θ_2, that are applied to each transmit element in the Alamouti STBC. Each phase shift is applied for one code duration. For a single codeword, the transmitter encodes source information, s_1 and s_2, as

$$\mathbf{X} = \begin{bmatrix} s_1 e^{j\theta_1} & s_2 e^{j\theta_2} \\ -s_2^* e^{j\theta_1} & s_1^* e^{j\theta_2} \end{bmatrix}$$

where the rows of $\mathbf{X}$ represent different transmit antennas and the columns correspond to time slots. Notice that this modified scheme still preserves the orthogonality of the Alamouti coding scheme. Figure 3 describes this scheme for a 2×1 system.

This is an application of the key-generation branch of PLS, but the key is used to encrypt the transmission at the physical layer rather than using a higher layer protocol. In the implementation described in this paper, the key generation is handled in software and the design is focused on the realization of the physical layer encryption.

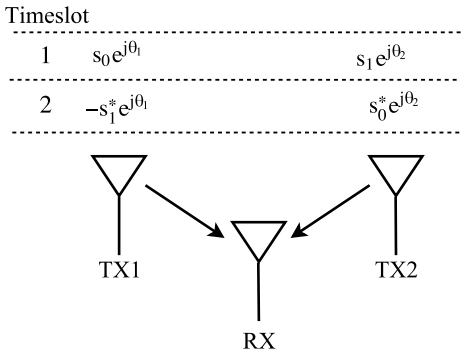

Figure 3. Phase-Enciphered Alamouti Coding Scheme.

Bob's received signal is $\mathbf{z} = \mathbf{X}\mathbf{h} + \mathbf{n}$ which can be written:

$$\begin{bmatrix} z_1 \\ z_2 \end{bmatrix} = \begin{bmatrix} s_1 e^{j\theta_1} & s_2 e^{j\theta_2} \\ -s_2^* e^{j\theta_1} & s_1^* e^{j\theta_2} \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ n_2 \end{bmatrix}$$

or more conveniently in the form $\tilde{\mathbf{z}} = \mathbf{H}(\theta_1, \theta_2)\mathbf{s} + \tilde{\mathbf{n}}$

$$\begin{bmatrix} z_1 \\ -z_2^* \end{bmatrix} = \begin{bmatrix} h_1 e^{j\theta_1} & h_2 e^{j\theta_2} \\ -h_2^* e^{j\theta_1} & h_1^* e^{j\theta_2} \end{bmatrix} \begin{bmatrix} s_1 \\ s_2 \end{bmatrix} + \begin{bmatrix} n_1 \\ -n_2 * \end{bmatrix}$$

Using the MRC algorithm, the source information can be estimated as

$$\hat{\mathbf{s}} = \mathbf{H}^+(\theta_1, \theta_2)\tilde{\mathbf{z}}$$

where $\mathbf{H}^+ = (\mathbf{H}^*\mathbf{H})^{-1}\mathbf{H}^*$ is the Moore-Penrose psuedoinverse of $\mathbf{H}$.

Eve's received signal is $\mathbf{y} = \mathbf{X}\mathbf{g} + \mathbf{e}$ which can be similarly decomposed into

$$\tilde{\mathbf{y}} = \mathbf{G}(\theta_1, \theta_2)\mathbf{s} + \tilde{\mathbf{e}}$$

where the source information can also be solved for

$$\hat{\mathbf{s}} = \mathbf{G}^{+}(\theta_1, \theta_2)\tilde{\mathbf{y}}.$$

In order to calculate $\hat{s}$, Eve will need an accurate estimate of $\mathbf{G}(\theta_1, \theta_2)$. Eve is presumed to have perfect CSI, and therefore knowledge of $\mathbf{g}$. Eve does not know the phase rotations, θ_1 and θ_2, but she will know the L^2 possible combinations of them. An exhaustive search over the phase rotations along with the L^2 possible symbol combinations will therefore require a search complexity of $O(L^4)$.

(Allen et al., 2014) generalizes Eve's maximum likelihood detector to discuss the relationship between the number of phase rotatations, N_{Rot}, applied at Alice and Eve's diversity order, D_{Eve}. This relationship can be characterized as $D_{Eve} = N_{Bob} - N_{Rot}$. This paper will only focus on the case where Alice applies the maximum number of phase rotations to completely deny Eve access to the source information. Additionally, (Allen et al., 2014) covers the design of a 4^{th} order STBC and generalizes this technique to securing STBCs of an arbitrary order. This paper will examine the 2×1 Alamouti case.

4. PEAC Design

4.1. Transmitter

The design of the PEAC transmitter is broken into the aspects of data management, modulation, space-time coding, pulse shaping, and interfacing with the RF front-end device.

4.1.1. Data Management and Digital Modulation

Data management and digital modulation in the PEAC transmitter are mainly handled by the `File Source`, `Chunks to Symbols`, and `Vector Insert` blocks. The `File Source` generates bytes from a source file which are packed into 2-bit chunks and mapped to a QPSK constellation in the `Chunks to Symbols` block. Since the STBC is only applied to the payload, the encoding is done before applying a header with the `Vector Insert` block.

The packet design is displayed in Figure 4. The Unique Words (UWs) are used to sound the channel for each antenna. To avoid self-interference, one antenna is muted while the other transmits its UW.

4.1.2. Space-Time Encoding

The PEAC space-time encoder is derived from the alamouti encoder in (Cribbs, 2015). The shared key in this implementation of the PEAC scheme is the seed for a Galois Linear Feedback Shift Register (GLFSR). The `GLFSR` block is used to apply psuedo-random phase shifts to each transmit element. The degree sets the length of the sequence, for the PEAC system this length is $2^{30} \approx 10^9$. The seed determines the initial fill of the registers used to generate the sequence, and will offset the sequence by the specified value. This means that Eve is assumed to know the sequence being used, but not the offset of the sequence.

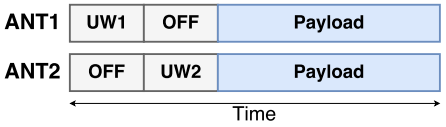

Figure 4. Packet Design for the PEAC System.

4.1.3. Pulse Shaping and RF Front-End Interface

The QPSK symbols are then up-sampled in the `Polyphase Arbitrary Resampler` block which also perform pulse shaping with a Root-Raised Cosine (RRC) filter.

Finally, the matched-filtered and upsampled baseband symbols are transmitted to the `UHD: USRP Sink block`. The Universal Hardware Driver (UHD) is the device driver provided by Ettus Research which interfaces with all USRPs. The complex samples received by the `UHD: USRP Sink` block are upconverted and transmitted by the USRP.

This system uses a single-carrier waveform and is centered at 2.489 GHz for testing. The sampling rate used is 1 MHz and the transmit and receive gains are adjusted at runtime.

4.2. Bob's Receiver

The design of Bob's PEAC receiver is broken up into the aspects of recovery loops, matched filtering, packet synchronization, channel estimation, and space-time decoding.

4.2.1. Recovery Loops and Matched Filtering

The USRP functioning as the receiver is tuned with the `UHD: USRP Source` block. Additionally, this block provides complex baseband samples from the USRP.

First, Automatic Gain Control (AGC) is performed with the `AGC2` block. The next step in the receiver chain is to eliminate any timing offset between the clock at receiver and transmitter. The timing recovery is implemented with a `Polyphase Clock Sync` block. This block also applies a RRC matched filter to eliminate Inter Symbol Interference (ISI).

Alamouti coding with QPSK does not lend itself to easy blind recovery of the carrier used by the transmitter. Since both transmit elements will send independent QPSK symbols, the received constellation is not QPSK, but rather a 3×3 grid of points formed by the combination of all possible QPSK sym-

bols. This constellation is shown in Figure 5. The costas loops

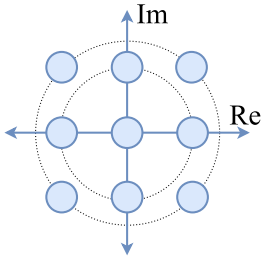

Figure 5. Received Constellation for Alamouti Coding with QPSK.

used in GNU Radio either in the `Costas Loop` block or more generally in the `Constellation Receiver` block both are not designed to perform frequency recovery of constellations without a constant modulus such as QAM or the constellation in Figure 5. Instead, the transmitter and receiver are connected to a common clock and timing source which eliminates the need to recover the carrier frequency at the receiver.

4.2.2. Packet Synchronization

To synchronize with a packet, the receiver correlates with the unique word using a `Decimating FIR Filter` block. The discrete complex cross-correlation of two sequences $p[n]$ and $u[n]$ of length N is defined as

$$R(p,u) = \sum_{m=0}^{N-1} p[m]u^*[m-n].$$

A FIR filter of order $N-1$ performs a convolution operation of the input $x[n]$ with the filter taps $h[n]$ to produce the output

$$y[n] = \sum_{m=0}^{N-1} x[m]h[n-m]$$

By substituting the taps $h_{corr}[n] = u^*[-n]$ into the FIR filter, the output becomes

$$y_{corr}[n] = \sum_{m=0}^{N-1} x[m]u^*[m-n] = R(x,u)$$

Therefore, to implement the cross-correlation of the input with the unique word using a FIR filter, the filter taps are set to the time-reversed and conjugated unique word. The hierarchical block implementing the `FIR Filter Correlator` is shown in Figure 14.

The unique words shown in Figure 4 are chosen to be 63-bit Maximum-Length Sequences (MLS) that are zero padded to 64 bits. The MLSs were chosen to have ideal autocorrelation and cross-correlation properties and the zero-padding was done to make handling the sequence easier in GNU Radio.

An example of the magnitude-squared values for the output of the two correlation filters in Figure 11 is shown in Figure 6. This graph corresponds to output seen with the `QT GUI Time Sink` in Figure 11. The magnitude-squared correlation value is used with the `Threshold` block to trigger a `Burst Tagger` which applies a stream tag to the input data when a correlation spike occurs. Since the correlation filter introduces a delay into the stream, a `Delay` block matches the input branch to the correlation branch to appropriately align the stream tag.

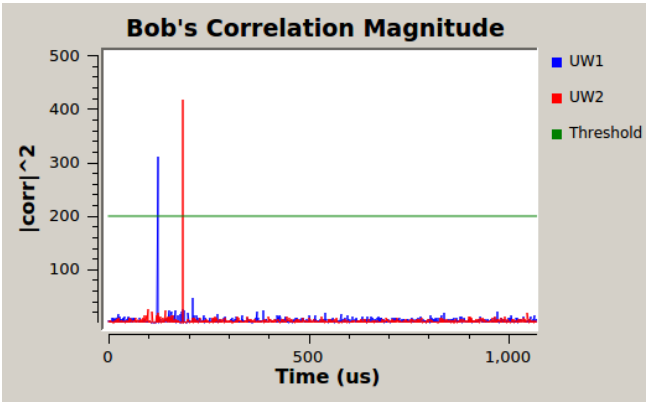

Figure 6. An example of the correlation filter outputs for each unique word and threshold level.

4.2.3. Channel Estimation

The output of the correlation filter can also be used to perform an estimate of the channel gains. Consider the cross-correlation of a unique word $w[n]$ of length N and amplitude 1 with the same unique word that experiences a complex Rayleigh flat fading gain h

$$R(hw[n], w[n]) = \sum_{m=0}^{N-1} hw[m]w^*[m-n].$$

The peak value occurs when the unique words overlap at $n = 0$, where $R_{peak} = \sum_{m=0}^{N-1} hw[m]w^*[m] = Nh$.

Therefore, the channel gain h can be estimated from the value of the correlation peak and the length of the unique word. The `Channel Estimator` block uses the stream tags applied by the `FIR Filter Correlator` to find the peak values and adds the channel gain estimates as stream tags to each unique word. Figure 7 shows an example of the scaled complex correlation value seen by the `Channel Estimator` block for a flat-faded Rayleigh channel with gain $h = 0.2 - 0.3j$.

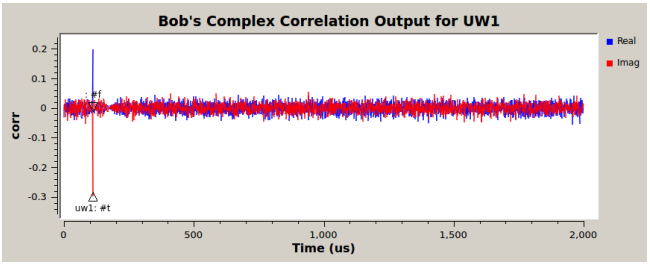

Figure 7. An example of the complex correlation filter output for one of the unique words with Rayleigh fading channel gain $h = 0.2 - 0.3j$.

4.2.4. Space-Time Decoding

The `PEA Decoding` block implements the Alamouti equalization while undoing the pseudo-random phase shifts applied at the transmitter. Prior to being fed into the `PEA Decoder` block, the stream is aligned based on the UW1 tag added by the `FIR Filter Correlator` block and then each packet is converted into a vector with the `Stream to Vector` block.

In the decoder, the stream tags for each channel gain are used to generate the channel estimates for each packet. A `GLFSR` block with a corresponding seed value to the transmitter applies inverted phase shifts to undo the phase offset in the channel estimate.

Eve's receiver is designed to be equivalent to Bob's, with the only difference being that Eve won't have the correct seed value for the `PEA Decoder` block.

5. AN Design

5.1. Transmitter

The AN transmitter's data management, header design, modulation, and pulse shaping are handled identically to the PEAC transmitter. The major differences between the AN and PEAC transmitters are the change from an Alamouti STBC in the PEAC system to a transmit beamformer in the AN system and the addition of an AN generator to the AN transmitter. Figure 15 displays the AN transmitter.

5.1.1. Transmit Beamforming

Consider the received channel model for the 2×1 system shown in Figure 8. The transmitter sends signals $\mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} \beta_1 s \\ \beta_2 s \end{bmatrix}$. The received signal is $r = \mathbf{hx} + n$ or $r = h_1\beta_1 s + h_2\beta_2 s + n$. Beamforming weights are chosen to be normalized phase shifts, $\beta_1 = \frac{h_1^*}{|h_1|}$ and $\beta_2 = \frac{h_2^*}{|h_2|}$. The received signal becomes

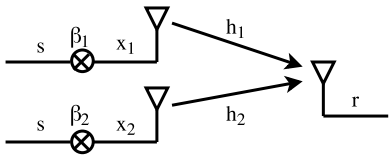

Figure 8. 2×1 Transmit Beamformer.

$$r = \frac{h_1 h_1^*}{|h_1|}s + \frac{h_2 h_2^*}{|h_2|}s + n = (|h_1| + |h_2|)s + n.$$

The transmitter makes use of CSI feedback from Bob to perform transmit beamforming with the `BF Weights` block.

5.1.2. Artificial Noise Generation

For a 2×1 system, Alice generates artificial noise such that $\mathbf{h}_k\mathbf{w}_k = 0$. $\mathbf{w}_k$ is generated from $\mathbf{w}_k = \mathbf{z}_k v$ where v is a Gaussian distributed complex scaler and $\mathbf{z}_k$ is a unit orthonormal basis vector for the nullspace of $\mathbf{h}_k$.

The AN is generated by using a Gaussian `Noise Source` block for v and multiply it with $\mathbf{z}$ which is generated from Bob's CSI feedback. The AN generation is implemented by the `AN Gen` block shown in Figure 15. The top and bottom entries in $\mathbf{w} = \begin{bmatrix} w_1 \\ w_2 \end{bmatrix}$ are applied to the first and second antennas, respectively.

5.2. Bob's Receiver

The AN receiver's recovery loops, packet synchronization, and channel estimation are implemented identically to the PEAC receiver. The major difference between the AN and PEAC receivers is the addition of CSI feedback in the former.

In the AN technique, CSI is required at the transmitter to generate noise in the nullspace of Bob's channel. To facilitate this in a test environment, the channel gains are sent to the transmitter using GNU Radio's asynchronous messaging protocol which updates the `AN Gen` and `BF Weights` blocks.

Eve's receiver functions identically to Bob's except that the CSI feedback mechanism is not implemented.

6. Testbed

The testbed for the experiments in this paper consists of the equipment in Table 1.

A networking diagram of this equipment is shown in Figure 9 which details the maximum throughput of each link. The network was designed to maximize the effective analog bandwidth of the X310s with UBX-160 daughtercards as described in (Pandeya, 2016).

Table 1. Equipment used in testbed.

Name	Quantity	Description
Ettus USRP X310	3	SDR Motherboard
Ettus UBX-160	6	SDR Daughtercard
Ettus Octoclock-G	1	Clock & Reference
Dell PowerEdge R820	1	Server
Intel SSD 3500 Series	4	800 GB SATA
Arista 7124SX	1	10 GigE Switch

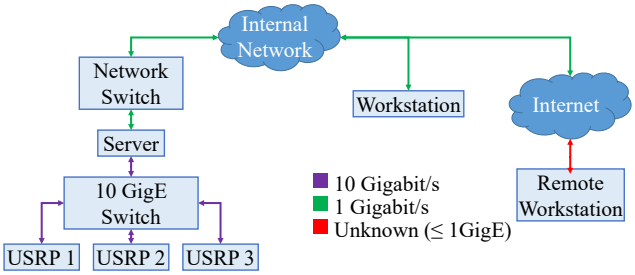

Figure 9. Network diagram of the testbed used for experimentation.

7. Conclusion

Many PLS techniques are well-researched and just on the edge of adoption into wireless standards. By designing and incorporating these techniques in OTA systems, the practical challenges of their implementation can be addressed.

An area of future work for the AN and PEAC systems is to perform a more strict OTA characterization for a standardized channel model. This will require setting up an OTA experiment in an environment that conforms to a particular channel model (e.g., using a channel emulator) and computing BER curves to compare against expected results from simulations or theory. A good candidate for this channel model would be an indoor WINNER 3GPP model. Another area for future work is to increase the array sizes of Alice, Bob, and Eve to compare the experimentally derived relationships between them using a masked beamformer with the theoretical results in (Khisti & Wornell, 2010).

References

Alamouti, S. M. A simple transmit diversity technique for wireless communications. *IEEE Journal on Selected Areas in Communications*, 16(8):1451–1458, Oct 1998.

Allen, T., Cheng, J., and Al-Dhahir, N. Secure space-time block coding without transmitter CSI. *IEEE Wireless Communications Letters*, 3(6):573–576, Dec 2014.

Cribbs, Michael R. *Multiple-input multiple-output wavelet packet modulation based software-defined radio transceiver design*. PhD thesis, Monterey, California: Naval Postgraduate School, 2015.

Daly, Michael P and Bernhard, Jennifer T. Beamsteering in pattern reconfigurable arrays using directional modulation. *IEEE Transactions on Antennas and Propagation*, 58(7): 2259–2265, 2010.

Jordan, Bruce R, Tollefson, Eric R, and Gaeddert, Joseph D. Characterization of out-phased array linearized signaling (opals). In *IEEE International Symposium on Phased Array Systems and Technology*, pp. 1–7. IEEE, 2016.

Khisti, A. and Wornell, G. W. Secure transmission with multiple antennas part II: The MIMOME wiretap channel. *IEEE Transactions on Information Theory*, 56(11):5515–5532, Nov 2010.

Mukherjee, A., Fakoorian, S. A. A., Huang, J., and Swindlehurst, A. L. Principles of physical layer security in multiuser wireless networks: A survey. *IEEE Communications Surveys Tutorials*, 16(3):1550–1573, 2014.

Mukherjee, Amitav. Physical-layer security in the internet of things: Sensing and communication confidentiality under resource constraints. *Proceedings of the IEEE*, 103(10): 1747–1761, 2015.

Negi, R. and Goel, S. Secret communication using artificial noise. In *VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.*, volume 3, pp. 1906–1910, Sept 2005.

Ngassa, Christiane L Kameni, Molière, Renaud, Delaveau, François, Sibille, Alain, and Shapira, Nir. Secret key generation scheme from WiFi and LTE reference signals. *Analog Integrated Circuits and Signal Processing*, 91(2):277–292, 2017.

Pandeya, Neel. About USRP bandwidths and sampling rates, May 2016. URL `https://kb.ettus.com/About_USRP_Bandwidths_and_Sampling_Rates`.

Pellegrini, Vincenzo, Principe, F, De Mauro, G, Guidi, R, Martorelli, V, and Cioni, R. Cryptographically secure radios based on directional modulation. In *IEEE International Conference on Acoustics, Speech and Signal Processing*, pp. 8163–8167, 2014.

Tollefson, Eric, Jordan, Bruce R, and Gaeddert, Joseph D. Out-phased array linearized signaling (opals): A practical approach to physical layer encryption. In *IEEE Military Communications Conference (MILCOM)*, pp. 294–299, 2015.

Wyner, A. D. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct 1975.

8. Appendix: GRC Flowgraphs

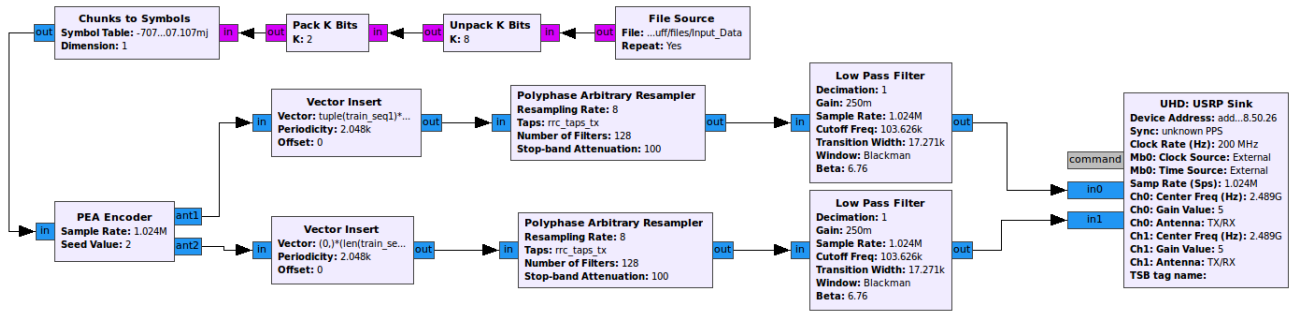

Figure 10. PEAC transmitter.

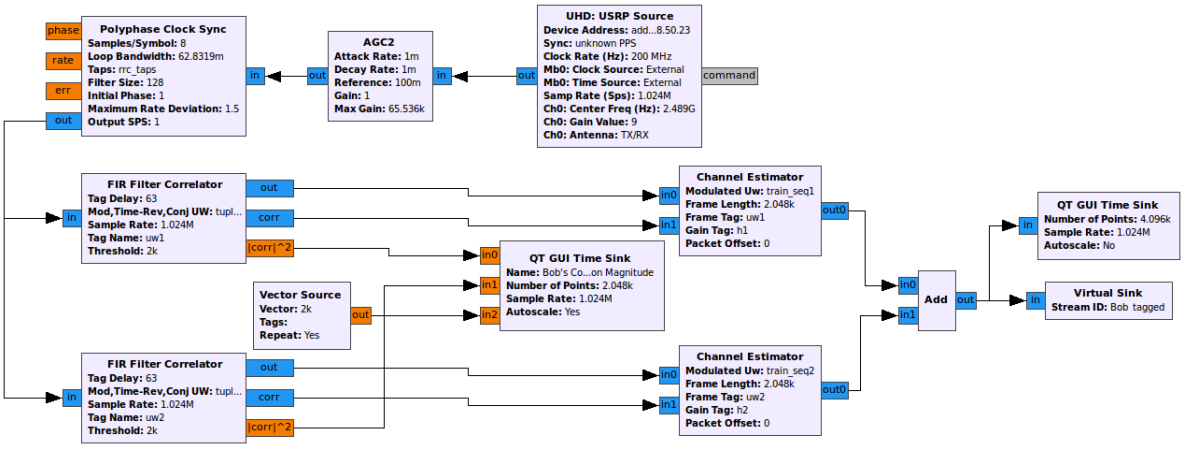

Figure 11. Part 1 of the PEAC receiver.

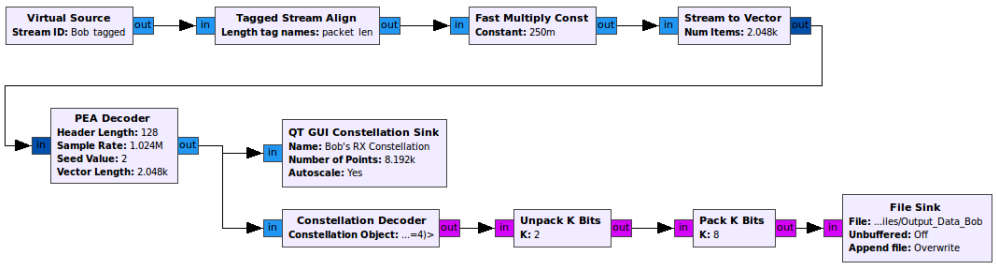

Figure 12. Part 2 of the PEAC receiver.

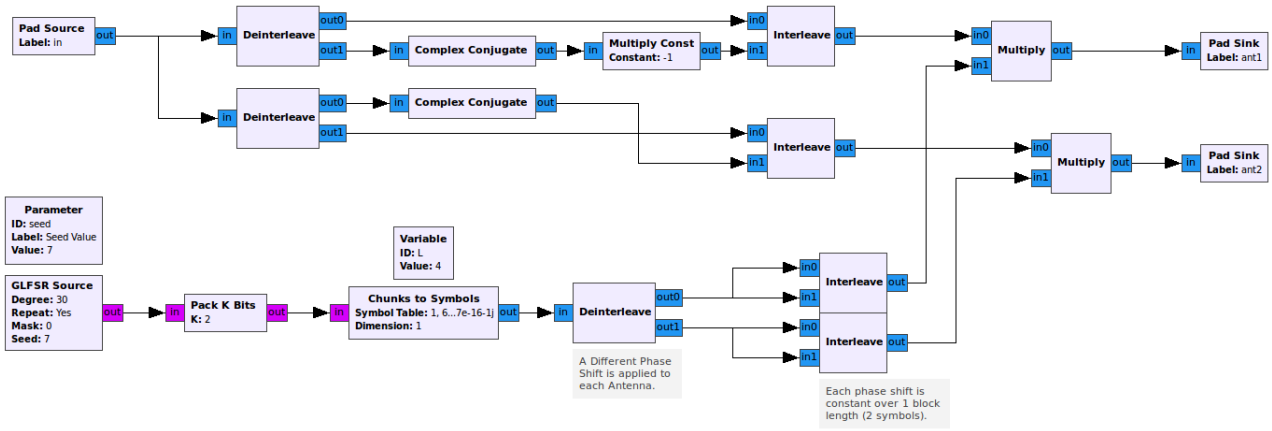

Figure 13. PEA Encoder hierarchical block.

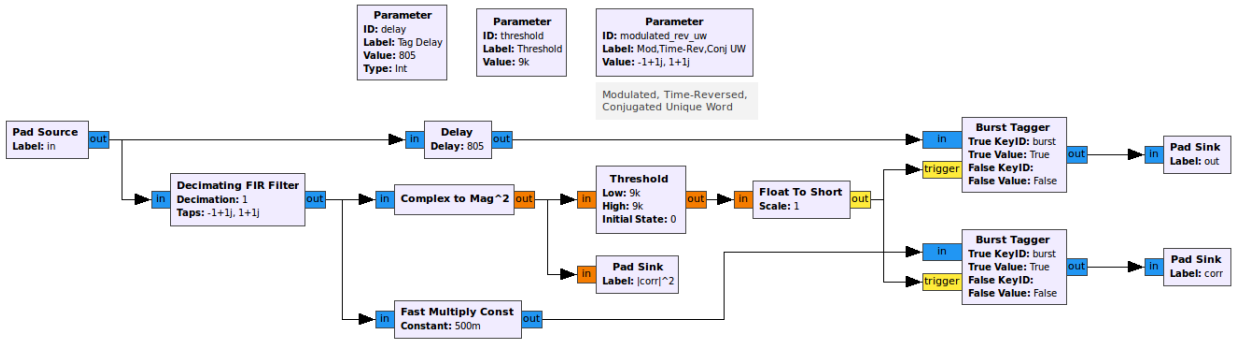

Figure 14. FIR Filter Correlator hierarchical block.

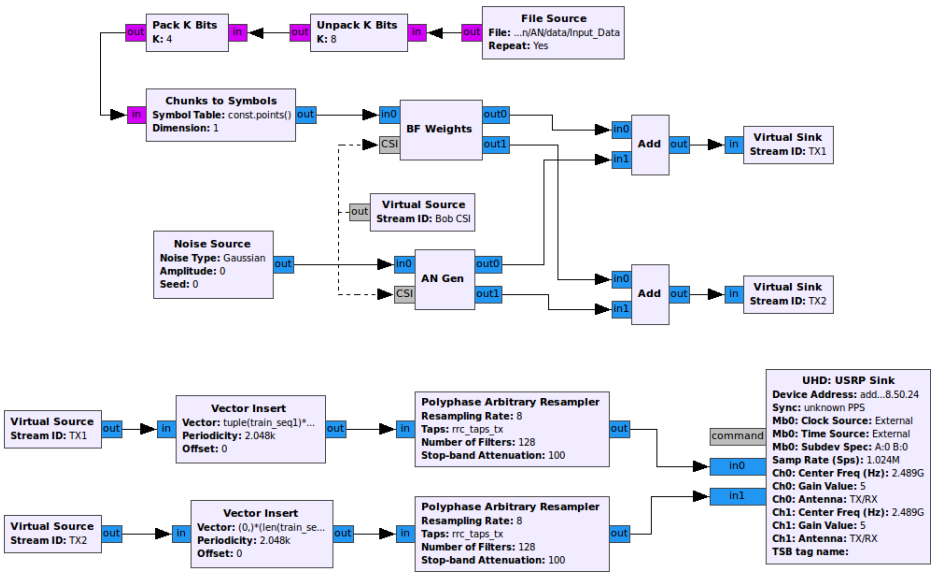

Figure 15. Artificial Noise transmitter.