Entrapment for Wireless Eavesdroppers

Song Fang*, Tao Wang†, Yao Liu†, Shangqing Zhao† and Zhuo Lu†
*University of Oklahoma, Norman, OK, 73019, songf@ou.edu
†University of South Florida, Tampa, FL, 33620, {taow@mail., yliu@cse., shangqing@mail., zhuolu@}usf.edu

***Abstract*—Due to the open nature of wireless medium, wireless communications are especially vulnerable to eavesdropping attacks. This paper designs a new wireless communication system to deal with eavesdropping attacks. The proposed system can enable a legitimate receiver to get desired messages and meanwhile an eavesdropper to hear "fake" but meaningful messages, thereby confusing the eavesdropper and achieving additional concealment that further protects exchanged messages. Towards this goal, we propose techniques that can conceal exchanged messages by utilizing wireless channel characteristics between the transmitter and the receiver, as well as techniques that can attract an eavesdropper to gradually approach a trap region, where the eavesdropper can get fake messages. We also implement and evaluate the proposed system on top of Universal Software Defined Radio Peripherals (USRPs). Experimental results show that an eavesdropper at a trap location can receive fake information with a bit error rate (BER) that is close to 0, and the transmitter with multiple antennas can successfully deploy a trap area.**

I. Introduction

The broadcast nature of wireless medium makes wireless communications vulnerable to eavesdropping, which has been a classic security threat [1]–[4]. Traditional methods to defend against eavesdropping attacks for emerging wireless communication systems mainly consider from the following aspects:

- *Cryptography:* A transmitter and a legitimate receiver can utilize a shared cryptographic key to encrypt a message so that eavesdroppers cannot correctly decrypt the message without the knowledge of the key.
- *Friendly jamming:* Recently, researchers have proposed to use friendly jamming to achieve the confidentiality of wireless communications (e.g., [5]–[8]). Specifically, a receiver sends out radio interference signals, i.e., jamming signals, to the wireless channel to prevent an eavesdropper from identifying and decoding the messages transmitted by the legitimate sender. Meanwhile, the receiver itself can cancel the impact of the interference signals and fully reconstruct original messages.
- *Proximity isolation:* Radio signal strength decreases as the distance between a receiver and an eavesdropper increases. Thus, the eavesdropper has a higher chance of intercepting exchanged messages if it can approach closer to the receiver. Accordingly, a natural way to address eavesdropping attacks against wireless communication is to enforce proximity isolation, i.e., providing physical protection on the receiver so that an eavesdropper cannot get close to the receiver.

These methods can greatly increase the difficulty for an eavesdropper to overhear exchanged messages, because the eavesdropper normally obtains random and meaningless bit sequences due to decryption failures, or signal interferences, or weak signal-to-noise ratio (SNR). However, they do not necessarily discourage the eavesdropper from making further efforts to access to the target information. The random-looking bit sequence inevitably delivers a side-channel message to the eavesdropper that her eavesdropping is unsuccessful, and she may try alternative techniques to infer exchanged messages. For example, she may adopt social engineering approaches to steal passwords, launch power analysis (e.g., [9]), time analysis (e.g., [10]), and dictionary attacks (e.g., [11]) to break cryptographic keys, utilize signal cancelation techniques to remove the impact of friendly jamming signals [12], move around to search for signals with best SNR, or try to disable the physical protection on a receiver.

On the other hand, what happens if an eavesdropper can correctly receive a meaningful message (e.g., a message that can pass the cyclic redundancy check) instead of a random bit sequence? In this case, she probably thinks that she has successfully obtained the information exchanged between a transmitter and a receiver. Intuitively, if the transmitter can enable the receiver to get desired messages and meanwhile the eavesdropper to hear "fake" but meaningful messages in lieu of random looking bit sequences, the communicators can achieve additional camouflage that further protects exchanged messages. Inspired by this intuition, we would like to design a secure wireless communication scheme to provide an eavesdropper bogus but meaningful information, thereby confusing the eavesdropper and mitigating the threat that an eavesdropper may adopt further ways to figure out the exchanged messages.

Existing Multi-user MIMO (MU-MIMO) technique can deliver a true message to the receiver and a fake one to an eavesdropper simultaneously. However, simply using MU-MIMO without considering security does not prevent eavesdropping. An eavesdropper can still access to the message intended for the receiver if she happens to be close to the receiver. Thus, it is highly desirable to create new techniques that achieve both security and concurrent delivery of messages.

Towards this end, we create a randomization channel construction technique to deliver original messages to a target receiver and meanwhile to attract an eavesdropper to gradually approach a *trap region*, where the eavesdropper can get fake messages. This is motivated by the observation that a dog chases prey by following its scent. In the wireless context, we provide an eavesdropper with attractive signals to lead the eavesdropper to move towards the trap region. The eavesdropper obtains fake information once she falls into the

trap. The defenders may also monitor the trap and arrest any eavesdropper who is lured to the trap.

The proposed scheme consists of two parallel tasks. The first one guides an eavesdropper to a trap, and the second establishes a secure communication channel between the transmitter and the legitimate receiver, so that the eavesdropper cannot decode exchanged messages even if she is nearby the receiver.

For the first task, our beginning step is to increase the probability that an eavesdropper can enter the trap. A very small trap region is not effective in catching an eavesdropper as the chance that the eavesdropper happens to be around this area is low. To enlarge the trap size, we propose to use multiple antennas to deliver fake messages to multiple neighborhood trap regions, so that these trap regions join together to form a trap area of a desired size. We then propose techniques to add specifically designed noise to signals to be transmitted, so that an eavesdropper observes increasing SNR of received signals and gradually clearer fake messages, as she moves close to the center of the trap area.

The second task establishes a secure channel between the transmitter and the receiver without leaking exchanged messages. A naive method is to send encrypted true messages to the receiver, and meanwhile send unencrypted fake messages to the traps. However, if an eavesdropper knows that traps are in use, the eavesdropper can tell if she is in a trap by examining whether or not received messages are encrypted. We would like the eavesdropper to obtain unencrypted fake messages even when she is nearby the receiver. In this paper, we propose techniques that can deceive the eavesdropper with fake messages and conceal true messages sent by the transmitter through utilizing wireless channel characteristics between the transmitter and the receiver. We discuss the details of the proposed technique in Section IV and adversarial indistinguishability in Section V-B. The contribution of this paper is summarized below.

- We propose to inject fake messages to an eavesdropper instead of random bit sequences, and meanwhile deliver true messages to a legitimate receiver to confuse the eavesdropper and camouflage exchanged information.
- We propose techniques that can set a trap to attract an eavesdropper, so that the eavesdropper obtains increasingly clear fake information as it approaches to the center of the trap area.
- We propose to establish a secure communication channel between a transmitter and a receiver, so that the eavesdropper cannot obtain true messages when she is close to the receiver. Moreover, the eavesdropper receives fake messages specified by the transmitter.
- Experimental results show that both a legitimate receiver and an eavesdropper at a trap location can receive true and fake information with a BER that is close to 0, respectively. We also demonstrate through experiments that the transmitter can use multiple antennas to successfully deploy a trap area, which entraps an eavesdropper by enabling the eavesdropper to experience increasing SNR from boundary to the center of the trap.

II. System Overview

A. Task I: Entrapping an Eavesdropper

The wireless channel introduces distortion to the signals that travel through the wireless medium [13]. To enable a receiver to correctly decode a message, a typical way is to perform precoding on outgoing messages so that the signal distortion can be canceled when the messages arrive at the receiver. This precoding process requires that a transmitter knows the channel effect, which is used to adjust outgoing messages to cancel the signal distortion. The channel effect can be measured from the channel between the transmitter and a desired receiver.

Thus, the transmitter needs to pre-code outgoing fake messages according to the channel effect between itself and a selected location, referred to as a *trap location*, and then transmits pre-coded messages with a reasonable power. The eavesdropper can then correctly decode these fake messages when she is at the trap location. However, the following research challenges exist to entrap the eavesdropper.

Enlarging the trap: According to channel spatial correlation property of wireless channel [14], if the eavesdropper is close to the trap location (e.g., less than several wavelengths away from this location), it may still decode received messages. We refer to the region centered at the trap location, within which the eavesdropper can probably decode received messages, as a *trap region*. For an eavesdropper residing in a trap region, the message decoding success rate increases as the eavesdropper moves closer to the trap location. In practice, the size of a trap region is determined by communication frequency, transmit power, and a number of environmental factors like geography, surrounding obstacles, etc. As mentioned earlier, if the trap region is too small, it may be difficult to lure the eavesdropper to fall in the trap. To solve this challenge, we propose to use multiple antennas to transmit fake messages to multiple trap locations simultaneously. The corresponding adjacent trap regions centered at these trap locations can thus form a larger *trap area* to trap the eavesdropper.

Attracting an eavesdropper: To enlarge a trap, fake messages are sent to multiple trap locations via multiple antennas. Thus, when an eavesdropper moves inside of a trap area, she may observe high message decoding rate at multiple nearby locations. This may make the trap area suspicious to the eavesdropper. Ideally, we would like an eavesdropper to find only one location that ensures a high communication quality. To solve this challenge, we propose to guide an eavesdropper in a trap area to move towards the center of this area, where she can receive fake information. We propose to introduce artificial noises to signals to be transmitted to control the SNR of signals received in a trap area. Specifically, signals received at the boundary of the trap area exhibits a weak SNR, which incurs a high BER and makes the message decoding difficult. As the eavesdropper moves from the boundary to the center of the trap area, the SNR increases and message decoding becomes increasingly easy. Signals received at the center show the strongest SNR, enabling the eavesdropper to have the highest communication quality.

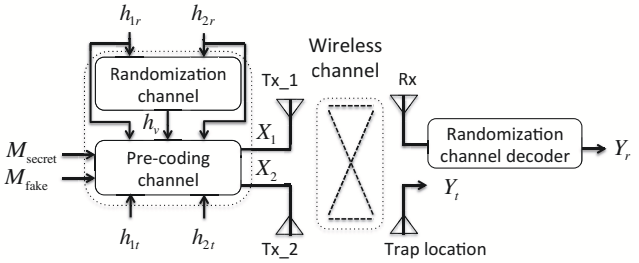


Fig. 1. Basic structure of the wireless randomization channel system

B. Task II: Establishing a Secure Channel

To prevent an eavesdropper from obtaining the target information, we add specially designed random signals to the original signals to be transmitted to the wireless channel. These random signals will randomize the entire traffic flow received by the eavesdropper and accordingly make the eavesdropper unable to recognize and decode signals sent by the transmitter.

Towards the design of a secure channel, we propose a method to allow the transmitter to further randomize the channel effect during the communication, such that the channel effect estimated by the receiver is a value specified by the transmitter and can be updated at any time. The transmitter pre-codes outgoing messages according to the value in lieu of the actual channel effect. The receiver can correctly decode the true messages, but an eavesdropper obtains fake messages after decoding when she is in the close proximity of the receiver.

C. System Design

The first and second tasks are parallel, because we would like to send the true messages and fake ones to a legitimate receiver and an eavesdropper at the same time. The parallelism is achieved by utilizing multiple antennas to concurrently transmit pre-coded signals. Without loss of generality, we assume that the transmitter has two transmit antennas Tx_1 and Tx_2. Figure 1 illustrates the parallel construction of the proposed system. Let h_{1r} and h_{2r} denote the channel effect between Tx_1 and the receiver Rx, and that between Tx_2 and Rx, respectively. Further Let h_{1t} and h_{2t} denote the channel effect between Tx_1 and a selected trap location, and that between Tx_2 and the trap location, respectively. With the knowledge of h_{1r} and h_{2r}, the transmitter can utilize the proposed randomization channel construction technique (detailed in Section IV) to agree on the specified channel effect h_v with the receiver. The specified channel can enable the transmitter and the receiver to establish a secure communication channel.

The transmitter then uses h_v, h_{1r}, h_{2r}, h_{1t}, h_{2t} as inputs to the trapping algorithm (detailed in Section V) to encode a true message M_{secret} and a fake message M_{fake}. The algorithm outputs are two encoded messages X_1 and X_2, which are sent by Tx_1 and Tx_2 concurrently. M_{secret} and M_{fake} are encoded in a way that when X_1 and X_2 arrive at the receiver, the combined signal cancels the fake message component, and when they arrive at the eavesdropper at the trap location, the combined signal cancels the true message component.

III. System Assumptions

We consider a generic wireless scenario that consists of a transmitter, a receiver, and an eavesdropper. We assume that the eavesdropper does not know the receiver's location and has the ability to move across a target area. Note that the legitimate receiver can be hidden from the eavesdropper's view. For example, in tactical communications, wireless transceivers are camouflaged so that they are not discovered by the enemy. If the eavesdropper cannot intercept a useful signal at the current location for a certain time window, the eavesdropper will move to other locations to search for interested wireless signal.

To facilitate the presentation, we consider a transmitter with two antennas. The transmitter aims to send a secret message to the receiver and meanwhile a fake message to entrap a potential eavesdropper. We assume that the transmitter can perform channel estimation to measure the channel effect between itself and the receiver's location or a trap location. This can be achieved by running existing channel estimation algorithms [14] on wireless signals emitted by the receiver, or a helper node pre-deployed at the trap location by the transmitter. We assume that the transmitter can authenticate received signals through traditional cryptography or device fingerprinting methods, while the eavesdropper is unable to impersonate the legitimate receiver to the transmitter.

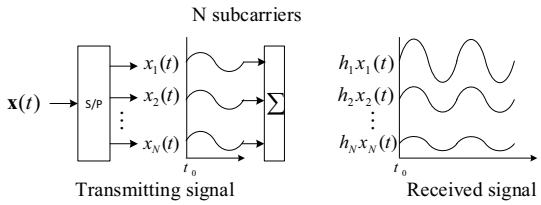
IV. Randomization Channel Design

Although two tasks are parallel, to understand the proposed entrapment, one needs to have the understanding about how to establish a secure communication channel. Therefore, we first describe how to establish such a channel, and then describe how to send fake and true messages to the trap and the receiver at the same time as well as how to enlarge the trap.

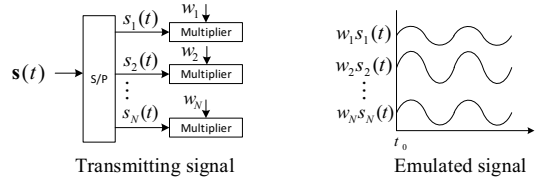
A. OFDM Preliminary

OFDM encodes digital signals using multiple subcarriers that are transmitted at multiple radio frequencies. As shown in Figure 2(a), an original signal $\mathbf{x}(t)$ is encoded into N subcarrier signals, represented by $[x_1(t), x_2(t), \ldots, x_N(t)]^T$, through a serial-to-parallel (S/P) module. The signals are transmitted at N different frequencies. The receiver accordingly observes the superposition of N signals, each of which is distorted by the wireless channel associated with the corresponding frequency.

The distortion h_i introduced by the i-th channel to the i-th subcarrier signal can be represented by a complex value, which is normally considered constant over a small time period called coherent time. The vector $[h_1, h_2, \ldots, h_N]^T$ is referred to as the channel impulse response of OFDM signals. The i-th received subcarrier signal $y_i(t)$ can be denoted with $y_i(t) = h_i x_i(t) + n(t)$, where $n(t)$ denotes the channel noise [14]. A normal way to estimate channel impulse response is that the transmitter sends a public training signal to the receiver. With $y_i(t)$ and the training signal, the receiver can then compute h_i from the above equation using existing estimation tools like the Minimum Mean Square Error (MMSE) estimator.



(a) Real OFDM wireless channel



(b) Real channel effect emulation

Fig. 2. Construction of a Specified Channel.

B. Construction of a Specified Channel

We consider a transmitter of two antennas and a receiver of one antenna. Accordingly, for the i-th subcarrier, the corresponding channel impulse response is formed by two values. We represent the channel impulse response between each of the transmitter's antenna and the receiver using a vector $\mathbf{H}_i = [h_{i_{1r}}, h_{i_{2r}}]$, and denote the training signal transmitted by each antenna as $\mathbf{s}_i(t) = [s_{i_1}(t), s_{i_2}(t)]^T$. As wireless channel is additive, the i-th subcarrier signal $y_i(t)$ received by the receiver can be represented by the sum of two signals transmitted by the two antennas of the transmitter. Mathematically,

$$y_i(t) = h_{i_{1r}} s_{i_1}(t) + h_{i_{2r}} s_{i_2}(t) + n(t) = \mathbf{H}_i \mathbf{s}_i(t) + n(t). \quad (1)$$

For normal channel estimation, the receiver can estimate $\mathbf{H}_i$ from Eq. 1. Unlike normal channel estimation, the goal for constructing a specified channel is to enable the receiver to estimate a channel specified by the transmitter. Towards this goal, we multiply selected coefficients with the training signals. Specifically, as shown in Figure 2(b), the signal $s_i(t)$ on each subcarrier goes through a multiplier with the coefficient w_i specified by the transmitter. After multiplication, $y_i(t)$ can be represented by (we omit the noise term to simplify the presentation)

$$y_i(t) = \begin{bmatrix} h_{i_{1r}} & h_{i_{2r}} \end{bmatrix} \begin{bmatrix} w_{i_1} & 0 \\ 0 & w_{i_2} \end{bmatrix} \begin{bmatrix} s_{i_1}(t) \\ s_{i_2}(t) \end{bmatrix} = \mathbf{H}_i \mathbf{W}_i \mathbf{s}_i(t), \quad (2)$$

where w_{i_1} and w_{i_2} denote the weight coefficients selected by the transmitter for the first and second antennas, respectively, and $\mathbf{W}_i = diag(w_{i_1}, w_{i_2})$. The transmitter would like the receiver to obtain a channel estimation outcome equal to the specified channel impulse response $\mathbf{H}_{vi} = [h_{i_v}, h_{i_v}]$ (both antennas are tuned to the same specified channel impulse response h_{i_v}). This means that the transmitter needs to make the following equation hold, $\mathbf{H}_i \mathbf{W}_i \mathbf{s}_i(t) = \mathbf{H}_{vi} \mathbf{s}_i(t)$. The transmitter can thus solve $\mathbf{W}_i$, and we obtain

$$\mathbf{W}_i = \begin{bmatrix} h_{i_{1r}}^{-1} h_{i_v} & 0 \\ 0 & h_{i_{2r}}^{-1} h_{i_v} \end{bmatrix}. \quad (3)$$

The transmitter then sets the weight coefficients for the i-th subcarrier according to $\mathbf{W}_i$, so that the receiver can estimate a specified channel impulse response $\mathbf{H}_{vi} = [h_{i_v}, h_{i_v}]$.

C. Receiver v.s. Eavesdropper

Once the specified channel is created, for an original transmit signal $\mathbf{x}_i(t) = [x_{i_1}(t), x_{i_2}(t)]^T$, the i-th subcarrier signal received by the receiver is

$$y_i(t) = \mathbf{H}_{vi} \mathbf{x}_i(t) = \begin{bmatrix} h_{i_v} & h_{i_v} \end{bmatrix} \begin{bmatrix} x_{i_1}(t) \\ x_{i_2}(t) \end{bmatrix}. \quad (4)$$

The receiver knows h_{i_v}, and thus can solve the combined original signal $x_{i_1}(t) + x_{i_2}(t)$ from Eq. 4, i.e., $y_i(t) = h_{i_v}(x_{i_1}(t) + x_{i_2}(t))$. To transmit an original signal $x(t)$ to the receiver, the transmitter can split $x(t)$ into two signals $r(t)$ and $x(t) - r(t)$, where $r(t)$ is a random signal, and then transmits $r(t)$ and $x(t) - r(t)$ through the first and second antennas respectively. The receiver obtains $x_{i_1}(t) + x_{i_2}(t) = r(t) + x(t) - r(t) = x(t)$.

For an eavesdropper, the i-th received subcarrier signal is

$$y_{ie}(t) = \begin{bmatrix} h_{i_{1e}} & h_{i_{2e}} \end{bmatrix} \begin{bmatrix} w_{i_1} & 0 \\ 0 & w_{i_2} \end{bmatrix} \begin{bmatrix} x_{i_1}(t) \\ x_{i_2}(t) \end{bmatrix}, \quad (5)$$

where $h_{i_{1e}}$ and $h_{i_{2e}}$ denote the real channel impulse responses between the transmitter's first and the second antenna and the eavesdropper, respectively. The eavesdropper does not know the coefficients w_{i_1} and w_{i_2}, because they are calculated based on secret value h_{i_v} that is selected by the transmitter (as shown in Eq. 3). As a result, she is unable to decode the message $x_{i_1}(t) + x_{i_2}(t)$ with Eq. 5.

When an eavesdropper happens to be at the receiver's location, $y_{ie}(t) = h_{i_v}(x_{i_1}(t) + x_{i_2}(t))$. The transmitter can set $y_{ie}(t)$ to a fake signal and solve the specified channel impulse response h_{i_v} from this equation.

The transmitter never transmits h_{i_v} through the wireless channel. The only way for the eavesdropper to know h_{i_v} is that she must be very close to the receiver at the moment when the specified channel is being established. However, the specified channel establishment process normally takes a short time (e.g., less than one second). The communicators can further randomize their schedule of channel establishment activities, i.e., the transmitter sends multiplied training signal to the receiver at random time. In this way, the eavesdropper cannot predict this schedule and thus take advantage of it to break the communication system, and surveillance tools may be adopted to detect eavesdroppers within this short time window. Once the specified channel is established, even if the eavesdropper moves very close to the receiver, she still cannot know the original signal $x_{i_1}(t) + x_{i_2}(t)$ due to the lack of the knowledge of h_{i_v}. Moreover, the communicators can update h_{i_v} frequently to enhance security.

If the eavesdropper can manage to be co-located with the receiver all the time, including the specified channel establishment process and the entire eavesdropping phase, it then knows h_{i_v} and is able to decode $x_{i_1}(t) + x_{i_2}(t)$. However, the eavesdropper meanwhile significantly increases the risk of being detected by the receiver.

D. Dealing with a Lucky Eavesdropper

A sneaker and lucky eavesdropper may successfully guess the specified channel impulse response h_{i_v} or the selected coefficients. To prevent such a guess attack, we propose to *further encode original signals to make decoding at an eavesdropper as hard as decoding a random signal* (even if the eavesdropper knows h_{i_v}), whereas decoding at a receiver remains the same way as discussed in Section IV-C. The basic idea is to generate one-time, non-repeated random signals for every transmission and add random signals to original signals, such that random signals cancel at the receiver but remain at the eavesdropper.

Specifically, let $n_{i_1}(t)$ and $n_{i_2}(t)$ denote the random signals added to the original signals $x_{i_1}(t)$ and $x_{i_2}(t)$ that are transmitted by the first and second antennas respectively. The i-th subcarrier signal received by the receiver is thus

$$\begin{aligned} y_i(t) &= \left[\begin{array}{cc} h_{i_v} & h_{i_v} \end{array}\right] \left[\begin{array}{c} x_{i_1}(t)+n_{i_1}(t) \\ x_{i_2}(t)+n_{i_2}(t) \end{array}\right] \\ &= h_{i_v}(x_{i_1}(t)+n_{i_1}(t)) + h_{i_v}(x_{i_2}(t)+n_{i_2}(t)). \end{aligned}$$

From the above equation, we can see that if $n_{i_1}(t)$ and $n_{i_2}(t)$ are of the opposite phase (i.e., $n_{i_2}(t) = -n_{i_1}(t)$), then the random signals can be canceled at the receiver. In this case,

$$\begin{aligned} y_i(t) &= h_{i_v}(x_{i_1}(t)+n_{i_1}(t)) + h_{i_v}(x_{i_2}(t)-n_{i_1}(t)) \\ &= h_{i_v}(x_{i_1}(t)+x_{i_2}(t)). \end{aligned} \quad (6)$$

The receiver can thus directly solve the desired signal $x(t) = x_{i_1}(t) + x_{i_2}(t)$ from this Equation.

We then analyze how the random signals impact on the eavesdropper when $n_{i_2}(t) = -n_{i_1}(t)$. Lemma 1 demonstrates that the eavesdropper indeed receives a random signal.

Lemma 1. *The received signal $y_{ie}(t)$ at the eavesdropper is random, represented by $h_{i_v}(h_{i_{1e}}h_{i_{1r}}^{-1}x_{i_1}(t) + h_{i_{2e}}h_{i_{2r}}^{-1}x_{i_2}(t) + x_{\text{rnd}}(t))$, where $x_{\text{rnd}}(t)$ is a non-zero random signal determined by the transmitter.*

Proof. For an eavesdropper, the i-th received subcarrier signal can be represented by

$$\begin{aligned} y_{ie}(t) &= \left[\begin{array}{cc} h_{i_{1e}} & h_{i_{2e}} \end{array}\right] \left[\begin{array}{cc} w_{i_1} & 0 \\ 0 & w_{i_2} \end{array}\right] \left[\begin{array}{c} x_{i_1}(t)+n_{i_1}(t) \\ x_{i_2}(t)-n_{i_1}(t) \end{array}\right] \\ &= h_{i_{1e}}h_{i_{1r}}^{-1}h_{i_v}(x_{i_1}(t)+n_{i_1}(t)) + h_{i_{2e}}h_{i_{2r}}^{-1}h_{i_v}(x_{i_2}(t)-n_{i_1}(t)) \\ &= h_{i_v}(h_{i_{1e}}h_{i_{1r}}^{-1}x_{i_1}(t) + h_{i_{2e}}h_{i_{2r}}^{-1}x_{i_2}(t) \\ &\quad + (h_{i_{1e}}h_{i_{1r}}^{-1} - h_{i_{2e}}h_{i_{2r}}^{-1})n_{i_1}(t)). \end{aligned} \quad (7)$$

We rewrite Eq. 7 as $y_{ie}(t) = h_{i_v}(h_{i_{1e}}h_{i_{1r}}^{-1}x_{i_1}(t) + h_{i_{2e}}h_{i_{2r}}^{-1}x_{i_2}(t) + x_{\text{rnd}}(t))$, where $x_{\text{rnd}}(t) = (h_{i_{1e}}h_{i_{1r}}^{-1} - h_{i_{2e}}h_{i_{2r}}^{-1})n_{i_1}(t)$. We can see that the random signals can be canceled at the eavesdropper (i.e., $x_{\text{rnd}(t)} = 0$) only when $h_{i_{1e}}h_{i_{1r}}^{-1} - h_{i_{2e}}h_{i_{2r}}^{-1} = 0$. Note that $h_{i_{1r}}$ and $h_{i_{2r}}$ are the channel impulse responses between the receiver and the transmitter's first and second antennas respectively, and $h_{i_{1e}}$ and $h_{i_{2e}}$ are the channel impulse responses between the eavesdropper and the transmitter's first and second antennas respectively. The transmitter can separate both antennas for a certain distance, such that the channel between the receiver/eavesdropper and the transmitter's first antenna is uncorrelated with that between the receiver/eavesdropper and the second antenna. This means $h_{i_{1r}} \neq h_{i_{2r}}$ and $h_{i_{1e}} \neq h_{i_{2e}}$. The chance that $h_{i_{1e}}h_{i_{1r}}^{-1}$ happens to be equal to $h_{i_{2e}}h_{i_{2r}}^{-1}$ can be negligible, since the eavesdropper is faraway from the receiver and $h_{i_{1e}} \neq h_{i_{1r}}$ and $h_{i_{2e}} \neq h_{i_{2r}}$. Therefore, $n_{i_1}(t)$ is not canceled, leading $x_{\text{rnd}(t)}$ not equal to 0. Even if the eavesdropper can know h_{i_v}, the received signal $y_{ie}(t)$ is still random to her due to the existence of $n_{i_1}(t)$. □

E. Multiple Collaborative Eavesdroppers

We consider a generic situation with λ eavesdroppers and N transmit antennas, each of which establishes a specified channel with the receiver. The transmitter can add random signals to any pair of antennas. Let $\mathcal{S} = \{i_1, i_2, \ldots, i_K\}$ and $\bar{\mathcal{S}} = \{p_1, p_2, \ldots, p_K\}$ denote the sets formed by the indexes of the antennas that transmit the original and the opposite random signals respectively, where $K = \frac{N}{2}$. Let h_{qe_j} represent the real channel impulse response between the q-th antenna and the j-th eavesdropper, w_q denotes the weight coefficient selected for the q-th antenna, $s(t)$ is the public training signal, and $n_i(t)$ is the i-th added random signal for $1 \leq i \leq K$. Correspondingly, the signals received by eavesdroppers can be modeled as:

$$\begin{cases} y_{e_1}(t) = s(t)\sum_{q=1}^{N} h_{qe_1}w_q + \sum_{k=1}^{K} n_k(t)(h_{i_k e_1}w_{i_k} - h_{p_k e_1}w_{p_k}) \\ \qquad\qquad \vdots \\ y_{e_\lambda}(t) = s(t)\sum_{q=1}^{N} h_{qe_\lambda}w_q + \sum_{k=1}^{K} n_k(t)(h_{i_k e_\lambda}w_{i_k} - h_{p_k e_\lambda}w_{p_k}) \end{cases}. \quad (8)$$

Suppose that each eavesdropper has the knowledge of the channel between each transmit antenna and herself, as well as the channel between each transmit antenna and the desired receiver. Then, the eavesdroppers can determine the channel state information h_{qe_j} for $1 \leq q \leq N$ and $1 \leq j \leq \lambda$. The unknowns of Eq. 8 are the coefficients $w_1, \ldots, w_N$ and random signals $n_1(t), \ldots, n_K(t)$. If the number of eavesdroppers are equal to or larger than the number of unknowns, i.e., $\lambda \geq N + K = \frac{3N}{2}$, Eq. 8 is a regular or overdetermined linear system and thus the eavesdroppers can solve the coefficients and random signals from Eq. 8.

Gaining all the channel information imposes a strong requirement for the eavesdroppers. Moreover, the eavesdroppers still face a significant challenge of solving the coefficients, as they do not know which random signal is associated with which transmitter. For each random signal, the transmitter randomly assigns two antennas to send the original and opposite ones, and thus for a given random signal the eavesdroppers cannot fill in the corresponding i_i and p_i in Eq. 8.

V. Placing the Trap

For the i-th subcarrier, let $m_{it}(t)$ and $m_{ir}(t)$ denote the fake and original signals to be delivered to the trap location and the receiver, respectively. Further let $h_{i_{1t}}$ and $h_{i_{2t}}$ denote channel impulse response between the trap location and the transmitter's first and second antennas. Let $y_{ir}(t)$ and $y_{it}(t)$

denote the i-th subcarrier signal received by the receiver and the trap location respectively. According to Eq. 6, to deliver $m_{ir}(t)$ to the receiver, we would like the equation $x_{i_1}(t)+x_{i_2}(t)=m_{ir}(t)$ to hold. On the other hand, according to Eq. 7, $y_{it}(t)$ received at the trap location can be represented by $y_{it}(t) = h_{i_{1t}}w_{i_1}(x_{i_1}(t)+n_i(t))+h_{i_{2t}}w_{i_2}(x_{i_2}(t)-n_i(t))$. Similarly, to deliver $m_{it}(t)$ to the trap location, we need the equation $y_{it}(t) = m_{it}(t)$ to hold. We thus have

$$\begin{cases} m_{it}(t)=h_{i_{1t}}w_{i_1}(x_{i_1}(t)+n_i(t))+h_{i_{2t}}w_{i_2}(x_{i_2}(t)-n_i(t)) \\ m_{ir}(t)=x_{i_1}(t)+x_{i_2}(t) \end{cases}. \quad (9)$$

Let $\Delta_{it}(t) = (h_{i_{1t}}w_{i_1} - h_{i_{2t}}w_{i_2})n_i(t)$ and rewrite Eq. 9 into

$$\begin{bmatrix} m_{it}(t) - \Delta_{it}(t) \\ m_{ir}(t) \end{bmatrix} = \begin{bmatrix} h_{i_{1t}} & h_{i_{2t}} \\ w_{i_1}^{-1} & w_{i_1}^{-1} \end{bmatrix} \begin{bmatrix} w_{i_1} & 0 \\ 0 & w_{i_2} \end{bmatrix} \begin{bmatrix} x_{i_1}(t) \\ x_{i_2}(t) \end{bmatrix}.$$

Therefore, the actual signals $x_{i_1}(t)$ and $x_{i_2}(t)$ to be transmitted by the first and second antennas are calculated by

$$\begin{aligned} \begin{bmatrix} x_{i_1}(t) \\ x_{i_2}(t) \end{bmatrix} &= \begin{bmatrix} w_{i_1} & 0 \\ 0 & w_{i_2} \end{bmatrix}^{-1} \begin{bmatrix} h_{i_{1t}} & h_{i_{2t}} \\ w_{i_1}^{-1} & w_{i_2}^{-1} \end{bmatrix}^{-1} \begin{bmatrix} m_{it}(t)-\Delta_{it}(t) \\ m_{ir}(t) \end{bmatrix} \\ &= \mathbf{C}_i \begin{bmatrix} m_{it}(t)-\Delta_{it}(t) \\ m_{ir}(t) \end{bmatrix}. \end{aligned} \quad (10)$$

where we refer to $\mathbf{C}_i$ as the pre-coding matrix of the original signals $m_{it}(t)$ and $m_{ir}(t)$.

A. Trapping an Eavesdropper

We would like to attract an eavesdropper to move towards the center of the trap area. Towards this goal, the transmitter uses multiple antennas to place multiple adjacent traps, and adjusts the SNR at trap locations, such that the signal decoding rate increases as the eavesdropper goes across trap locations.

1) Placing Multiple Traps: The transmitter uses M antennas to concurrently transmit the fake signal $m_{it}(t)$ to N trap locations, and the original signal $m_{ir}(t)$ to the receiver. From previous discussion, we know that two antennas can deliver two different signals to two locations simultaneously. In general, $N+1$ antennas can send signals to $N+1$ locations (i.e., N trap locations plus the receiver's location), and thus $M = N+1$. Remember that we use $\mathcal{S} = \{i_1, i_2, \ldots, i_K\}$ and $\bar{\mathcal{S}} = \{p_1, p_2, \ldots, p_K\}$ to denote the sets formed by the indexes of the antennas that transmit the original and the opposite random signals respectively, where $K = \frac{M}{2}$.

We can extend Eq. 10 from one trap location to N trap locations. Let $\alpha_{it}(t) = m_{it}(t) - n_i(t)\sum_{j=1}^{M/2}(h_{i_j}w_{i_j} - h_{p_j}w_{p_j})$, where $i_j \in \mathcal{S}$ and $p_j \in \bar{\mathcal{S}}$. Let $h_{i_{kt_j}}$ denote channel impulse response between the trap location j and the transmitter's k-th antenna, where $j \in \{1, 2, \ldots, N\}$ and $k \in \{1, 2, \ldots, M\}$. Let $x_{i_k}(t)$ denote the signal to be transmitted by the k-th antenna. After generalizing Eq. 10, we get

$$\begin{bmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \cdot \\ x_{i_M}(t) \end{bmatrix} = \mathbf{W}_i^{-1} \begin{bmatrix} h_{i_{1t_1}} & h_{i_{2t_1}} & \cdot & h_{i_{Mt_1}} \\ h_{i_{1t_2}} & h_{i_{2t_2}} & \cdot & h_{i_{Mt_2}} \\ \cdot & \cdot & \cdot & \cdot \\ h_{i_{1t_N}} & h_{i_{2t_N}} & \cdot & h_{i_{Mt_N}} \\ w_{i_1}^{-1} & w_{i_2}^{-1} & \cdot & w_{i_M}^{-1} \end{bmatrix}^{-1} \begin{bmatrix} \alpha_{it}(t) \\ \alpha_{it}(t) \\ \cdot \\ m_{ir}(t) \end{bmatrix}.$$

where $\mathbf{W}_i = diag(w_{i_1}, ..., w_{i_M})$ and w_{i_k} is the weight coefficients selected by the transmitter for the k-th antenna.

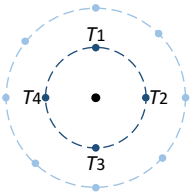


Fig. 3. An example of entrapment.

2) Adjusting SNR: The transmitter would like to control the decoding quality at trap locations. Towards this goal, the transmitter disturbs signal $\alpha_{it}(t)$ by adding a disturbance signal to $\alpha_{it}(t)$. Accordingly, $x_{i_k}(t)$ can be calculated by

$$\begin{bmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \cdot \\ x_{i_M}(t) \end{bmatrix} = \mathbf{W}_i^{-1} \begin{bmatrix} h_{i_{1t_1}} & h_{i_{2t_1}} & \cdot & h_{i_{Mt_1}} \\ h_{i_{1t_2}} & h_{i_{2t_2}} & \cdot & h_{i_{Mt_2}} \\ \cdot & \cdot & \cdot & \cdot \\ h_{i_{1t_N}} & h_{i_{2t_N}} & \cdot & h_{i_{Mt_N}} \\ w_{i_1}^{-1} & w_{i_2}^{-1} & \cdot & w_{i_M}^{-1} \end{bmatrix}^{-1} \begin{bmatrix} \alpha_{it}(t)+D_1(t) \\ \alpha_{it}(t)+D_2(t) \\ \cdot \\ \alpha_{it}(t)+D_N(t) \\ m_{ir}(t) \end{bmatrix}, \quad (11)$$

where $D_j(t)$ is the disturbance signal generated for the j-th trap location. Figure 3 shows a simple example of configuring the SNR. Dots on this figure represent trap locations. The trap location at the center has the highest SNR and the trap locations on the inner circle have weaker SNRs than the center trap location. The trap locations on the outer circle have the weakest SNR. Note that trap locations on the same circle (e.g., T1, T2, T3, and T4) experience the similar SNRs.

The power of the disturbance signal $D_j(t)$ can be selected according to the BER required at the specific trap location. The theoretical BER can be denoted by $\alpha_M Q(\sqrt{\beta_M SNR_{bit}})$ [14], where SNR_{bit} denotes the SNR per information bit, and Q-function is defined as $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{x^2}{2}}dx$, and α_M and β_M are constants determined by the modulation scheme. When we specify the BER at a particular trap location, we can then derive the required SNR using the given BER functions. As we know, SNR is the ratio of the transmit power to the noise power (i.e. $SNR=\frac{P_t}{N_c+P_j}$, where P_t is the transmit power, N_c is the channel noise power and P_j is the disturbance signal power). Since disturbance signal is usually chosen much larger than the channel noise, we neglect the impact from the channel noise on SNR. Now we have both SNR and P_t, we can obtain the disturbance signal power P_j. In general, we can generate a random gaussian noise signal of zero-mean and variance of P_j. Then, we can construct the combined transmit signals by adding disturbance signals to the original transmit signals.

B. Adversarial Indistinguishability

One concern is what happens *if the trap strategy is disclosed and an eavesdropper knows N trap locations have been set up to catch her*? In this case, receiving increasingly better signals can trigger the eavesdropper's alert and cautiousness. She may bypass trap locations and search for the transmitter's signal at other locations. Therefore, we need to achieve adversarial indistinguishability, i.e., making an adversary unable to distinguish the trap from the receiver's location. We define *reception area* as the geographical region centered at the the legitimate receiver. Two requirements should be satisfied in

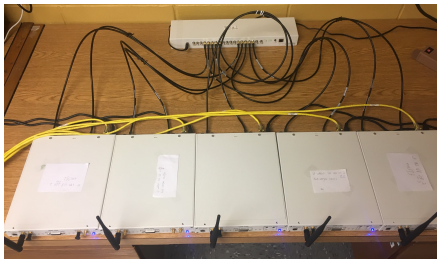


Fig. 4. Five-antenna transmitter with USRPs.

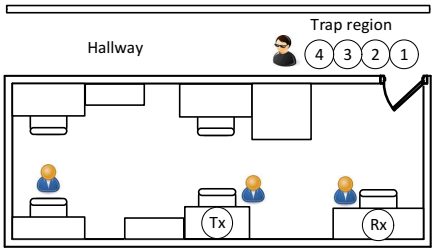


Fig. 5. Experiment environment.

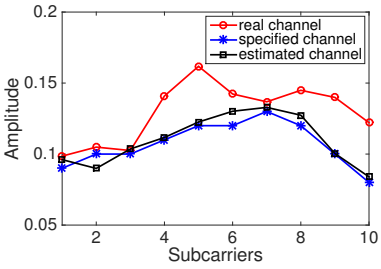


Fig. 6. Specified channel example.

order to achieve adversarial indistinguishability, 1) from an eavesdropper's perspective, the trap area and the reception area should have the same size; 2) when an eavesdropper enters either the reception area or the trap area, she should have the same SNR observation. Two strategies are proposed to provide adversarial indistinguishability.

1) Strategy I: The transmitter also deploys a trap area centered at the receiver's location. Instead of using $N+1$ antennas, as demonstrated in V-A, the transmitter utilizes $M = N + (N-1) + 1$ antennas to create a trap area and a reception area, each consisting of N neighboring trap regions. Accordingly, Eq. 11 can be rewritten into

$$\begin{bmatrix} x_{i_1}(t) \\ x_{i_2}(t) \\ \cdot \\ x_{i_M}(t) \end{bmatrix} = \mathbf{W}_i^{-1} \begin{bmatrix} h_{i_1t_1} & h_{i_2t_1} & \cdot & h_{i_Mt_1} \\ h_{i_1t_2} & h_{i_2t_2} & \cdot & h_{i_Mt_2} \\ \cdot & \cdot & \cdot & \cdot \\ h_{i_1t_{M-1}} & h_{i_2t_{M-1}} & \cdot & h_{i_Mt_{M-1}} \\ w_{i_1}^{-1} & w_{i_2}^{-1} & \cdot & w_{i_M}^{-1} \end{bmatrix}^{-1} \times \begin{bmatrix} \alpha_{it}(t)+D_{t1}(t) \\ \cdot \\ \alpha_{it}(t)+D_{tN}(t) \\ \alpha_{it}(t)+D_{r1}(t) \\ \cdot \\ \alpha_{it}(t)+D_{r(N-1)}(t) \\ m_{ir}(t) \end{bmatrix},$$

where $D_{tj}(t)$ and $D_{rj}(t)$ are the disturbance signals generated for the j-th trap location in the trap area and the reception area respectively. To make the trap area and reception area exhibit the same SNR for an eavesdropper, we let $D_{tj}(t) = D_{rj}(t)$ ($j \in \{1, \cdots, N-1\}$). The transmitter changes the original message $m_{ir}(t)$ into $m_{it}(t) + D_{tN}(t)$, such that when an eavesdropper is at the receiver's location, it will receive the fake message $m_{it}(t)$.

2) Strategy II: We confuse the eavesdropper by using randomization to indistinguish between the trap and reception areas. Specifically, the transmitter works in two modes.

- Trapping mode: the transmitter sets a trap area centered at a selected trap location, while sending secret messages to the receiver, as described in previous Section V-A;
- Disturbing mode: the transmitter sets a trap area centered at the receiver's location, while dismantling the trap area that has been set during the trapping mode.

The transmitter randomly alternates between the trapping mode and the disturbing mode. As a result, when an eavesdropper receives increasingly better signals, she cannot figure out whether she is at the trap area or at the reception area. She faces a dilemma: if she trusts the received signals, she may be trapped, monitored, and arrested. On the other hand, if she chooses to believe that this is a trap area, she will be unable to approach the receiver to steal the true messages.

VI. Experimental Evaluation

A. System Setup and Evaluation Metrics

We build the system on top of USRPs [15]. We use VERT2450 and VERT400 antennas of 2.4GHz and 1.2GHz respectively, and CBX daughter boards operating at the 1.2∼6GHz range as transceivers. The software toolkit is GNURadio [16]. The prototype system includes a transmitter (Tx), a receiver (Rx), and an eavesdropper (Ex). Tx consists of five USRP X300s connected with a host computer through an Ethernet switch, and synchronized with OctoClock-G [17], as shown in Figure 4. Rx and Ex are both standalone USRP X300s connected to PCs. Tx aims to deliver secret messages to Rx, and meanwhile deploy a trap area to mislead Ex. We run experiments in a campus building, with offices, computers, and assorted furniture. Figure 5 shows our experiment topology. We select 4 neighboring trap locations in a hallway to attract Ex. We use BPSK to modulate an OFDM subcarrier, the bandwidth of which is set to 500KHz in our experiments. We consider a total of 64 subcarriers, including 48 occupied tones (i.e., subcarriers that are used for actual data transmission).

We utilize the following evaluation metrics: (1) SNR: the ratio of the power of a signal of interest to that of of noise signals, including disturbance signals plus the channel noise; (2) Packet error rate (PER): the number of packets that are unsuccessfully decoded at the receiver to the number of totally received packets; (3) BER: the ratio of the number of incorrectly received bits to the total number of received bits; and (4) Channel similarity rate (CSR): it is utilized to model the relationship between the calculated Euclidean distance of two channels and channel similarity, denoted with $\rho = 1 - \frac{d}{d_0}$, where d is the Euclidean distance of two channels and the d_0 is the threshold, above which the two channels are thought to be quite different (i.e., measured at different places).

PER is used to evaluate the packet reception performance. Here, we append a data packet with a 4-byte cyclic redundancy check (CRC) code for error detection, and this packet is regarded as correctly decoded if it can successfully pass the CRC check. Both BER and PER can demonstrate the throughput performance of a communication system. However, PER reflects the link quality at a coarse-grained level, while BER provides a fine-grained indication of the link quality.

B. Specified Channel Example

To establish the specified channel with Rx, Tx first estimates the real channel between itself and Rx, and then calculates

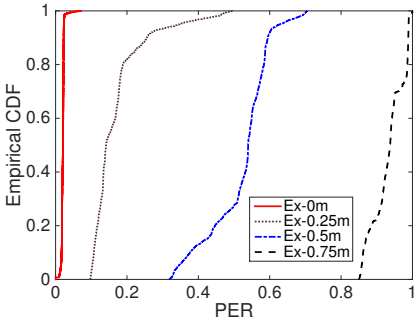


Fig. 7. Eavesdropper's PER.

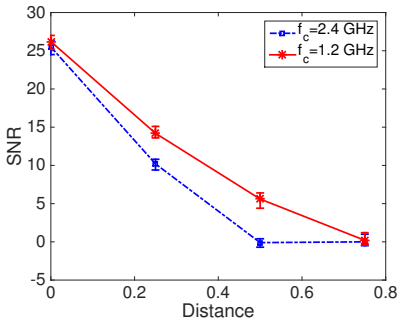


Fig. 8. Trap region exploration.

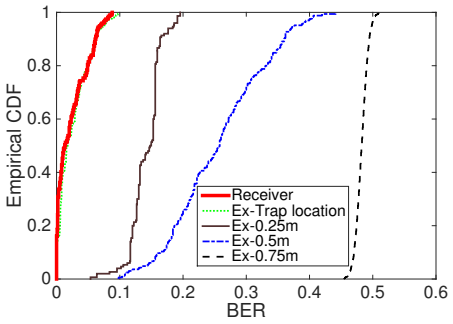


Fig. 9. Receiver's and Eavesdropper's BERs.

the weight coefficients. Figure 6 shows a specified channel example across 10 subcarriers. We can see that the estimated channel at Rx is similar to the channel specified at Tx, and both channels significantly deviate from the real channel. This demonstrates the feasibility of constructing a specified camouflage channel between the transmitter and the receiver.

To measure the concealment capability of the specified camouflage channel, we measure and compare the SNRs for Ex at different distance away form Rx. We calculate SNR as $10 * log_{10} \frac{P_{signal}}{P_{noise}}$. We draw a circle originating at Rx and place Ex at a radius ranging outward from 0.25 to 1 meter every 0.25m. Table I shows the results of the observed SNRs at the receiver and the eavesdropper. We can see that SNR at the receiver is much higher than that at the eavesdropper. With the distance between the eavesdropper and the receiver increasing, both the calculated channel similarity ρ and observed SNR gradually decrease. In particular, when the eavesdropper is 0.75m away from Rx, the observed SNR is as low as 0.2 dB, which is below the required SNR for the eavesdropper to correctly decode received messages.

TABLE I
OBSERVED SNRS AT DIFFERENT LOCATIONS

	Rx	Ex-0.25	Ex-0.50	Ex-0.75	Ex-1
ρ	0.8889	0.5926	0.3333	-0.0741	-0.0370
SNR (dB)	25.04	12.2	1.8	0.2	-0.1

Without specified channel, the eavesdropper at around the receiver is more likely to intercept secret messages. Figure 7 shows the calculated PER at the eavesdropper when she is at the exact receiver's location and the locations that are 0.25m, 0.5m, 0.75m away from the receiver's location respectively. We can see that without specified channel, when the eavesdropper reaches the exact location of the receiver, the packet error rate is less than 0.025 with a probability of 98.5%, i.e., secret communication between the transmitter and the receiver cannot be guaranteed. Meanwhile, the observed PER reduces as the eavesdropper moves closer to the receiver.

However, due to the existence of the specified channel, the PER observed by the eavesdropper is always close to 100%. Because of failures in decoding received messages, the eavesdropper will continue to search for other locations that can enable her to correctly decode received messages.

C. SNR and BER at a Trap Location

After establishing a specified channel, Tx begins to send true messages to Rx and meanwhile fake messages to Ex. In our experiment, we select Location 1 (as shown in Figure 5) as a trap location. We first move Ex to Location 1 and record the observed SNR, and then gradually increase the distance d between Ex and the trap location at a step of 0.25m.

SNR analysis: Central carrier frequency can also affect the size of the trap region as its change can cause the change of the signal wavelength and accordingly the distance required for the channel uncorrelation. Figure 8 shows the observed SNRs at Ex when we gradually move it away from the trap location for different central frequencies. We can see that for 2.4GHz, when Ex is 0.5m away from the trap location, the observed SNR at Ex approaches to 0. This means that the radius of the trap region is about 0.5m, whereas for 1.2GHz, a larger radius of 0.75m can decrease SNR to a value that is approximately equal to 0. Thus, the size of a trap region can be changed by adjusting the central frequency.

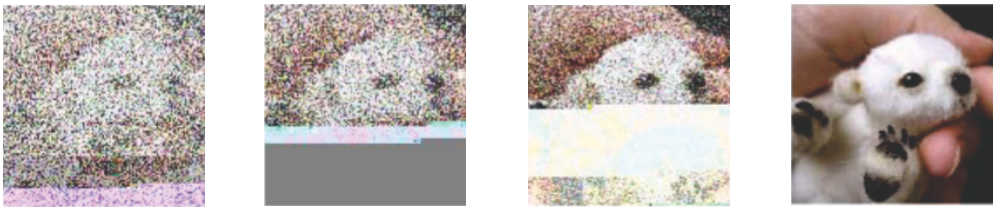
BER analysis: Figure 9 compares the BER at Rx with that encountered by Ex when Ex is 0m, 0.25m, 0.50m, and 0.75m from a trap location. We can see that both Rx and Ex at the trap location can obtain low BERs below 0.06 with a probability of 90%. This means that our scheme can successfully enable Rx to obtain a true message and Ex entering the trap location to receive a fake message. Meanwhile, the BER observed by Ex increases as Ex moves away from the trap location. In particular, when Ex is 0.75m away from the trap location, the observed BER is close to 0.5, and hence it is difficult for Ex to receive any meaningful message.

D. Deployment of Multiple Traps

We select four neighboring trap locations (Location 1 to 4) and choose Location 1 as the center, as shown in Figure 5. We add a disturbance noise signal to the fake picture and then transmit them to trap locations. Figure 10 shows the picture received by the eavesdropper when she enters the trap area. We can see that the eavesdropper experiences the best picture quality when she is at Location 1, and the picture quality increases as the eavesdropper moves from Locations 4 to 1. Thus, the eavesdropper will be eventually guided to Location 1 if she searches for pictures of high quality.

VII. RELATED WORK

MIMO has been widely studied due to its capability of improving the spectral efficiency of wireless systems [18]–[21]. MU-MIMO, as an advanced MIMO, has drawn increas-



(a) Location 4 (b) Location 3 (c) Location 2 (d) Location 1

Fig. 10. We transmit a picture to the trap area. We select Location 1 as the trap center, where an eavesdropper can obtain the highest SNR. Here, the eavesdropper receives pictures with increasing quality as the eavesdropper moves from Location 4 to Location 1.

ing attention in recent years [22], [23], enabling a transmitter with multiple antennas to concurrently transmit messages to different receivers. The proposed system also uses multiple antennas but completely differs from a traditional MU-MIMO.

First, the proposed system provides secret communication. We achieve this by (1) constructing a specified channel between the transmitter and the receiver, and (2) inserting random signals to original signals, such that the random signals disrupt the decoding at an eavesdropper but cancel at a receiver. Second, instead of merely aiming to increase diversity or multiplexing gain, the proposed system aims to create a trap area. Due to the existence of specified channels and random signals, we cannot simply adopt the traditional MU-MIMO to pre-code transmit signals. Accordingly, we create a technique compatible to the randomization channel design. The proposed technique not only transmits messages to multiple potential wireless devices, but, more importantly, it can entrap an eavesdropper to move towards a target location.

Though our work and friendly jamming technique [6]–[8] both utilize the constructive signal canceling, they have multiple differences. First, both methods take different strategies. Friendly jamming disrupts unauthorized communication and enables authorized receiver to get services, while our work enables adversaries to receive meaningful signals and makes legitimate parties communicate securely. Second, our work sets up an entrapment by attracting an eavesdropper to observe increasing SNR, while friendly jamming makes an eavesdropper unsuccessfully decode the message. Furthermore, the two tasks in our scheme, i.e., the secret communication between legitimate parties and the entrapment for adversaries, are parallel, while friendly jamming has no such design.

VIII. Conclusion

In this paper, we design an entrapment wireless system that attracts an eavesdropper to a specified trap location, where the eavesdropper can obtain a meaningful but fake message. We create techniques that can enable a transmitter to establish a secure communication channel with the desired receiver. We also create techniques that can utilize multiple antennas to generate a large trap area to increase the probability of successfully entrapping an eavesdropper. We perform real-world evaluation on the USRP X300 platforms running GNURadio to validate the performance of the proposed scheme.

ACKNOWLEDGEMENT

This work was supported in part by NSF CNS-1553304, CNS-1717969, and ARO W911NF-17-1-0180.

References

[1] E. Shi and A. Perrig, "Designing secure sensor networks," *IEEE Wireless Communications*, vol. 11, pp. 38–43, Dec 2004.
[2] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proc. ACM CCS*, 2007.
[3] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. on Wireless Communications*, vol. 7, no. 6, pp. 2180–2189, 2008.
[4] S. Fang, I. Markwood, and Y. Liu, "Manipulatable wireless key establishment," in *IEEE CNS*, pp. 393–401, Oct 2017.
[5] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. on Info. Forensics and Security*, vol. 6, pp. 256–266, June 2011.
[6] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. IEEE INFOCOM*, 2011.
[7] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time," in *Proc. IEEE Symposium on Security and Privacy*, 2013.
[8] D. S. Berger, F. Gringoli, N. Facchi, I. Martinovic, and J. Schmitt, "Gaining insight on friendly jamming in a real-world IEEE 802.11 network," in *Proc. ACM WiSec*, 2014.
[9] A. Moradi, A. Barenghi, T. Kasper, and C. Paar, "On the vulnerability of FPGA bitstream encryption against power analysis attacks: Extracting keys from Xilinx Virtex-II FPGAs," in *Proc. ACM CCS*, 2011.
[10] D. X. Song, D. Wagner, and X. Tian, "Timing analysis of keystrokes and timing attacks on ssh," in *USENIX Security Symposium*, 2001.
[11] C. Kaufman, R. Perlman, and M. Speciner, *Network security : private communication in a public world*. Prentice Hall series in computer networking and distributed systems, Upper Saddle River (N. J.): Prentice Hall, 2002.
[12] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Čapkun, "On limitations of friendly jamming for confidentiality," in *Proc. IEEE Symposium on Security and Privacy*, 2013.
[13] S. Fang, Y. Liu, and P. Ning, "Mimicry attacks against wireless link signature and new defense using time-synched link signature," *IEEE Trans. on Information Forensics and Security*, vol. 11, pp. 1515–1527, July 2016.
[14] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.
[15] "USRP X300." https://www.ettus.com/product/details/X300-KIT, 2018.
[16] "GNU Radio Software." http://gnuradio.org, 2018.
[17] M. Ettus, "USRP user's and developer's guide," *Ettus Research LLC*, 2005.
[18] L. Zheng and D. N. C. Tse, "Diversity and multiplexing: a fundamental tradeoff in multiple-antenna channels," *IEEE Trans. on Information Theory*, vol. 49, pp. 1073–1096, May 2003.
[19] D. Gesbert, M. Kountouris, R. W. H. Jr., C. b. Chae, and T. Salzer, "Shifting the MIMO paradigm," *IEEE Signal Processing Magazine*, vol. 24, pp. 36–46, Sept 2007.
[20] E. Aryafar, N. Anand, T. Salonidis, and E. W. Knightly, "Design and experimental evaluation of multi-user beamforming in wireless lans," in *Proc. ACM MobiCom*, pp. 197–208, ACM, 2010.
[21] X. Xie, E. Chai, X. Zhang, K. Sundaresan, and A. K. S. Rangarajan, "Hekaton: Efficient and practical large-scale MIMO," in *Proc. ACM MobiCom*, pp. 304–316, ACM, 2015.
[22] Y.-C. Tung, S. Han, D. Chen, and K. G. Shin, "Vulnerability and protection of channel state information in multiuser MIMO networks," in *Proc. ACM CCS*, 2014.
[23] S. Sur, I. Pefkianakis, X. Zhang, and K.-H. Kim, "Practical MU-MIMO user selection on 802.11ac commodity networks," in *Proc. ACM MobiCom*, pp. 122–134, ACM, 2016.