Signal Entanglement based Pinpoint Waveforming for Location-restricted Service Access Control

Tao Wang†, Yao Liu†, Tao Hou†, Qingqi Pei‡ and Song Fang†
†University of South Florida, Tampa, FL
‡Xidian University, Xi'an, China
{taow@mail, yliu@cse, taohou@mail, songf@mail}.usf.edu, qqpei@mail.xidian.edu.cn

Abstract—We propose a novel wireless technique named pinpoint waveforming to achieve the location-restricted service access control, i.e., providing wireless services to users at eligible locations only. The proposed system is inspired by the fact that when two identical wireless signals arrive at a receiver simultaneously, they will constructively interfere with each other to form a boosted signal whose amplitude is twice of that of an individual signal. As such, the location-restricted service access control can be achieved through transmitting at a weak power, so that receivers at undesired locations (where the constructive interference vanishes), will experience a low signal-to-noise ratio (SNR), and hence a high bit error rate that retards the correct decoding of received messages. At the desired location (where the constructive interference happens), the receiver obtains a boosted SNR that enables the correct message decoding. To solve the difficulty of determining an appropriate transmit power, we propose to entangle the original transmit signals with jamming signals of opposite phase. The jamming signals can significantly reduce the SNR at the undesired receivers but cancel each other at the desired receiver to cause no impact. With the jamming entanglement, the transmit power can be any value specified by the system administrator. To enable the jamming entanglement, we create the channel calibration technique that allows the synchronization of transmit signals at the desired location. We develop a prototype system using the Universal Software Defined Radio Peripherals (USRPs). The evaluation results show that the receiver at the desired location obtains a throughput ranging between 0.9 and 0.93, whereas an eavesdropper that is 0.3 meter away from a desired location has a throughput approximately equal to 0.

Index Terms—Location-restricted service; Pinpoint waveforming; Access control; MIMO

1 Introduction

With the rapid development of wireless technologies, it is highly desirable to enforce location-restricted service access control that provides wireless services to users at eligible locations only. For example,

- Companies may allow wireless network access only to employees working in selected office cubicles, in order to comply export control policies.
- In wireless surveillance system, the monitor cameras may need to deliver their video streams to specific users at specific locations, e.g, personnel in the security control room, to reduce the privacy leakage.
- To focus limited resources on legitimate customers, restaurants and cafes may offer internet access to wireless users only when they are sitting at tables.

Surprisingly, existing techniques fail to achieve this goal in a secure and efficient manner. We discuss existing techniques and their shortcomings below.

- **User account control:** The service access control can be achieved by creating individual accounts for each user, where a user can obtain the wireless service by providing a correct username and password. However, this may be insufficient for secure access control to location-restricted services, as a user might share the account information with friends. This method also requires active account administration which is impractical for location-restricted services with high turnover such as in the restaurant example.
- **MAC address binding:** MAC address binding is a variant of the user account control. A wireless router allows the access of wireless users only when they have valid Media Access Control (MAC) addresses. Nevertheless, users may share their MAC addresses with others who are not at the desired locations.
- **Beamforming techniques:** Beamforming techniques (e.g., [1], [2]) use antenna arrays for directional signal transmission or reception. These techniques may be utilized to send the service data to wireless users at the specified directions, but again they cannot enable the location-restricted service access control, because all other wireless users are able to receive the service data as long as they reside in the signal coverage range of the antenna arrays.
- **Localization plus encryption:** Service providers may use existing localization algorithms like time-of-arrival (TOA) and angle-of-arrival (AOA) to find the locations of wireless users, and encrypt the service data so that users at target locations can use appropriate keys to decrypt it. However, cryptographic encryption may cause a significant latency, and thus fail to support common services like high-speed downloading and online video watching. Also, like the password case, with compromised cryptographic

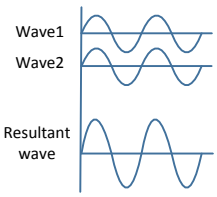


Fig. 1: Constructive interference of two waves.

Fig. 2: A naive idea

keys, undesired receivers at other locations can still obtain the service.

In this paper, we would like to develop a novel and practical wireless system that achieves the aforementioned location-restricted service access control to support emerging wireless requirements. Our basic idea is to leverage the effect of *constructive interference* as shown in Figure 1. The crests of two identical waves meet at the same point, and both waves form a new wave with the same shape but the magnitude is boosted to twice of that of an individual wave.

This observation inspires us to propose a new wireless system that pinpoints wireless services to users at eligible locations only. Intuitively, we can set up a naive system as illustrated in Figure 2. The service provider concurrently sends identical service packets (e.g., down-link internet data) using two (or more) transmitters. Assume an ideal synchronization algorithm is in use and these packets arrive at the receiver at the service location simultaneously. Thus, they constructively interfere with each other to form a boosted received packet whose magnitude is twice of that of an individual packet.

In practice, a small time shift among the packet arrival times may exist due to synchronization imperfections. At the service location, such a time shift should be less than a certain threshold, so that the constructive interference still exists and the receiver is able to decode received packets. To prevent leaking the service to undesired receivers, including receivers close to the service provider, an intuitive way is to transmit at a weak power so that receivers at undesired locations (where the constructive interference vanishes) will experience a low signal-to-noise ratio (SNR), and hence a high bit error rate that retards the correct decoding of received messages. At the desired location (where the constructive interference happens), the receiver obtains a boosted SNR that enables the correct message decoding.

However, how to select an appropriate signal transmit power becomes a challenging question. If the transmit power is too small, the constructive interference may not incur enough power to allow receivers at the service location to correctly decode the received data. On the other hand, if the transmit power is too large, receivers outside of the service location may recognize the signal and thus can decode the received data. To avoid the difficulty of determining the transmit power, we propose to entangle the original transmit signals with jamming signals, so that the jamming signals can significantly reduce the SNR at the undesired receivers but cancel each other at the desired receiver to cause no impact.

Specifically, for a pair of transmitters T_1 and T_2, we generate a pair of jamming signals j_1 and j_2, where j_1 and j_2 are of the opposite phase (i.e., $j_1 = -j_2$). The transmitter T_1 then adds the jamming signal j_1 to its transmit signal. Similarly, T_2 adds the jamming signal j_2 to its transmit signal. Finally, T_1 and T_2 send $s + j_1$ and $s + j_2$ to the wireless channel respectively, where s is the original signal to be sent by both transmitters. At the service location, due to the constructive interference, the original signal s boosts, but the jamming signals j_1 and j_2 cancel each other (they are of opposite phase). At other locations where constructive interference vanishes, j_1 and j_2 do not cancel each other, and instead they serve as jamming signals to decrease the SNR at receivers at these locations. Consequently, the receivers will experience a service of bad quality.

We point out that in an ideal free space propagation environment, constructive interference of electromagnetic waves occur whenever the phase difference between the waves is a multiple of a half period. This means there exist multiple locations, where the constructive interference may happen. However, in a practical wireless environment, because wireless channels are uncorrelated, every a half wavelength, the original transmit signals sent by different transmitters may experience different channel distortions when they propagate to the receiver. Therefore, at the locations where the constructive interference should happen, signals received from different transmitters show different shapes due to distortions and thus achieve a poor constructive interference. To solve this problem and pinpoint the service to the desired location only, we propose a channel synchronization technique that compensates the channel distortion at the desired constructive interference location, so that received signals exhibit the same wave shape when they arrive at this location. The channel synchronization technique is customized for the desired location only. For other constructive interference locations, the arrived signals still show different shapes, thereby yielding the same low SNR as other non-constructive interference locations as proved in Section 6.2.

We name the proposed system as the *pinpoint waveforming* system. Figure 2 is a naive example of this system. Nevertheless, to transform this naive system to a real-world system, non-trivial effort should be done to answer the following basic questions:

- **Synchronization:** How can the system achieve propagation synchronization, so that signals sent by multiple transmitters can arrive at the service location concurrently? Moreover, how can we achieve the aforementioned channel synchronization?
- **Tolerable time shift:** Signals sent by transmitters are expected to arrive at the desired receiver simultaneously to form the constructive interference, but in practice a small time shift among them might exist due to the processing delay and synchronization imperfections. What is the tolerable time shift that can still enable the constructive interference at the desired receiver?
- **Service area size:** The service area is defined as the neighborhood area, within which the constructive interference happens and receivers can receive the

service data with a good quality. It should be hard for receivers outside of the service area to obtain the data. To ensure the accurate service access control, a critical question is how large the service area is.

In this paper, we demonstrate the feasibility of the pinpoint waveforming system by answering the above essential concerns about synchronization, tolerable time shift, and service area size. We further analyze how entangled jamming signals improve the SNR of the receiver at the desired location. In addition, we further investigate the impact of tolerable time shift on SNR in multi-transmitter scenario, and exhibit the relationship between the expected SNR of the desired receiver and the number of transmitters. We also explore the service area size using channel uncorrelation property in multi-transmitter scenario. The analysis shows that the proposed technique can still enable a small service area size with multiple transmitters. Furthermore, we give a detail discussion on how to integrate the proposed scheme into traditional multiple access techniques (e.g. CDMA, TDMA, FDMA) to support multiple users.

We implement a prototype of the pinpoint waveforming system on top of the Universal Software Radio Peripherals (USRPs), and evaluate the performance of the prototype system through comprehensive experiments. Our results show that receivers obtain a high throughput ranging between 0.90 and 0.93 when they are at the desired location, but this throughput dramatically decreases when receivers are moved from the desired location. In particular, at a distance of 0.3 meter, throughput of receivers approaches to 0.

2 Synchronization

We discuss synchronization first, because synchronization is the basis for the proposed pinpoint waveforming system to achieve the constructive interference of original signals and the cancelation of the jamming signals. Synchronization includes three components, and they are *clock synchronization*, *propagation synchronization*, and *channel synchronization*.

2.1 Clock and Propagation Synchronization

Clock synchronization deals with the discrepancy of the clocks of multiple transmitters, so that they transmit service packets at the same time. In the proposed system, all transmitters are connected to the same service provider, and thereby their clocks are roughly the same.

The distances between the receiver and each transmitter may be different. Accordingly, signals sent by these transmitters may arrive at the receiver at different time even if they are sent at the same time. To compensate the propagation difference, the service provider needs to perform propagation synchronization through adjusting the transmit time of each transmitter. Propagation synchronization has been extensively studied in the context of wireless sensor networks (e.g., [3], [4]). In a traditional way, the receiver broadcasts a beacon signal, and the service provider adjusts each transmitter's transmit time based on beacon arrival time recorded at this transmitter [5]. Since transmitter clocks are inherently the same, the proposed system is compatible with the traditional synchronization approach.

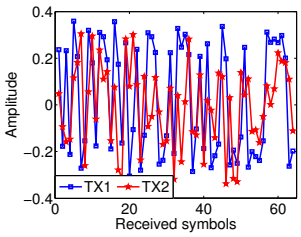


Fig. 3: Without channel synchronization

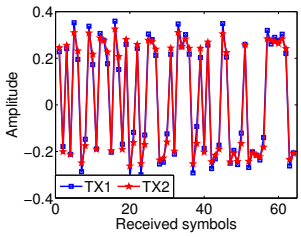


Fig. 4: With channel synchronization

Note that after clock and propagation synchronization, due to the processing delay and synchronization imperfections, the time shift will still exist between the signal arrival times. In section 5, we show the impact of the time shift and the maximum time shift that can be tolerated by the system.

2.2 Channel Synchronization

The impact of channel effect cannot be neglected. The signals sent by different transmitters may undergo different channel effects. When the signals arrive at the receiver, their shapes accordingly exhibit different distortions, and thus the constructive interference may diminish due to the wave shape discrepancy. The transmit (jamming) signals should be calibrated so that they have the same (reverse) shapes when they arrive at the receiver.

Figure 3 shows a real measured example of the channel impact without the channel synchronization. Two transmitters are separated by a certain distance to result in uncorrelated channels (i.e., 0.75 meter for a 2.4 GHz channel). The receiver is 3 meters away from both transmitters. Each device is a USRP connected to a PC. Both transmitters send the same sequence of 64 symbols (i.e., the transmission unit at the wireless physical layer) to the receiver. As seen in Figure 3, the amplitude of symbols received from both transmitters are different from each other due to the different channel distortions. Figure 4 shows the amplitude of received symbols after the channel synchronization. Both received symbols then become similar to each other.

Signal modulation: Before we discuss the proposed channel calibration algorithm, we first introduce the signal modulation/demodulation to facilitate the reader's understanding. We focus our discussion on I/Q modulation, because it is widely used in modern wireless systems. In I/Q modulation, signals are transmitted in the form of symbols, which are the transmission unit at the wireless physical layer. We use Quadrature Phase-Shift Keying (QPSK) modulation, a typical I/Q modulation, as an example to show how I/Q modulation works.

QPSK encodes two bits into one symbol at a time. In Figure 5 (a), bits 00, 01, 10, and 11 are represented by points whose coordinates are (-1,-1), (-1,1), (1,-1), and (1,1) in an I/Q plane, respectively. The I/Q plane is called a *constellation diagram*. A symbol is the coordinate of a point on the constellation diagram. Due to the channel noise, a received symbol is not exactly the same as the original symbol sent by the sender. To demodulate, the receiver outputs the point that is closest to the received symbol on the constellation diagram as the demodulation result.

2.2.1 Basic Channel Synchronization

Same signals from different transmitters will exhibit distinct wave shapes when they come to the receiver, because they undergo different channel distortions. Thus, on the constellation diagram, the receiver not only receives multiple symbols from multiple transmitters at the same time, but these symbols have different phases and amplitudes. As an example shown in Figure 5 (a), the receiver receives four symbols from four transmitters and these symbols are at different positions on the constellation diagram. Received symbols can interfere with each other, and consequently it becomes difficult for the receiver to correctly decode received packets. Hence, channel synchronization is required in the scheme so that received symbols can converge to the same ideal point to form a good constructive interference.

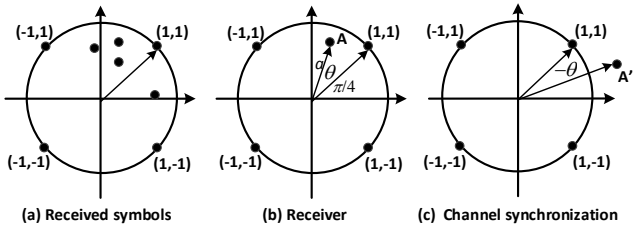


Fig. 5: Basic channel synchronization

In our basic idea, we propose to calibrate the symbols before they are transmitted to offset the channel distortion. As shown in Figure 5 (b), the original symbol sent by the transmitter is (1,1) and the corresponding received symbol is at point A on the constellation diagram. For QPSK, the angle between the ideal point (1, 1) and the horizontal axis is $\frac{\pi}{4}$. Thus, the coordinate of the received symbol can be represented by $(\frac{\sqrt{2}}{2}a\cos(\theta+\frac{\pi}{4}), \frac{\sqrt{2}}{2}a\sin(\theta+\frac{\pi}{4}))$, where a is amplitude attenuation factor, and θ is the phase shift between the received symbol and the ideal point (1, 1).

Channel synchronization aims to calibrate the received symbols to the corresponding ideal points. Toward this end, rather than transmitting the ideal points, the transmitter transmits symbols that deviate from the ideal points in a way that offset the channel distortion. As shown in Figure 5 (c), the transmitter transmits a symbol A', whose phase shift from the ideal point (1,1) is $-\theta$ and the magnitude is $\frac{1}{a}$, in lieu of the ideal point (1, 1). Thus, the coordinate of the calibrated symbol is $(\frac{\sqrt{2}}{2a}\cos(\frac{\pi}{4}-\theta), \frac{\sqrt{2}}{2a}\sin(\frac{\pi}{4}-\theta))$. When this symbol arrives at the receiver, the calibration offset cancels the channel effect, and thereby the received symbol will converge to the ideal point.

The transmitter needs to know θ and a for the channel synchronization. Due to the channel reciprocity property, the wireless channel remains the same if the roles of the transmitter and the receiver are exchanged [6]. Thus, training stages can be utilized for the transmitter to measure θ and a from the training symbols sent by the receiver. To further reduce the communication overhead, the transmitter can obtain θ and a in the piggyback way. Specifically, it can measure them from the symbols that are contained in the existing up-link packets (e.g., service request packets and acknowledgement packets) sent by receivers.

2.2.2 Refined Channel Synchronization against the Multipath Effect

Multipath effect is the phenomena that signals sent by the transmitter travel along multiple paths to reach the receiver. Thus, the receiver can receive multiple copies of the original signal from the multiple paths. These signal copies can interfere with each other and confuse the receiver to obtain an incorrect message decoding results.

The signal propagation paths can be generally classified as unresolvable and resolvable paths. For a transmitted symbol, the copies traveling on unresolvable paths arrive at the receiver with an arrival time difference less than one symbol duration, i.e., the transmission time of one symbol. Thus, they form one symbol on the constellation diagram. For resolvable paths, the copies traveling on these paths arrive at the receiver with a time difference larger than one symbol duration, and therefore on the constellation diagram they form separate symbols that interfere future transmitted symbols. In this paper, we only consider the impact of signal copies from resolvable paths, because they are the major factors that contribute to the inter-symbol interference and the decoding failures. Specifically, for L resolvable paths, the receiver will then receive L copies of subsequently transmitted symbols.

Figure 6 (a) shows an example of a 3-path channel. The transmitter transmits three symbols S_0, S_1, and S_2. At time t_0, the receiver receives S_0 from Path 1. At time t_1, the receiver receives S_1 from Path 1 and a delayed copy of S_0 from Path 2. At time t_2, the receiver receives S_2 from Path 1, the delayed copy of S_1 from Path 2, and the delayed copy of S_0 from Path 3.

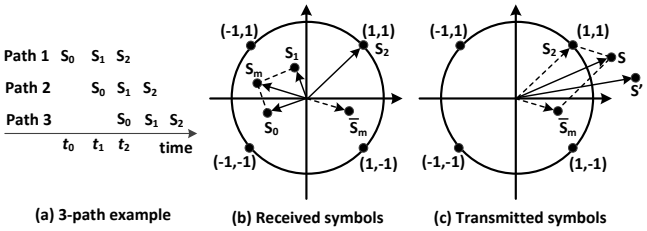


Fig. 6: Refined channel synchronization against the multipath effect

We propose to cancel the interference caused by multipath symbols via adding a complementary symbol to the transmitted symbol. Specifically, Figure 6 (b) shows the snapshot of the constellation diagram at time t_2 for the aforementioned 3-path channel, the superposed impact of the delayed copies of S_0 and S_1 can be represented by an equivalent symbol S_m, which is the vector sum of S_0 and S_1. To eliminate the multipath symbols, in addition to sending the desired symbol S_2, the transmitter also needs to send a cancelation symbol $\bar{S_m}$ that is at the reverse position of S_m. The magnitude of S_m and $\bar{S_m}$ are the same but $\bar{S_m}$ shifts from S_m by an angle of π. As shown in figure 6 (c), the vector sum of the desired symbol S_2 and $\bar{S_m}$ is S. Thus, the transmitter performs the basic synchronization to calibrate S to S' to resist against the channel noise, and the actually transmitted symbol is S'.

We would like to point out that $\bar{S_m}$ can only eliminate multipath effects from previous symbols S_0 and S_1.

However, subsequent symbols will still be interfered by the calibrated $\bar{S_m}$ due to multipath effects. So all these symbols should be calibrated in the same way, and the i-th symbol can be calibrated only after all its previous $L-1$ symbols are already calibrated. We discuss the details in Section 3.

3 Multipath Channel Calibration

To achieve the channel calibration, the transmitter must first get the channel impulse response (CIR), which includes the amplitude attenuation coefficient, phase shift, and the effects of the multipath propagation. Traditionally, channel estimation algorithms [7] are applied at the receiver to adapt received signals to the current channel conditions. However, we cannot directly use these methods in the proposed scheme, because we require that signals to reach the receiver with same shapes to gain the constructive interference. Inspired by the channel reciprocity that the channel effects observed by the transmitter and the receiver are the same during the communication, we propose to directly estimate the CIR at the transmitter and then use this information to calibrate the transmit signals.

3.1 Preliminary

To facilitate the presentation of the proposed technique, we first give the preliminary knowledge about the channel estimation. Channel is usually estimated using a predefined training sequence that are composed of multiple symbols. Specifically, the training sequence is known to both the transmitter and the receiver prior to their communication. The transmitter sends the training sequence to the receiver through the wireless channel, and upon receiving, the receiver uses the original training sequence and the received copy to estimate the channel.

In general, the received training sequence is distorted by both channel effects and the noise. It can be expressed by $\mathbf{r} = \mathbf{h} * \mathbf{d} + \mathbf{n}$, where $\mathbf{h}$ is the channel state information, $\mathbf{d}$ is the original training sequence, $*$ is the convolution operator, and $\mathbf{n}$ is the channel noise that is normally considered as a zero-mean Gaussian noise. We can rewrite this equation in the matrix form below.

$$\mathbf{r} = \begin{bmatrix} d_1 & 0 & . & 0 \\ d_2 & d_1 & . & 0 \\ . & . & . & . \\ d_L & d_{L-1} & . & d_1 \\ . & . & . & . \\ d_K & d_{K-1} & . & d_{K-L+1} \end{bmatrix} \begin{bmatrix} h_1 \\ h_2 \\ . \\ . \\ h_L \end{bmatrix} + \mathbf{n},$$

where vector $[d_1, d_2, ..., d_k]^t$ denotes the known training data $\mathbf{d}$, vector $[h_1, h_2, ..., h_L]^t$ denotes the unknown channel $\mathbf{h}$, and vector $[n_1, n_2, ..., n_k]^t$ denotes the unknown channel noise $\mathbf{n}$. Note that k is the length of the training sequence and it must be larger than L to enable the channel estimation.

To facilitate our analysis, we rewrite the above matrix equation into the compact form and we can obtain $\mathbf{r} = \mathbf{Dh} + \mathbf{n}$. Normally, least-square (LS) estimator can be used to solve $\mathbf{h}$ from the compact equation for channel estimation [9], yielding the estimation result $\hat{\mathbf{h}} = \{\mathbf{D^H D}\}^{-1}\mathbf{D^H r}$, where H denotes the complex conjugate transpose operator.

In our scheme, channel estimation is done at the transmitter, and the training sequence is sent from the receiver. Due to the channel reciprocity property, the channel estimated by the transmitter will represent the channel between itself and the receiver. To cope with the channel changes, the training sequence can be sent periodically so that the transmitter can capture the current CIR.

3.2 Advanced Channel Calibration

As discussed earlier, we propose to construct a complementary symbol for each transmitted symbol to cancel the multipath effect. The complementary symbol for the i-th transmitted symbol is constructed not only based on the i-th transmitted symbol but also based on $L-1$ previously transmitted symbols.

Obtaining calibrate symbols: Let $\hat{\mathbf{h}} = [\hat{h_1}, \hat{h_2}, ..., \hat{h_L}]^T$ denote the estimated channel, and $\mathbf{d_r} = [d_{1_r}, d_{2_r}, ..., d_{k_r}]^T$ denote the desired, interference-free received symbols. Further let $\mathbf{d_t} = [d_{1_t}, d_{2_t}, ..., d_{k_t}]^T$ denote the calibrated symbols to be transmitted to the receiver. Note that $\mathbf{d_t}$ combines both complementary and original symbols. At time t_0, d_{1_t} is sent and it arrives at the receiver through the first path. The corresponding received symbol is $d_{1_r} = d_{1_t} \cdot \hat{h_1}$. At time t_1, d_{2_t} is sent, it arrives at the receiver through the first path, and meantime the multipath copy of d_{1_t} arrives through the second path. The second received symbol can hence be presented as $d_{2_r} = d_{1_t}\hat{h_2} + d_{2_t}\hat{h_1}$. Finally, at time t_k, the receiver will receive both the symbol d_{k_t} via the first path and the multipath copies of the previous $L-1$ symbols. The received symbol d_{k_r} is $d_{k_r} = \sum_{i=1}^{L} d_{k-i+1_t}\hat{h_i}$. We rewrite this linear relation using the matrix form and we obtain:

$$\begin{bmatrix} d_{1_r} \\ d_{2_r} \\ . \\ . \\ d_{k_r} \end{bmatrix} = \begin{bmatrix} d_{1_t} & 0 & . & 0 \\ d_{2_t} & d_{1_t} & . & 0 \\ . & . & . & . \\ d_{L_t} & d_{L-1_t} & . & d_{1_t} \\ . & . & . & . \\ d_{k_t} & d_{k-1_t} & . & d_{k-L+1_t} \end{bmatrix} \begin{bmatrix} \hat{h_1} \\ \hat{h_2} \\ . \\ . \\ \hat{h_L} \end{bmatrix}$$

We use the compact matrix form $\mathbf{d_r} = \mathbf{D_t}\hat{\mathbf{h}}$ to represent the above equation. Because $\mathbf{D_t}$ includes the calibrated symbols to be sent by transmitters, we would like to solve $\mathbf{D_t}$ from this equation. Intuitively, it can be computed by $\mathbf{D_t} = \mathbf{d_r}\hat{\mathbf{h}}^{\mathbf{H}}\{\hat{\mathbf{h}}\hat{\mathbf{h}}^{\mathbf{H}}\}^{-1}$. However, since $\hat{\mathbf{h}}$ is a column vector, $\hat{\mathbf{h}}\hat{\mathbf{h}}^{\mathbf{H}}$ is always a singular matrix and it's not feasible to find its matrix reverse $\{\hat{\mathbf{h}}\hat{\mathbf{h}}^{\mathbf{H}}\}^{-1}$.

In the proposed scheme, the desired data $[d_{1_r}, d_{2_r}, ..., d_{k_r}]$ and channel impulse response $[\hat{h_1}, \hat{h_2}, ..., \hat{h_L}]$ are known. We can thus find $\mathbf{D_t}$ by recursively solving linear equations. Specifically, the first calibrated symbol d_{1_t} can be directly calculated by $d_{1_t} = \frac{d_{1_r}}{\hat{h_1}}$. With d_{1_t}, we can then compute the second calibrated symbol d_{2_t} by $d_{2_t} = \frac{d_{2_r} - d_{1_t}\hat{h_2}}{\hat{h_1}}$. In general, the k-th calibrated symbol can be computed by $d_{k_t} = \frac{d_{k_r} - \sum_{i=2}^{L}\hat{h_i}d_{k-i+1_t}}{\hat{h_1}} (k > L)$, where $-\sum_{i=2}^{L}\hat{h_i}d_{k-i+1_t}$ is the complementary component to eliminate the previous multipath copies, and $\frac{1}{\hat{h_1}}$ is the basic calibration component to compensate the power attenuation and phase shift of the current symbol.

Reducing channel estimation errors: To eliminate the channel noise and accommodate normal temporal variance, we would like to utilize the zero-mean property of the channel noise, i.e., to use the average values of multiple channel estimations to reduce the estimation error. Specifically, we set a window of size N, and advance the window so that it always keeps the most recent N channel estimations. The ultimate output channel impulse response is the average of the N channel estimations in the window. Since the channel estimation is given by $\hat{\mathbf{h}} = \{\mathbf{D^H D}\}^{-1}\mathbf{D^H r}$, and the estimated error is thus $\{\mathbf{D^H D}\}^{-1}\mathbf{D^H n}$. The average $\hat{\mathbf{h}}_{\mathbf{avg}}$ of the N estimations is $\frac{1}{N}\sum_{i=1}^{N}\mathbf{h_i} = \frac{1}{N}\sum_{i=1}^{N}\{\mathbf{D^H D}\}^{-1}\mathbf{D^H r_i}$, and the average estimation error becomes $\{\mathbf{D^H D}\}^{-1}\mathbf{D^H}\sum_{i=1}^{N}\mathbf{n_i}$. When N is chosen large, due to the zero mean property of the channel noise, this error approximates to a zero vector.

4 Jamming Entanglement

Signal to noise ratio (SNR) is always a key metric to evaluate the reliability of a wireless communication system. According to Shannon Theorem [1], a large SNR can support a high speed service than a small SNR on the same channel bandwidth. Thus, we would like to enable a receiver at the desired location to always achieve a large SNR, and an eavesdropper at an undesired location to encounter a low SNR, so that it cannot distinguish the received signal from the background noise and fails to decode received data.

The basic idea is to intentionally introduce noise to the raised transmit signal, so that the noise can significantly reduce the SNR at the eavesdroppers but cancel each other at the desired receiver to cause no impact.

In order to generate such noise signals for all transmitters, we randomly divide the N transmitters into $\frac{N}{2}$ pairs. For each pair, we assign one transmitter with a randomly generated sequence, whose length is the same as the message length. Then, we generate the opposite sequence for the other transmitter. For example, if the randomly generated sequence is $1, 1, -1, 1$, then the corresponding opposite sequence is $-1, -1, 1, -1$. The pair of transmitters add the corresponding noise sequences to the message and send the combined signals to the wireless channel. Because the noise signals are embedded in combined signals, which can synchronize at the desired receiver, the noise signals naturally achieve the synchronization to enable the cancelation. However, for the eavesdroppers, due to the lack of the time synchronization and channel calibration, the noise signals fail to cancel each other and the sum of them still confuse the eavesdroppers. Moreover, the noise sequences are randomly generated for each message, and thus the eavesdroppers cannot guess and pre-determine them.

Let P_t denotes the transmit power of the desired signal and P_j denotes the power of the jamming signal. Since jamming signals is served as noise, SNR at an individual transmitter is thus $\frac{P_t}{P_j+N_c}$, where N_c is the power of channel noise. Normally, to compensate the propagation loss, the transmit power P_t is chosen much larger than the channel noise N_c. Accordingly, the jamming signal power P_j should be also larger than the channel noise N_c to let the SNR lower than 1. For N transmitters, at the desired location, the amplitude for each received signal is $a\sqrt{P_t}$, where a is amplitude attenuation of the channel, and the combined signal power is then $(aN\sqrt{P_t})^2 = (aN)^2 P_t$. In addition, all the jamming signals are canceled at the desired location. The combined noise power at the receiver is then $N \cdot N_c$, because the channel noise is independent from each other. Hence, the corresponding SNR becomes $\frac{a^2N^2P_t}{N\cdot N_c} = \frac{a^2NP_t}{N_c}$, no jamming signal is involved in it. The equation of SNR indicates that P_t dominates the SNR. Because a can be measured during training stage and N_c can be obtained by sensing the background power, the transmitters can thus select a proper value for P_t to get a required boosted SNR at the desired receiver.

On the other hand, for a receiver that is not located at the desired service location, due to the lack of channel synchronization, it will experience distorted received signals in various shapes, and consequently the jamming signals cannot cancel each other, yielding a low SNR at the undesired location. In Section 6.2, we show how the channel distortion affects the SNR at the undesired location.

5 Tolerable Time Shift

In the above discussion, we consider the ideal case where the arrival signals are perfectly synchronized. In practice, as mentioned, after clock and propagation synchronization, a slight time shift may still exists among the received signals due to the processing delay and synchronization imperfections. In the following, we identify the tolerable time shift, within which received signals can achieve the constructive interference to obtain a boosted SNR.

5.1 Impact of the Time Shift on SNR

SNR is the ratio of the received signal power to the noise power. Because the noise power is independent from the time shift, the received signal power remains as the key metric to determine the SNR at the desired receiver. Lemma 1 gives the threshold of the time shift based on the received signal power. Without loss of generality, we assume that there are two arrival signals to facilitate the presentation.

Lemma 1. The constructive interference does not happen if $\delta_t > \frac{1}{4f_0}$, where δ_t is the time shift between two arrival signals and f_0 is the frequency of the baseband signal.

Proof can be found in our previous work [8]. As a practical example, for the 1Mbps and 10Mbps transmission speed with the QPSK modulator, a tolerable time shift of $\frac{1}{4f_0}$ equals to 500 and 50ns respectively.

5.2 Impact of the Time Shift on SNR with Jamming Entanglement

In Section 4, we propose to increase the SNR through transmitting jamming signals that can cancel each other at the receiver. In what follows, we will investigate the impact of the tolerable time shift on the effectiveness of this scheme. We present Lemma 2 below.

Lemma 2. After the jamming entanglement, the expected SNR at the desired receiver is $\frac{2\{\frac{N}{2}+\sum_{i=1}^{N}\sum_{j=1,j>i}^{N}\cos[2\pi f_0\frac{\Delta(j-i)}{N-1}]\}}{N[1-\cos(2\pi f_0\frac{\Delta}{2})]}$, where N is the number of transmitters, and Δ is the maximum tolerable time shift.

Proof: The modulated signal $S(t)$ is $Re[\sqrt{2}A_m g(t)e^{j\theta_m}] = \sqrt{2}A_m g(t)\cos\theta_m$, where A_m and θ_m are the amplitude and the phase of the transmit signal respectively, and $g(t)$ is the baseband signal. Typically, $g(t)$ is a sine, cosine or rectangle wave [7]. Assume $g(t) = \sin(2f_0t)$, $S(t)$ then equals to $\sqrt{2}A_m \sin(2f_0t)\cos\theta_m$, and its power is $A_m^2\cos\theta_m^2$. Assume the signal arrival times for N transmitters are $t_0, ...t_{N-1}$. For the tolerable time shift Δ, all signals arrive the receiver within the range $t_0 \sim t_0 + \Delta$. The boosted power at the receiver can be represented by

$$P_{cN} = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} \{\sum_{i=1}^{N} \sqrt{2}A_m \sin[2f_0(t+t_i)]\cos\theta_m\}^2 \mathrm{d}t$$

$$= 2A_m^2\cos\theta_m^2\{\frac{N}{2} + \sum_{i=1}^{N}\sum_{\substack{j=1\\j>i}}^{N}\cos[2\pi f_0(t_j - t_i)]\}$$

Further assume that the arrival time of all the signals follows the uniform distribution between 0 and Δ. The expected time shift between any two signals is thus $\frac{\Delta}{N-1}$. Accordingly, the expected boosted power $E(P_{cN})$ can be derived by $2A_m^2\cos\theta_m^2\{\frac{N}{2} + \sum_{i=1}^{N}\sum_{\substack{j=1\\j>i}}^{N}\cos[2\pi f_0\frac{\Delta(j-i)}{N-1}]\}$. We can see that $E(P_{cN})$ increases as N increases.

As discussed in Section 4, the boosted SNR is $\frac{a^2NP_t'}{N_c}$ in the ideal case when the jamming signals are totally canceled out. When the jamming signals cannot completely cancel each other, their combined power dominates the actual noise because the jamming signal power as well as the transmit power are usually chosen much higher than the channel noise power to result in a satisfiable SNR at the receiver. Hence, we neglect the channel noise to facilitate the following analysis. Assume the modulated jamming signal for one transmitter is $\sqrt{2}A_m\sin(2f_0t)\cos\theta_m$. The corresponding opposite counterpart is thus $-\sqrt{2}A_m\sin(2f_0t)\cos\theta_m$. Then the combined power of both signals is $2A_m^2\cos\theta_m^2[1-\cos(2\pi f_0\delta_t)]$, and the expected SNR can be derived by

$$E(SNR) = \frac{2\{\frac{N}{2} + \sum_{i=1}^{N}\sum_{j=1,j>i}^{N}\cos[2\pi f_0\frac{\Delta(j-i)}{N-1}]\}}{N[1-\cos(2\pi f_0\frac{\Delta}{2})]},$$

where $\frac{\Delta}{2}$ is the expected time shift between the arrival times of camouflage signals. □

$E(SNR)$ increases as N increases or Δ decreases. For example, with 4 transmitters and a tolerable time shift of $\frac{1}{4f_0}$, the expected SNR at the receiver reaches approximately 10 dB. When the number of transmitters is 8, the expected SNR can be boosted to approximately 13 dB. For a reduced tolerable time shift of $\frac{1}{8f_0}$, the achieved SNR is about 20 dB. In a conclusion, for a service system with the maximum tolerable time shift Δ, the jamming signals still significantly help to boost the SNR at the desired receiver.

6 Service Area Size

Because signals travel at the speed of light, it seems that a small tolerable time shift may result in a large service area (e.g. 50ns indicates a distance of 15m). In this section, we attempt to obtain a fine-grain service area using the channel uncorrelation property, which states that two receivers will observe different channels from the same transmitter if they are separate by a couple of wavelength away [18]. In particular, [10] indicates that a distance of half wavelength can lead to uncorrelated channels. In the following part, we investigate how uncorrelated channels affect the boosted SNR.

6.1 Channel Uncorrelation Property

We first describe the channel uncorrelation property and explore the distance required to generate the uncorrelated channels. Channel correlation coefficient is normally used to indicate the similarity between two channels. When two channels are fully correlated, the coefficient approximates to 1; while when two channels are uncorrelated from each other, the coefficient is 0. Theoretically, the multipath channel is usually modeled as the Rayleigh fading channel [11]. In a rich, isotropic scattering environment, multipath components arrive at the receiver from all the directions, and the corresponding channel correlation coefficient can be described as a zeroth order Bessel function [12]: $\rho(d,f) = J_0(2\pi d/\lambda)$, where d is the distance between the receiver and the eavesdropper, f is the carrier frequency of the signal, and $\lambda = \frac{c}{f}$ is the wavelength of the signal. When we substitute $d = \frac{\lambda}{2}$ into this function, the channel correlation coefficient approximates to 0, which indicates that two channels are uncorrelated. In practice, [13] presents that a longer distance (e.g. a couple of wavelength) may be required to get the uncorrelated channels when there are less scatterings.

6.2 Power Attenuation by the Channel Uncorrelation

In this part, we discuss how the uncorrelated channels affect the boosted SNR. As mentioned earlier, channels observed by the eavesdropper are uncorrelated from the calibrated ones. Thus, channel effects cannot be eliminated and signals will exhibit different shapes when they arrive at the eavesdropper. Lemma 3 gives the SNR at the desired location and undesired location respectively.

Lemma 3. The SNR at desired location and undesired location are $\frac{2P_h\cdot P_t}{N_c}$ ($P_t \gg \frac{N_c}{P_h}$) and $\frac{P_t}{P_j}$ respectively, where P_t is the transmit power of orignal signal, N_c is the channel noise power, P_j is the jamming signal power and P_h is the channel variance.

Proof: Without loss of generality, we assume two transmitters. The calibrated signals from two transmitters are denoted as S_1 and S_2 respectively. Let P_t be the transmit power for both signals. Assume the receiver observes two channels $h_1(\tau)$ and $h_2(\tau)$. According to [1], Multipath channel is described as $h(\tau) = \sum_{l=1}^{L} a_l e^{j\phi_l}\delta(\tau-\tau_l)$, where a_l and $e^{j\theta_l}$ are the amplitude attenuation and phase shift of the signal copy that travel along the i-th path. At time τ_l, channel $h_1(\tau_l)$ and $h_2(\tau_l)$ can be modeled as the random variables with zero mean and a variance that is usually denoted as P_h [14]. Thus, at this time, the received signal is $S_1\cdot h_1(\tau_l) + S_2\cdot h_2(\tau_l)$. Since the mean value of the received signal is 0, we can get the received power by calculating its variance. Specifically, for a random variable x with the zero mean, its power $P = \int x^2 f(x)\mathrm{d}t = Var(x)$, where $Var(.)$

donates the variance. Thus, the combined transmit power at the receiver is as follows,

$$\begin{aligned} P_s &= Var[S_1 \cdot h_1(\tau_l) + S_2 \cdot h_2(\tau_l)] \\ &= P_t E[|h_1(\tau_l)|^2 + 2|h_1(\tau_l) \cdot h_2(\tau_l)^*| + |h_2(\tau_l)|^2] \\ &= 2P_h \cdot P_t + 2\rho P_h \cdot P_t, \end{aligned}$$

where ρ is defined as the channel correlation coefficient and equals to $\frac{|h_1(\tau_l) \cdot h_2(\tau_l)^*|}{\sqrt{Var(|h_1(\tau_l)|)Var(|h_2(\tau_l)|)}} = \frac{|h_1(\tau_l) \cdot h_2(\tau_l)^*|}{P_h}$ [15], and * denotes the complex conjugate operator.

At the undesired location, the channels of two transmitters are uncorrelated from each other. Thus, their coefficient ρ equals to 0 and the received power is $P_s = 2P_h \cdot P_t$. On the other hand, two channels observed by the desired receiver are calibrated and are quite correlated with each other. So their coefficient ρ equals to 1 and thus the received power is $P_s = 4P_h \cdot P_t$.

The power of jamming signals can be derived in the same way. Assume two calibrated jamming signals are denoted as C_1 and C_2 ($C_1 = -C_2$) with the power P_j for each of them. Assume the receiver observes two channels $h_1(\tau)$ and $h_2(\tau)$. At time τ_l, the combined power of two jamming signals is given by $P_c = Var[C_1 \cdot h_1(\tau_l) + C_2 \cdot h_2(\tau_l)] = 2P_h \cdot P_j - 2\rho P_h \cdot P_j$.

At the desired location, the receiver observes two correlated channels. Thus, ρ equals to 1 and the combined power equals to 0. At undesired location, two channels observed by the receiver are uncorrelated. Thus, ρ equals to 0, and the combined power equals to $2P_h \cdot P_j$, which can significant affect the SNR of the receiver.

Note that SNR is represented as the ratio of the original signal power (given by P_s) to the sum of jamming signal power (given by P_c) and channel noise power N_c (i.e. $SNR = \frac{P_s}{P_c + 2N_c}$). Note that the power of channel noise is doubled at the receiver, because channel noise from two received signals combines together. At the desired location, channels are synchronized, and original signals get boosted and jamming signals cancel each other, yielding an SNR that equals to $\frac{2P_h \cdot P_t}{N_c}$. The transmit power P_t as well as the jamming signal power P_j are usually chosen much higher than the channel noise power N_c to result in a satisfiable SNR at the receiver ($P_t \gg \frac{N_c}{P_h}$). So N_c is negligible compared to the jamming power. Accordingly, at the undesired location, the channel is not synchronized(i.e. ρ is close to zero) and the SNR is represented by $SNR = \frac{P_s}{P_c + N_c} \approx \frac{P_t}{P_j}$. If $P_j = P_t$, SNR approximates to 0dB and the receiver cannot distinguish between the original and jamming signals. □

6.3 Power Attenuation by the Channel Uncorrelation of Multiple Transmitters

In this section, we extend Lemma 3 from a two-transmitter scenario to the multi-transmitter one, where N transmitters are connected to the same service provider, and each one transmits a signal that is calibrated based on the channel between the transmitter and the desired location. The SNR at desired location and undesired locations are given by

Lemma 4. With multiple transmitters, the SNR at desired location and undesired location are $\frac{NP_h \cdot P_T}{N_c}$ ($P_T \gg \frac{N_c}{P_h}$) and $\frac{P_T}{P_J}$ respectively, where P_T is the power of transmit signals, N_c is the power of channel noise, P_J is the power of the jamming signal, and P_h is the channel variance.

Proof: We assume N transmit signals $[S_1, S_2, ...S_N]$ have the same transmit power P_T. The signal S_i will propagate through the channel $h_i(\tau)$ and each channel $h_i(\tau)(0 \leq i \geq N)$ has the same channel variance P_h. Therefore, the combined signal power P_{ms} at time t_τ is as follows,

$$\begin{aligned} P_{ms} &= Var[\sum_{i=1}^{N} S_i \cdot h_i(\tau_l)] \\ &= P_T E[\sum_{i=1}^{N} |h_i(\tau_l)|^2 + \sum_{i=1}^{N} \sum_{\substack{j=1 \\ j \neq i}}^{N} |h_i(\tau_l) \cdot h_j(\tau_l)^*|] \\ &= NP_h \cdot P_T + \sum_{i=1}^{N} \sum_{\substack{j=1 \\ j \neq i}}^{N} \rho_{ij} P_h \cdot P_T, \end{aligned}$$

where ρ_{ij} is the channel correlation coefficient between i^{th} channel and j^{th} channel. At the desired location, all the transmitted signals are calibrated and channels observed by the receiver are correlated. Thus, ρ_{ij} equals one and P_{ms} becomes $N^2 P_h \cdot P_T$. On the other hand, channels are not calibrated at undesired locations, and thus the receiver observes uncorrelated channels and ρ_{ij} decreases to zero. P_{ms} then becomes $NP_h \cdot P_T$, which is N times less than the combined power when all the channels are synchronized.

To enable the jamming signal entanglement, N jamming signals $[C_1, C_2, ...C_N]$ are transmitted with the same power P_J and propagate through different channels $[h_1, h_2, ...h_N]$. As mentioned in Section 4, all the transmitters are randomly divided into pairs and each pair is assigned with a pair of randomly generated jamming signals, whose phases are opposite to each other. Therefore, if two jamming signals C_i and C_j belong to the same pair, then $C_j = -C_i$ and their combined power is $Var[C_i \cdot h_i(\tau_l) + C_j \cdot h_j(\tau_l)] = 2P_h \cdot P_j - 2\rho P_h \cdot P_j$. Otherwise, C_i and C_j are from different pairs and independent to each other. Thus, the combined power becomes $2P_h \cdot P_j$, and we can get the combined power of jamming signals as shown below:

$$\begin{aligned} P_{mc} &= Var[\sum_{i=1}^{N} C_i \cdot h_i(\tau_l)] \\ &= \sum_{\substack{i=1 \\ j \neq i}}^{N/2} Var[C_i \cdot h_i(\tau_l) + C_j \cdot h_j(\tau_l)], where\ C_i = -C_j \\ &= NP_h \cdot P_J - \sum_{i=1}^{N/2} 2\rho_i P_h \cdot P_J \end{aligned}$$

At the desired location, all the channels observed by the receiver are correlated, ρ_i then becomes 1, and jamming signals cancel each other. However, receivers at undeisred locations observe uncorrelated channels due to channel uncorrelation property. Thus jamming signals still exist at the receiver and can interfere with transmit signals. The combined power of jamming signals is $NP_h \cdot P_J$.

The SNR of the receiver is the ratio of the combined transmit power to the combined noise (i.e. $SNR = \frac{P_{ms}}{P_{mc} + N \cdot N_c}$). At the desired location, channels are synchronized, transmit signals boost each other and jamming signals cancel each other. Thus, the maximum SNR obtained by the receiver is $\frac{NP_h \cdot P_T}{N_c}$, which is dominated by the transmit

signal power, and the receiver can get the desired SNR if appropriate transmit signal power is selected. At the undesired location, constructive interference vanishes and channels become uncorrelated to each other. Accordingly, the SNR at the receiver is $\frac{P_h \cdot P_T}{P_h \cdot P_J + N_c}$. In general, the power of jamming signals is chosen much larger than the channel noise N_c. Thus, the SNR is approximately to $\frac{P_T}{P_J}$. Furthermore, if jamming signal power is chosen at the same level as the transmit signal power, the SNR at undesired receivers approximately reaches 0dB, which means transmit signals cannot be recognized from the noise. □

Impact of SNR on service area size: As the above discussion, when channels are uncorrelated to each other (i.e. $\rho = 0$), the SNR at the receiver will achieve the minimum value and the receiver can hardly distinguish transmit signals from jamming signals. Theoretically, $\rho = 0$ happens when the receiver is half wavelength far from the desired location. For example, modern wireless devices like WIFI, Bluetooth devices usually uses $2.4GHz$ as their central frequency to transmit signals. The corresponding wavelength is $0.125m$ (i.e. $(3 \times 10^8)/(2.4 \times 10^9) = 0.125m$), and the service area size is $6.125 \times 6.125cm^2$, when real signal and jamming signal have the same power.

In practice, a couple of wavelength may be required to gain such uncorrelated channels. For example, if the uncorrelation is caused by 4 wavelengths, the service size will be $0.5 \times 0.5m^2$. SNR at the undesired location also shows that SNR decreases as the jamming signal power P_j increases. Thus, if we require a smaller service area size in this scenario, we may properly increase the jamming signal power to meet the requirements.

6.4 Security Discussion

An attacker against the proposed system can be either active or passive. An active attacker tries to create, interrupt, intercept, block or overwrite the transmit signals to prevent the receiver from obtaining the legitimate service. The active attacker may launch multiple attacks. For example, It may impersonate as an authorized service provider to gain the trust of a receiver; It may inject malicious information into the channel to mislead the receiver; It may jam the receiver so that the receiver cannot obtain the service. However, these active attackers are not unique to our scheme. Existing approaches have been proposed to deal with these attacks. For example, the receiver can establish the cryptographic authentication protocol with the service provider to deal with impersonation attacks and confirm the message integrity [16] [17], and spread spectrum techniques like Frequency Hopping Spread Spectrum(FHSS) and Direct Sequence Spread Spectrum (DSSS) can be designed to defend against jamming attacks [19] [20].

A specific active attack in the proposed scheme is the replay attack. It seems that an attacker may intentionally introduce a time shift of the received signal at the desired location by duplicating and transmitting the received signal with a small delay. Nevertheless, we can consider such replay attacks as the traditional jamming attacks. Because even the attacker can replay the delayed signal, it cannot disrupt the alignment and cancellation of the original transmit signals at the desired location, which means the receiver will obtain both desired signal and replayed signal. The replayed signal will be served as the noise to decrease the SNR at the receiver and interfere the decoding process. Such attack is different from the scenario when the receiver is located at undesired locations. First, at undesired location, desired signals are distorted and can only achieve poor alignment due to lack of channel and time synchronization. Therefore, the desired signal itself at the undesired location is distorted and may be not able to decode. In addition, jamming signals in the undesired locations cannot cancel each other. Since the jamming signals are usually chosen the same level as the desired signals, the SNR at the undesired locations will always remain small and can hardly provide a good service.

Therefore, we can apply traditional methods to defend against such replay attacks. First, we may increase the power of transmit signals (both desired signal and jamming signal at the transmitter) to increase the SNR at the desired locations. In addition, we may also apply FHSS or DSSS to increase the robustness of received signals against the replayed signals.

A passive attacker is usually an eavesdropper, which attempts to obtain the legitimate service from the service provider. For a basic eavesdropper, as shown in Lemma 3, when the eavesdropper's channel is totally uncorrelated from the receiver's channel, it will not achieve a boosted SNR to decode the received service data. It seems that multiple eavesdroppers with high-gain, directional antennas may collaborate to add their received signals together to form a boosted signal, with which they can decode the original service data. Nevertheless, even collaborated attackers can obtain jamming entangled signals from different transmitters respectively, these transmit signals are calibrated to accommodate the distinct channels between transmitters and the desired receiver only, and consequently received signals are uncorrelated to each other at attackers. Therefore, the sum of received signals is equivalent to that of multiple random signals, and both channel distortions and jamming signals can significantly interfere the correct decoding of the combined signal. Thus, no matter how many eavesdroppers exist, signals received by these eavesdroppers always suffer from the distortion from jamming signals and the wireless channel fading, and exhibit different shapes as long as their channels are not calibrated for homomorphism at the service provider side. As such, a boosted SNR cannot be obtained for correct decoding.

7 Multi-user Mode

Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA), and Frequency Division Multiple Access (FDMA) are three typical methods adopted by modern wireless communication systems to support multi-user access. For CDMA, users are assigned with special designed codes that are orthogonal to each other, and an individual user can extract its own data by correlating received signals with the assigned codes. For TDMA and FDMA, users are assigned with distinct, non-overlapping time slots/frequency bands to send and receive wireless signals. By utilizing different codes, time slots, and frequencies, the interferences among wireless users can be eliminated.

In the following, we demonstrate how to integrate traditional multiple access techniques into the pinpoint system

to support multiple users. Because the location-restricted service is delivered from the service provider to the receiver, we only discuss how to implement the pinpoint system for the downlink flow of these multiple access techniques.

CDMA integrated pinpoint waveforming: With CDMA, the transmitter can pinpoint the service to each user using their assigned CMDA code. In particular, service provider first assigns each user with a unique code $A^{(n)}$ and the transmitter can then directly encode original signals using the CDMA codes to deliver information to all users. In addition, because users are located at different locations, transmit signals of different users may need to be sent at distinct times to compensate the time difference of arrivals. The following equation exhibits the transmit signals of N users at the m^{th} transmitter.

$$S_m = \sum_{n=1}^{N}[(D^{(n)} + J^{(n)}) \sum_{k=1}^{L} a_k^{(n)} g(t - kT_c - T_{md}^{(n)})],$$

where $D^{(n)}$ and $J^{(n)}$ are the desired signal and jamming signal of the n^{th} user respectively. $a_k^{(n)}$ is the k^{th} chip in the code $A^{(n)}$ and T_c is chip time. $T_{md}^{(n)}$ is the time delay of transmit signal of the n^{th} user at m^{th} transmitter. In general, each specific code $A^{(n)}$ is designed to be orthogonal to each other, so that users can extract the desired information by correlating the received signals with their assigned codes. However, in the proposed scheme, because M transmitters cooperate together to pinpoint the service to N users at different positions, time delay $T_{md}^{(n)}$ may vary from different transmitters and different users. Thus, the orthogonality between codes cannot be maintained due to the time difference, and information decoding is significantly interfered by transmit signals of other users.

To eliminate such interference, asynchronous coding scheme is required at the transmitter. In particular, we may apply the pseudo-noise (PN) code adopted by the uplink flow of the traditional CDMA. PN code is a binary sequence that appears random but can be generated in a deterministic manner. Different PN codes are nearly orthogonal and statistically uncorrelated to each other. Therefore, if signals are encoded by different PN codes, their correlation always remains small even when there exists time shift between them. This means undesired signals can only slightly interfere the decoding, and the correct information can be recovered by using the appropriate error correction code.

TDMA integrated pinpoint waveforming: With TDMA, the transmitter can pinpoint the service to each user during its time slot. Specifically, the service provider divides each signal frame into time slots and assigns each user with a particular slot. The transmitter then sends entangled signal of each user at their corresponding time slot. Transmit signal of n^{th} user at m^{th} transmitter is described as follows:

$$S_m^{(n)} = (D^{(n)} + J^{(n)})[u(t - T_{md}^{(n)}) - u(t - T_{md}^{(n)} - T_s - T_g)],$$

where $D^{(n)} + J^{(n)}$ are the jamming entangled signals of the n^{th} user. $u(t)$ is the step function (i.e. $u(t) = 1$, when $t \geq 0$). $T_{md}^{(n)}$ is the delay time of corresponding transmit signals and it is used to compensate for the time difference of arrivals caused by the distinct propagation distance between different transmitters and users. T_s is the time period of each slot. T_g is the guard time to avoid the interference from undesired transmit signals. In particular, the propagation synchronization may introduce overlapping time slots due to the varying time shifts experienced by different users. To solve this, transmitters can insert an appropriate time guard T_g between time slots to eliminate the overlaps and avoid the interference among multiple users.

FDMA integrated pinpoint waveforming With FDMA, the transmitter can pinpoint the service to each user at the assigned frequency band. If the Orthogonal Frequency-division Multiplexing (OFDM) is enforced, each user will be assigned with a particular sub-carrier and jamming entangled signals of each user will be sent within the corresponding sub-carrier. The transmit signals generated by the OFDM system can be represented by

$$S_m = \frac{1}{\sqrt{T}} \sum_{n=1}^{N} (D^{(n)} + J^{(n)}) e^{j\frac{2\pi}{T} n(t - T_{md}^{(n)})},$$

where T is the symbol duration, $D^{(n)} + J^{(n)}$ are the corresponding jamming entangled signals, and $T_{md}^{(n)}$ is the time delay of the n^{th} transmit signal. $e^{j\frac{2\pi}{T}n}$ is the assigned subcarrier of the n^{th} user and the whole bandwidth is divided into N pieces in an OFDM system, and accordingly the spectrum assigned to each user is limited. Thus, the receiver may experience a weak multipath effect that causes less distortion to jamming entangled signals. Nevertheless, the amplitude attenuations and phase shifts are different from different locations, without channel synchronization, the jamming entangled signals still exhibit random shapes when arriving at an undesired receiver, and consequently the jamming portion cannot cancel each other.

8 Performance Evaluation

We develop a prototype pinpoint service system on top of the Universal Software Defined Radio Peripherals (USRPs), which are radio frequency (RF) transceivers with high bandwidth and high dynamic range processing capability. The USRPs use SBX broadband daughter boards operating in the 400 - 4400 Mhz range as RF front ends. The software toolkit implementing the prototype is the GNURadio [21].

8.1 System Design

The receiver is a standalone USRP, and the transmitter (i.e., the service provider) consists of two USRPs connected by an multiple-input and multiple-output (MIMO) cable. Both USRPs follow the master and slave protocol. Specifically, the master USRP connects to both the slave USRP and the host computer, and the slave USRP only connects to the master USRP. The master provides the clock scale and the time reference to the slave USRP through the MIMO cable. The master and slave USRPs are separated by about 0.75 meter to achieve uncorrelated channels between each USRP and the receiver.

Our software program is developed from the Benchmark TX/RX Program, which is the communication tool provided by GNURadio for data transmission between two USRPs. The source codes are located at gnuradio/gr-digital/examples. For the transmitter, we redesign the modulation block of the Benchmark TX program by adding

two new modules, namely jamming signal entanglement and channel calibration modules. We also add a delay compensation module to compensate the difference of signal arrival times measured at the master and slave USRPs. An input bit sequence is first modulated into physical layer symbols, then entangled with jamming signals, and finally transmitted to the receiver after channel calibration and delay compensation. Because the receiver requires no specific changes, we directly run the Benchmark RX Program at the receiver but add a constellation sink to observe the real time constellation diagram for analyzing the performance.

8.2 Evaluation Metrics

We evaluate the prototype system using the following typical metrics for measuring the service of quality:

- **Signal to noise ratio (SNR)**: This is the ratio of the received signal power to the noise power, which is the sum of both the jamming signal power and the channel noise power.
- **Packet delivery rate**: This is the ratio of the number of correctly received packets to the total number of received packets. In the prototype implementation, each packet is appended with a 32-bit cyclic redundancy check (CRC) code for error detection, and prefixed with a 64-bit access code for packet synchronization. The length of each packet is 500 bytes. The receiver detects packets by correlating received bits with the access code. A high correlation indicates the arrival of a packet, and the receiver verifies this packet by checking the CRC. We consider a packet to be received correctly only if the packet passes CRC check.
- **Throughput**: Throughput is the number of correctly received packets per unit time. To facilitate the comparison, we normalize the throughput into the range of $0-1$. If the throughput is close to 1, the bit rate at the receiver is close to that at the transmitter, and thus the service delay is near zero. If the throughput is 0, no information bits are received at the receiver and the service delay is regarded as infinity.

In addition to the pervious metrics, we also introduce a fourth metric, **channel cross-decorrelation**, which quantifies the disparity between two channels. A small cross-decorrelation value indicates a strong correlation between two channels, and a large value indicates two channels are uncorrelated with each other. We include channel cross-decorrelation as an extra evaluation metric, because the service quality is also highly relevant with this metric. The cross-decorrelation between the channels of desired and undesired locations should be large, so that a receiver at a undesired location cannot obtain a service of good quality.

8.3 Measuring Channel Cross-decorrelation

SNR values, packet delivery rate and throughput can be easily measured from the communication traffic based on their definitions above. However, how to measure channel cross-decorrelation is not as straightforward as the pervious three metrics, because it reflects the disparity among wireless

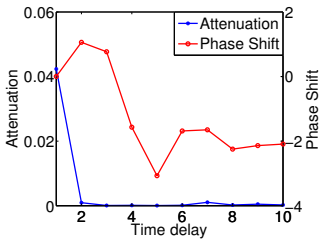


Fig. 7: USRP 1

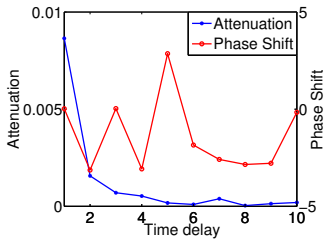


Fig. 8: USRP 2

channels that cannot be directly observed. In the following, we discuss our methodology to measure this metric.

To achieve the channel calibration, an accurate channel estimation between the transmitter and the receiver is required. We estimate the channel in a training stage, where the receiver broadcasts a beacon signal to the transmitter, and transmitter then measures the corresponding channel impulse response from the received beacon signal. At the training stage, we measure the channel for 500 times and took the average value as the current channel impulse response. Thus, we can eliminate the impact of the unexpected disturbance caused by the channel noise, normal temporal variations, and other interferences.

Figures 7 and 8 plot the magnitude (i.e. amplitude attenuation) and phase (i.e phase shift) of the average channel impulse response measured at the two USRPs respectively. The system operates on the central frequency of 2.4 GHz and adopts the binary phase shift keying (BPSK) modulation. The unit of the X-axis is a symbol duration, which is approximately the minimum time required to resolve two paths. We can see that the channels of both USRPs are quite different in shape and magnitude. This observation is consistent with the basic experiment setting, in which both USRPs are separated by a certain distance to ensure the uncorrelated channels.

Cross and auto-variance: Before we introduce how to measure the channel cross-decorrelation to quantize such channel difference, we first define two terms *cross-variance* and *auto-variance* that will be involved in calculating the channel cross-decorrelation. The cross-variance is defined as the Euclidean distance between two different channels. For channels i and j, their average cross-variance V_{ij} is calculated by $\frac{1}{N}\sum_{n=1}^{N}|h_{in}-h_{avgj}|$, where N is the total number of channel measurements, h_{in} is the n-th estimated channel impulse response of channel i, and h_{avgj} is the average channel impulse response of channel j. When $i=j$, the cross-variance degenerates to the auto-variance V_{ii}, which is the Euclidean distance between an one-time channel measurement and the average of multiple channel measurements for the same channel. In the experiment, we use the average value of the auto-variance over all the channel estimations. Figure 9 plots the distributions of the cross and auto-variance of previous channels measured at two USRPs. In addition, we also plot the cross variance of two channels measured after the channel calibration. The cross-variance before the calibration is much larger than the auto-variance, because the channels of both USRPs are uncorrelated from each other. After the calibration, the cross-variance is closed to the auto-variance within one channel that indicates two

channel are quite correlated.

Channel cross-decorrelation: We use channel cross-decorrelation to normalize the cross-variance to facilitate the comparisons of the similarity and difference among wireless channels, and the cross-decorrelation R_{ij} between channels i and j is defined as $R_{ij} = \frac{|V_{ij}-V_{jj}|}{\frac{1}{2}|h_{avgi}+h_{avgj}|}$.

A cross-decorrelation value of 0.5 means that the channel difference is as large as 50% of the magnitude of the averages of the two channels. The cross-decorrelation ranges between 0 and 2. If it is larger than 1, the channel difference is even larger than the magnitude of the averages of the two channels. In Figure 9, for USRP 1 (master) and USRP 2 (slave), their cross-decorrelations are $R_{12} = 1.28$ and $R_{21} = 1.30$, which indicate that the channels measured at both USRPs are quite different from each other. In addition, after the calibration, their cross-decorrelations measured are $R_{12} = 0.040$ and $R_{21} = 0.043$, which indicates two channels after the calibration are highly correlated.

8.4 Jamming Signal Entanglement

As mentioned earlier, we entangle the jamming signals into transmit signals to conceal the real information. The jamming signals should cancel each other at the desired location but jam the original signals at undesired locations, so that eavesdroppers at those locations cannot distinguish the original signals from the jamming signals, and thus fail to decode the data.

We randomly choose an indoor location, namely Position 1, to place the receiver and calibrate the channel between the receiver and the transmitter. We mark this location as the desired location. We then randomly choose three other locations, namely Positions 2, 3, and 4, that are about 0.1, 0.2, and 0.3 meter away from the desired location respectively. We mark these locations as the undesired locations. Figure 12(a) plots the symbols on the constellation diagram with jamming signal entanglement for the desired location, i.e., Position 1. We can see that received symbols converge to the ideal points at Position 1. Due to slightly imperfect synchronization and normal oscillator shift, jamming signals may not exactly cancel each other and the residue introduces an additional noise that cause the deviation of the received symbols. Nevertheless, such noise is too small to impact the decoding accuracy and the received symbols still closely fluctuate around the ideal points.

Figures 12(b), 12(c), and 12(d) plot received symbols at undesired locations, i.e., Positions 2, 3, and 4, when jamming signal entanglement is enforced. As mentioned earlier, for undesired locations, transmit signals are not calibrated and they arrive at the receiver in different shapes. Thus jamming signals do not cancel each other, leading to a high demodulation error rate. As seen in these figures, received symbols randomly scatter around the entire constellation diagram, and become more and more difficult to decode with the increasing distance from Position 1, the desired location.

8.5 Service Area Size

We would like to explore the service area size achieved by the prototype system in the real world. The experiment environment is a typical indoor room with wooden doors, metal and wooden obstacles, and electronic devices. Figure 10 shows the positions of the transmitter and the receiver. The transmitter is placed at Position 0 and we pinpoint the service to Positions 1, 2, 3, and 4. For each test, the transmitter sends 3000 packets to the receiver.

Impact of distance: Without loss of generality, we choose four moving directions for the four positions. For Positions 1, 2, 3, and 4, the receiver moves towards(⇑), backwards(⇓), to the right(⇒), and to the left(⇐) of the transmitter. Table 1 shows the impact of the distance between the receiver and the desired location on the aforementioned four evaluation metrics, i.e., SNR, packet delivery rate, throughput, and the channel cross-decorrelation. In this test, the system operates on the central frequency of 2.4GHz and the ratio of desired signal power to jamming signal power is set to 1. In this table, Pos., Dir., D, Corr., and PDR denote position, moving direction, distance between the receiver and the desired location, cross-decorrelation, and packet delivery rate respectively. These abbreviations are also applied for the subsequent tables. As seen in Table 1, moving directions cause no noticeable impact on the four metrics. For each of the four desired locations, when the receiver is located at this location, i.e., distance is equal to 0, the receiver achieves the maximum SNR, packet delivery rate, and throughput. When the receiver moves away from this location, the channel cross-decorrelation increases and the corresponding SNR, packet delivery rate, and throughput decrease significantly. In particular, when the distance reaches 0.3 meter, the throughput at all four positions approximately reaches to 0 and thus no service is received.

TABLE 1: Impact of the distance

Pos.	Dir.	D(cm)	Corr.	SNR	PDR	Throughput
1	⇑	0	0.038	14.0	99.71%	0.93
1	⇑	10	0.33	5.1	68.75%	0.53
1	⇑	20	0.66	3.5	57.41%	0.35
1	⇑	30	1.25	-1.4	6.28%	0.012
2	⇓	0	0.039	14.0	99.18%	0.93
2	⇓	10	0.30	7.0	80.65%	0.61
2	⇓	20	0.76	3.4	39.70%	0.17
2	⇓	30	1.12	0	19.74%	0.031
3	⇒	0	0.012	14.9	97.61%	0.92
3	⇒	10	0.31	8.2	74.79%	0.47
3	⇒	20	0.72	3.5	41.57%	0.26
3	⇒	30	1.10	0.8	20.08%	0.078
4	⇐	0	0.013	14.9	96.53%	0.90
4	⇐	10	0.25	9.5	85.85%	0.64
4	⇐	20	0.77	4.4	58.95%	0.30
4	⇐	30	1.15	1.5	21.43%	0.062

Impact of central frequency: Theoretically, reducing the central frequency can enlarge the service area, because it can increase the signal wavelength and therefore raise the distance required for the channel uncorrelation. In this test, we reduce the central frequency from 2.4 GHz to 1.2 GHz to remeasure the four metrics at Positions 1 and 2, the ratio of desired signal power to jamming signal power remains unchanged (i.e 1), and the results are shown in Table 2. For the 2.4 GHz central frequency shown in table1, when the receiver is moved 0.3 meter away from the desired location, the channel cross-decorrelation is 1.21 and 1.16 at Positions 1 and 2 respectively. For the 1.2 GHz central frequency shown

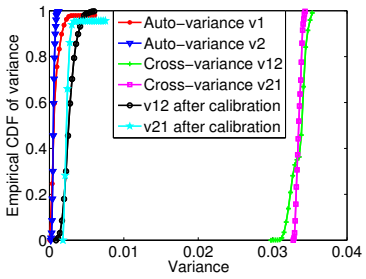


Fig. 9: Distribution of different variance

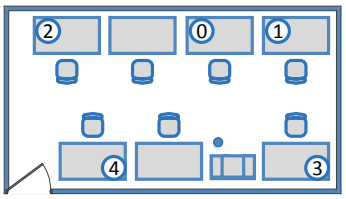


Fig. 10: Floor plan: Service area size

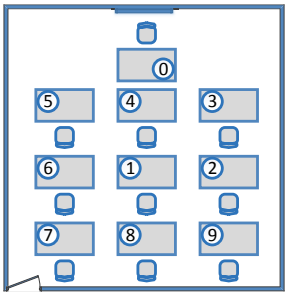
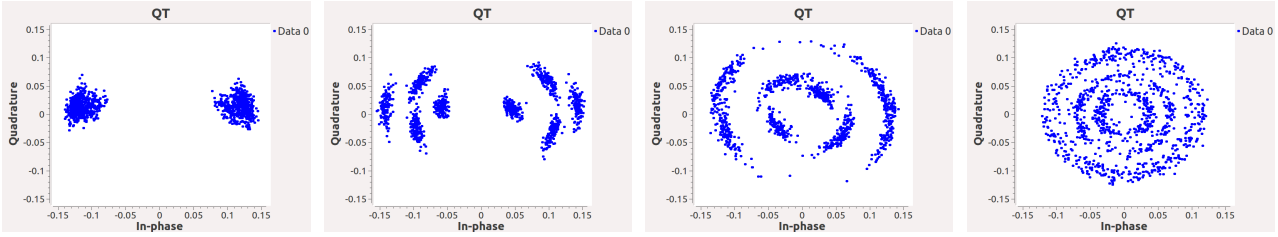


Fig. 11: Floor plan: pinpoint accuracy



(a) Position1 (b) Position2 (0.1 meter from Position1) (c) Position3 (0.2 meter from Position1) (d) Position4 (0.3 meter from Position1)

Fig. 12: Jamming signal entanglement

in table2, a similar channel cross-decorrelation, i.e., 1.25 at Positions 1 and 1.12 at position 2, is achieved with an increased distance of 0.45 meter. Thus, a lower frequency can cause a larger service area. This experimental observation is consistent with the theoretical conclusion.

TABLE 2: Impact of the central frequency (1.2GHz)

Pos.	Dir.	D(cm)	Corr.	SNR	PDR	Throughput
1	⇑	0	0.018	26.0	99.42%	0.96
1	⇑	15	0.29	10.45	88.33%	0.77
1	⇑	30	0.65	4.1	63.93%	0.33
1	⇑	45	1.21	0	20.66%	0.089
2	⇓	0	0.025	22.5	99.33%	0.98
2	⇓	15	0.34	8.0	88.75%	0.56
2	⇓	30	0.74	4.4	62.27%	0.35
2	⇓	45	1.16	0	14.45%	0.055

Impact of signal to jamming power ratio: As discussed in Section 6.2, we can reduce the service area size by decreasing the ratio of desired signal power to jamming signal power. Unlike previous experiment settings that use a ratio of 1, we decrease the ratio from 1 to 0.5 to test the impact in position 1 and 2, and our experimental observation matches the previous discussion result. Specifically, as shown in table1 with a ratio of 1, the throughput reduces to approximately 0 when the receiver is 0.3 meter away from a desired location. However, with a ratio of 0.5, the throughput reaches zero when the receiver is 0.2 meter away from the desired location as shown in table3. So the service area shrinks with decreasing signal to jamming power ratio.

Service area size of different modulations: We also investigate the service area size for different modulations. In the experiment, we adopt QPSK modulation in both position 1 and position 2. As shown in table4, the proposed

TABLE 3: Impact of the power ratio of desired signal to jamming signal (ratio = 0.5)

Pos.	Dir.	D(cm)	Corr.	SNR	PDR	Throughput
1	⇑	0	0.042	10.1	90.33%	0.72
1	⇑	10	0.36	1.3	25.76%	0.12
1	⇑	20	0.67	-1.15	4.78%	0.01
2	⇓	0	0.039	11.0	96.28%	0.69
2	⇓	10	0.35	1.9	32.33%	0.13
2	⇓	20	0.74	-1.3	23.93%	0.024

technique is still valid for QPSK modulation. At the desired location, the receiver gets the maximum SNR that is approximately 15dB, and thus obtains the service with good quality. However, when the receiver is 0.2 meter away from the desired location, SNR decreases significantly, leading to a poor throughput at the receiver. In addition, we find that the service area size of QPSK is smaller than that of BPSK. In QPSK, each symbol carries two bits instead of one. Therefore a QPSK symbol requires a higher SNR to decode the correct information than a BPSK symbol. With the same SNR, using the QPSK modulation results in more bit errors for decoding, and accordingly a reduced pinpoint accuracy and a smaller service area size. Nevertheless, if we need QPSK to achieve the same service area size as BPSK, we can always increase the signal to jamming power ratio to enforce a higher SNR at the receiver.

8.6 Pinpoint Accuracy

We test how accurate the prototype system can pinpoint the service to a desired location in a meeting room. Figure 11 shows the positions of the transmitter and receivers. We place the transmitter in the front of the room (i.e. position 0) and the desired receiver in the middle of the room (i.e.

TABLE 4: Impact of the modulation scheme

Pos.	Dir.	D(cm)	Corr.	SNR	PDR	Thoughput
1	⇑	0	0.040	15.1	90.59%	0.83
1	⇑	10	0.34	6.1	15.19%	0.033
1	⇑	20	0.66	3.0	10.78%	0.01
2	⇓	0	0.039	15.0	87.03%	0.86
2	⇓	10	0.32	7.1	4.0%	0.01
2	⇓	20	0.75	2.25	0.00%	0.00

Position 1). We also place 8 eavesdroppers scattering around the desired receiver (i.e. at Positions 2 to 9). The wireless communication system operates on the central frequency of 2.4GHz and adopts the binary phase shift keying (BPSK) modulation. The power ratio of the desired signal to jamming signal is set to 1 and the bit rate is 1Mbps.

TABLE 5: Pinpoint accuracy

Pos.	Cross-decorrelation	SNR	PDR	Throughput
1	0.026	14.0	99.27%	0.98
2	0.65	2.4	31.68%	0.20
3	0.81	2.4	19.39%	0.12
4	0.92	0.8	13.70%	0.02
5	1.14	1.6	23.26%	0.03
6	0.91	1.9	23.71%	0.07
7	1.66	-1.5	2.69%	0.003
8	1.62	-1.0	24.72%	0.02
9	0.96	0	29.69%	0.04

The pinpoint accuracy is displayed in Table 5. The receiver at the desired location can approximately achieve a SNR of 14dB, a packet delivery rate of 99.27%, and a throughput of 0.98, while eavesdroppers at undesired locations get a much worse performance. For example, an eavesdropper at position 5 can only achieve a SNR of 1.6dB, a packet delivery rate of 23.26%, and a throughput of 0.03. In addition, even an eavesdroppers is located closer to the transmitter than the receiver (e.g. position 4), its performance is still quite limited (e.g., a SNR of 0.8dB, a packet delivery rate of 13.70%, and a throughput of 0.02) due to the poor jamming signal cancelation.

9 Related work

The proposed pinpoint system utilizes multiple antennas to deliver the service data to desired locations. The existing Multiple Input Multiple Output (MIMO) techniques (e.g., [22] and [1]) also explore multiple antennas to achieve high transmission efficiency. The antennas used in MIMO systems can send same signals to enhance the reliability of the data transmission (e.g., [22]), or different signals to increase the capacity of the wireless channel (e.g., [1]). With the proliferation of beamforming techniques [2], multiple directional antennas have been recently integrated into MIMO systems to grant the wireless accesses to different users simultaneously. This technique is known as MU-MIMO. However, MIMO and MU-MIMO techniques do not aim to pinpoint service data to desired locations. For these techniques, any user residing in the signal coverage range of the antennas can hear the transmit data.

There exist two other recent papers that are relevant to this one. The scheme proposed in [23] utilizes multiple directional antennas to deliver the service to desired locations. Specifically, each antenna sends different portion of an original message, and thus this message can be reconstructed at locations where transmit signals overlap each other. However, due to the lack of channel calibration, an attacker with high-gain, directional antennas can still capture the transmit signals to recover the original information, even if they are not at the desired locations. The scheme presented in [24] proposes to jam undesired locations to prevent illegal accesses to the confidential data, whereas this paper provides service to desired locations through jamming entanglement. Both papers are complementary to each other.

10 Conclusion

In the paper, we propose the pinpoint waveforming system to enable location-restricted service access control. To design such a system, we create the channel calibration technique that compensates the channel distortion and enables signals sent by different transmitters to arrive at the desired receiver with the same shapes. We also created the jamming entanglement technique that introduces jamming signals to significantly reduce the SNR at the eavesdropper but raise the SNR at the desired receiver. We develop a prototype system using USRPs and the experiment evaluation results validate the feasibility of the proposed system.

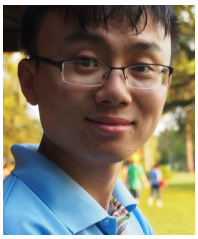
Acknowledgement

Tao Wang, Yao Liu, Tao Hou, and Song Fang are supported by NSF under grants 1527144 and 1553304, ARO under grant W911NF-14-1-0324, and Florida Cyber Security Center. Qingqi Pei are supported by NSFC under grants 61373170, U153602, and U1401251.

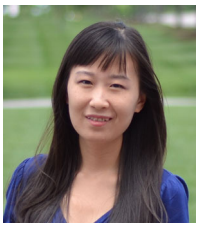
References

[1] A. Goldsmith. *Wireless communications.* Cambridge university press., 2005.
[2] R. R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya. Using directional antennas for medium access control in ad hoc networks. In *Proceedings of the MobiCom '02*, 2002.
[3] F. Sivrikaya and B. Yener. Time synchronization in sensor networks: a survey. *Network, IEEE*, 2004.
[4] J. E. Elson and D. Estrin. *Time synchronization in wireless sensor networks*. PhD thesis, University of California, Los Angeles, 2003.
[5] J. Elson, L. Girod, and D. Estrin. Fine-grained network time synchronization using reference broadcasts. *SIGOPS Oper. Syst. Rev.*, 2002.
[6] C. A. Balanis. *Antenna Theory: Analysis and Design*. Wiley-Interscience, 2005.
[7] J. Proakis and M. Salehi. *Digital Communications*. McGraw-Hill Education, 2007.
[8] T. Wang, Y. Liu, Q. Pei and T. Hou. Location-restricted Services Access Control Leveraging Pinpoint Waveforming. *Proceedings of CCS '15*, 2015.
[9] M. Biguesh and A.B. Gershman. Training-based mimo channel estimation: a study of estimator tradeoffs and optimal training signals. *Signal Processing, IEEE Transactions on*, 2006.
[10] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam. Proximate: proximity-based secure pairing using ambient wireless signals. In *Proceedings of the MobiSys'11*, 2011.
[11] M. K. Simon and M. S. Alouini. *Digital communication over fading channels*. John Wiley & Sons, 2005.
[12] J. Salz and J.H. Winters. Effect of fading correlation on adaptive arrays in digital mobile radio. *Vehicular Technology, IEEE Transactions on*, 1994.

[13] X. He, H. Dai, W. Shen, and P. Ning. Is link signature dependable for wireless security? In *INFOCOM, 2013 Proceedings IEEE*, 2013.
[14] K. Yu and B. Ottersten. Models for mimo propagation channels: a review. *Wireless Communications and Mobile Computing*, 2002.
[15] J. S. Bendat and A. G. Piersol. *Random data: analysis and measurement procedures*. John Wiley & Sons, 2011.
[16] C. Boyd and A. Mathuria. *Protocols for authentication and key establishment*. Springer Science & Business Media, 2003.
[17] H. Krawczyk, R. Canetti, and M. Bellare. *HMAC: Keyed-hashing for message authentication*. RFC Editor, 1997.
[18] S. Fang, Y. Liu, W. Shen, H. Zhu and T. Wang. *Virtual Multipath Attack and Defense for Location Distinction in Wireless Networks. Mobile Computing, IEEE Transactions on*, 2016.
[19] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential dsss: Jamming-resistant wireless broadcast communication. In *Proceedings of the INFOCOM'10*, 2010.
[20] M. Strasser, C. Pöpper, and S. Čapkun. Efficient uncoordinated fhss anti-jamming communication. In *Proceedings of the MobiHoc'09*, 2009.
[21] Gnu radio. http://gnuradio.org/redmine/projects/gnuradio/wiki.
[22] A. Lozano and N. Jindal. Transmit diversity vs. spatial multiplexing in modern mimo systems. *Wireless Communications, IEEE Transactions on*, 2010.
[23] S. Sheth, A. Seshan and D. Wetherall. Geo-fencing: Confining wi-fi coverage to physical boundaries. *Pervasive Computing*, 2009.
[24] Y. S. Kim, P. Tague, H. Lee, and H. Kim. Carving secure wi-fi zones with defensive jamming. In *Proceedings of the ASIACCS '12*, 2012.



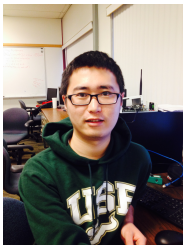
Tao Wang is currently a third-year Ph.D. student in the Department of Computer Science and Engineering, University of South Florida, Tampa, FL. His research is related to wireless network, mobile security and cyber-physical system security. Currently, his research mostly focuses on securing the wireless communication by exploring the physical-layer features of the wireless channel.



Yao Liu received the Ph.D. degree in Computer Science from North Carolina State Univ. in 2012. She is now an assistant professor at the Dept. of Computer Science and Engineering, Univ. of South Florida, Tampa, FL. Dr. Liu's research is related to computer and network security, with an emphasis on designing and implementing defense approaches that protect emerging wireless technologies from being undermined by adversaries. Her research interest also lies in the security of cyber-physical systems, especially in smart grid security. Dr. Liu's research work has appeared in premier journals and conferences including ACM Transactions on Information and Systems Security, IEEE Symposium on Security and Privacy (IEEE S&P), ACM Conference on Computer and Communications Security (CCS), and IEEE International Conference on Computer Communications (INFOCOM). She was the recipient of Best Paper Award for the 7th IEEE International Conference on Mobile Ad-hoc and Sensor Systems.

Tao Hou is a Ph.D. student in the Department of Computer Science and Engineering, University of South Florida, Tampa, FL. He received his B.S. degree from Jilin University, Changchun, China in 2013. His research mostly focuses on Big Data, Distributed Systems, and High Performance Computing.

Qingqi Pei received B.Sc., M.Sc. and Ph.D. degrees from Xidian University, Xi'an, China, in 1998, 2004 and 2008, respectively. Since 1998, he has worked in Xidian University and is now a Professor. In 2011, he was supported by the program for New Century Excellent Talents in University of China by MOE. student supervisor in Xidian University. He is a member of IEEE and ACM, senior member of Chinese Institute of Electronics and senior member of China Computer Federation. His research interests focus on wireless communication networks & security, and information security.



Song Fang is a Ph.D. candidate in Computer Science at Univ. of South Florida, Tampa, FL, USA. He received the B.S. degree in information engineering from the South China Univ. of Technology, Guangzhou, China, in Jul. 2011, and the M.S. degree in communication and information engineering from the Beijing Univ. of Posts and Telecommunications, Beijing, China, in Mar. 2014. And he started to pursue his Ph.D. from Aug. 2013. His research interests are in the area of network and system security. And his current research mainly focuses on utilizing novel physical layer techniques to improve the security in wireless networks.