Location-restricted Services Access Control Leveraging Pinpoint Waveforming

Tao Wang[†], Yao Liu[†], Qingqi Pei[‡], and Tao Hou[†]
[†]University of South Florida, Tampa, FL
[‡]Xidian University, Xi'an, China
{taow@mail, yliu@cse, taohou@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.

Categories and Subject Descriptors

C.2.1 [**Computer-Communication Networks**]: Network Architecture and Design—*wireless communication*

CCS'15, October 12–16, 2015, Denver, Colorado, USA.

DOI: http://dx.doi.org/10.1145/2810103.2813709.

Keywords

Location-restricted service; Pinpoint waveforming; 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,

- To focus limited resources on legitimate customers, restaurants and coffee shops may offer internet access to wireless users only when they are sitting at tables.
- 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.

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, the 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

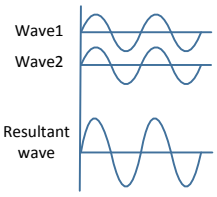


Figure 1: Constructive interference of two waves.

Figure 2: A naive idea

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 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 then 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 the received packet. 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 the 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 a receiver can receive the service data with a good quality. It should be hard for receivers outside of the service area to obtain the service 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 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 the receiver obtains a high throughput ranging between 0.90 and 0.93 when it is at the desired location, but this throughput dramatically decreases when the receiver is moved from the desired location. In particular, at a distance of 0.3 meter, the throughput of the eavesdropper 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 transmitter (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.

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.

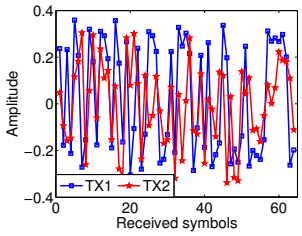


Figure 3: Without channel synchronization

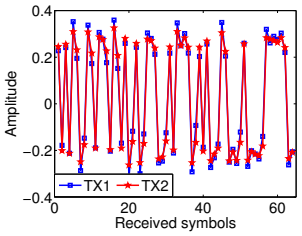


Figure 4: With channel synchronization

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 the 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. The received symbols can interfere with each other, and consequently it becomes difficult for the receiver to correctly decode the received packets. Hence, channel synchronization is required in the proposed scheme so that the received symbols can converge to the same ideal point to form a good constructive interference.

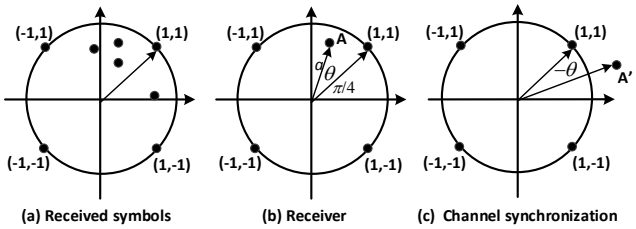


Figure 5: Basic channel synchronization

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.

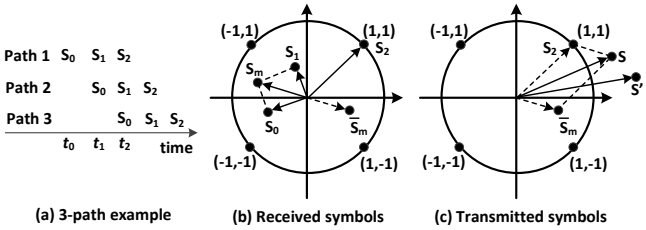


Figure 6: Refined channel synchronization against the multipath effect

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 the 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 the 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 the 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 $[n_1, n_2, ..., n_k]^t$ 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 estimation of the channel.

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 [8], 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.

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: The modulated transmit signal $S(t)$ can be writen as $S(t) = Re[\sqrt{2}A_m g(t)e^{j\theta_m}] = \sqrt{2}A_m g(t)\cos\theta_m$, 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 $A_m^2\cos\theta_m^2$. When two signals arrive at the receiver with a time shift of δ_t, the combined signal power P_c becomes $P_c = \frac{1}{T}\int_{-\frac{T}{2}}^{\frac{T}{2}} 2\{A_m\sin(2f_0t)\cos\theta_m + A_m\sin[2f_0(t+\delta_t)]\cos\theta_m\}^2 dt = 2A_m^2\cos\theta_m^2[1+\cos(2\pi f_0\delta_t)]$. We can see that P_c is highly associated with the time shift δ_t. When $\delta_t = \frac{1}{4f_0}$, the combined signal power P_c is $2A_m^2\cos\theta_m^2$. On the other hand, the SNR is $\frac{A_m^2\cos\theta_m^2}{N_c}$ at each transmitter, where N_c is the noise power. Because two arrival signals bring twice of the noise power to the receiver, the received signal power P_c must be larger than $2A_m^2\cos\theta_m^2$ to achieve a boosted SNR (i.e., the constructive interference). Thus, the tolerable time shift should be less than $\frac{1}{4f_0}$ so that $P_c > 2A_m^2\cos\theta_m^2$. □

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.

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. In particular, [9] indicates that a distance of half wavelength can lead to uncorrelated channels. In the following part, we will 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 [10]. 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 [11]: $\rho(d, f) = J_0(2\pi d/\lambda)$, 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, [12] 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 ob-

served 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 2 gives the SNR at the desired location and undesired location respectively.

LEMMA 2. *The SNR at the desired location and the undesired location are* $\frac{4P_h \cdot P_t}{N_c}$ *(*$P_t \gg \frac{N_c}{P_h}$*) 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 [13]. 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 eavesdropper's 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, $P_s = Var[S_1 \cdot h_1(\tau_l) + S_2 \cdot h_2(\tau_l)] = P_t E[|h_1(\tau_l)|^2 + 2|h_1(\tau_l) \cdot h_2(\tau_l)^*| + |h_2(\tau_l)|^2] = 2P_h \cdot P_t + 2\rho P_h \cdot P_t$, where ρ is defined as the channel correlation coefficient and equals to $\frac{|h_1(\tau_l)\cdot h_2(\tau_l)^*|}{\sqrt{Var(|h_1(\tau_l)|)Var(|h_2(\tau_l)|)}} = \frac{|h_1(\tau_l)\cdot h_2(\tau_l)^*|}{P_h}$ [14], 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. At the desired location, channels are synchronized, and original signals get boosted and jamming signals cancel each other, yielding an SNR that equals to $\frac{4P_h \cdot P_t}{N_c}$. 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 $SNR = \frac{P_s}{P_c + N_c} \approx \frac{P_t}{P_j}$. □

Impact of SNR on service area size: Assume $P_j = P_t$, from Lemma 2, we can see that SNR approximate to 1 when $\rho = 0$ and the value 1 is the minima of SNR. With $SNR = 1$, the receiver cannot distinguish between the original and 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.

6.3 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 [15] [16], and spread spectrum techniques like Frequency Hopping Spread Spectrum(FHSS) and Direct Sequence Spread Spectrum (DSSS) can be designed to defend against jamming attacks [17] [18].

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 2, when the eavesdropper's channel is totally uncorrelated from the receiver's channel, it will not achieved 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, no matter how many eavesdroppers exist, the signals received by these eavesdroppers still suffer from the wireless channel fading like the multipath fading, and always exhibit different shapes as long as their channels are not calibrated for homomorphism at the service provider side. Both the channel distortion and the jamming signal cause the sum of received signals equivalent to that of multiple random signals. 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.

These traditional techniques can be integrated into the pinpoint system to support multiple users. Specifically, for CDMA, the transmitter can directly encode jamming entangled signal using the CDMA codes to deliver information to all users. Since users are located at different locations, the transmit signals may need to be sent at distinct times to compensate the time difference, and thus asynchronous CDMA scheme is required at the transmitter. For TDMA, the transmitter can pinpoint the service to each user during its time slot. Note that the propagation synchronization may introduce overlapping time slots due to the varying time shifts experienced by different users. Thus, proper time guard should be inserted between time slots to eliminate the overlaps and avoid the interference among multiple users. For FDMA, the transmitter can pinpoint the service to each user at the assigned frequency band. If the Orthogonal Frequency-division Multiplexing (OFDM) is enforced, because the spectrum assigned to each user by OFDM is normally limited, the receiver may have a weak multipath effect that causes less distortion to jamming entangled signals. Nevertheless, the amplitude attenuations are different for different locations, without channel synchronization, the jamming entangled signals still exhibit random amplitudes when arrive at an undesired receiver, and consequently the jamming portion cannot cancel each other, ensuring the service exclusiveness.

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 [19].

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 and file transfer 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 Example Pinpoint Service

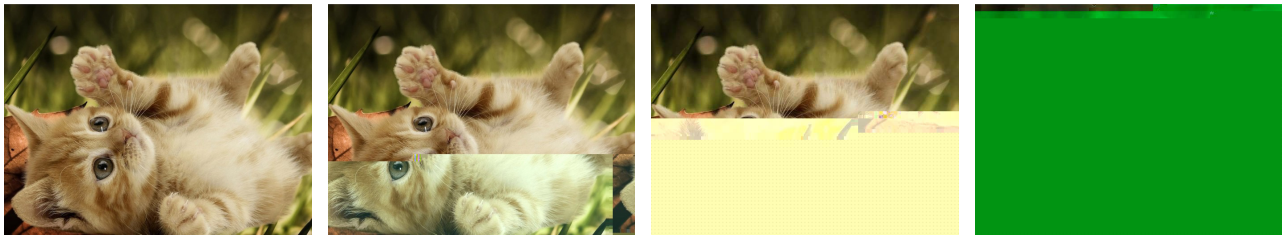
We choose two typical types of service data, pictures and videos, to visually validate the effect of the pinpoint prototype. Figure 7 shows the received pictures at different positions. At the desired location, the receiver can successfully download the original picture sent by the transmitter. We then move the receiver 0.1, 0.2, and 0.3 meter away from the desired location, and find a drastic worsening of the packet delivery rate. When the receiver is 0.3 meter away, the picture cannot be displayed at all due to the huge number of packet loss.

We also implement the real-time video transmission that sends a live scene captured by a web camera to the receiver. Specifically, a web camera is connected to the transmitter to surveillance the surrounding of the transmitter. We encode the video stream using MPEG-4 AVC, which is the most commonly used format for video compression, and input the stream into the USRPs through the Linux socket interface. We then pinpoint the stream to the receiver at the desired location. The receiver downloads and decodes packets from the transmitter and displays them on a video player. We observe a clear and fluent video when the receiver is located at the desired position, and the video quality deteriorates when the receiver moves away from undesired locations. In particular, we encounter frequent video stuck while playing, and severely distorted images. At the physical layer, we find that received symbols significantly deviate from the ideal points on the constellation diagram, thereby yielding a huge amount of demodulation errors. We recorded the video deterioration process and an anonymous demo video on youtube can be found at `https://youtu.be/lJ64bxYP5SM`. In the following, we discuss the details of the evaluation results.

8.3 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



(a) Desired location (b) 0.1 meter away (c) 0.2 meter away (d) 0.3 meter away

Figure 7: Received pictures at different positions

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 looking at 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.

8.4 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 the last metric channel cross-decorrelation is not as straightforward as the pervious three metrics, because it reflects the disparity among wireless 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 8 and 9 plot the magnitude (i.e. amplitude attenuation) and phase (i.e phase shift) of the average channel

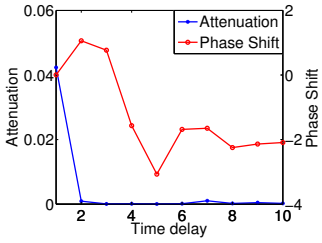


Figure 8: USRP 1

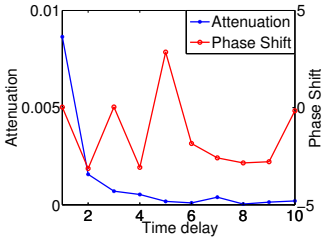


Figure 9: USRP 2

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 10 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 10, 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.

8.5 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 13(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 13(b), 13(c), and 13(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 and thus the 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.

8.6 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 11 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 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.

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

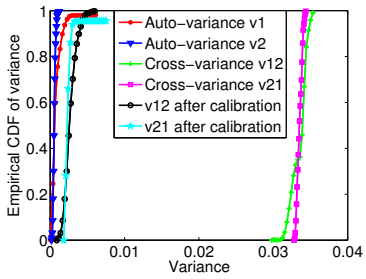


Figure 10: Distribution of different variance

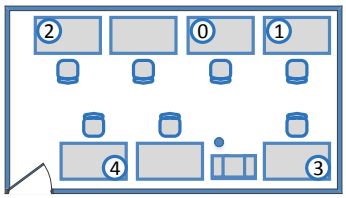


Figure 11: Floor plan: Service area size

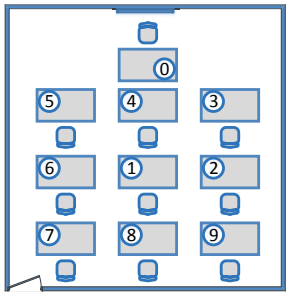
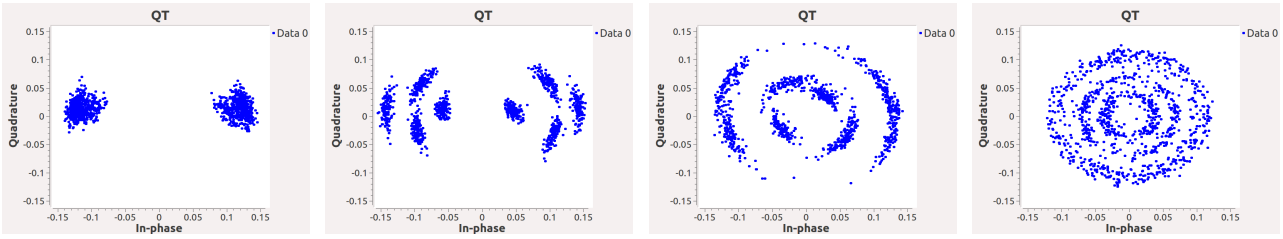


Figure 12: Floor plan: pinpoint accuracy



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

Figure 13: Jamming signal entanglement

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

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 the decreasing signal to jamming power ratio.

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

8.7 Pinpoint Accuracy

We test how accurate the prototype system can pinpoint the service to a desired location in a meeting room. Figure 12 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. 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 4: 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 4. 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., [20] 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., [20]), 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 [21] 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 [22] 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.

11. ACKNOWLEDGEMENT

This work is supported by the Army Research Office under grant W911NF-14-1-0324, Florida Cyber Security Center, and NSFC under grants U1401251 and 61373170.

12. 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] 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.

[9] 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.

[10] M. K. Simon and M. S. Alouini. *Digital communication over fading channels*. John Wiley & Sons, 2005.

[11] J. Salz and J.H. Winters. Effect of fading correlation on adaptive arrays in digital mobile radio. *Vehicular Technology, IEEE Transactions on*, 1994.

[12] X. He, H. Dai, W. Shen, and P. Ning. Is link signature dependable for wireless security? In *INFOCOM, 2013 Proceedings IEEE*, 2013.

[13] K. Yu and B. Ottersten. Models for mimo propagation channels: a review. *Wireless Communications and Mobile Computing*, 2002.

[14] J. S. Bendat and A. G. Piersol. *Random data: analysis and measurement procedures*. John Wiley & Sons, 2011.

[15] C. Boyd and A. Mathuria. *Protocols for authentication and key establishment*. Springer Science & Business Media, 2003.

[16] H. Krawczyk, R. Canetti, and M. Bellare. Hmac: Keyed-hashing for message authentication. 1997.

[17] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential dsss: Jamming-resistant wireless broadcast communication. In *Proceedings of the INFOCOM'10*, 2010.

[18] M. Strasser, C. Pöpper, and S. Čapkun. Efficient uncoordinated fhss anti-jamming communication. In *Proceedings of the MobiHoc'09*, 2009.

[19] Gnu radio. `http://gnuradio.org/redmine/projects/gnuradio/wiki`.

[20] A. Lozano and N. Jindal. Transmit diversity vs. spatial multiplexing in modern mimo systems. *Wireless Communications, IEEE Transactions on*, 2010.

[21] S. Sheth, A. Seshan and D. Wetherall. Geo-fencing: Confining wi-fi coverage to physical boundaries. *Pervasive Computing*, 2009.

[22] 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.