# CloseTalker: Secure, Short-Range Ad Hoc Wireless Communication

Timothy J. Pierson
Dartmouth College

Travis Peters
Dartmouth College

Ronald Peterson
Dartmouth College

David Kotz
Dartmouth College

## ABSTRACT

Secure communication is difficult to arrange between devices that have not previously shared a secret. Previous solutions to the problem are susceptible to man-in-the-middle attacks, require additional hardware for out-of-band communication, or require an extensive public-key infrastructure. Furthermore, as the number of wireless devices explodes with the advent of the Internet of Things, it will be impractical to manually configure each device to communicate with its neighbors.

Our system, *CloseTalker*, allows simple, secure, ad hoc communication between devices in close physical proximity, while jamming the signal so it is unintelligible to any receivers more than a few centimeters away. CloseTalker does not require any specialized hardware or sensors in the devices, does not require complex algorithms or cryptography libraries, occurs only when intended by the user, and can transmit a short burst of data or an address and key that can be used to establish long-term or long-range communications at full bandwidth.

In this paper we present a theoretical and practical evaluation of CloseTalker, which exploits Wi-Fi MIMO antennas and the fundamental physics of radio to establish secure communication between devices that have never previously met. We demonstrate that CloseTalker is able to facilitate secure in-band communication between devices in close physical proximity (about 5 cm), even though they have never met nor shared a key.

**ACM Reference Format:**
Timothy J. Pierson, Travis Peters, Ronald Peterson, and David Kotz. 2019. CloseTalker: Secure, Short-Range Ad Hoc Wireless Communication. In *The 17th Annual International Conference on Mobile Systems, Applications, and Services (MobiSys '19), June 17–21, 2019, Seoul, Korea.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3307334.3326100

## 1 INTRODUCTION

Analysts predict *billions* of everyday devices will soon become "smart" with the addition of wireless communication capabilities [26]. These Internet of Things (IoT) devices are envisioned to share data and control information among themselves, some of which may be privacy sensitive or have security implications. With so many IoT devices being deployed, people will find it increasingly inconvenient to configure and connect new devices, or to arrange short-lived contact with the dozens of new devices they may encounter every day.

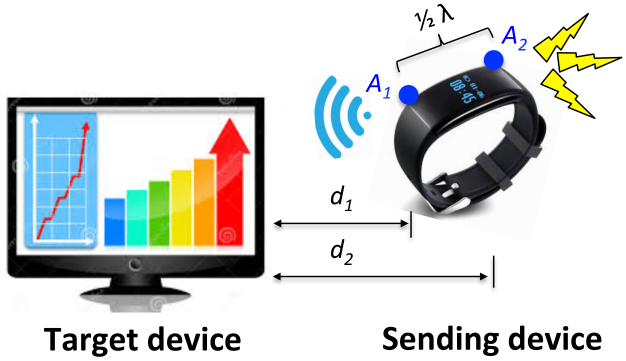

**Figure 1: A multiple-antenna 'sending' device uses antenna $A_1$ to send a data signal to a 'target' device located at distance $d_1$, while antenna $A_2$ located $d_2$ from the target transmits jamming.**

As one concrete illustration of this problem, imagine a person who collects health-related data on a wearable device and wants to show that data to her physician. The wearable device has a limited display or no display whatsoever, making it difficult or impossible for the patient and physician to view the information together. There may, however, be a display in the physician's exam room and the goal is to get data securely from the wearable to the display as shown in Figure 1. In this scenario the two devices have never met nor shared a key, but need to share sensitive medical information. If that data were revealed, others may learn something about the patient that the patient would prefer remain confidential.

There are many situations like this – where data must be securely transferred to a newly encountered device in close physical proximity, or where it is important to ensure data is not accidentally exposed to distant devices. Creating secure communication in these circumstances is difficult for several reasons, including: (1) devices that have not been previously encountered cannot be preconfigured with shared secrets, (2) exchanging secrets over the air creates the possibility for man-in-the-middle attacks, (3) manual secret entry becomes increasingly impractical as the number of devices grows, and (4) IoT devices often have limited or non-existent user interfaces, making manual secret entry such as Bluetooth's Simple Secure Pairing difficult or impossible.

*MobiSys '19, June 17–21, 2019, Seoul, Korea*
© 2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-6661-8/19/6...$15.00
https://doi.org/10.1145/3307334.3326100

## 1.1 CloseTalker

To enable secure communications where devices discover each other in an ad hoc manner, we present a theoretical and practical evaluation of a novel system called *CloseTalker*. CloseTalker uses jamming to cover information exchanged between a multiple-antenna 'sending' device and another nearby 'target' device as shown in Figure 1. We use Wi-Fi to demonstrate CloseTalker, but the technique could be adapted for other protocols such as Bluetooth or Zigbee. CloseTalker has the following attributes.

*One antenna transmits data, another jams.* The sending device uses antenna $A_1$ to transmit a data signal to the target device located at distance $d_1$, while using a second antenna $A_2$ located $d_2$ from the target to broadcast barrage jamming (random noise). Multiple antennas are becoming common in mobile devices, and in fact multiple antennas are required to take advantage of advanced features such as beam forming in the Multiple-Input, Multiple-Output (MIMO) configurations of 802.11n [15] and 802.11ac [14].

To perform effective beam forming, antennas are typically separated by one-half wavelength [27]. With Wi-Fi 2.4 GHz devices, one-half wavelength is roughly 6.2 cm. Some devices may simply be too small to support multiple antennas. In these cases, the small device can act as a CloseTalker target, but not a sender. We discuss a bi-directional communication scenario in Section 7.

*Inverse-Square Law protects data transfer.* CloseTalker's multiple antennas, separated by one-half wavelength, create a situation where the legitimate target device is able to correctly receive the transmitted data, despite the presence of jamming, while denying a more distant adversary the ability to recover the data. Below we show that when a target device is in close physical proximity (about 5 cm) to a sending device, due to the Inverse-Square Law governing the physics of radio signal propagation, the data signal can be received with up to 50 times more strength than the jamming. This arrangement ensures data is correctly received only by devices that are in close physical proximity. More distant devices receive roughly equal data and jamming strength, making data recovery unlikely.

*Meant for user-intended ad hoc encounters.* CloseTalker is intended to transfer data under jamming cover when a user moves devices into close proximity *and* initiates communication by taking an action such as pressing a button on the sending device. In this case, proximity combined with the user's deliberate action can serve as a root of trust between devices that have not previously shared a secret.

*Supports long-range and long-term data transfer, too.* If the amount of data to transfer is small, CloseTalker's jamming can cover the one-time data transfer. If the amount of data to transfer is large, or devices need to communicate many times or at long distances, CloseTalker can transfer a secret key, which the two devices can then use to bootstrap a secure data-transfer session or long-term / long-distance secure relationship using traditional methods like TLS, with or without an AP, with or without the Internet.

*No need for additional hardware, pre-shared secrets, or complex algorithms.* Unlike other approaches, CloseTalker does not require any specialized hardware in the target devices, any hardware to support out-of-band communication, any pre-shared secrets, any complex algorithms or cryptography libraries, or any infrastructure such as access points or PKI authorities. In fact, the receiving device need not be aware that the sender is using CloseTalker's techniques.

*No additional network interference.* CloseTalker conforms to the Wi-Fi specification by performing Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to avoid interference with other devices operating in an environment [15]. CloseTalker transmits both the data and jamming signals simultaneously during the time a normal Wi-Fi device would transmit only data. In this way CloseTalker does not create additional interference for other devices.

## 1.2 Assumptions

We evaluate our system using commercial-off-the-shelf (COTS) receivers and assume either the target or the sender (or both) can be moved so that the devices can be placed in close physical proximity, at least temporarily. We make the following assumptions about the target device: 1) it has at least one radio antenna to receive wireless data, 2) it might not have sensors such as cameras, microphones or accelerometers, and 3) new hardware or software cannot be added.

We assume the transmitting device has: 1) a radio compatible with that of the target device, 2) at least two antennas located approximately one-half wavelength apart, and 3) one antenna can send data while a second antenna transmits barrage jamming. The transmitting device may also be adorned with an indicator such as an arrow to reveal how to best align the devices for maximum throughput (see Section 4).

Finally, we assume adversaries are located more than about 7 cm away. Adversaries face the same difficulties legitimate devices face separating data from jamming. Our experimental results in Section 5 are for single-antenna COTS Wi-Fi receivers only, but in Section 6 we examine CloseTalker's theoretical security against adversaries with two antennas. We do not present any experimental data regarding the resilience of CloseTalker against attacks nor any analysis of it against attacks using more than two antennas.

## 1.3 Contributions

CloseTalker is a novel approach for securely transferring data between adjacent devices, even though the devices have never met, nor have any secrets been pre-shared. This paper makes the following contributions:

(1) a consistent, fast, easy, and secure method to transfer any kind of information between commodity wireless devices, regardless of device type or manufacturer, without hardware modifications to the devices,

(2) a theoretical analysis of jamming at close range to facilitate data transfer, and
(3) an experimental evaluation of the feasibility of using CloseTalker to transfer data to unmodified receivers.

## 2 RADIO SIGNAL PROPAGATION

In this section we review some background information useful for understanding CloseTalker's strategy. CloseTalker's approach for overcoming jamming when devices are in close physical proximity relies on the fact that radio waves attenuate proportionally with the distance the signal travels. CloseTalker's insight is that the signal from the nearby data antenna can be sufficiently stronger than the signal from the farther jamming antenna for the receiver to recover the data signal despite the presence of jamming, while a more distant adversary cannot. The nature of the signal, however, depends on the distance between transmitter and receiver. When a receiver is extremely close to a transmitter, the receiver is said to be in the *near field* of the transmitter. At longer range, the receiver is said to be in the *far field* (also called the *Fraunhofer* region).

The boundary between the near and far field for a finite-length transmitting dipole antenna is estimated at distance $d$ from the antenna as follows [5]:

$$d = \frac{2D^2}{\lambda} \tag{1}$$

where $D$ is the length of the transmitting antenna plus the length of the receiving antenna, and $\lambda$ is the signal wavelength. Equation (1) projects that the far field for quarter-wavelength antennas at Wi-Fi's 2.4 GHz band begins at roughly 6.2 cm and is as short as 3.1 cm for Wi-Fi's 5 GHz band.[1] This boundary is not sharp, but instead transitions gradually between the near and far fields.

In the far field radio waves attenuate proportionally to the square of the distance between the transmitter and receiver. This signal propagation relationship is captured in the far field by the well-known Friis transmission model [27]:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 \tag{2}$$

where $P_r$ is the power at the receiving antenna in milliwatts, $P_t$ is the power transmitted, $G_t$ is the gain of the transmitting antenna, $G_r$ is the gain of the receiving antenna, $\lambda$ is the wavelength of the signal, and $d$ is the distance between the transmitting and receiving antennas. From Equation (2) it is clear that if the distance $d$ between transmitter and receiver is reduced by one-half, then the received power is increased by a factor of four.

### 2.1 Estimating signal power density at close range

Equation (1) gives an estimate for the boundary between the near and far field, but in reality the boundary is not sharply defined. Instead, the electric **E** and magnetic **H** fields generated by a transmitting antenna begin to align more fully so that they are orthogonal (perpendicular) to each other, transverse to the radial direction of propagation, as the signal moves substantially into the far field.

Because the boundary is not sharp and CloseTalker is designed for communications between devices separated by approximately the estimated distance from Equation (1), we cannot simply use Equation (2) to estimate signal strength at the receiver because Equation (2) is only valid in the far field.

Balanis, however, gives approximations for the **E** and **H** fields and shows that they are valid everywhere, except on the surface of the antenna, for a thin-wire (radius $r \ll l$) finite-length dipole [5]:

$$\mathbf{E} \simeq j\eta \frac{I_0 e^{-jkd}}{2\pi d}\left[\frac{\cos(\frac{kl}{2}\cos\theta) - \cos(\frac{kl}{2})}{\sin\theta}\right] \tag{3}$$

$$\mathbf{H} \simeq j \frac{I_0 e^{-jkd}}{2\pi d}\left[\frac{\cos(\frac{kl}{2}\cos\theta) - \cos(\frac{kl}{2})}{\sin\theta}\right] \tag{4}$$

where $j = \sqrt{-1}$, $\eta = 120\pi$ is the intrinsic impedance of free space, $I_0$ is the current applied to the transmitter, $k = 2\pi/\lambda$ is the wavenumber, $d$ is the distance from the transmitting antenna, and $\theta$ is the vertical angle between the transmitter and receiver (below we assume $\theta = \pi/4$ indicating the two antennas are vertically aligned).

Given Equations (3) and (4), we can estimate the average power density [5]:

$$\mathbf{W}_{av} = \frac{1}{2}\Re[\mathbf{E} \times \mathbf{H}^*]. \tag{5}$$

where $\Re$ is the real component of these complex numbers and $^*$ is the complex conjugate.

Equation (5) suggests that power density drops with the square of distance. If the distance $d$ between transmitter and receiver is reduced by one-half, then the average received power is increased by a factor of four. This relationship between distance and power is often referred to as the *Inverse Square Law.*

The relationship is particularly stark when a receiver is in close proximity to a transmitter. Figure 2 shows the expected average power density according to Equation (5), where transmitting antenna $A_1$ and $A_2$ are separated by a fixed distance of one-half wavelength, and a receiver is located $d_1$ cm away from $A_1$, such that $d_2 = d_1 + \lambda/2$. Antenna $A_1$ transmits a data signal while antenna $A_2$ transmits barrage jamming. Each antenna transmits at equal magnitude. In this figure we model a 24 dBm Wi-Fi signal transmitted on channel 1's center frequency of 2.412 GHz, which has wavelength $\lambda \approx 12.5$ cm.

We see in Figure 2 that when a receiver is very close to a transmitter, it receives a significantly stronger signal than a signal from a transmitter located only one-half wavelength farther away. In this case, when antenna $A_1$ is located at $d_1 = 1$ cm, then $d_2 \approx 7.25$ cm, that is, 7.25 times farther than $d_1$. Because the power received is relative to the square

[1] Some sources suggest the far field for short antennas (where $l \ll \lambda$) are best approximated by $d = \frac{\lambda}{2\pi}$ which yields distances of 1.9 cm and 0.8 cm for the 2.4 and 5 GHz bands respectively.

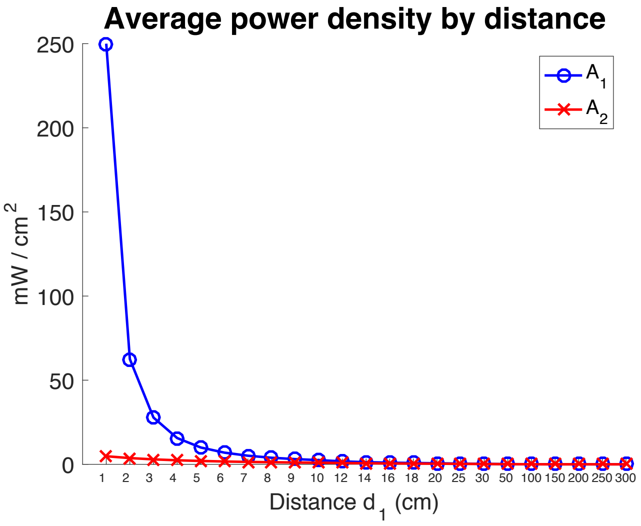

**Figure 2: Expected power received from two transmitting antennas, each sending a 24 dBm signal, with antenna $A_1$ located at distance $d_1$ cm from the receiver and antenna $A_2$ located $d_2 = d_1 + \lambda/2$ from the receiver.**

of distance, even though both transmitting antennas are physically close to the receiver, the signal from $A_1$ is roughly 50 times stronger than the signal from antenna $A_2$. The difference in power between a signal sent from antenna $A_1$ and $A_2$ drops quickly as distance from the transmitter increases. When $A_1$ is more than about 7 cm away from the target, the received signal strength from each transmitter is virtually identical. A distant device therefore receives roughly equal-strength signals from each antenna.

When devices are in close proximity they enjoy a unique channel advantage over devices located farther away. That channel superiority vanishes quickly as devices move apart. CloseTalker uses this channel advantage between nearby devices to provide secure communications while denying a more distant adversary the ability to recover the data.

# 3 SIGNAL ERRORS

The performance of wireless digital communication systems carrying data in the presence of noise (both natural and intentional) has been well studied and has produced analytical models that predict the number of communication errors expected to occur given three factors: 1) data signal strength, 2) noise intensity, and 3) modulation scheme. In this section we use those models to calculate the theoretical error rates given the physical arrangement of transmitter and receiver described in Section 2 where a target device is located near data antenna $A_1$ and one-half wavelength farther from jamming antenna $A_2$. In Section 5 we present the results from experiments using real, commercial-off-the-shelf Wi-Fi receivers.

## 3.1 Data signal strength and noise intensity

The relationship between a signal and noise is captured by the Signal-to-Noise Ratio (SNR) [11]:

$$\text{SNR} = \frac{P_r}{N_0 B} = \frac{E_s}{N_0 B T_s} = \frac{E_b}{N_0 B T_b} \tag{6}$$

where $P_r$ is the received power of the data signal, $N_0$ is the power spectral density of the noise, $B$ is the bandwidth, $E_s$ is the energy per symbol, $E_b$ is the energy per bit, $T_s$ is the symbol time, and $T_b$ is the bit time. For pulse-shaping systems such as Wi-Fi where $T_s = N/B$, Equation (6) simplifies to SNR $= E_s/(N_0 N)$ where $N$ is the number of samples per symbol.

In the presence of barrage noise jamming, where the jammer interferes across the entire signal bandwidth (as opposed to tone jamming where noise is only transmitted on specific frequencies), the total power spectral density of the noise becomes [17]:

$$N_t = N_0 + N_j \tag{7}$$

where $N_t$ is the total noise power spectral density, $N_0$ is the power spectral density of any background noise, and $N_j$ is the power spectral density of the barrage jamming. Accounting for noise provides the Signal-to-Interference-plus-Noise Ratio (SINR) where:

$$\text{SINR} = \frac{P_r}{(N_0 + N_j)B} = \frac{P_r}{N_t B}. \tag{8}$$

Equation (8) can be used to provide the SINR per symbol, $\gamma_s$ [11]:

$$\gamma_s = \frac{P_r T_s}{N_t B T_s} = \frac{E_s}{N_t B T_s} = \frac{E_s}{N_t N}. \tag{9}$$

## 3.2 Modulation schemes

802.11a/g/n/ac uses Orthogonal Frequency Division Multiplexing (OFDM) [15] to send data symbols over several different subcarriers simultaneously, resulting in higher data rates than serial single-channel communications. Speed can be further enhanced with the type of modulation used on each subcarrier. In Wi-Fi the simplest modulation type is Binary Phase Shift Keying (BPSK), where each symbol represents one bit. More complex than BPSK, Quadrature Phase Shift Keying (QPSK) symbols represent two bits of information. Finally, Quadrature Amplitude Modulation ($M$QAM) is the most complex Wi-Fi modulation type where each symbol represents $\log_2(M)$ bits and $M$ is 16, 64, or 256. More complex modulation schemes increase the data rate because each symbol represents more bits. Figure 3 shows these modulation types in a constellation diagram where a symbol, representing one or more bits, is shown as a dot in the complex plane.

To send a symbol, a transmitter selects the complex number on the constellation diagram representing the desired bit pattern, then modulates a cosine wave on a carrier frequency with the real component of the complex number, and also modulates a sine wave on the same carrier frequency with

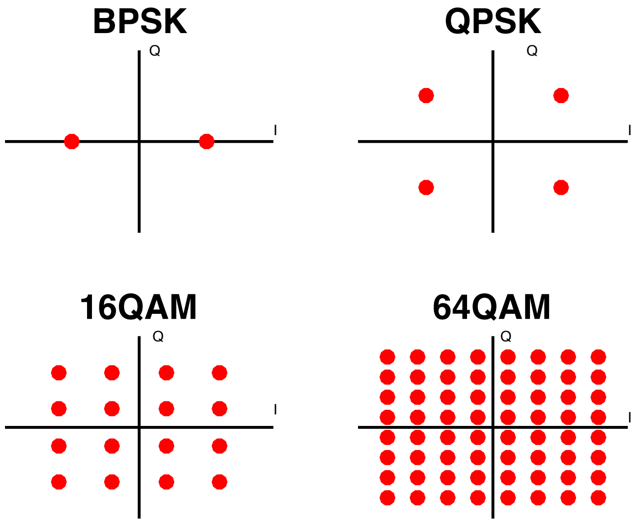

**Figure 3: Wi-Fi constellation diagrams. Dots represent symbols in the complex plane.**

the imaginary component of the complex number. In this way the transmitter can send both the real and imaginary component of the complex number simultaneously on a single radio frequency.

After compensating for channel effects, the receiver receives the signal according to the Additive White Gaussian Noise (AWGN) model as:

$$y[t] = x[t] + n[t] \tag{10}$$

where $y[t]$ is the received signal, $x[t]$ is the transmitted signal, and $n[t]$ is the noise on the channel at time $t$.

The receiver then determines the nearest symbol to $y[t]$ on the complex plane. Because $y[t]$ includes noise, it may not fall exactly on a symbol, so the receiver chooses the closest symbol and infers that symbol is what the transmitter sent. Using a more complex modulation increases the susceptibility to noise because there are more possible symbols and smaller amounts of noise can cause the receiver to misinterpret a symbol corrupted by noise.

To compensate for noise, Wi-Fi uses convolutional coding to create redundancy by adding duplicate bits to each transmission. For example, 1/2 coding means that each bit is duplicated, resulting in 2 bits for every input bit. Coding redundancy reduces the overall data rate (e.g., 1/2 coding reduces the data rate by half), but can improve throughput by increasing reliability, especially in noisy environments.

A modulation type combined with a coding scheme is known as a Modulation Coding Scheme (MCS). 802.11g can use one of eight different schemes: BPSK 1/2, BPSK 3/4, QPSK 1/2, QPSK 3/4, 16QAM 1/2, 16QAM 3/4, 64QAM 2/3, and 64QAM 3/4. 802.11n and 802.11ac can use these modulation schemes as well, but can also use more complex modulation schemes. In Section 5, however, we see that more complex schemes cannot survive the jamming from antenna $A_2$, so we focus on these eight modulation coding schemes.

| Modulation | M | $P_s$ |
|---|---|---|
| BPSK | 2 | $Q\left(\sqrt{2\gamma_b}\right)$ |
| QPSK | 4 | $2Q\left(\sqrt{\gamma_b}\right) - Q^2\left(\sqrt{\gamma_b}\right)$ |
| 16QAM | 16 | $4Q\left(\sqrt{\frac{4\gamma_b}{5}}\right)$ |
| 64QAM | 64 | $4Q\left(\sqrt{\frac{3\gamma_b}{7}}\right)$ |

**Table 1: Probability of symbol error $P_s$ by modulation type.**

### 3.3 Energy per bit

The MCS influences the energy per bit because a symbol may represent many bits, and each bit may be duplicated. Taking the energy per symbol from Equation (9) as a constant, the bit redundancy yields the SINR per bit, $\gamma_b$ [11]:

$$\gamma_b \approx \frac{\gamma_s}{R_c \log_2 M} \tag{11}$$

where $\log_2 M$ is the number of bits per symbol and $R_c$ is the coding rate (e.g., 1/2). There is a trade off in Equation (11): as the number of bits per symbol increases, the energy per data bit deceases, but as the coding scheme produces more redundant bits, the energy per data bit increases.

### 3.4 Estimating errors

Assuming an AWGN channel between sender and receiver, that all symbols in a modulation scheme are equally likely to be transmitted, and that Gray coding is used, so that one symbol error corresponds to one bit error (a conservative estimate, especially for complex modulation schemes), we can calculate the probability of a symbol error, $P_s$. Goldsmith [11] gives an excellent information-theoretic derivation of the error estimate equations shown in Table 1 where the $Q$ function is

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-\frac{x^2}{2}} dx. \tag{12}$$

Table 1 indicates the probability of a symbol error depends on the signal's power relative to noise and the modulation type chosen. Assuming Gray coding, we can also estimate the probability of a bit error, $P_b$, as

$$P_b \approx \frac{P_s}{\log_2 M}. \tag{13}$$

Next we use these estimates to predict the ability of CloseTalker to successfully transmit data to nearby devices while denying more distant devices.

## 4 THEORETICAL PERFORMANCE

Section 3 provided the mathematical underpinning to estimate CloseTalker's theoretical performance. In this section we

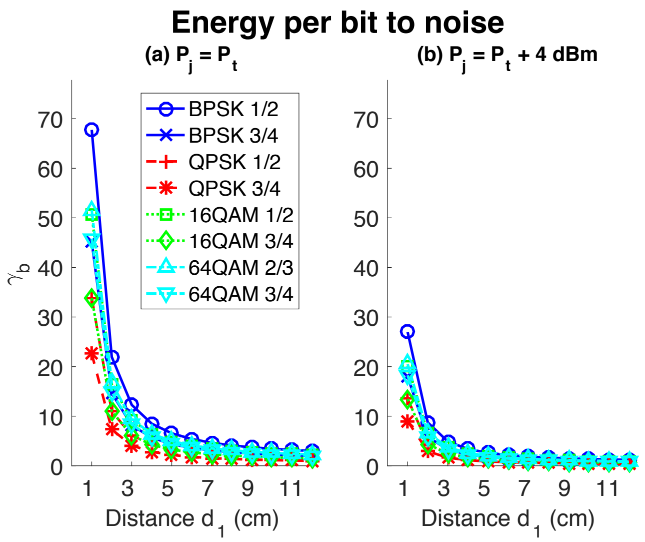

**Figure 4: Energy per bit vs. noise at close range.**

use those equations to model CloseTalker's expected performance and in Section 5 we provide the results of experiments using COTS Wi-Fi devices. For all experiments and theoretical estimates we separate antennas $A_1$ and $A_2$ by one-half wavelength, with $d_2 = d_1 + \lambda/2$, and arbitrarily choose Wi-Fi channel 1. We model jamming phase and amplitude using a normal Gaussian distribution with zero mean and unit standard deviation, $X \sim \mathcal{N}(\mu = 0, \sigma^2 = 1)$.

Table 1 shows that the key to estimating errors, regardless of modulation scheme, is the ratio between the energy per bit and the energy in the noise. For CloseTalker, that ratio is primarily driven by two factors: 1) the geometry between the target device and the sending device's antennas, and 2) the ratio of transmit power of the two antennas (there is of course other noise in the environment; we model it at $-92$ dBm [13] but it typically has little impact on the error estimates).

## 4.1 Geometry

Geometry drives the ratio between signal and noise as shown in Figure 4a. We estimate the received power of the data signal, $P_r$, using Equation (5) at distance $d_1$. We estimate the noise power similarly, but using the transmit power $P_j$ from jamming antenna $A_2$ at distance $d_2$. Assuming that antenna $A_1$ transmits data at the same strength that $A_2$ transmits jamming, due to redundancy in some modulation coding schemes, when the target device is located near antenna $A_1$, the energy per bit will be up to 70 times stronger than the jamming signal. That ratio is maximized when the target device is located where $d_1$ is small and the antennas are aligned so that $d_2 = d_1 + \lambda/2$ as shown in Figure 1.

We assume CloseTalker devices can be adorned with an indicator such as an arrow to reveal how to align the devices. If the target is not well aligned relative to the transmit antennas, the ratio of signal strength to jamming will be reduced, resulting in increased noise relative to the signal. This works to CloseTalker's advantage because legitimate receivers can be placed near the transmit antennas and easily aligned to maximize $d_2$, leveraging the Inverse-Square Law, whereas more distant or less geometrically aligned devices will see a lower $\gamma_b$ as shown in Figure 4a.

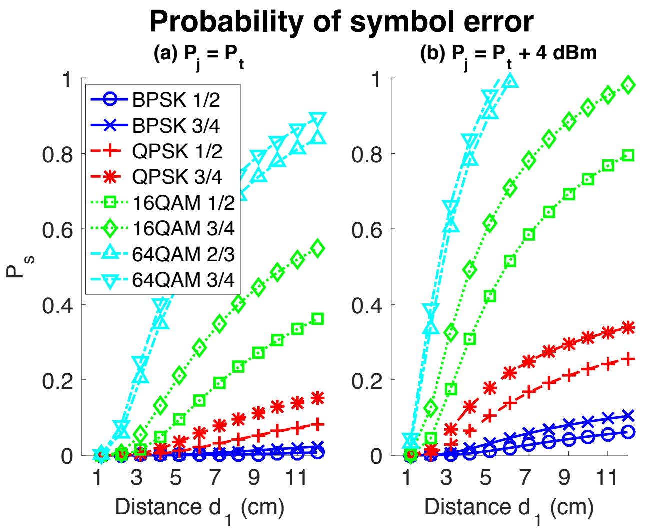

**Figure 5: Probability of symbol error by MCS for devices in close proximity.**

## 4.2 Jamming transmit power

Another factor that can affect the ratio of energy per symbol to noise is the transmit power of the data and jamming signals. We model the jamming transmit power as $P_j = P_t + \delta$ dBm, where $\delta \in \{0, 4\}$. In the first case the data and noise signal transmit power are equal; in the second case the jamming power is 4 dBm (2.5 times) higher than the data signal. In this latter case, shown in Figure 4b, CloseTalker relies even more heavily on the geometry and Inverse-Square Law to ensure the receiver is able to recover the data signal in the presence of more noise. If the legitimate target device is placed near the data antenna, the received data signal can still be almost 30 times stronger than the jamming signal.

Figure 5 plots the theoretical probability of a symbol error, $P_s$, using the equations in Table 1 and the energy per bit to noise, $\gamma_b$, when CloseTalker uses each of the eight modulation schemes and the target is aligned with the transmit antennas. We see symbols transmitted with the simpler modulation types of BPSK and QPSK are more likely to be received without error than the more complex $M$QAM modulation schemes.

Wi-Fi groups bits into frames for transmission. If a frame contains $b$ bits, then the probability a frame is received without error, $P_f$, is:

$$P_f = (1 - P_s)^{b/\log_2 M}. \quad (14)$$

Figure 6 shows $P_f$ for each modulation scheme, assuming the frame contains a modest payload of $b = 1,024$ bits. We see that frames are likely to be received without error for BPSK and QPSK when the target is close (less than about

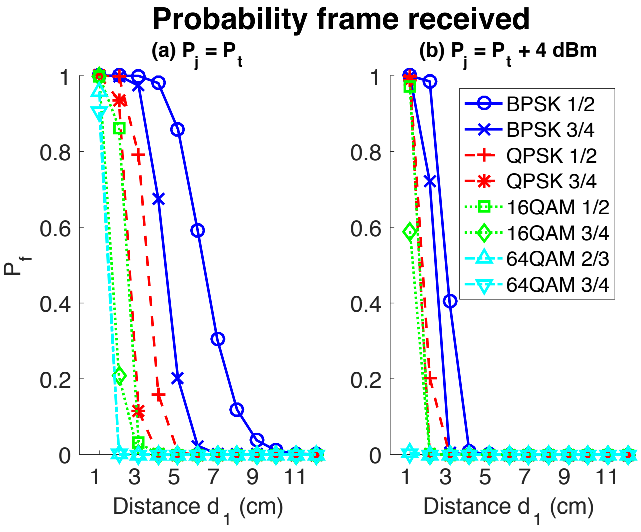

**Figure 6: Probability a frame is received without error, given a 1,024 bit frame.**

5 cm), and the probability of receiving a frame without error becomes extremely low at greater distances.

These estimates suggest that BPSK will likely be a good candidate to securely and reliably transfer data to a device in close physical proximity in the presence of jamming, while denying a more distant eavesdropper. This distance limitation may also help mitigate innocent errors where data is unintentionally transferred to a device located farther away from the multiple-antenna device.

### 4.3 Data transmit power

Another possible approach to securely transferring data between two nearby devices is to lower the data transmit power and naively hope that a more distant eavesdropper would not able to receive the weak signal. Reducing the typical Wi-Fi transmit power of approximately 24 dBm to 4 dBm would reduce the transmit power by a factor of 100. Intuitively, that approach appears to be an easy way to reduce an adversary's range by a factor of 100. Because the signal attenuates with the square of distance, however, that is not the case. If we know the minimum signal strength at which a device can receive a signal, $P_r$, and assuming the device is in the far field, we can derive the maximum distance where a transmitted signal is recoverable by re-writing Equation (2) as:

$$d = \frac{\lambda}{4\pi\sqrt{\frac{P_r}{P_t G_t G_r}}} \tag{15}$$

where $P_t$ is the transmit power, $G_t$ and $G_r$ are the gain of the transmitter and receiver respectively.

For example, if a system is able to recover a signal at $P_r = -73$ dBm [13], and no obstacles attenuate a 24 dBm signal, then by Equation (15), the received power will reach the device's minimum after the signal travels approximately 700 m. Dropping the transmit power to 4 dBm, however, yields a distance of roughly 70 m, only 10 times less than when transmitted at high power, not the 100 times reduction in range that one might have expected.

These calculations suggest that to avoid detection by an adversary located less than 1 m away, the transmit power will need to be reduced to an extremely low level. In theory, reducing the transmit power to $-50$ dBm would result in a $-73$ dBm received signal at 20 cm. While these calculations suggest the possibility that extremely low power could be helpful, there are two important considerations. First, an adversary can use a high-gain directional antenna to boost his receive range. A 9 dBi antenna would increase $G_r$, making the adversary's effective range roughly one-half meter. Second, environmental noise is likely to create significant issues for the legitimate target device at these levels.

Even though reducing transmit power alone does not assure that a signal will not be recovered by a distant device, lowering transmit power still makes an eavesdropping adversary's task more difficult. In the next section we experiment with commercial Wi-Fi devices and 4 dBm transmit power.

## 5 EVALUATION

To test the ability of COTS Wi-Fi devices to receive a signal in the presence of jamming, we tested four devices with electronics similar to those found in embedded devices: a Panda Ultra Wireless N USB Adapter [23], an Edimax Nano EW-7811Un [8], an external Alfa Networks AWUS036H [3], and an internal Intel Ultimate N WiFi Link 5300 [16] connected to a Planar Inverted-F antenna.

On the transmit side, we used two calibrated Ettus Research N210 Universal Software Radio Peripheral (USRP) radios [9], each connected to a quarter-wavelength dipole antenna to simulate a multiple-antenna device. One USRP transmitted data using the GNU Radio 802.11a/g/p transceiver code developed by Bloessl [6], while the second USRP transmitted barrage jamming across the entire Wi-Fi 20 MHz channel during frame transmission. This arrangement allowed us to precisely control the signal strength and coordinate the timing of both the data and the jamming signals. The antennas were separated by one-half wavelength in keeping with Figure 1. We conducted all experiments on Wi-Fi channel 1, used 4 dBm as transmit power for data, and either 4 or 8 dBm as transmit power for jamming.

### 5.1 Frame reception without jamming

We first tested the ability of the four COTS devices to receive frames containing a 1,024-bit payload sent from the USRP without the presence of jamming. In this test we transmitted 1,000 Wi-Fi frames for each of the eight modulation schemes, with an interval of 100 ms between frames. To minimize outside interference, we tested these receivers in a remote indoor facility where there were no other Wi-Fi transmitters within at least 100 meters. We found each commercial device performed similarly; and for brevity, in this paper we report the average results across all four devices.

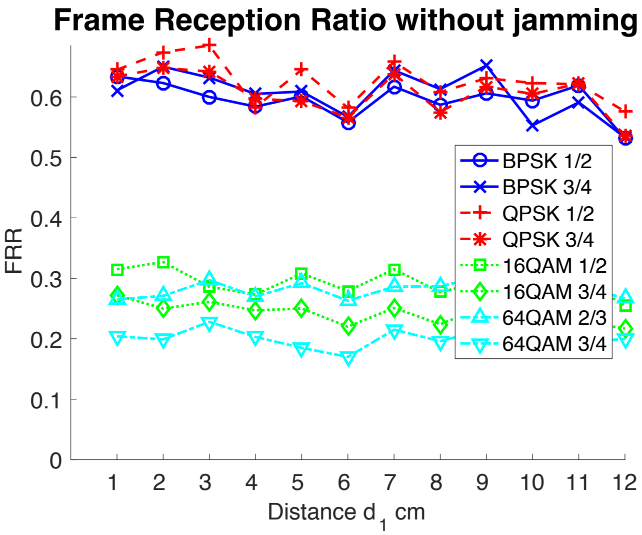

**Figure 7: Frame Reception Ratio for 1,000 packets sent on each MCS.**

Figure 7 shows the average Frame Reception Ratio (FRR) – the number of frames received by the Wi-Fi device, divided by the number of frames transmitted, for all four receivers where $d_1$ ranged from 1 to 12 cm. We see that the simpler modulation schemes were received with significantly higher probability than more complex modulation schemes, although theory suggests all modulation schemes should be received with nearly 100% FRR without jamming interference. Pierson et al., however, show that non-propagating energy near a transmitting antenna can cause channel estimation errors [25]. These channel estimation errors in turn can cause frames to fail CRC checks and these frames are dropped by COTS Wi-Fi devices. The non-propagating energy dies out quickly as distance increases and does not cause problems for devices further than about 14 cm apart. Because CloseTalker is intended for communication between devices in close physical proximity, however, these errors reduce the FRR and are not modeled in Section 4. This reduced FRR is significantly more pronounced for complex modulation schemes because small channel-estimation errors often cause the receiver to decode symbols incorrectly. Simpler modulation schemes are more robust against these errors because symbols are spaced further apart (see Figure 3).

## 5.2 Frame reception with jamming

Next we tested the ability of the Wi-Fi devices to receive frames in the presence of jamming. Figure 8 shows the average FRR across all four devices when jamming signal strength was equal to the data signal strength (i.e., $P_j = P_t$), normalized to the FRR when no jamming was present (we refer to this ratio as NFRR). We see that BPSK 1/2, BPSK 3/4, and QPSK 1/2 performed relatively well when $d_1$ was less than 5 cm. More complex modulation schemes were received with low probability at close range, and all modulation schemes performed poorly at longer ranges. This is by design, as CloseTalker's purpose is to transfer data to nearby devices, but not allow reception by more distant devices.

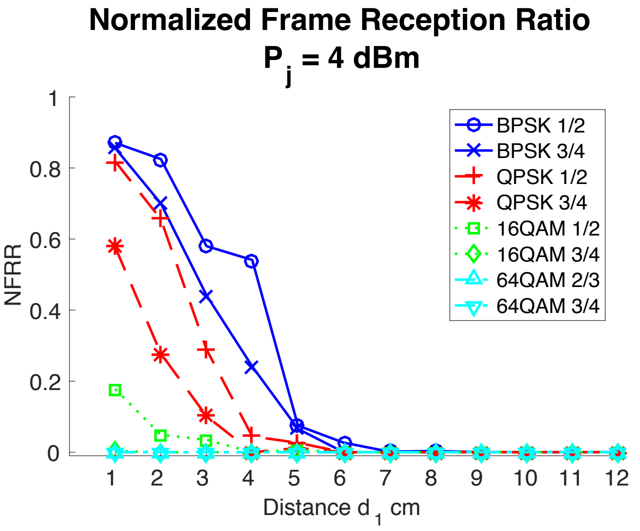

**Figure 8: NFRR for 1,000 packets sent on each MCS when $P_j = 4$ dBm.**

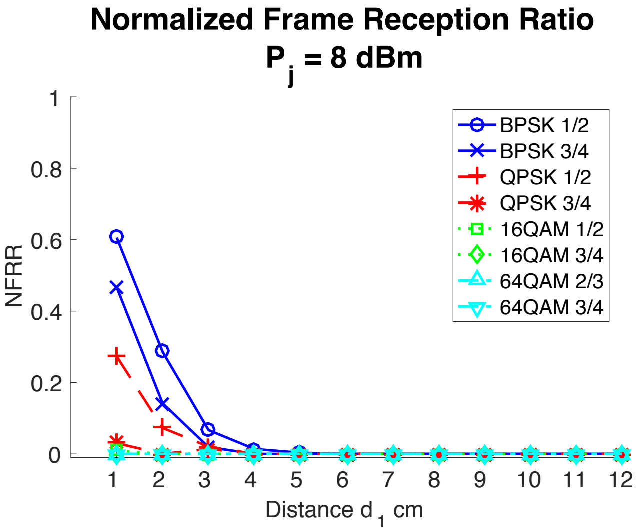

**Figure 9: NFRR for 1,000 packets sent on each MCS when $P_j = 8$ dBm.**

We then tested CloseTalker's ability to transfer data to nearby devices when the jamming signal was 2.5 times stronger than the data signal (i.e., $P_j = P_t + 4$ dBm). Figure 9 shows the results when $d_1$ ranged from 1 to 12 cm. We see that BPSK has some ability to transfer data in this environment up to 3 cm, but all other schemes and distances had virtually no reception. In all cases after 6 cm, no frames were received using any modulation scheme.

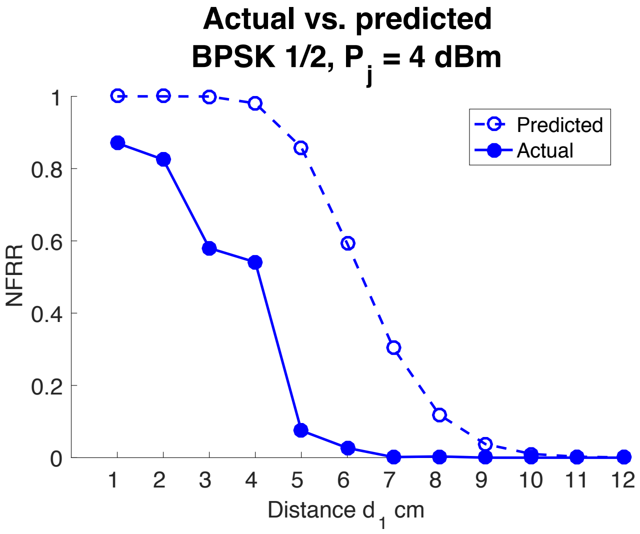

Figure 10: NFRR for 1,000 packets sent with BPSK 1/2 vs predicted when $P_j = 4$ dBm.

## 5.3 Actual performance vs. theory

Based on Section 3, we expect BPSK 1/2 to tolerate more noise than other modulation schemes and consistent with predictions, in Figure 8 and 9 we see that BPSK 1/2 actually does perform much better in the presence of jamming than other modulation schemes. In Figure 10 we compare BPSK 1/2 performance when the data and jamming strength are equal (i.e., $P_j = P_t$), with the theoretical performance discussed in Section 4 and shown in Figure 6. We see that actual performance follows the theoretical performance, but lags somewhat because as discussed in Section 5.1, unmodeled near-field effects cause channel-estimation errors that in turn lead to dropped frames that are not considered in Equation (14). We also examine the performance of BPSK 1/2 when the jamming signal is 2.5 times stronger than the data signal (i.e., $P_j = P_t + 4$ dBM) in Figure 11. Here also we see that the real world lags theory due to near-field effects. Despite these differences, theory elucidates the real world.

In summary, we see that CloseTalker was able to use BPSK 1/2 to provide communication in the presence of jamming when the data and jamming signals are of equal strength and the devices were closer than about 5 cm. No data was recovered by devices at longer ranges. FRR at close range, however, was lower than might otherwise be expected. In cases where the application must transmit large amounts of data, it should not rely CloseTalker's jamming to cover the entire transmission; instead, it can use CloseTalker to send a secret key to the receiver in a single frame and the devices could then use that key to bootstrap a secure connection over standard protocols (such as TLS over TCP over Wi-Fi). Even if the key needs to be retransmitted, due to low FRR, it should be received with high probability after a few attempts; we thus have no concern about the efficiency of CloseTalker even when used for large data transmissions.

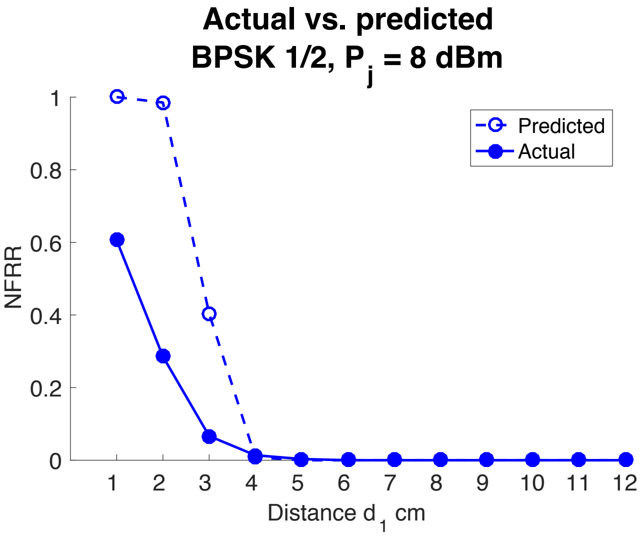

Figure 11: NFRR for 1,000 packets sent with BPSK 1/2 vs predicted when $P_j = 8$ dBm.

# 6 THEORETICAL ANALYSIS OF SECURITY

In our threat model, we consider an adversary attempting to eavesdrop or to inject frames during CloseTalker's data transfer. We assume the adversary understands CloseTalker data and jamming technique and is able to employ sophisticated equipment. We argue below that the fundamental physics of radio make it extremely unlikely even such an advanced adversary will succeed, and a practical adversary would be even less successful.

## 6.1 Eavesdropping

An adversary might attempt to eavesdrop on the data transferred between CloseTalker devices, but faces the same issues legitimate devices face when trying to extract the data signal in the presence of the jamming signal. If the adversary uses CloseTalker's technique, the most favorable geometric alignment for the adversary is the same as it is for legitimate devices – where the jamming antenna is located farthest from adversary as discussed in Section 4.1. We have demonstrated above, however, that provided the adversary is located more than about 7 cm away, the data and jamming signals received by the adversary will be roughly equal, making signal recovery difficult. In fact, if the adversary is aligned such that the jamming antenna is closer than the data antenna, the jamming signal could very well be stronger than the data signal. Regardless of signal strength, an adversary might attempt to separate the data and jamming signals with a directional antenna or with signal processing and MIMO antennas instead of relying on the Inverse-Square Law as CloseTalker does.

*6.1.1 Directional antennas.* A directional antenna with a narrow main lobe pointed precisely at the data antenna, but excluding the jamming antenna, would allow the adversary to receive the data signal only. CloseTalker's antennas, however,

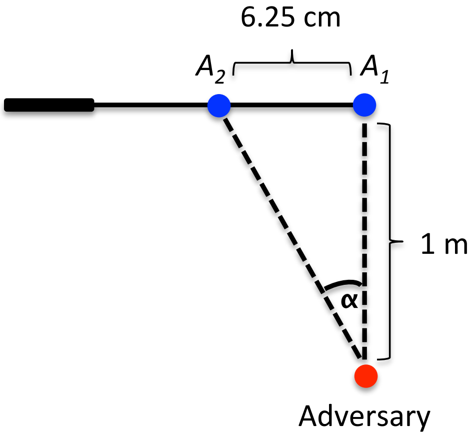

**Figure 12: Since CloseTalker's antennas are separated by a half wavelength, an adversary located 1 m away and aligned with one of the CloseTalker's antennas would need a half beam width of $\alpha$ =tan$^{-1}$(6.25/100) $\approx$ 3.5 degrees to avoid receiving a signal from the second antenna.**

are only one-half wavelength apart and because the main lobe expands with distance, the lobe will encompass both antennas if the adversary is located a reasonable distance away or is inline with CloseTalker's antennas. For example, as shown in Figure 12, an adversary located 1 m away and bore-sighted on one of the CloseTalker's antennas would need to have a one-half beam width of $\alpha$ =tan$^{-1}$(6.25/100) $\approx$ 3.5 degrees to avoid the signal from the jamming antenna.

A 0.5 m dish antenna operating at Wi-Fi frequencies would have a one-half beam width of 8.1 degrees [5], far wider than the width required to avoid the jamming if the adversary is located only 1 m away. A more distant adversary would need an even narrower beam width. Furthermore, because at least one of the CloseTalker's devices is typically mobile, the exact orientation and location of devices is difficult to predict a priori.

*6.1.2 Signal processing and MIMO antennas.* Alternatively, an adversary might try sophisticated signal-processing techniques to separate the data from the jamming signal based on an estimate of the channel between sender and receiver. The environment between transmitter and receiver can be represented mathematically as [32]

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{w} \tag{16}$$

where $\mathbf{y}$ is the received signal, $\mathbf{H}$ models the channel between sender and receiver, $\mathbf{x}$ is the transmitted signal, and $\mathbf{w}$ is noise. The elements in channel matrix $\mathbf{H}$ are calculated as [32]

$$h_{ik} = a\ exp(-j2\pi d_{ik}/\lambda) \tag{17}$$

where $i = 1 \ldots$ number of receiving antennas, $k = 1 \ldots 2$ (one for each of CloseTalker's two transmit antennas), $a$ is an attenuation factor based on the path length, $d_{ik}$ is the path length between transmit antenna $k$ and receive antenna $i$.

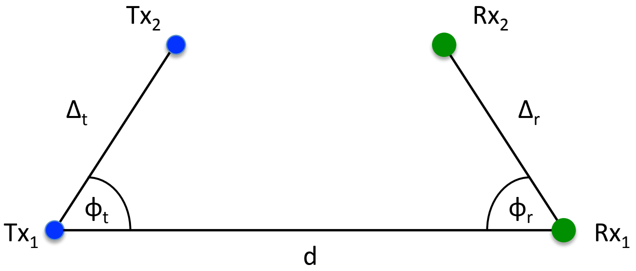

**Figure 13: A transmitter with antennas $Tx_1$ and $Tx_2$ separated by $\Delta_t$ and oriented with angle $\phi_t$ relative to a receiver with antennas $Rx_1$ and $Rx_2$ separated by $\Delta_r$ and oriented with angle $\phi_r$ relative to the transmitter. In a line of sight environment, the channel between these two devices separated by distance $d$ and with $\Delta_t < \lambda/2$ has Rank 1 when $d \gg \Delta_t$ [32].**

When the transmitter and receiver are far apart, then $d_{ik}$ is approximated by [32]

$$d_{ik} = d + (i-1)\Delta_r\lambda\cos\phi_r - (k-1)\Delta_t\lambda\cos\phi_t \tag{18}$$

where $d$ is the distance between transmit antenna 1 and receive antenna 1, $\phi_t, \phi_r$ are the angle of incidence on the transmit and receive antenna arrays respectively, and $\Delta_t, \Delta_r$ represent the spacing between the transmit and receive antennas respectively, normalized to the signal wavelength as illustrated in Figure 13.

If the channel matrix $\mathbf{H}$ is estimated accurately, has Rank greater than 1, and is not ill-conditioned, an adversary may be able to separate the data signal from the jamming. It can be shown, however, that for line of sight environments where the transmitter and receiver are much farther apart than the distance between transmitting antennas (e.g., $d \gg \Delta_t$), and when the two transmit antennas are within one-half wavelength of each other (as they are with CloseTalker), the channel matrix $\mathbf{H}$ has Rank 1 [32]. This Rank suggests the data and jamming signals cannot be separated.

Tippenhauer et al., however, exploited the fact that a receiver must be located at a significantly greater distance than the transmit antenna spread to ensure the channel matrix has Rank 1 [31]. They showed that by using a two-antenna array at relatively close range, signals *can* be separated in some cases (multipath signals can also create a full-Rank matrix when a Rank 1 matrix might otherwise be expected). Their analysis evaluated an adversary attempting to separate a 400 MHz data signal sent by one antenna using simple Frequency Shift Keying (FSK) from a jamming signal sent by a second antenna separated by 15 cm or more. They showed that it is theoretically possible to extract a signal with less than a 20% bit error rate at ranges around two meters. In practice, however, they often failed due to multipath effects *even with precise alignment of the antennas and control over the position of every component.*

Furthermore, separating Wi-Fi's more complex modulation schemes, with greater bandwidth, at higher frequencies and smaller antenna spreads is more difficult than separating simple low-frequency FSK signals with large antenna separation. Those researchers did not demonstrate the ability to separate BPSK 1/2 Wi-Fi signals from jamming. In short, it remains unproven that an eavesdropping attack using a two-antenna receiver is feasible with Wi-Fi when the data and jamming antennas are separated by less than one-half wavelength. Attacks with more antennas are theoretically feasible.

## 6.2 Frame injection

An adversary may attempt to inject his own frames while data is transferred between CloseTalker devices. In that case the adversary's signal would have to exceed the jamming strength. Because the jamming is in close proximity to the receiving device, the Inverse-Square Law helps CloseTalker defend against such an injection attack. Even though CloseTalker transmits at 4 dBm, an adversary located only 2 m away using a 9 dBi omni-directional antenna would need to roughly double the maximum transmit power limits set by the U.S. Federal Communications Commission to exceed CloseTalker's signal strength. While this transmit power is possible, it is well above the capabilities of commercial off-the-shelf hardware.

## 6.3 Raising the bar for an adversary

Although CloseTalker does not make it *impossible* for an adversary to eavesdrop or to inject frames, it raises the bar extremely high. Prior work (mentioned above) demonstrates that a skilled adversary, under highly controlled stationary conditions, can sometimes succeed in eavesdropping on the data signal of simple protocols. Our analytic results demonstrate that it is *theoretically possible* for sophisticated adversaries to eavesdrop on a complex protocol like Wi-Fi, *if* they are located *within a few centimeters*, and *if* all components are stationary, although it has not been demonstrated with actual hardware.

Furthermore, although the geometry of nearby devices or multipath effects might result in a full-Rank channel matrix, the increased Rank is only useful if the receiver is able to estimate the channel accurately. Our own experience shows that beyond 6 cm single-antenna COTS receivers simply did not detect incoming frames in the presence of jamming and thus made no channel estimate at all. A more sophisticated adversary may continuously monitor the channel trying to detect frames and accurately estimate the channel. This task is particularly challenging because at least one of CloseTalker's devices are mobile, making it difficult to accurately assess the channel a priori, and the data is usually transferred in a single frame – giving the adversary only one chance to succeed!

Similarly, an adversary with an unlawfully powerful transmitter and directional antenna may be able to inject frames, but this is not possible with consumer-grade electronics. While it is therefore not impossible for adversary to eavesdrop or inject frames, CloseTalker significantly "raises the bar" an adversary must overcome while still allowing unaltered legitimate target devices to recover data.

# 7 BI-DIRECTIONAL COMMUNICATIONS

Above we discuss uni-directional communication – data moves from a multiple-antenna device to a single-antenna target device. Here we discuss bi-directional communication.

If the target device also has two antennas, bi-directional communication is possible simply by reversing roles. If one device only has one antenna, however, we posit that secure bi-directional communications may still be possible. In this case, the single-antenna device can alert the multiple-antenna device that it has data to send and the multiple-antenna device initiates jamming on one antenna while listening on its other antenna. The single-antenna device can then monitor the noise floor. When the noise floor rises above a preset threshold, strong jamming is in place and it then transmits its data. In this way, a single-antenna device can bi-directionally communicate with a multiple-antenna device.

This approach, however, has some limitations. If the adversary is able to raise the noise floor above a threshold, the adversary may be able to trick the single-antenna device. The adversary could time his jamming such that after reaching the threshold on the single-antenna device, the adversary stops jamming just as the single-antenna device transmits. In this case the data is transmitted without jamming coverage. To counter this attack, however, the single-antenna device could wait a random amount of time after the noise threshold is reached before sending the data. This way if the adversary stopped jamming, the single-antenna device would detect it.

# 8 RELATED WORK

CloseTalker securely transfers data among devices in close proximity using jamming. Prior research has looked at accomplishing the same goal with various techniques.

## 8.1 Cryptography

Many approaches involve cryptographic mechanisms, such as Diffie-Hellman key exchange. Despite impressive mathematics, Diffie-Hellman and related approaches have been shown to be vulnerable to man-in-the-middle attacks [1]. Other approaches build on public-key cryptography, which relies on a trusted certificate authority and may not be computationally feasible for many embedded devices common in some IoT environments.

## 8.2 Out-of-band communications

Out-of-band communication systems exchange a secret key between devices over a secondary communication channel that is impervious to observation and interference by an adversary. The devices then bootstrap a secure connection over the primary channel using the information exchanged over the secondary channel. Proposed secondary channels have included visual [19], audio [21], gesture [35], or secondary radios such as NFC or RFID. In each of these cases an additional sensor (light sensor, microphone, accelerometer, or second radio) is required. That required sensor or radio will not be present on many devices. Additionally, NFC has been shown to be vulnerable to interception at much longer distances than originally thought [36]. CloseTalker uses the in-band Wi-Fi radio and does not require additional sensors, radios, or complicated algorithms. As noted in Section 1 though, CloseTalker could be used to share a secret that can be used to bootstrap a long-term, long-distance, full-bandwidth session between devices.

### 8.3 Jamming

Jamming has been well studied as a means of covering in-band communication. While there are many uses for jamming, "friendly jamming" attempts to use jamming to assist with a purpose like data transfer. More information on friendly jamming can be found in a recent comprehensive survey covering 182 academic papers [2]. For example, Kuo et al. proposed a solution for imparting secret keys onto IoT-type devices. They suggest putting devices into a Faraday cage to exchange information and use a jammer to cover any RF leakage from the cage [18]. This approach may work for small devices but is impractical for large ones. Several papers use cooperating relay nodes to jam and prevent eavesdroppers from decoding network traffic over large distances [4, 7, 10, 22]. CloseTalker does not rely on additional "helper" devices. Other researchers consider remote jamming, where unlike CloseTalker, the data source and jammer are located a large distance apart or have a pre-shared key [28–30, 33, 34, 37].

Another friendly-jamming survey by Huo et al. segregated approaches on three criteria: (1) non-self cooperative jamming (where additional devices aid the jamming) versus self-cooperative jamming (where the only legitimate devices are the transmitter and receiver), (2) uniform (omni-directional) versus directional jamming (jamming is beam-formed to keep the receiver free of jamming), and (3) perfect versus imperfect knowledge of eavesdroppers CSI. None of the papers listed in their survey take CloseTalker's approach. All of those approaches rely on either additional helper devices, directional jamming, or perfect knowledge of an eavesdropper's CSI.

### 8.4 Proximity

Like CloseTalker, other approaches to secure data transfer rely on proximity between devices. *ProxiMate*, for instance, uses fluctuations in television or FM radio broadcast signals to develop a common key between devices located within one-half wavelength of each other [20]. CloseTalker can securely transfer arbitrary data, not just a key. Separately, a project called *Wanda* exploits the difference in signal strength between two nearby antennas to securely transmit data to a target device [24]. Wanda, however, can only transmit *one bit* with each Wi-Fi packet, whereas CloseTalker can send a much larger data payload – 2,304 *bytes* in each Wi-Fi packet [15] – making it more than 18,000 times faster than Wanda! Furthermore, CloseTalker expands Wanda's security protection by adding jamming and by shortening the period of communication.

### 8.5 Jamming and proximity

One approach that uses both jamming and proximity is a system called *Shield* [12]. Shield uses a necklace-worn friendly jammer to protect a nearby implanted medical devices from accepting outside commands. CloseTalker, however, addresses a different problem in that it conveys information to a target device rather than preventing the target from receiving potentially malicious data.

## 9 CONCLUSION

As the number of deployed IoT devices grows, users will find it increasingly cumbersome to establish secure relationships among devices, particularly for brief, ad hoc communications. Manual entry of secret keys on each device will simply not scale. To help alleviate that problem, we designed, implemented, and evaluated a system called *CloseTalker,* which leverages multiple antennas and the physics of near-field radio to ensure wireless devices in close physical proximity can securely communicate while more distant devices cannot recover the information transmitted. CloseTalker works irrespective of device type or manufacturer and without additional hardware, out-of-band channels, complicated computation, or manual configuration. In fact, because CloseTalker conforms to the Wi-Fi standard, the receiving device need not even be aware that the sender is using CloseTalker's techniques. We show that by using the BPSK 1/2 modulation coding scheme, CloseTalker is able to reliably and securely transfer data at ranges of 5 cm or less while preventing adversaries from receiving the data. CloseTalker is perfect for quick exchanges of data between mobile or IoT devices, leveraging physical proximity to establish secure device relations consistent with user intent. This same capability allows CloseTalker to share address and key information that can bootstrap a long-term, long-distance, full-bandwidth connection over conventional protocols, when desired.

## ACKNOWLEDGEMENTS

We thank our shepherd, Professor Lin Zhong, as well as Professor Ashutosh Sabharwal for their invaluable help shaping this paper. We also thank the National Science Foundation for their support. This paper results from a research program at the Institute for Security, Technology, and Society at Dartmouth College, supported by the National Science Foundation under award number CNS-1329686. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsors.

## REFERENCES

[1] David Adrian, Karthikeyan Bhargavan, Zakir Durumeric, Pierrick Gaudry, Matthew Green, J. Alex Halderman, Nadia Heninger, Drew Springall, Emmanuel Thomé, Luke Valenta, Benjamin VanderSloot, Eric Wustrow, Santiago Z. Béguelin, and Paul Zimmermann. Imperfect forward secrecy: How Diffie-Hellman fails in practice. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 5–17. ACM, 2015.

[2] Haithem Al-Mefleh and Osameh Al-Kofahi. Taking advantage of jamming in wireless networks: A survey. *Computer Networks*, 99:99–124, 2016.

[3] Alfa Networks. Alfa Networks AWUS036H Wi-Fi adapter, http://www.alfa.com.tw, visited 4/15/2018.

[4] Alvaro Araujo, Javier Blesa, Elena Romero, and Octavio Nieto-Taladriz. Cooperative jam technique to increase physical-layer security in CWSN. In *International Conference on Advances in Cognitive Radio (COCORA)*, pages 11–14, 2012.

[5] Constantine A. Balanis. *Antenna Theory: Analysis and Design*. Wiley, third edition, 2005.

[6] Bastian Bloessl, Michele Segata, Christoph Sommer, and Falko Dressler. An IEEE 802.11a/g/p OFDM receiver for GNU Radio. In *Proceedings of the Workshop on Software Radio Implementation Forum (SRIF)*, pages 9–16. ACM, 2013.

[7] Lun Dong, Zhu Han, Athina P Petropulu, and H Vincent Poor. Cooperative jamming for wireless physical layer security. In *IEEE Workshop on Statistical Signal Processing*, pages 417–420. IEEE, 2009.

[8] Edimax Techology Company, Ltd. EW-7811Un, http://us.edimax.com, visited 3/22/2018.

[9] Ettus Research. USRP N210 Software Defined Radio, https://www.ettus.com, visited 3/18/2018.

[10] Satashu Goel and Rohit Negi. Guaranteeing secrecy using artificial noise. *IEEE Transactions on Wireless Communications*, 7(6):2180–2189, 2008.

[11] Andrea Goldsmith. *Wireless communications*. Cambridge University Press, 2005.

[12] Shyamnath Gollakota, Haitham Hassanieh, Benjamin Ransford, Dina Katabi, and Kevin Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. *SIGCOMM Computer Communication Review*, 41(4):2–13, August 2011.

[13] Daniel Halperin, Wenjun Hu, Anmol Sheth, and David Wetherall. 802.11 with multiple antennas for dummies. *SIGCOMM Computer Communication Review*, 40(1):19–25, January 2010.

[14] Institute of Electrical and Electronics Engineers. 802.11ac standard, http://standards.ieee.org/about/get/802/802.11.html, visited 3/22/2018.

[15] Institute of Electrical and Electronics Engineers. 802.11n standard, http://standards.ieee.org/findstds/standard/802.11n-2009.html, visited 7/20/2018.

[16] Intel. Intel Ultimate N Wi-Fi Link 5300: Product Brief, http://www.intel.com, visited 4/15/2018.

[17] Luo Jun, Jean H. Andrian, and Chi Zhou. Bit error rate analysis of jamming for OFDM systems. In *Wireless Telecommunications Symposium*, pages 1–8. IEEE, April 2007.

[18] Cynthia Kuo, Mark Luk, Rohit Negi, and Adrian Perrig. Message-in-a-bottle: User-friendly and secure key deployment for sensor nodes. In *Proceedings of the International Conference on Embedded Networked Sensor Systems (SenSys)*, pages 233–246. ACM, 2007.

[19] Xiaohui Liang, Tianlong Yun, Ronald Peterson, and David Kotz. LightTouch: Securely connecting wearables to ambient displays with user intent. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, pages 1–9, May 2017.

[20] Suhas Mathur, Robert Miller, Alexander Varshavsky, Wade Trappe, and Narayan Mandayam. ProxiMate: Proximity-based secure pairing using ambient wireless signals. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 211–224. ACM, 2011.

[21] Markus Miettinen, N. Asokan, Thien D. Nguyen, Ahmad-Reza Sadeghi, and Majid Sobhani. Context-based zero-interaction pairing and key evolution for advanced personal devices. In *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, pages 880–891. ACM, November 2014.

[22] Rohit Negi and Satashu Goel. Secret communication using artificial noise. In *IEEE Vehicular Technology Conference*, page 19. IEEE, 2005.

[23] Panda Wireless. Panda Ultra Wireless N USB Wi-Fi adapter, http://www.pandawireless.com, visited 4/15/2018.

[24] Timothy J. Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. Wanda: securely introducing mobile devices. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, pages 1–9. IEEE, April 2016.

[25] Timothy J. Pierson, Travis Peters, Ronald Peterson, and David Kotz. Poster: Proximity detection with single-antenna IoT devices. In *Proceedings of the International Conference on Mobile Computing and Networking (MobiCom)*, pages 663–665. ACM, 2018.

[26] Gill Press. Internet Of Things (IoT) Predictions, https://tinyurl.com/ybe99l5m, visited 4/15/2018.

[27] Theodore S. Rappaport. *Wireless communications: principles and practice*. Prentice Hall, 2002.

[28] A. Sheikholeslami, D. Goeckel, and H. Pishro-Nik. Jamming based on an ephemeral key to obtain everlasting security in wireless environments. *IEEE Transactions on Wireless Communications*, 14(11):6072–6081, Nov 2015.

[29] W. Shen, P. Ning, X. He, and H. Dai. Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time. In *IEEE Symposium on Security and Privacy (S & P)*, pages 174–188, May 2013.

[30] Xiaojun Tang, Ruoheng Liu, Predrag Spasojević, and H Vincent Poor. Interference assisted secret communication. *IEEE Transactions on Information Theory*, 57(5):3153–3167, 2011.

[31] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun. On limitations of friendly jamming for confidentiality. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pages 160–173, May 2013.

[32] David Tse and Pramod Viswanath. *Fundamentals of wireless communication*. Cambridge University Press, 2005.

[33] Joao P Vilela, Matthieu Bloch, Joao Barros, and Steven W McLaughlin. Friendly jamming for wireless secrecy. In *IEEE International Conference on Communications (ICC)*, pages 1–6. IEEE, 2010.

[34] Joao P Vilela, Matthieu Bloch, Joao Barros, and Steven W McLaughlin. Wireless secrecy regions with friendly jamming. *IEEE Transactions on Information Forensics and Security*, 6(2):256–266, 2011.

[35] Jiansong Zhang, Zeyu Wang, Zhice Yang, and Qian Zhang. Proximity based IoT device authentication. *IEEE International Conference on Computer Communications (INFOCOM)*, April 2017.

[36] Ruogu Zhou and Guoliang Xing. nShield: A noninvasive NFC security system for mobile devices. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*, pages 95–108. ACM, 2014.

[37] Xiangyun Zhou and Matthew R McKay. Physical layer security with artificial noise: Secrecy capacity and optimal power allocation. In *International Conference on Signal Processing and Communication Systems (ICSPCS)*, pages 1–5. IEEE, 2009.