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

Timothy J. Pierson, Travis Peters, Ron Peterson, **David Kotz**
Dartmouth College
June 2019

DARTMOUTH

Billions of IoT devices are projected to be deployed in the next few years

- Huge growth projected for connected devices
- Many devices are likely to have limited user interfaces
- Devices that have never met will need to communicate

Example: sharing data between a mobile health device and a display

Display

m-Health device

- Patient and doctor want to review m-Health data
- m-Health device display too small; use monitor in doctor's exam room
- Devices have never met

Two goals:

1. Protect information in transit
2. Ensure data makes it to intended display (not adjacent exam room)

CloseTalker uses jamming to ensure unmodified nearby devices can receive data, but distant devices cannot

- Assume m-Health device has multiple antennas (now called "MIMO" device)
- Bring MIMO device and "target" device in close proximity
- Antenna A_1 at distance d_1;
  Antenna A_2 at distance $d_2=d_1+\lambda/2$
- Transmit data on antenna A_1 and jamming on A_2
- In close proximity, unmodified target recovers data despite jamming
- At long range, devices unable to decode data
- Used to send small amounts of data (e.g., crypto key)

If close proximity, target receives up to 50 times more power from A_1 than A_2

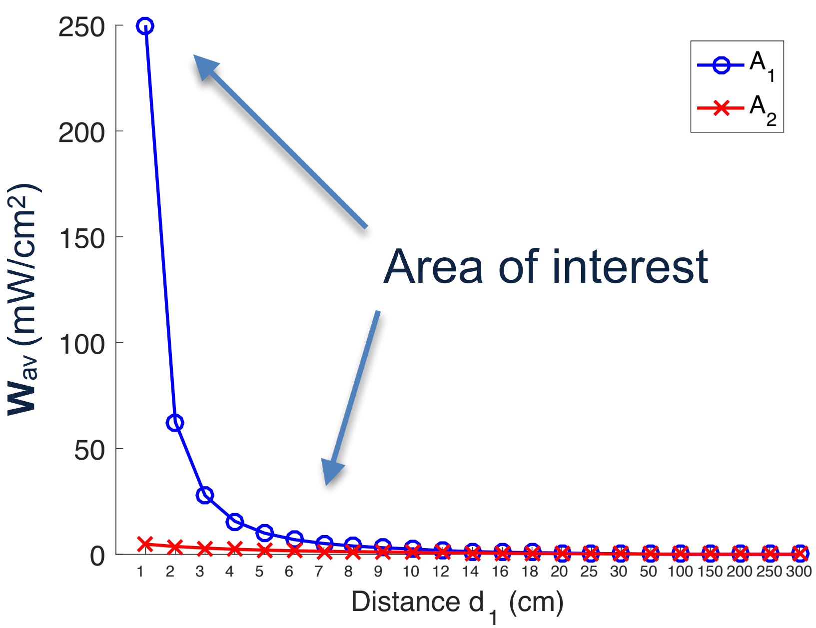
Average power[1]

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

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

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

Average power by distance

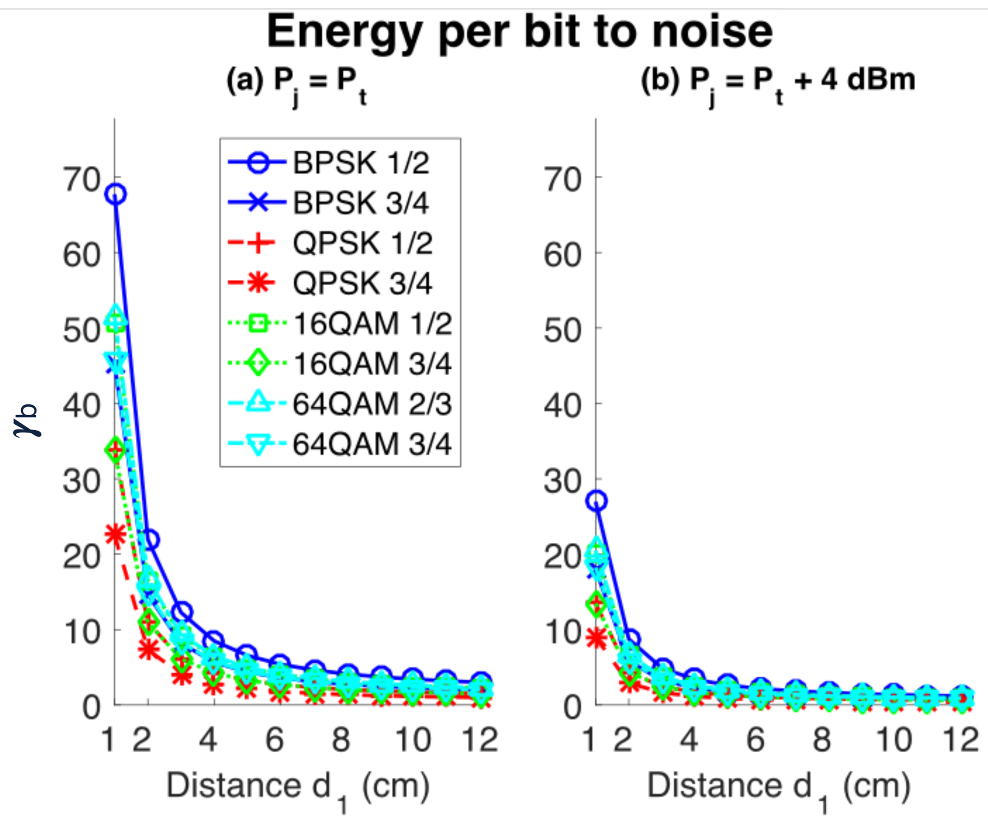


- Can not use well-known Friis equation at close range
- Must use other equations [1]
- When d_1 small, target receives data ≫ jamming
- At $d_1 = 1$ cm, $d_2 \approx 7.25$ cm; A_2 approximately 7.25 times farther away than A_1; data ≈ 50×jamming
- When $d_1 > 7$ cm, data and jamming strength roughly equal
- Counting on strong data strength to overcome jamming when at close range

$j = \sqrt{-1}$; $\eta = 120\pi$; I_0 = current applied to transmitter; λ = wavelength; $k = 2\pi/\lambda$; d = distance; l = antenna length; θ = vertical angle between transmitter and receiver (assumed to be $\pi/2$)

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

Theoretical data reception in presence of jamming depends on energy per bit to noise (γ_b)



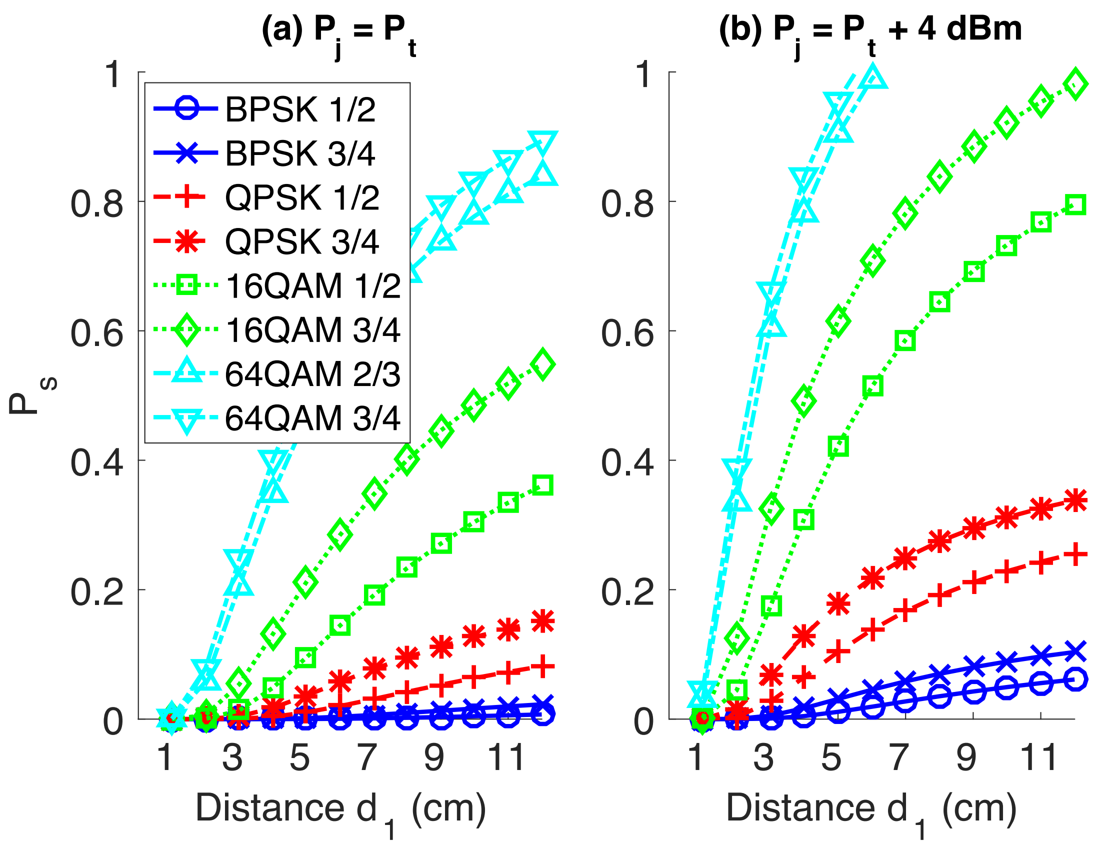
Jamming = data **Jamming = 2.5×data**

- Data signal = energy/bit; jamming = noise
- Energy per bit to noise (γ_b) depends on:
  - Data signal energy received
  - Wi-Fi Modulation Coding Scheme (MCS)
  - Jamming signal energy received
- Goldsmith[1] provides a great explanation of how to calculate γ_b
- At close range, γ_b is high, even when jamming is 2.5 times stronger (4 dBm) than data signal

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

Given γ_b, we can estimate the theoretical probability of a symbol error (P_s)

Probability of symbol error[1]

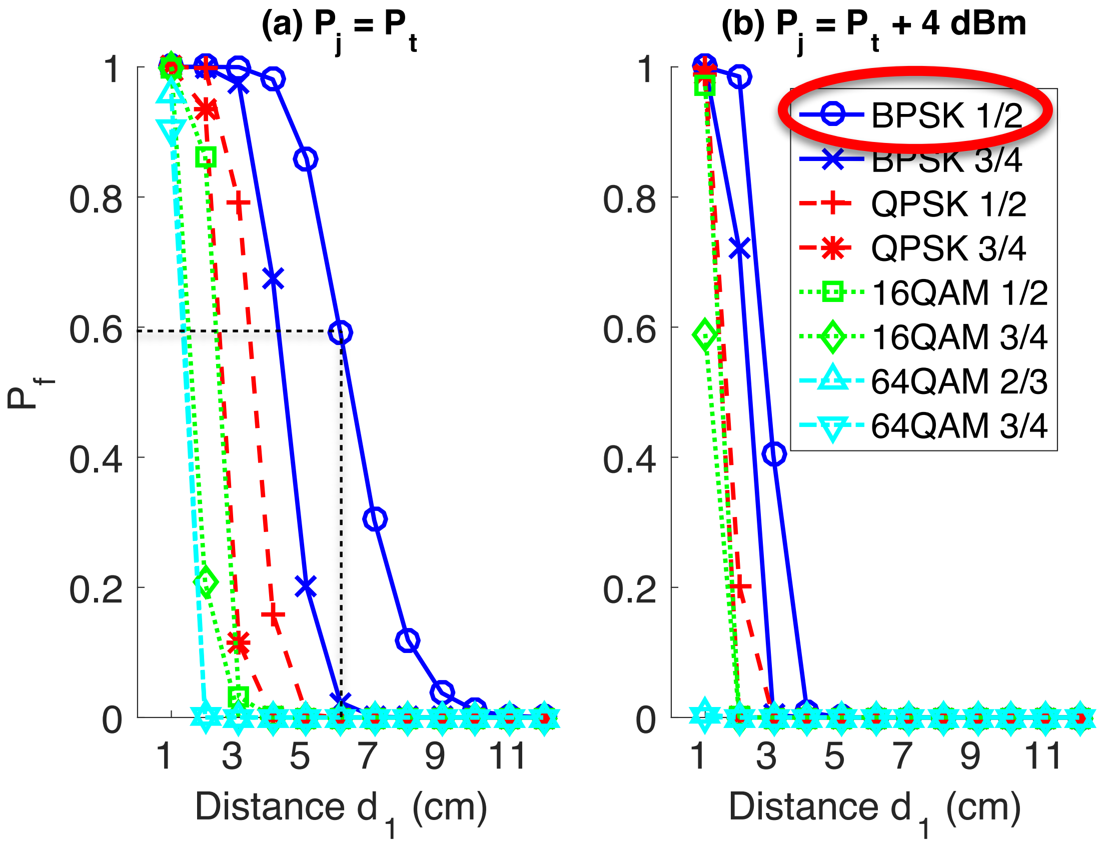


- Complex modulations (e.g., QAM) likely to have symbol errors
- Simple modulations (e.g., QPSK and BPSK) less likely to have symbol errors
- 1/2 coding scheme less likely to have errors than 2/3 or 3/4

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

From probability of a symbol error, we can calculate the probability a frame is received in the presence of jamming

Probability frame received[1]

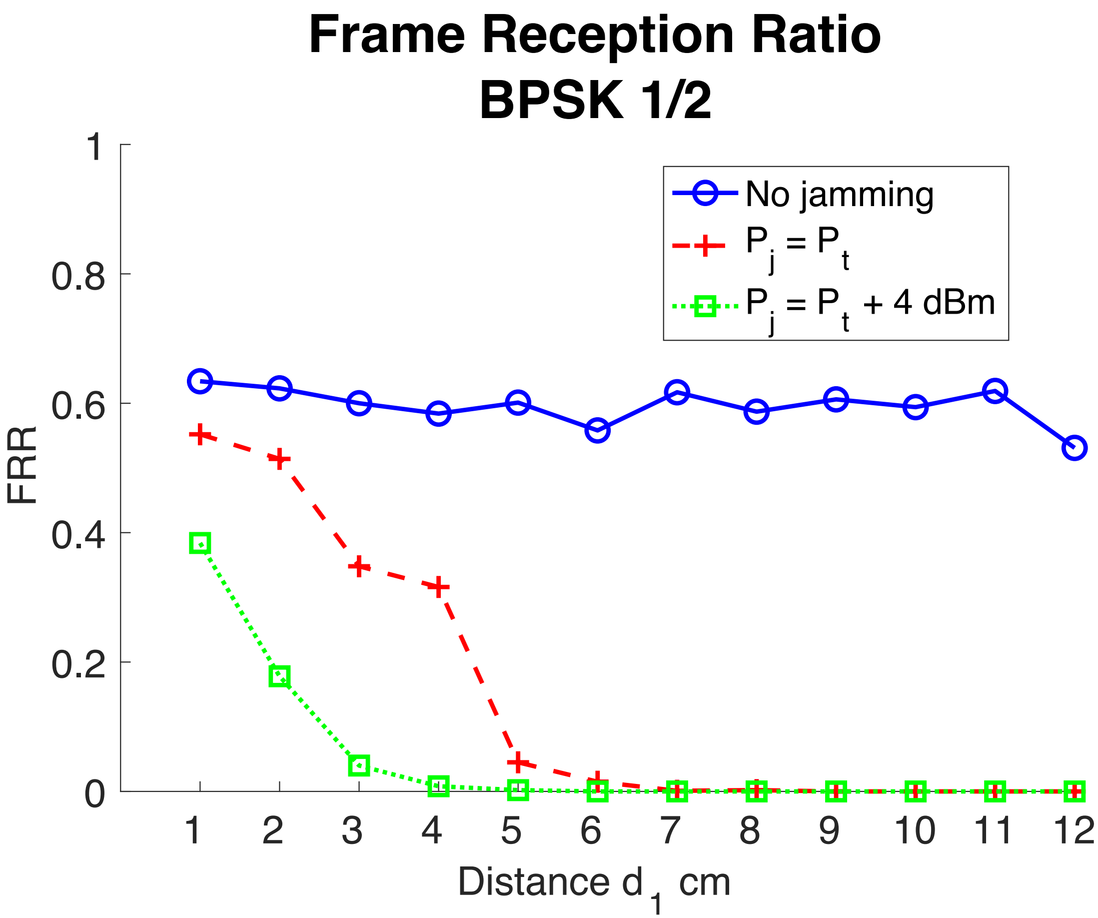


- BPSK 1/2 looks promising when data and jamming are the same strength
- Theory predicts useable reception out to about 6 cm
- More distant receivers unlikely to recover data

Assumes 1,024 bits per frame

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

Experiments with BPSK 1/2 received with lower probability than predicted

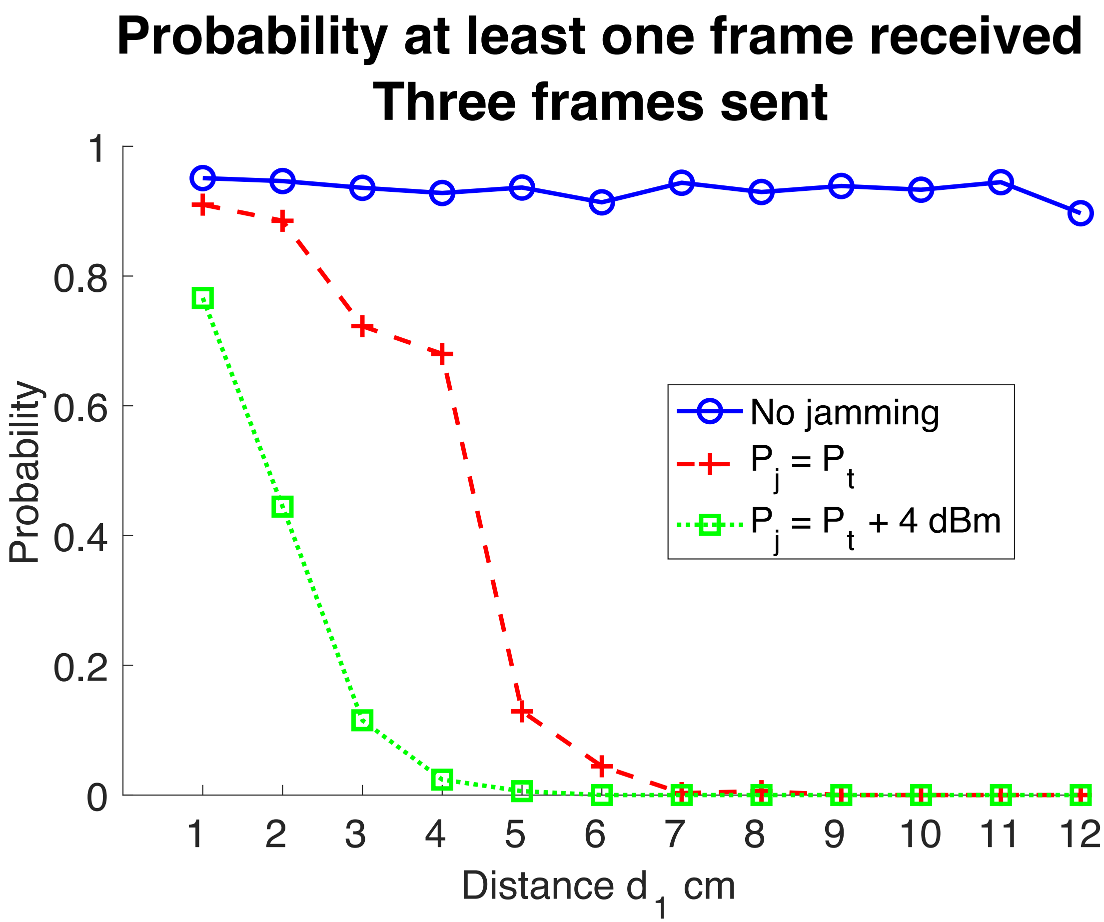


Frame Reception Ratio (FRR) = number of frames received/total number of frames transmitted
1,000 frames transmitted on each MCS, at each distance, to each COTS device; 1,024 bits per frame

- Used SDR to send Wi-Fi frames using GNU Radio package[1]
- Frames received with four different COTS devices:
  - Alfa Networks AWUS036H
  - Panda Ultra Wireless N USB
  - Edimax EW-7811Un USB
  - Intel Ultimate WiFi Link 5300
- All devices received similarly; average shown
- Without jamming FRR theoretically nearly 100%
- Near-field energy causes more errors than predicted[2]

[1] B. Bloessl. IEEE 802.11 a/g/p transceiver. https://github.com/bastibl/gr-ieee802-11
[2] T.J. Pierson, T. Peters, R. Peterson, D. Kotz. Proximity detection with single-antenna IoT devices. In *Proceedings of the International Conference on Mobile Computing and Networking (MobiCom)*, pages 663-665. ACM, 2018

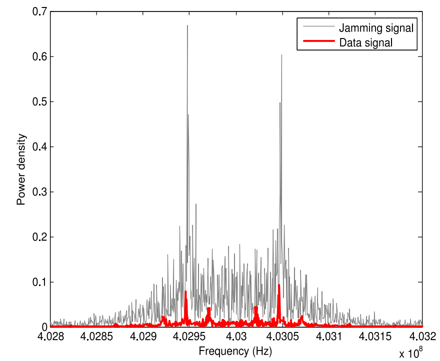
Even though FRR is low with jamming, data likely to be received with small number of retries



- Probability at least one frame is received increases with number of retries
- BPSK 1/2 frames likely to be received at close range with only three retries, even with jamming!
- More distance devices unlikely to recover data

FRR = Frame Reception Ratio
1,000 frames transmitted on each MCS, at each distance, to each COTS device; 1,024 bits per frame

Security: separating data and jamming signal is difficult for an eavesdropper



Directional antennas

- Directional antennas to receive only data signal
- CloseTalker's antennas only 6.25 cm apart
- Need extremely narrow beam width
- Unlikely to work if adversary located more than 0.5m away

Signal processing

- Signals separable if channel matrix Rank > 1 and well conditioned
- Tippenhauer separated low frequency, FSK data from jamming[1]
- No demonstrated ability to separate high frequency Wi-Fi

Raises bar

- Eavesdropping not theoretically impossible
- In our experiments COTS Wi-Fi devices could not decode data when located more than 6 cm away

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

CloseTalker provides a number of benefits for transferring data between nearby devices

Key benefits

- Consistent, fast, easy, and secure method to transfer any kind of information between commodity wireless devices
  - Regardless of device type or manufacturer
  - Without hardware modification
- Inverse-square law protects data transfer
- Useful for user-intended ad hoc encounters
- Supports long-range and long-term data transfer
- No additional network interference
- No need for additional hardware, pre-shared secrets, or complex algorithms
- Target device need not be aware sender is using CloseTalker

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

Timothy J. Pierson, Travis Peters, Ron Peterson, **David Kotz**
Dartmouth College
June 2019

Questions, contact Tim Pierson: tjp@cs.dartmouth.edu

DARTMOUTH

This research was supported by NSF award 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.