Entrapment for Wireless Eavesdroppers

Song Fang[*], Tao Wang[†], Yao Liu[†], Shangqing Zhao[†], **Zhuo Lu**[†]

[*]University of Oklahoma
[†]University of South Florida

Content

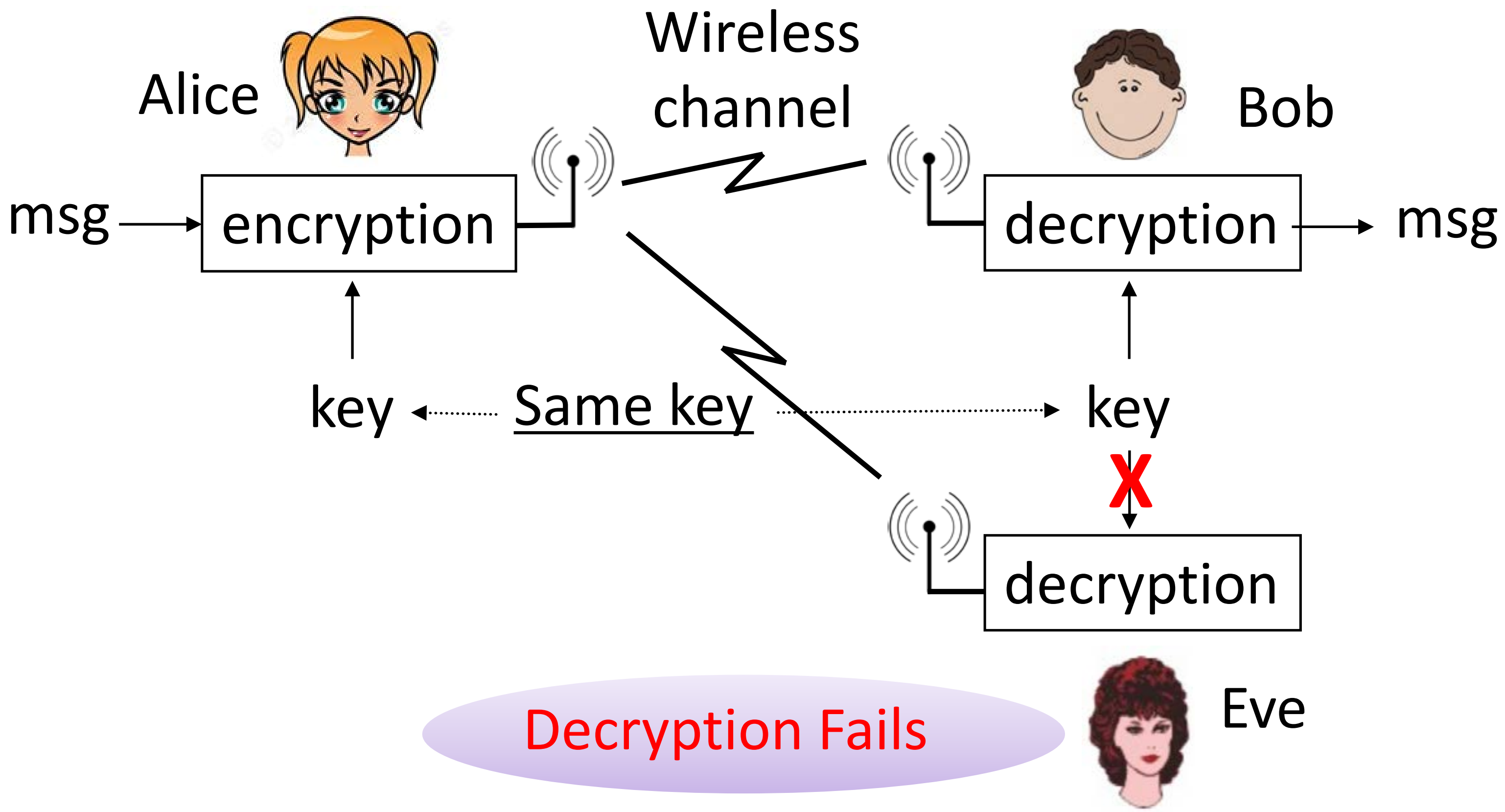
- Background
- System Design
  - Randomization Channel Design
  - Placing the Trap
- Experimental Evaluation
- Conclusion

Wireless Eavesdropping

- ✓ Open nature of wireless medium

- ✓ Traditional Anti-Eavesdropping Methods
  1. Cryptography
  2. Friendly jamming
  3. Proximity isolation

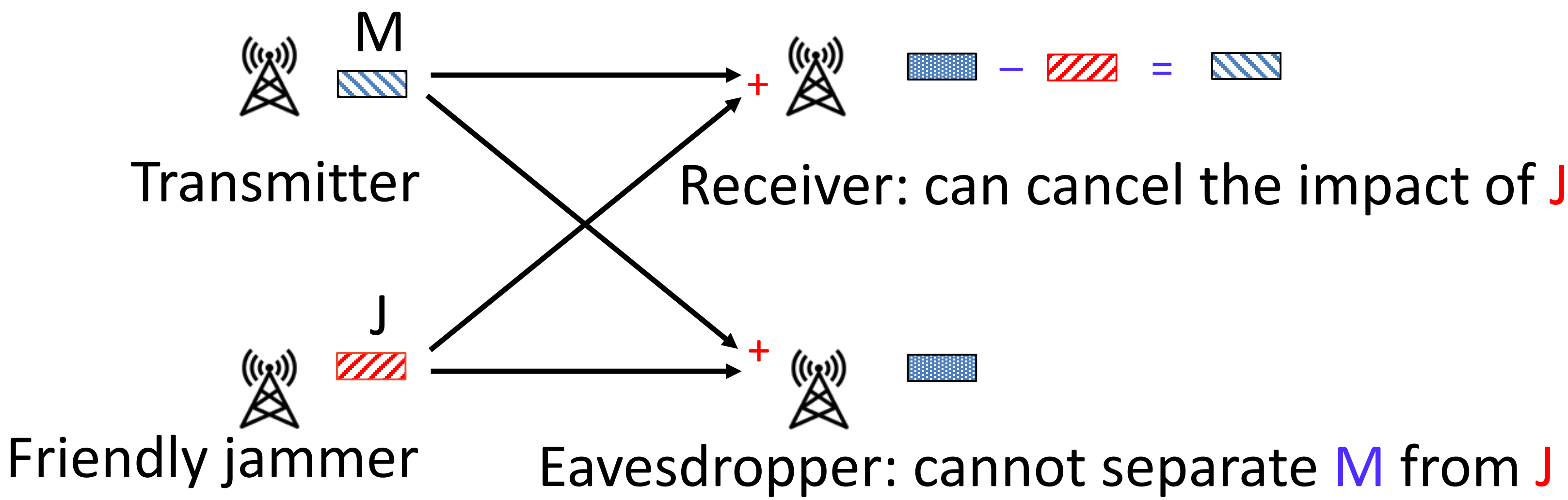
(1) Cryptography



(2) Friendly Jamming

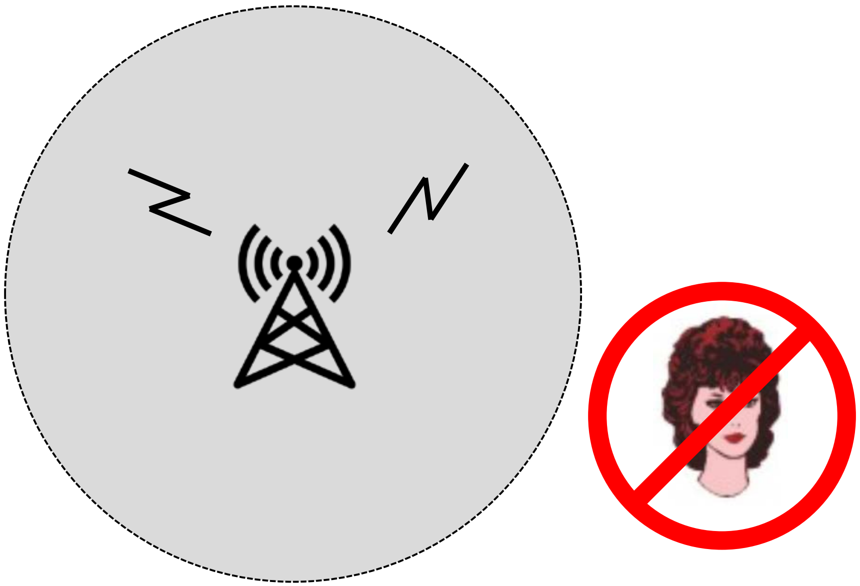
: original message, M

: jamming signals, J



Signal Interferences

(3) Proximity Isolation



Eavesdroppers cannot get close

Weak signal Strength

As a result,

Random and meaningless bit sequences

Eavesdropping is unsuccessful, motivating Eve to perform more attacks

Steal passwords	Adopt social engineering approaches
Break keys	Do power/time analysis, dictionary attacks
Remove jamming	Utilize signal cancellation techniques
Search best SNR	Circumvent proximity protection to find LOS

What if Eve receives a meaningful message instead of a random bit sequence?

~~Increase difficulties~~ → Actively attack the attacker

#fg kd%1u@ = Sask,jlkhiu^d

Meaningful (but fake) msg

Eavesdropping fails

Take further ways

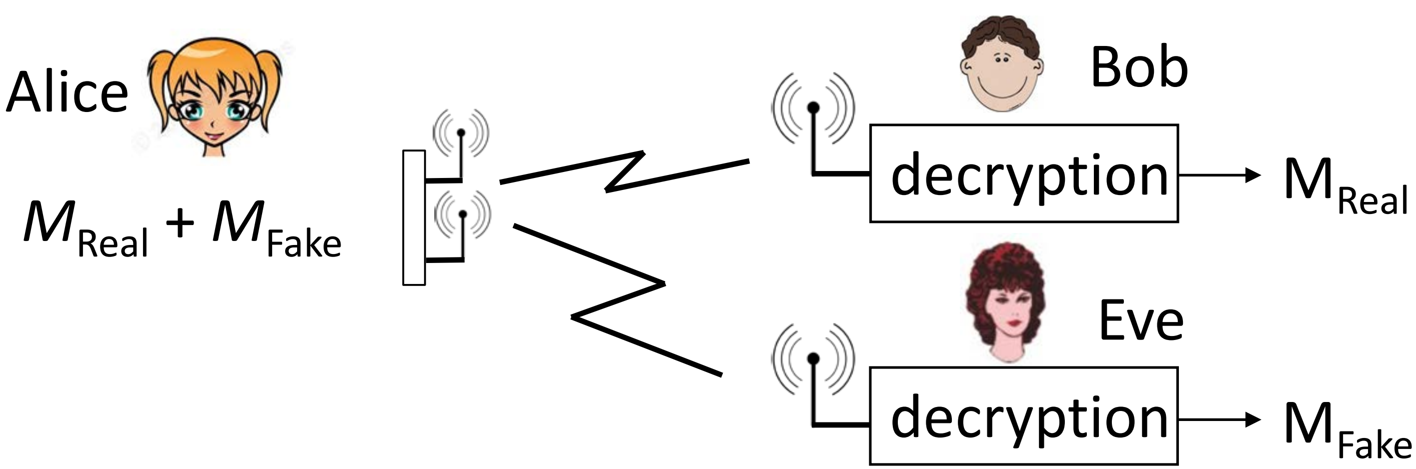
Believe It or Not

Entrapment

- Intuition: a dog chases prey by following its scent
- Method: provide an eavesdropper with attractive signals to lead her to move towards the trap region

T1 Guide an eavesdropper to a trap

T2 Establish a secure channel

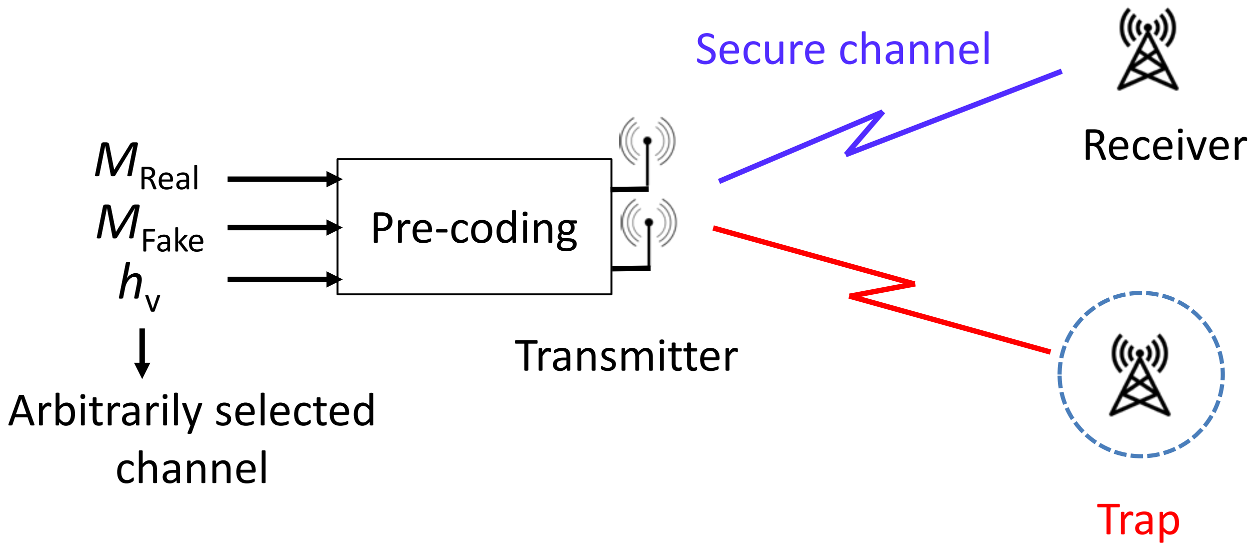


Content

- Background
- System Design
  - Randomization Channel Design
  - Placing the Trap
- Experimental Evaluation
- Conclusion

System Structure

- Utilize multiple antennas to concurrently transmit pre-coded signals



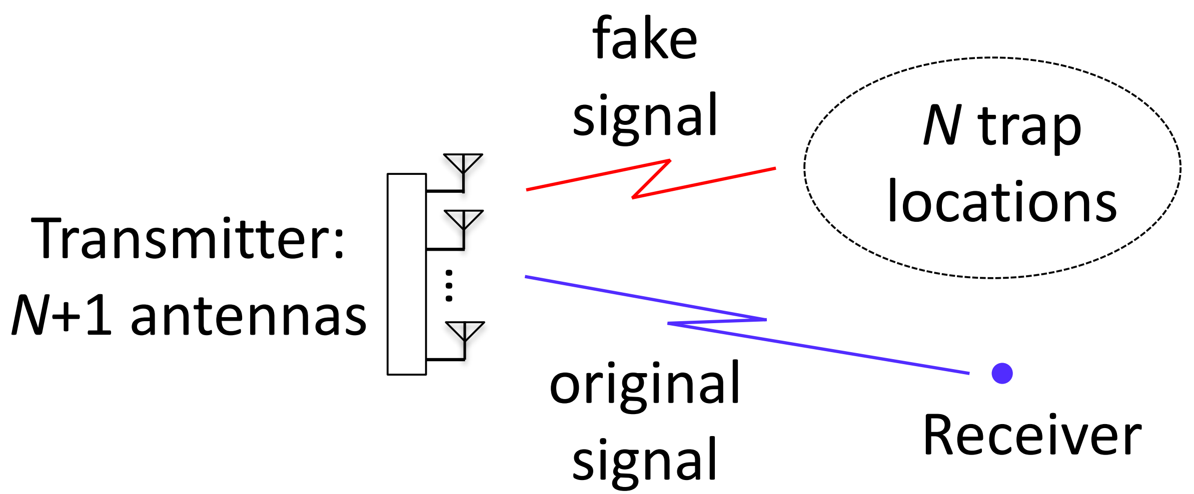
Why not Traditional MU-MIMO

- Simply using MU-MIMO without considering security does not prevent eavesdropping
  - An eavesdropper can still access to the message intended for the receiver if she happens to be close to the receiver

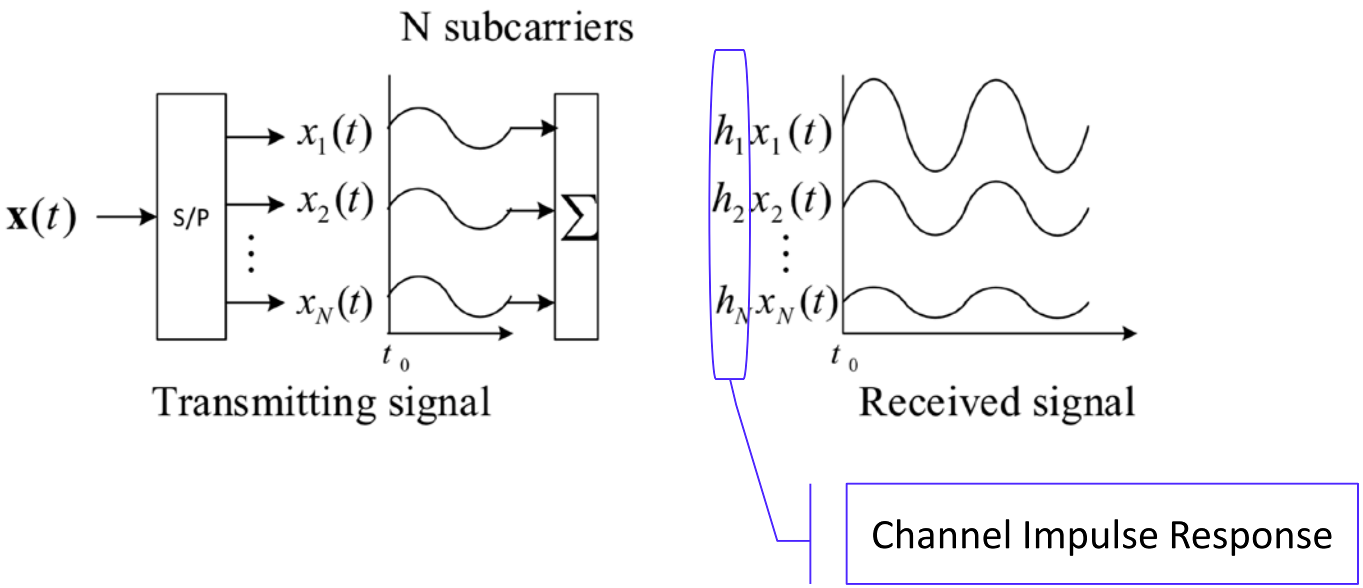
- Instead, we aim to provide secure communication as well as entrap eavesdroppers by
  - Constructing a specified channel between the transmitter and the receiver
  - Pre-coding the transmit signals based on the entrapment deployment

Trapping an Eavesdropper

- Placing multiple traps:



OFDM Preliminary



- The *i*-th received subcarrier signal:

$$y_i(t) = h_i \cdot x_i(t) + \underbrace{n(t)}_{\text{Chanel noise}}$$

Construction of a Specified Channel

- Goal: enable the receiver to estimate a channel specified by the transmitter

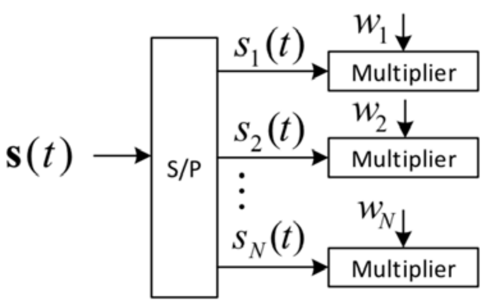
Training signal

$$s_i(t) = [s_{i_1}(t), s_{i_2}(t)]^T$$

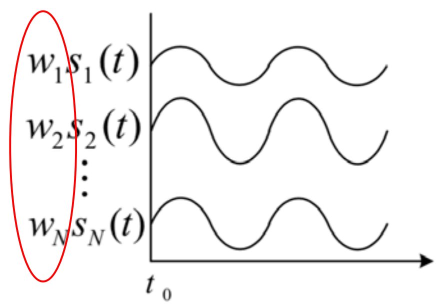
The received signal

$$y_i(t) = h_{i_{1r}} s_{i_1}(t) + h_{i_{2r}} s_{i_2}(t) + n(t)$$
$$= \mathrm{H}_i s_i(t) + n(t)$$

- Real channel effect emulation



Transmitting signal



Emulated signal

Calculation the Coefficients

- After multiplication, the received signal

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

- The receiver obtains the specified channel $\mathbf{H}_{vi} = [h_{i_v}, h_{i_v}]$

$$\mathbf{H}_i \mathbf{W}_i \, s_i(t) = \mathbf{H}_{vi} \, s_i(t)$$

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

After the Specified Channel is Created

- Original transmit signal $\mathbf{x}_i(t) = [x_{i_1}(t), x_{i_2}(t)]^T$

Receiver

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

$$x_{i_1}(t) + x_{i_2}(t) = \boxed{r(t)} + x(t) - r(t) = x(t)$$

VS

Eavesdropper

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

Unable to decode

Encoding Original Signals

- A lucky eavesdropper may successfully guess the specified channel
- Defense: generate one-time, non-repeated random signals for every transmission and add them to original signals

Receiver

$$y_i(t) = \begin{bmatrix} h_{i_v} & h_{i_v} \end{bmatrix} \begin{bmatrix} x_{i_1}(t) + n_{i_1}(t) \\ x_{i_2}(t) + n_{i_2}(t) \end{bmatrix}$$

$$n_{i_2}(t) = -n_{i_1}(t)$$

$$= h_{i_v}(x_{i_1}(t) + x_{i_2}(t))$$

VS

Eavesdropper

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

$$= h_{i_v}(h_{i_{1e}} h_{i_{1r}}^{-1} x_{i_1}(t) + h_{i_{2e}} h_{i_{2r}}^{-1} x_{i_2}(t)$$

$$+ (h_{i_{1e}} h_{i_{1r}}^{-1} - h_{i_{2e}} h_{i_{2r}}^{-1}) n_{i_1}(t))$$

Random

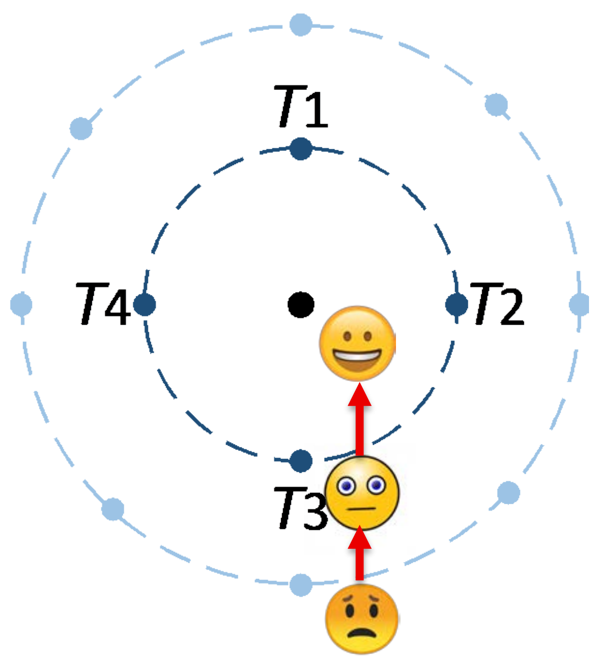
Trapping an Eavesdropper (Cont'd)

- Adjusting SNR: control the decoding quality at trap locations by adding disturbance signals to the original transmit signal

SNR High

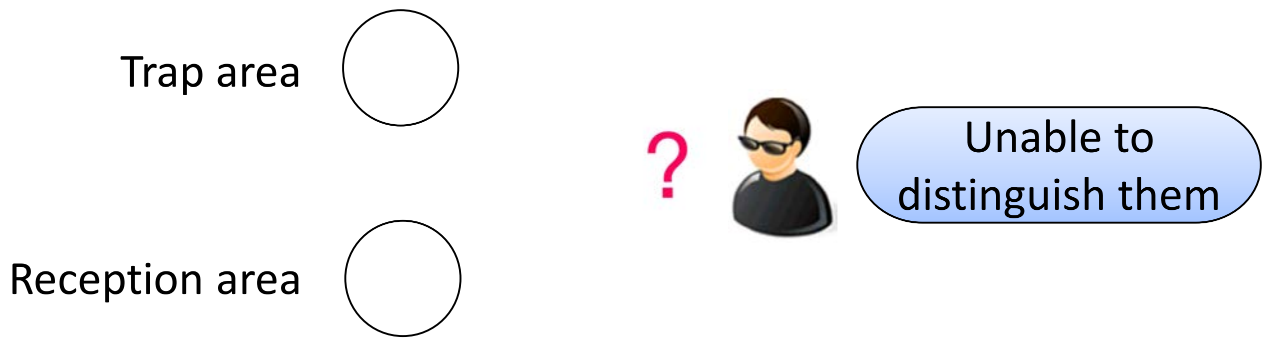
SNR Medium

SNR Low



Adversarial Indistinguishability

What happens if the presence of trap strategy is disclosed and an eavesdropper knows *N* trap locations set up to catch her?



- ☑ The two areas should have the same size
- ☑ An eavesdropper should have the same SNR observation when entering either of them

Strategies

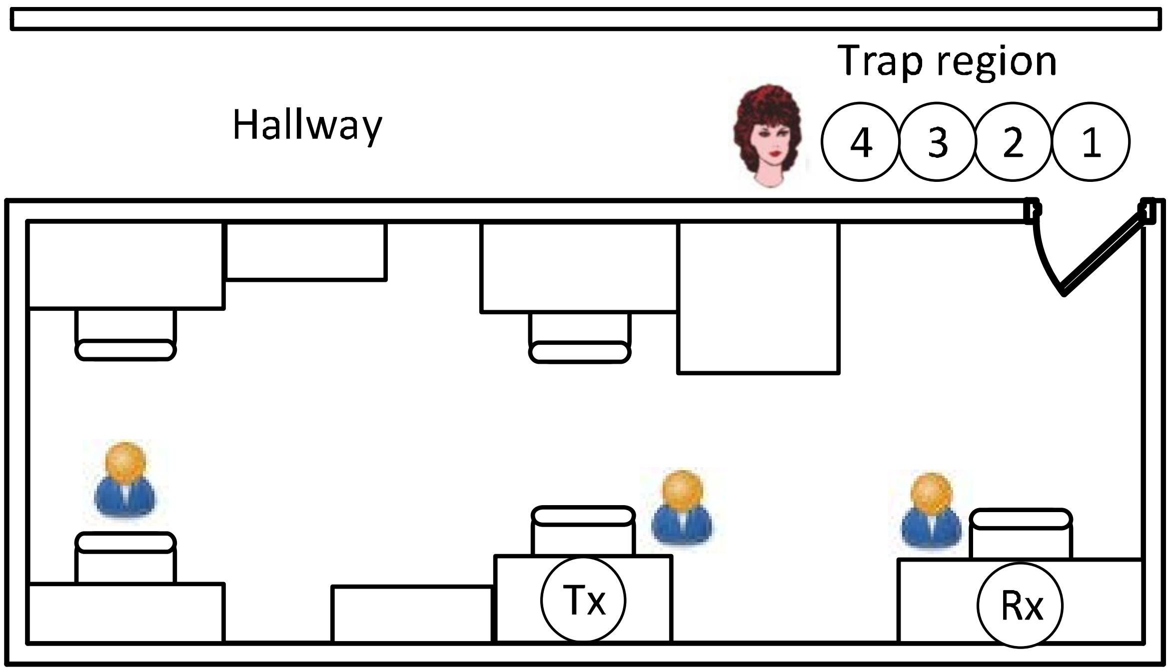
I. The transmitter also deploys a trap area centered at the receiver's location

II. The transmitter randomly alternates between the following modes:
   - Trapping mode: set a trap area centered at a selected trap location; send secret messages to the receiver
   - Disturbing mode: set a trap area centered at the receiver's location; dismantle the trap area set during the trapping mode

Content

- Background
- System Design
  - Randomization Channel Design
  - Placing the Trap
- Experimental Evaluation
- Conclusion

Experimental Floorplan



- Tx: Transmitter (Five USRPs + Ethernet switch + a PC)
- Rx/Ex: Receiver/ Eavesdropper (a USRP + a PC)
- VERT2450 and VERT400 antennas
- 4 neighboring trap locations

Evaluation Metrics

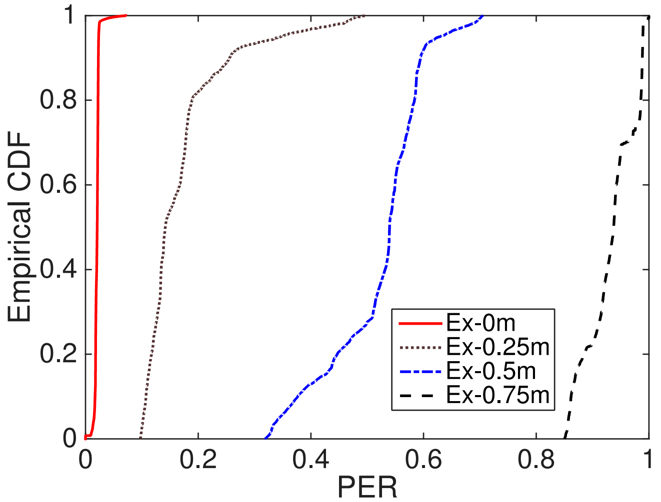
- $$\text{SNR} = \frac{\text{power of a signal of interest}}{\text{power of disburbance plus channel noise signals}}$$

- $$\text{PER} = \frac{\text{\# of packets that are unsuccessfully}}{\text{\# of totally received packets}}$$

- $$\text{BER} = \frac{\text{\# of incorrectly received bits}}{\text{\# of totally received bits}}$$

Concealment of the Specified Channel

- Without specified channel



Distance ↓ PER ↓

When Ex reaches the exact location of Rx, PER is less than 0.025 with a probability of 98.5%

- With specified randomized channel, the PER observed by the eavesdropper is always close to 100%

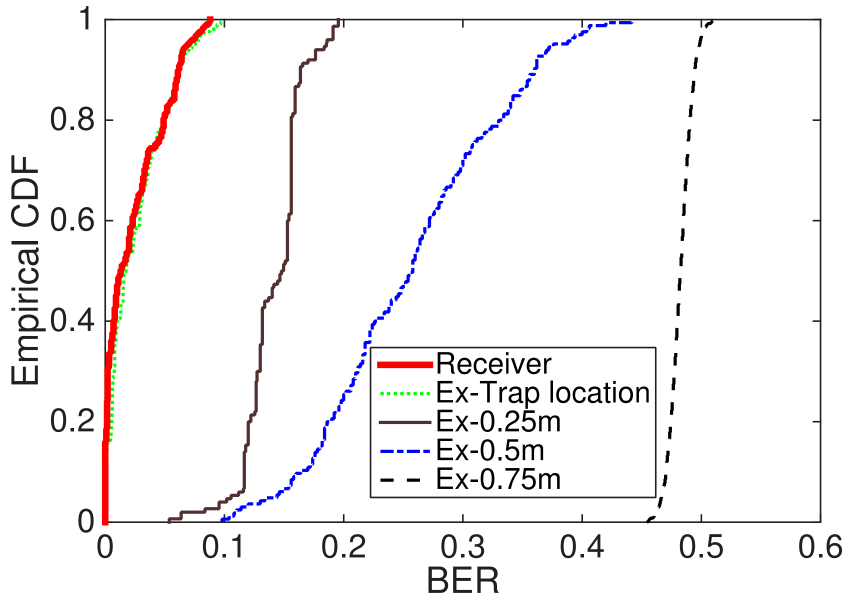
search for other locations

Launching the Entrapment

- After establishing a specified channel, Tx begins to sned true messages to Rx, and meanwhile fake messages to trapping locations

- Move Ex to Location 1 and record SNR, and then gradually increase the distance between Ex and the trap location at a step of 0.25m

BER Analysis



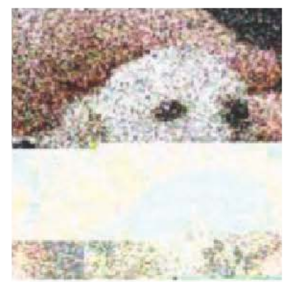
- Both Rx and Ex at the trap location can obtain low BERs below 0.06 with a probability of 90%
- The BER observed by Ex increases as Ex moves away from the trap location

Deployment of Multiple Traps

- The eavesdropper will be eventually guided to Location 1 if she searches for pictures of high quality

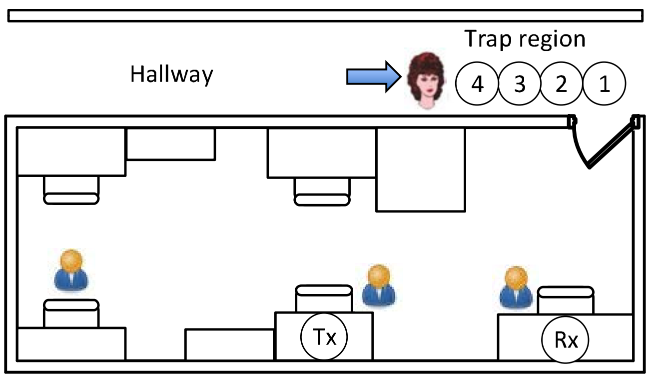

(a) Location 4


(b) Location 3


(c) Location 2


(d) Location 1

picture quality



Content

- Background
- System Design
  - Randomization Channel Design
  - Placing the Trap
- Experimental Evaluation
- Conclusion

Conclusion

- Design an entrapment wireless system:
  - attracting an eavesdropper to a specified trap location
  - utilizing multiple antennas to generate a large trap area
- Create techniques enabling a transmitter to establish a secure communication channel with the desired receiver
- Perform real-world evaluation to validate the performance of the proposed scheme

Thank you!

Any questions?