Investigation and Optimization of Secrecy Capacity for Intelligent Reflective Surfaces-Assisted Secure mmWave Indoor Wireless Communication

Ozlem Yildiz[1,2], Mohammad Alavirad[1], **Tejinder Singh**[1,3]
[1] Dell Technologies, [2] New York University, [3] University of Waterloo

January 23, 2022

X

Introduction

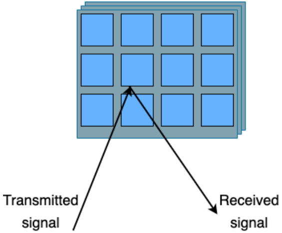
Next generation wireless communication requires

- high data rates
- low-latency
- reliability
- security.

New techniques to meet the requirements → Intelligent Reflective Surfaces (IRSs)

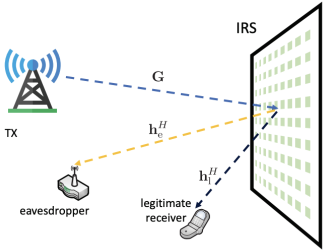
What is IRS?

IRS is an electromagnetic two-dimensional engineered surface to reconfigure the propagation path by reflecting the incoming signal by introducing a *pre-determined phase shifts*; therefore, they can create **smart** and **programmable radio environments**



IRS and Security [1]

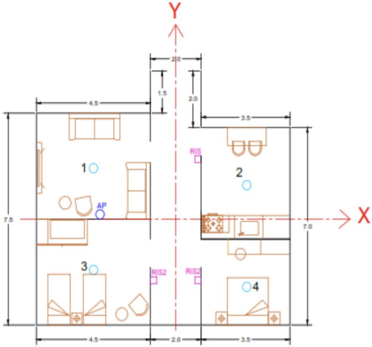
- IRSs can enhance the *physical layer security* in a communication link by using *passive beamforming* since it is directly correlated with directing the user's communication link into a desired direction



[1] X. Yu, D. Xu and R. Schober, IEEE GLOBECOM, 2019

IRS and Placement [2]

- Typically, a fixed IRS location is assumed for the performance measurements
- Issa et al. investigate *IRS placement* to enhance the coverage in different rooms for sub-6 GHz frequencies



[2] Issa, Mariam, and Hassan Artail, IEEE WiMob 2021

System Model

The system includes

- a transmitter (TX) with N_{TX} antennas,
- a legitimate receiver (RX) with N_{RX} antennas,
- an eavesdropper with N_{RX} antennas,
- an IRS with M phase shifting elements.

Channels between these are defined as follows:

- IRS-TX $\rightarrow \mathbf{G} \in \mathbb{R}^{M \times N_{TX}}$
- IRS- Legitimate RX $\rightarrow \mathbf{H} \in \mathbb{R}^{N_{RX} \times M}$
- IRS-Eavesdropper $\rightarrow \mathbf{H}_e \in \mathbb{R}^{N_{RX} \times M}$

Demonstration

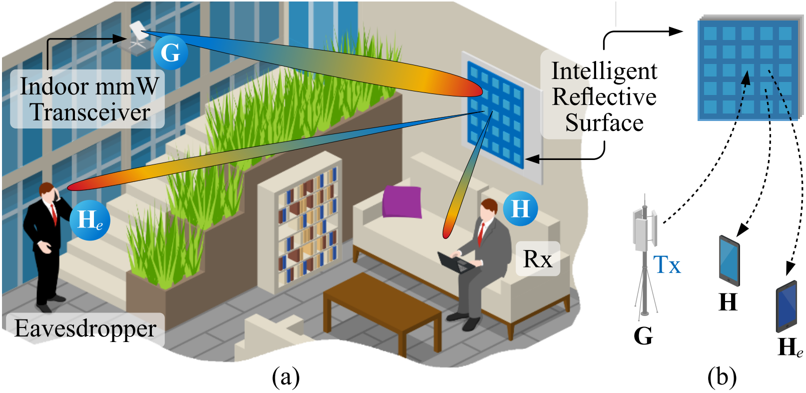


Figure 1: (a) Demonstration of the IRS in an indoor scenario (b) Schematic of the IRS, transmitter, Tx, legitimate receiver, and eavesdropper

Received Signal

- Transmitted symbol → s
- Additive white gaussian channel noise → n
- The transmitter beamforming vector → $\mathbf{f} \in \mathbb{R}^{N_{\mathrm{TX}} \times 1}$
- The receiver beamforming vector → $\boldsymbol{\omega_i} \in \mathbb{R}^{N_{\mathrm{RX}} \times 1}$
  - $i \in \{l, e\}$ to denote the legitimate Rx and eavesdropper
- The phase shift matrix of IRS → $\mathbf{\Phi} = \mathrm{diag}(e^{j\theta_1}, \ldots, e^{j\theta_M})$
  - $\mathrm{diag}(\cdot)$ → diagonal matrix with the given diagonal values
  - θ_i → the phase shift angles for $i \in [1, M]$
- Legitimate receiver's received signal → y
- Eavesdropper's received signal→ y_e

$$
\begin{aligned}
y &= \boldsymbol{\omega_l}^H \mathbf{H}\mathbf{\Phi}\mathbf{G}\mathbf{f}s + n \\
y_e &= \boldsymbol{\omega_e}^H \mathbf{H}_e\mathbf{\Phi}\mathbf{G}\mathbf{f}s + n
\end{aligned} \tag{1}
$$

Assumptions

- No line-of-sight (LoS) communication link between the legitimate RX or the eavesdropper and the TX
- IRS is considered without the noise effect
- TX transmits with transmit power P_{TX}
- CSI is known in the receiver
- Eavesdropper beamforming vector, $\boldsymbol{\omega}_e$, is fixed towards the best direction in $\boldsymbol{H}_e$

Secrecy Capacity

- Secrecy capacity:

$$C = \max\left\{\log\left(\frac{1+\frac{1}{\sigma^2}|\boldsymbol{\omega_l}^H\mathbf{H}\boldsymbol{\Phi}\mathbf{G}\mathbf{f}|^2}{1+\frac{1}{\sigma^2}|\boldsymbol{\omega_e}^H\mathbf{H}_e\boldsymbol{\Phi}\mathbf{G}\mathbf{f}|^2}\right), 0\right\} \tag{2}$$

- Modification for the optimization:

$$C^{'} = \log\left(\frac{1+\frac{1}{\sigma^2}|\boldsymbol{\omega_l}^H\mathbf{H}\boldsymbol{\Phi}\mathbf{G}\mathbf{f}|^2}{1+\frac{1}{\sigma^2}|\boldsymbol{\omega_e}^H\mathbf{H}_e\boldsymbol{\Phi}\mathbf{G}\mathbf{f}|^2}\right) \tag{3}$$

Optimization

- Formulation of the optimization:

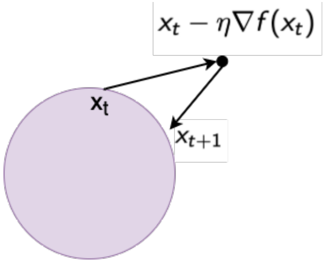
$$\begin{aligned} \mathcal{P}:\ & \underset{\boldsymbol{\omega_l},\mathbf{f},\boldsymbol{\Phi}}{\text{maximize}}\, C' \\ \text{subject to}\quad & |\mathbf{f}|^2 < P_{Tx} \\ & |\boldsymbol{\omega_l}| < 1 \\ & \boldsymbol{\Phi} = diag(e^{j\theta_1}, ..., e^{j\theta_M}) \end{aligned} \tag{4}$$

- Constraint change:

$$\begin{aligned} \mathcal{P}:\ & \underset{\boldsymbol{\omega_l},\mathbf{f},\boldsymbol{\theta}}{\text{maximize}}\, C' \\ & \text{subject to}\quad |\mathbf{f}|^2 < P_{TX} \text{ and } |\boldsymbol{\omega_l}| < 1 \\ & \text{when } \boldsymbol{\Phi} = diag(e^{j\theta_1}, ..., e^{j\theta_M}) \end{aligned} \tag{5}$$

Projected Gradient Descent

The secrecy capacity is convex for $\mathbf{f}$, $\boldsymbol{\omega}_l$, and $\boldsymbol{\Phi}$, when the other parameters are fixed and there are constraints for the optimization due to power. Therefore, we use *projected gradient descent* (PGD) as an optimization algorithm.



Simulation Setup

- Mathworks Ray-Tracer toolbox is used to calculate pathloss according to the location and the room specifications
- Optimal learning rate is an exhaustive search
- Maximum PGD iteration number is 10^6 but after the average of the change in 100 iterations is lower than 10^{-6}, we accept as a convergence

Simulation Parameters

Table 1: Simulation Parameters

Parameter	Values
Transmit Power, P_{TX}	26 dBm
Noise Figure	6 dBm
Center frequency, f_c	28 GHz
Symbol duration, T_{dur}	8.92×10^{-6} s
Number of Tx antennas, N_{TX}	64
Number of Rx antennas, N_{RX}	16
Number of reflecting elements, M	20
IRS fixed Location, (x, z)	(−3.05, -3, 1.5)

Simulation Environment

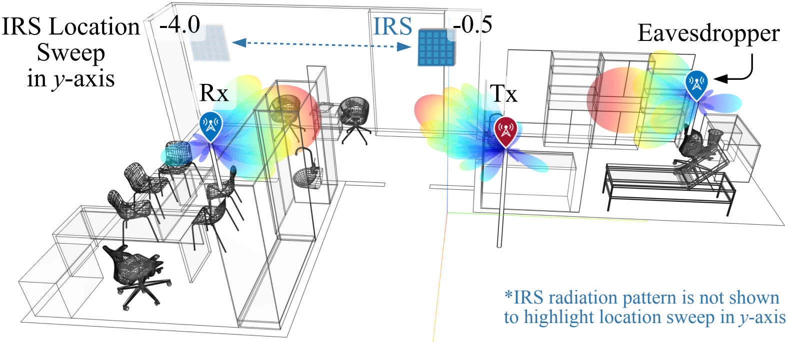
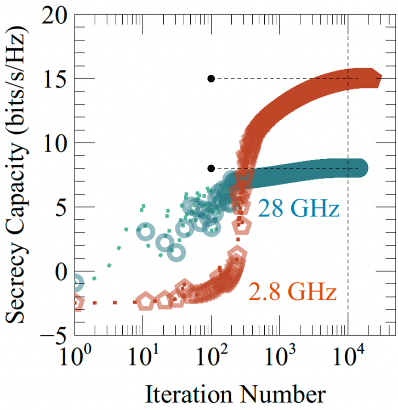


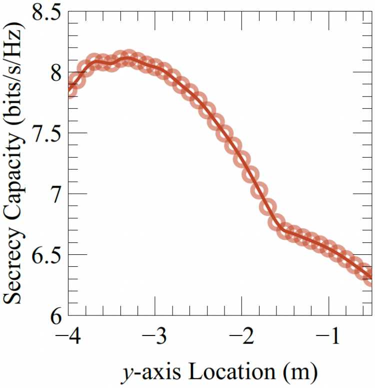
Figure 2: 3D indoor environment highlighting Tx, legitimate Rx, and eavesdropper. Dashed line represent optimization path for the IRS placement.

The Optimization with Different Carrier Frequencies



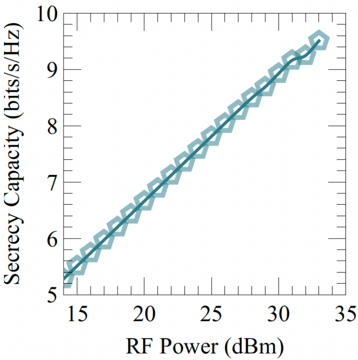
- At $f_c = 2.8$ GHz, the secrecy capacity is higher by a factor of two compared to $f_c = 28$ GHz because path loss increases with the frequency increase.
- At $f_c = 28$ GHz, the convergence duration reduces by at least a factor of three.

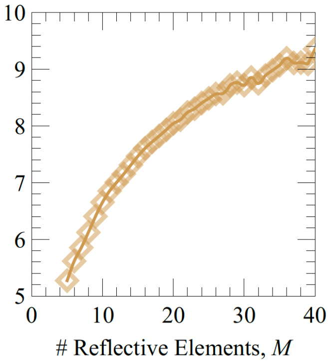
The Effect of the Location



- When the location in y-axis approaches towards −3.5, the IRS's distance with the legitimate Rx decreases while the distance with the eavesdropper increases, so the secrecy capacity increases by more than 1 bits/s/Hz.

RF Power and Number of Reflecting Elements





- Changing the P_{TX} from 26 dBm to 31 dBm and M from 20 to 36 have the same effect on secrecy capacity improvement

Conclusion

- Security capability investigation of an IRS-assisted indoor wireless communication system in mmWave regime
- Optimal indoor placement of IRS for secrecy capacity using Ray-Tracing
- New optimization technique by Projected Gradient Descent

Future Work

- The comparison of different secrecy capacity optimization schemes
- Generalization to different room settings
- Investigation of different measures for physical layer security
- Investigation with more realistic IRS phase shift matrix

References

- X. Yu, D. Xu, and R. Schober, "Enabling secure wireless communications via intelligent reflecting surfaces," in *2019 IEEE Global Commu. Conf. (GLOBECOM)*, 2019, pp. 1–6.
- M. Issa and H. Artail, "Using reflective intelligent surfaces for indoor scenarios: Channel modeling and ris placement," in *2021 17th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*. IEEE, 2021, pp. 277–282.