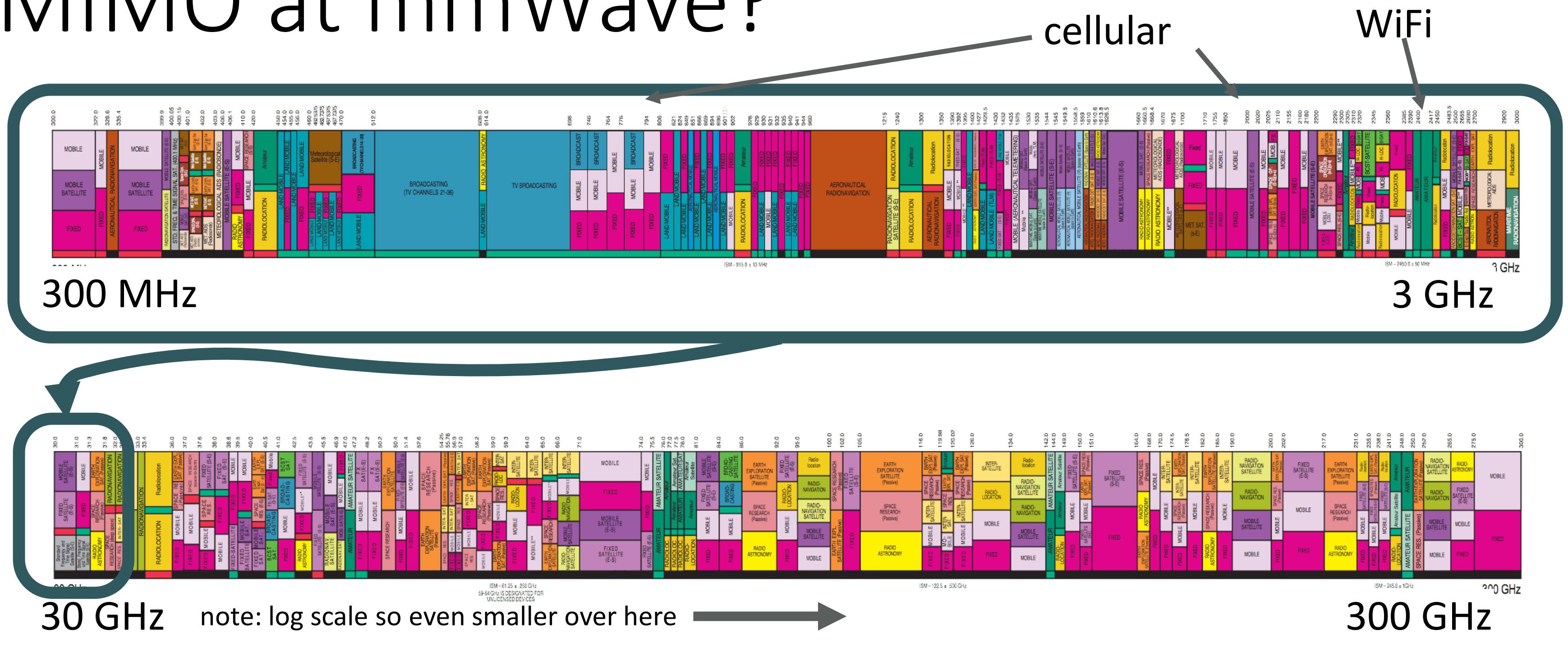
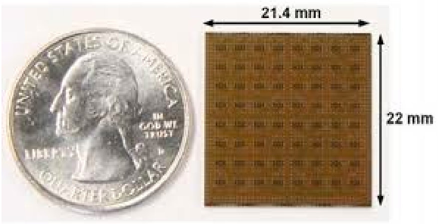
SACRAMENTO STATE

Exploiting Multi-Path for Safeguarding mmWave Communications Against Randomly Located Eavesdroppers

Rohith Talwar
Nancy Amala
George Medina
Akshadeep Singh Jida
Mohammed E. Eltayeb

Why MIMO at mmWave?





64 element phase array [2]

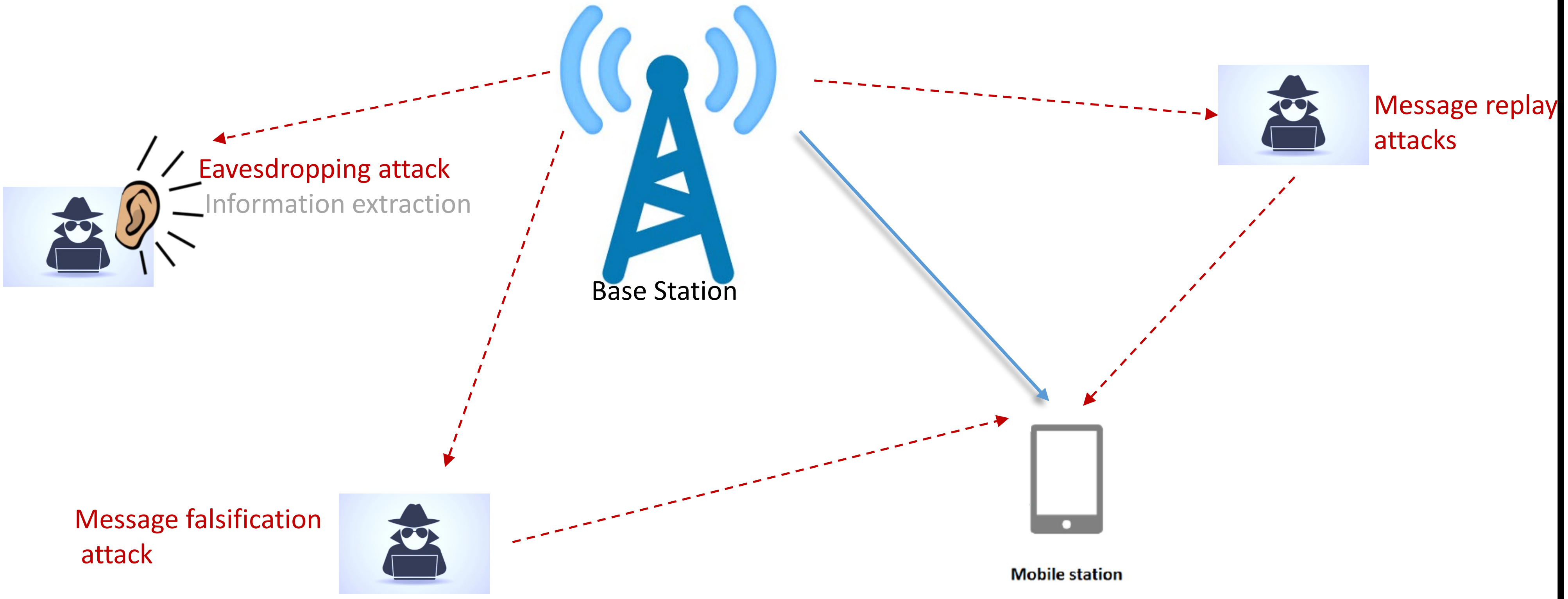
Abundance of bandwidth to support Gpbs data rates

Small wavelength enables small-sized arrays

Large arrays provide high directivity to combat path loss

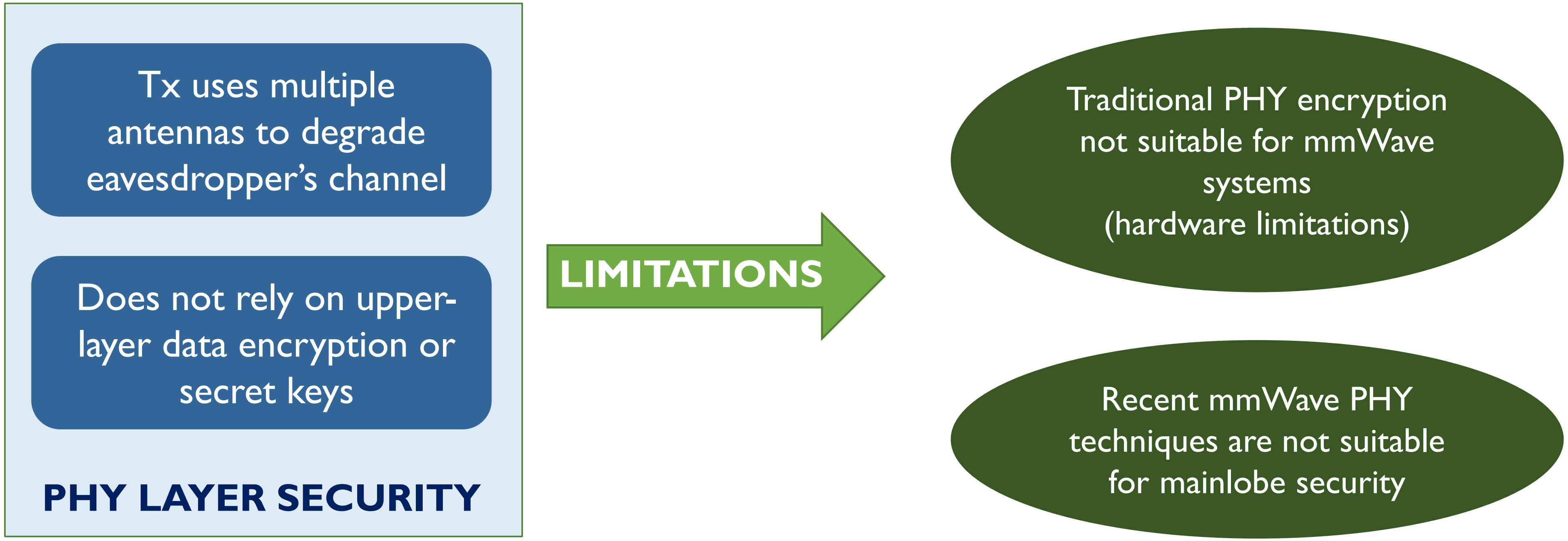
[1] Shu Sun, T. Rappapport, R. W. Heath, Jr., A. Nix, and S. Rangan, `` MIMO for Millimeter Wave Wireless Communications: Beamforming, Spatial Multiplexing, or Both?," IEEE Communications Magazine, December 2014.
[2] S. Zihir, O. Gurbuz, A. Karroy, S. Raman, and G. Rebeiz, "A 60 GHz 64-element wafer-scale phased-array with full-reticle design," in Microwave Symposium (IMS), 2015 IEEE MTT-S International , vol., no., pp.1-3, 17-22 May 2015.

Examples of security threats



Important to secure communication links

Physical layer encryption



Contributions

Address the problem of overlapped communication channel paths between the receiver and eavesdropper

Two transmission techniques that enhance the security of mmWave systems with NLoS channels are proposed

Proposed techniques enhances secrecy by employing path and antenna selection to jam eavesdroppers.

System model

- We consider a mmWave system where the transmitter communicates with a single antenna receiver via NLoS communications paths.
- The transmitter has one RF chain and *N* antennas.
- To transmit k_{th} information symbols $s(k)$ to the receiver the transmitter multiplies $s(k)$ by unit norm transmitting vector ***f****(k)*.
- The received signal at the receiver in the presence of additive noise *z(k)* is given by

$$y(k) = \mathbf{h}^* \mathbf{f} s(k) + z(k)$$

- The channel ***h*** is given by

$$\mathbf{h} = \sqrt{\frac{N}{L}} \sum_{l=1}^{L} \alpha_l \mathbf{a}_{\mathrm{T}}(\theta_l)$$

Number of channel paths

*l*th AoD

Transmitter array response

*l*th path complex gain

Enhancing Secrecy with random path selection

- In this technique the transmitter transmits each data symbol along random path. The transmitters inner antenna phase shifts are set as:

$$\gamma_n(k) = \left(\frac{N-1}{N} - n\right)\pi \frac{2d}{\lambda}\cos(\theta_l)$$

- The beam forming vector is given by $f_n(k) = \frac{1}{\sqrt{N}} \mathrm{e}^{jr_n(k)}$
- At the receivers end we get

$$\begin{aligned} y_{\mathrm{R}}(k,\theta_l) &= \mathbf{h}^* \mathbf{f}(k) s(k) + z_{\mathrm{R}}(k) \\ &= \underbrace{s(k)}_{\substack{\text{information} \\ \text{symbol}}} \underbrace{\alpha_l \sqrt{\frac{N}{L}}}_{\substack{\text{effective channel} \\ \text{and array gain}}} + \underbrace{z_{\mathrm{R}}(k)}_{\substack{\text{additive} \\ \text{noise}}} . \end{aligned}$$

Enhancing Secrecy with random path selection

- At the eavesdropper we get

$$y_{\mathrm{E}}(k,\theta_{\mathrm{E}}) = \mathbf{h}^{*}\mathbf{f}(k)s(k) + z_{\mathrm{E}}(k)$$

$$= \underbrace{s(k)}_{\substack{\text{information}\\ \text{symbol}}} \underbrace{\alpha_{\mathrm{E}}}_{\substack{\text{channel}\\ \text{gain}}} \underbrace{\sqrt{1/LN}B(\theta_l)}_{\substack{\text{artifical}\\ \text{noise}}} + \underbrace{z_{\mathrm{E}}(k)}_{\substack{\text{additive}\\ \text{noise}}}$$

Enhancing Secrecy with random path selection

- The drawback here is that we require large number of paths L, to induce randomness.
- We propose to randomize both antennas and angle of departure to maximize artificial noise when L is small.

Enhancing secrecy with joint path and antenna selection

- A random set I_M of antennas is used to transmit along the strongest path and the remaining set I_L of antennas are used to transmit along a random path.
- The transmit antenna phase shifts are set as

$$\Upsilon_n(k) = \begin{cases} \left(\frac{N-1}{2} - n\right) 2\pi \frac{d}{\lambda} \cos(\theta_S), & n \in \mathcal{I}_M(k) \\ \left(\frac{N-1}{2} - n\right) 2\pi \frac{d}{\lambda} \cos(\theta_i), & n \in \mathcal{I}_L(k) \end{cases}$$

- The receiver receives

$$\begin{aligned} y_R(k, \theta_S, \theta_i) &= \mathbf{h}^* \mathbf{f}(k) s(k) + z_R(k) \\ &= \underbrace{s(k)}_{\text{information symbol}} \underbrace{\frac{1}{\sqrt{LN}} \left(\alpha_S M + \alpha_i (N - M) + \beta_R \right)}_{\text{effective beamforming and channel gain}} + \underbrace{z_R(k)}_{\text{additive noise}}, \end{aligned}$$

Enhancing secrecy with joint path and antenna selection

- The eavesdropper receives

$$y_{\mathrm{E}}(k, \theta_{\mathrm{S}}, \theta_i, \theta_{\mathrm{E}}) = \mathbf{h}^* \mathbf{f}(k) s(k) + z_{\mathrm{E}}(k)$$

$$= \underbrace{s(k)}_{\substack{\text{information}\\ \text{symbol}}} \quad \underbrace{\alpha_{\mathrm{E}} \beta_{\mathrm{E}}}_{\substack{\text{effective artificial}\\ \text{noise}}} + \underbrace{z(k)}_{\substack{\text{additive}\\ \text{noise}}}$$

Performance evaluation

Setup

- A transmitter (Tx) with a single RF chain is communicating to a single antenna receiver (Rx) via NLoS links.
- Tx is equipped with ULA with half wavelength separation and N= 32 antennas.
- Eavesdropper and strongest receiver AoD overlap at AoD 40 degrees.

Assumptions

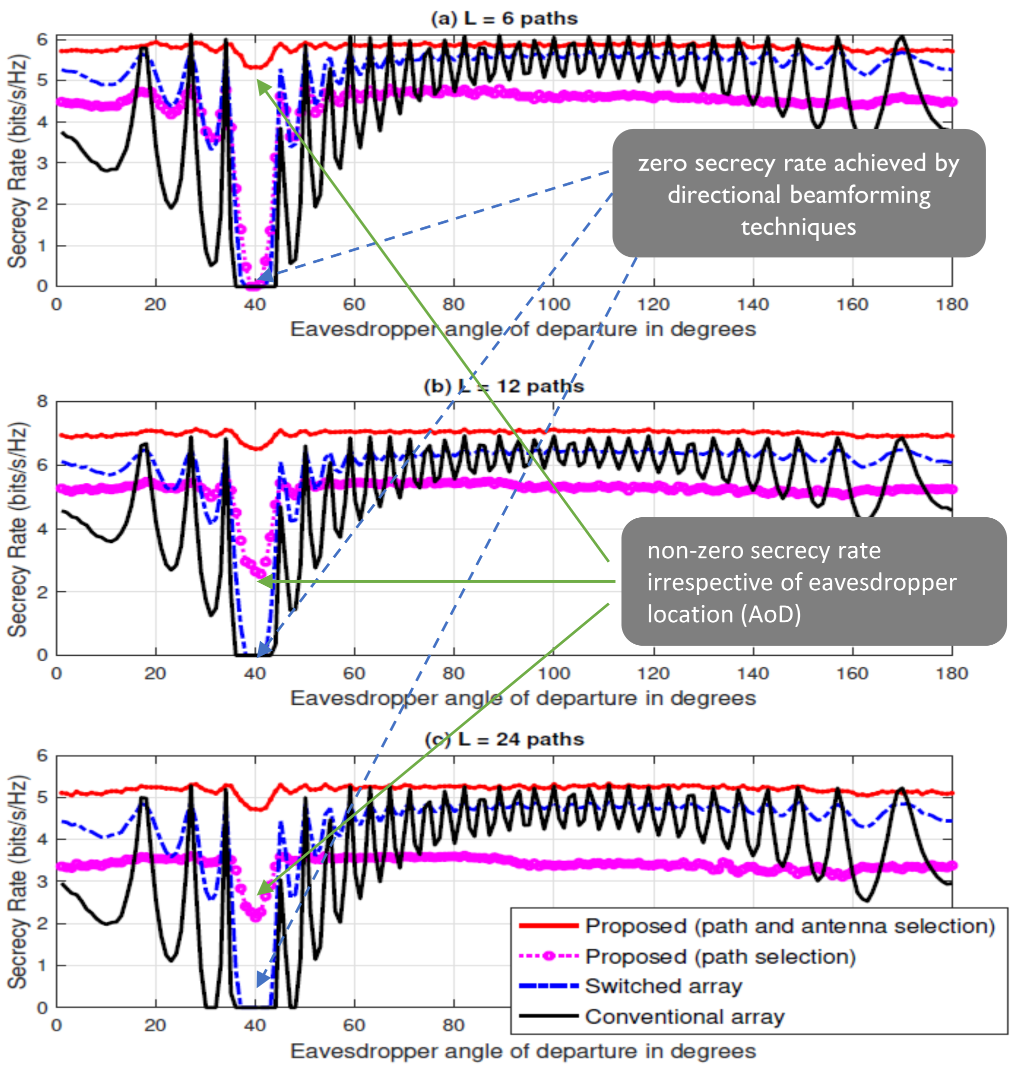
- Tx and Rx have perfect knowledge of their channels and path/antenna selection sequence.
- Tx and Rx are not aware of eavesdropper presence.

Secrecy Rate

$$R = [\log_2(1 + \mathrm{SNR_R}) - \log_2(1 + \mathrm{SNR_E})]^+$$

SNR at target receiver

SNR at eavesdropper



Secrecy rate versus the eavesdropper's angle of departure for different number of transmission paths

Performance evaluation

Setup

- A transmitter (Tx) with a single RF chain is communicating to a single antenna receiver (Rx) via NLoS links.
- Tx is equipped with ULA with half wavelength separation and *N*= 32 antennas.
- Eavesdropper and strongest receiver AoD overlap at AoD 40 degrees.

Assumptions

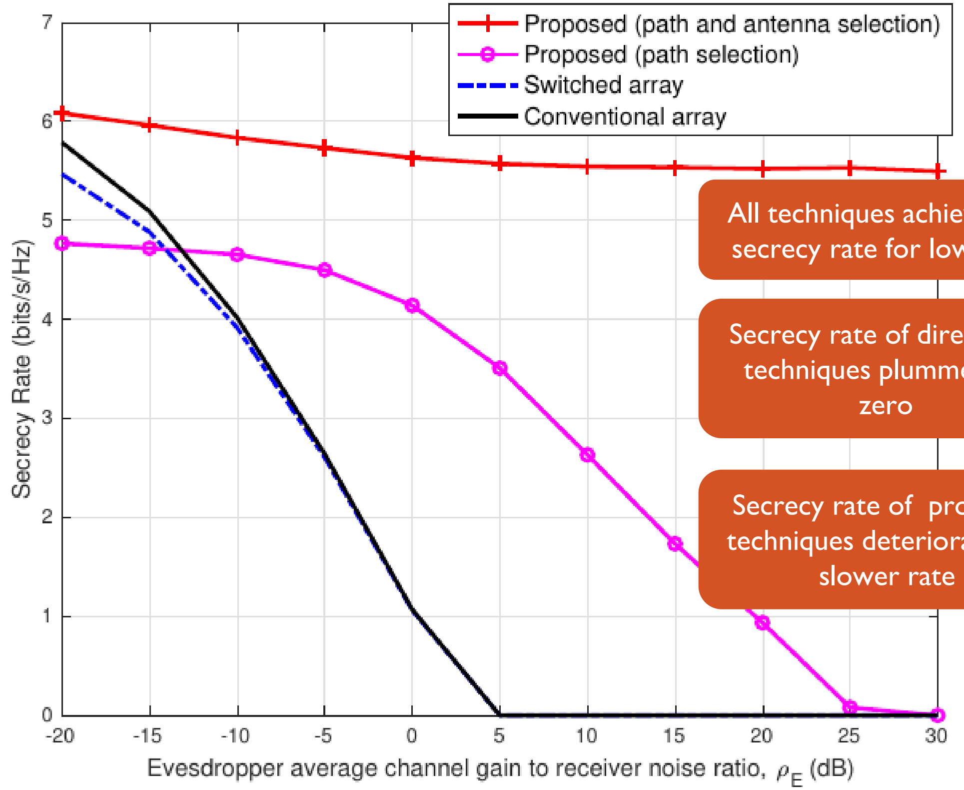
- Tx and Rx have perfect knowledge of their channels and path/antenna selection sequence.
- Tx and Rx are not aware of eavesdropper presence.

Secrecy Rate

$$R = [\log_2(1 + \mathrm{SNR_R}) - \log_2(1 + \mathrm{SNR_E})]^+$$

SNR at target receiver

SNR at eavesdropper



All techniques achieve high secrecy rate for low $\mathrm{SNR_E}$

Secrecy rate of directional techniques plummets to zero

Secrecy rate of proposed techniques deteriorate at a slower rate

Secrecy rate versus the eavesdropper’s Evesdropper average channel gain to receiver noise ratio; *L* = 12, eavesdropper located along the strongest path AoD 40 deg.

Conclusions

- Problem of PLS in the presence of an eavesdropper with overlapped channel paths with the target receiver is addressed.
- Two transmission techniques suitable for mmWave systems with analog antenna architectures are proposed.
- Random path selection and joint path and antenna selection induces noise-like signals at an arbitrary eavesdropper and improves the secrecy of the communication system.
- Proposed techniques require the number of paths $L>1$. For single path, LoS link, the proposed techniques can not safeguard against eavesdropping.

Questions

Please forward all questions/comments to the authors

Rohith Talwar, Nancy Amala, George Medina, Akshadeep Singh Jida, and Mohammed E. Eltayeb
Department of Electrical & Electronic Engineering
California State University, Sacramento, USA
Emails: {rohithtalwar, nancyamalajosephraj, gm739, asjida, mohammed.eltayeb}@csus.edu