KTH VETENSKAP OCH KONST

Should We **Be Afraid** of **Uncontrolled** or **Malicious Reconfigurable Surfaces?**

Emil Björnson

Professor of Wireless Communication

Fellow of IEEE, Digital Futures, and Wallenberg Academy

KTH Royal Institute of Technology, Stockholm, Sweden

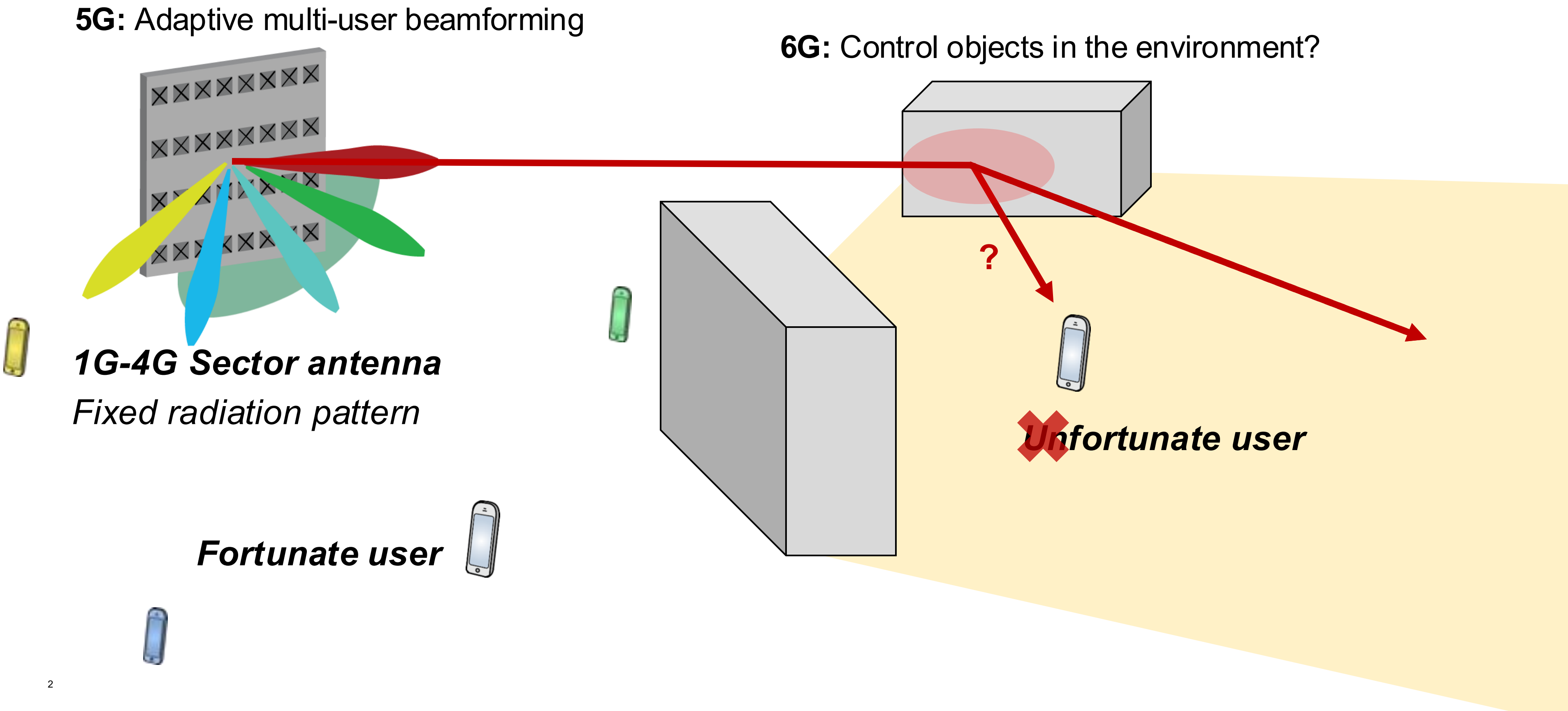
A special thanks to

Haifan Yin
Ziya Gülgün
Gabor Fodor
Steven Rivetti
Elina Björnson
Erik G. Larsson
Mikael Skoglund
Luca Sanguinetti
Doğa Gürgünoğlu
Özgecan Özdogan
Özlem Tuğfe Demir

Knut and Alice Wallenberg Foundation

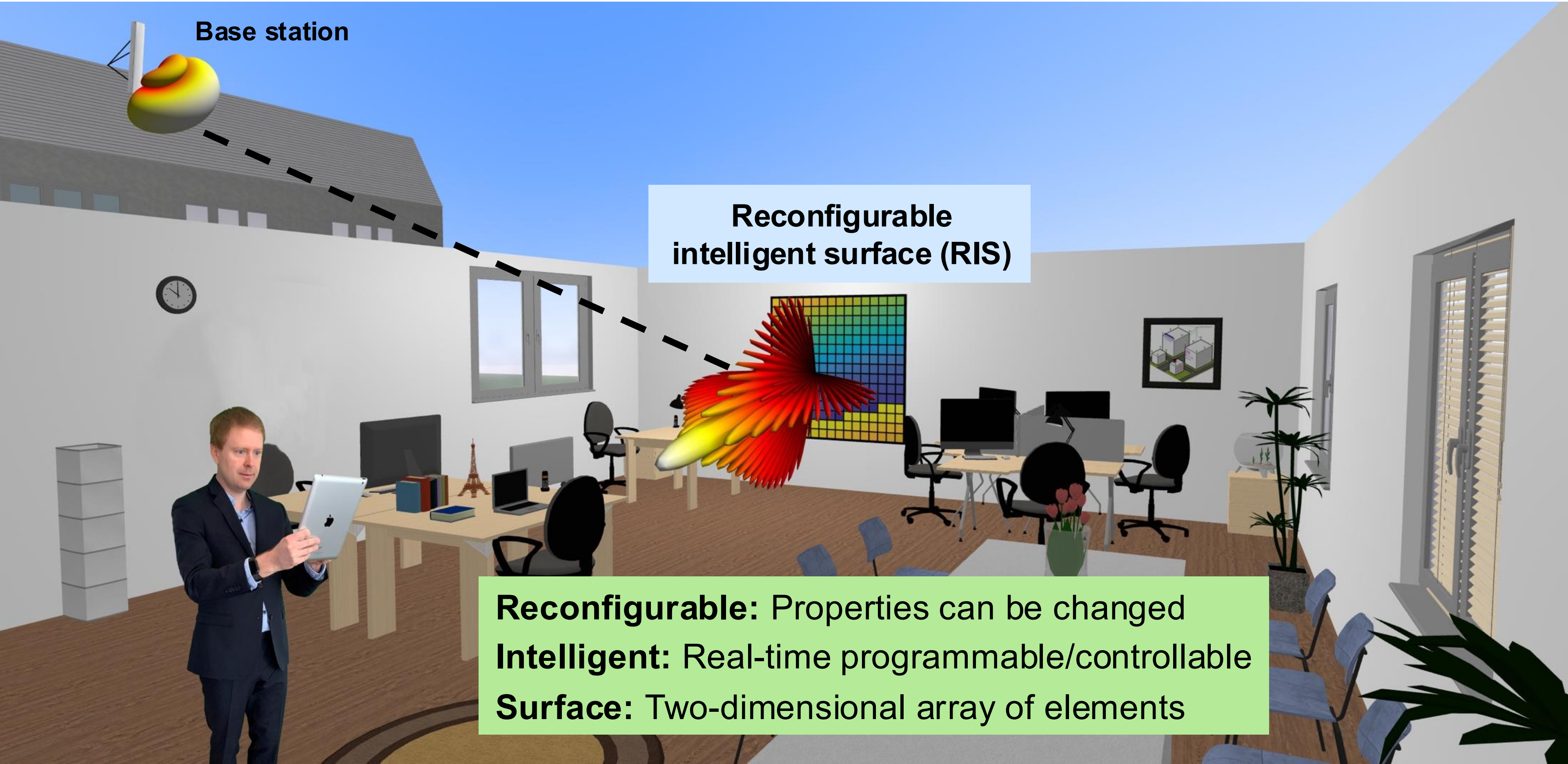
Swedish Research Council

Evolution of Wireless Infrastructure




Base station
Wall penetration:
– 20 dB or more
Reflection

Virtual Line-of-Sight (LOS) Path

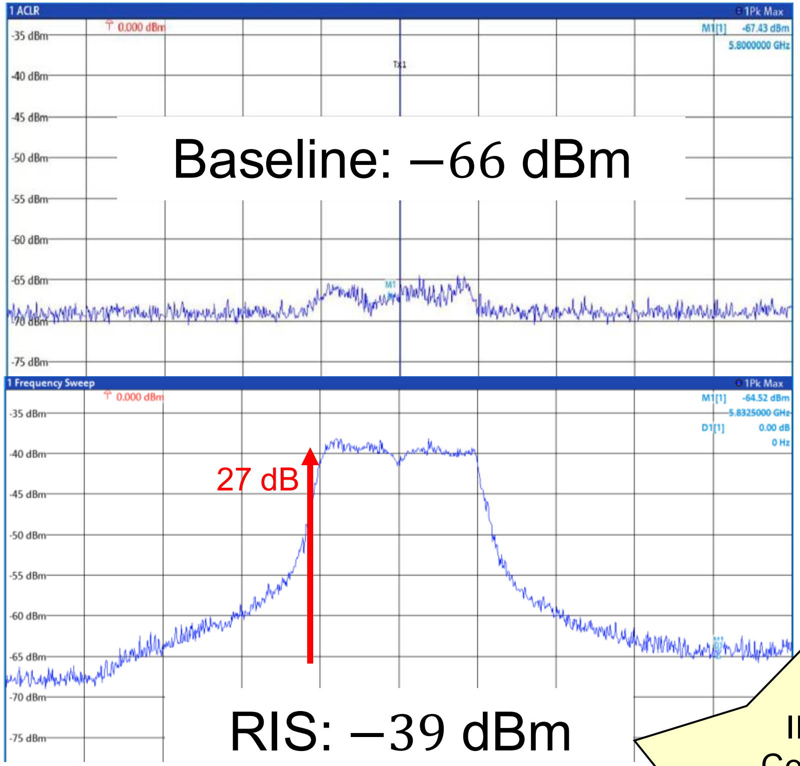


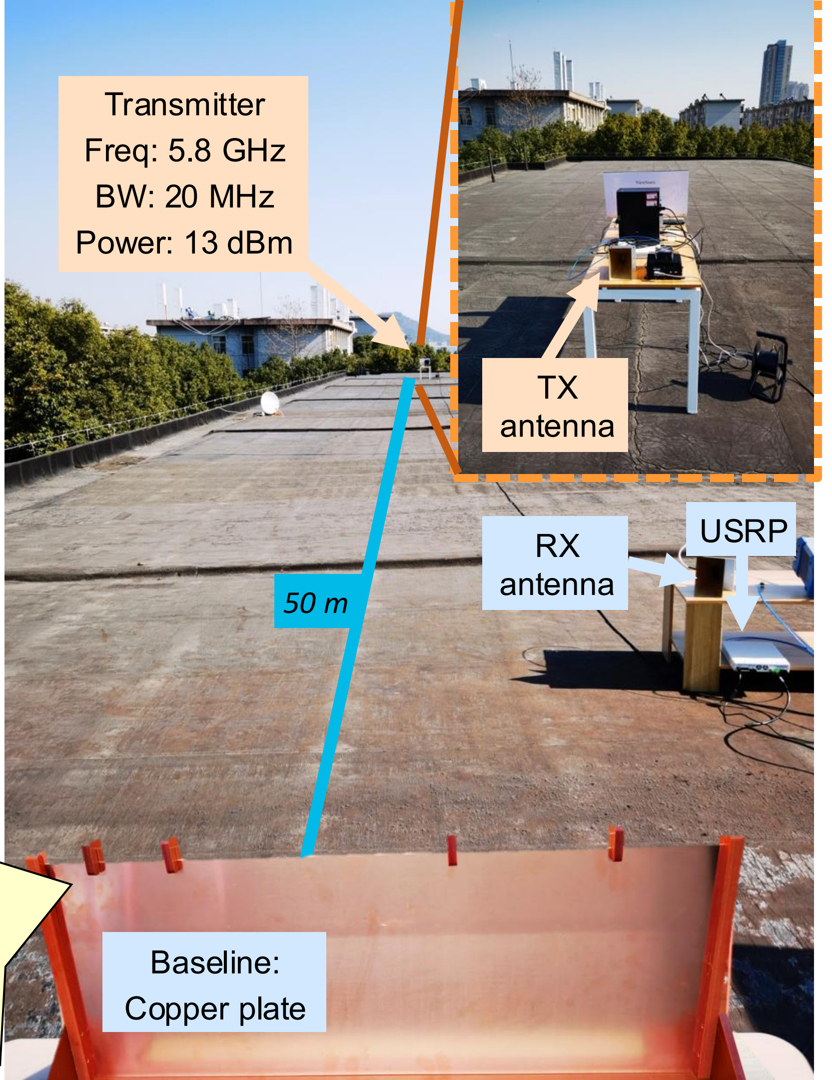
Reconfigurable: Properties can be changed

Intelligent: Real-time programmable/controllable

Surface: Two-dimensional array of elements

Experimental Demonstration

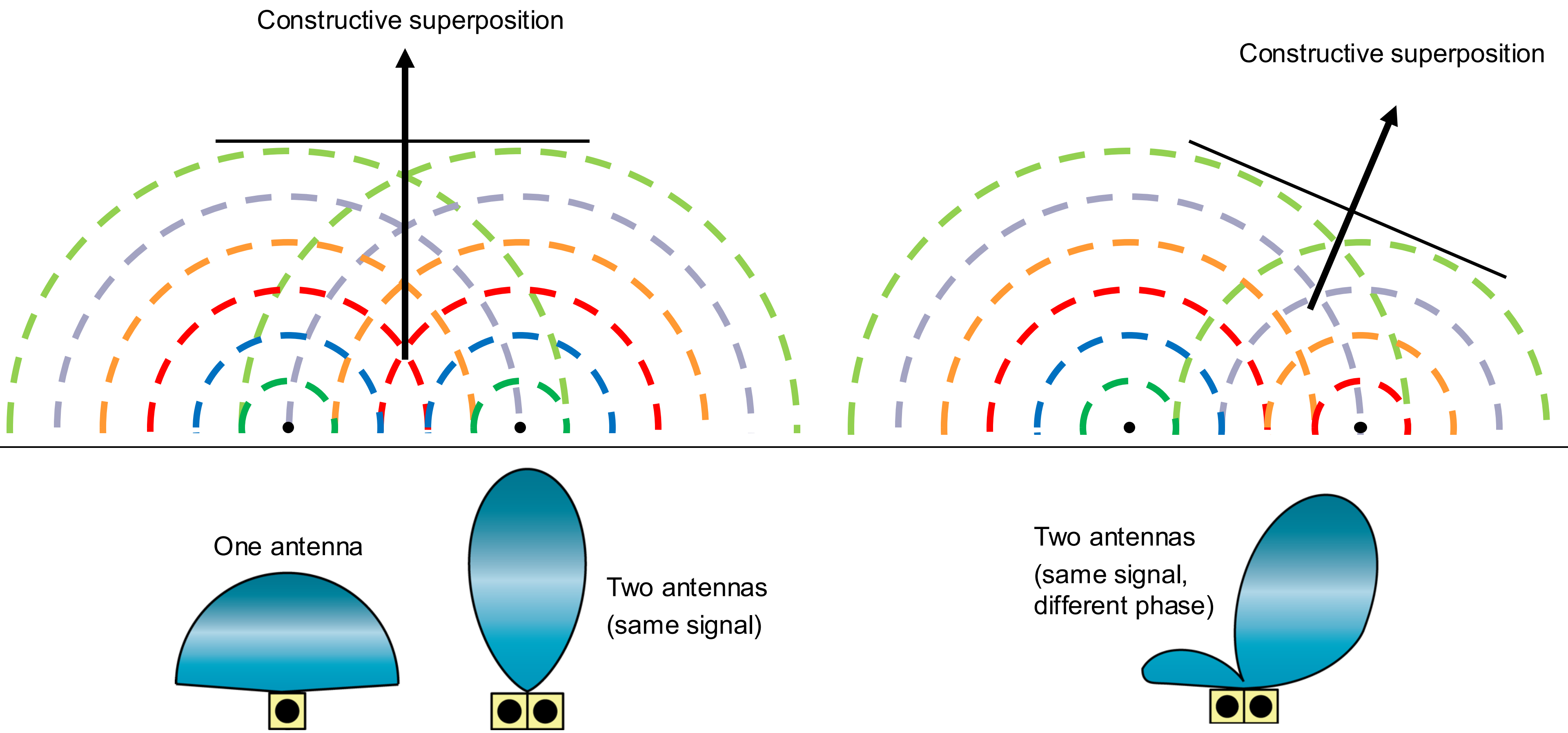




IEEE ComSoc Stephen O. Rice Prize 2024

Reference: X. Pei, H. Yin, L. Tan, L. Cao, Z. Li, K. Wang Björnson, “RIS-Aided Wireless Communications: Prototy Beamforming, and Indoor/Outdoor Field Trials,” IEEE TC M, 2021

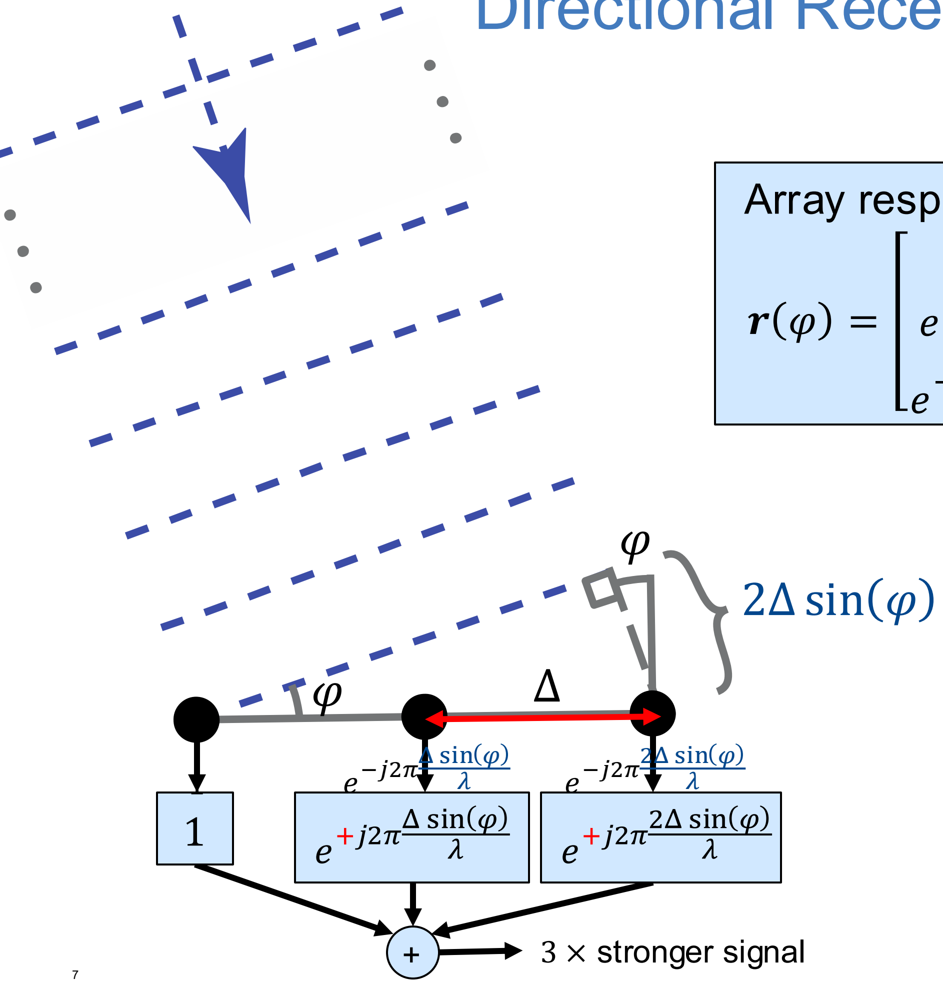
Adaptive Beamforming

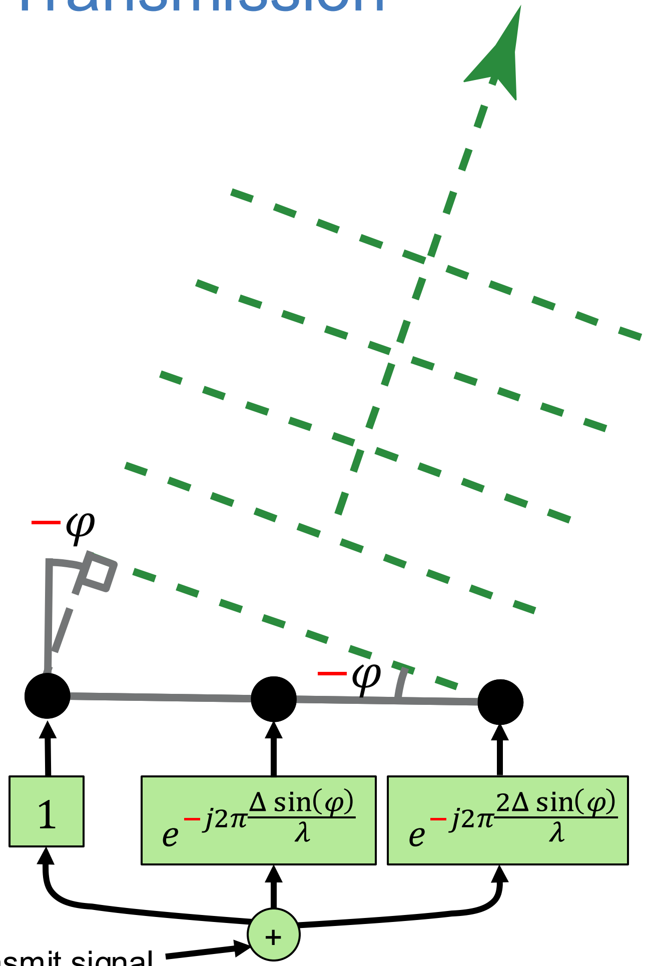


Directional Reception and Transmission

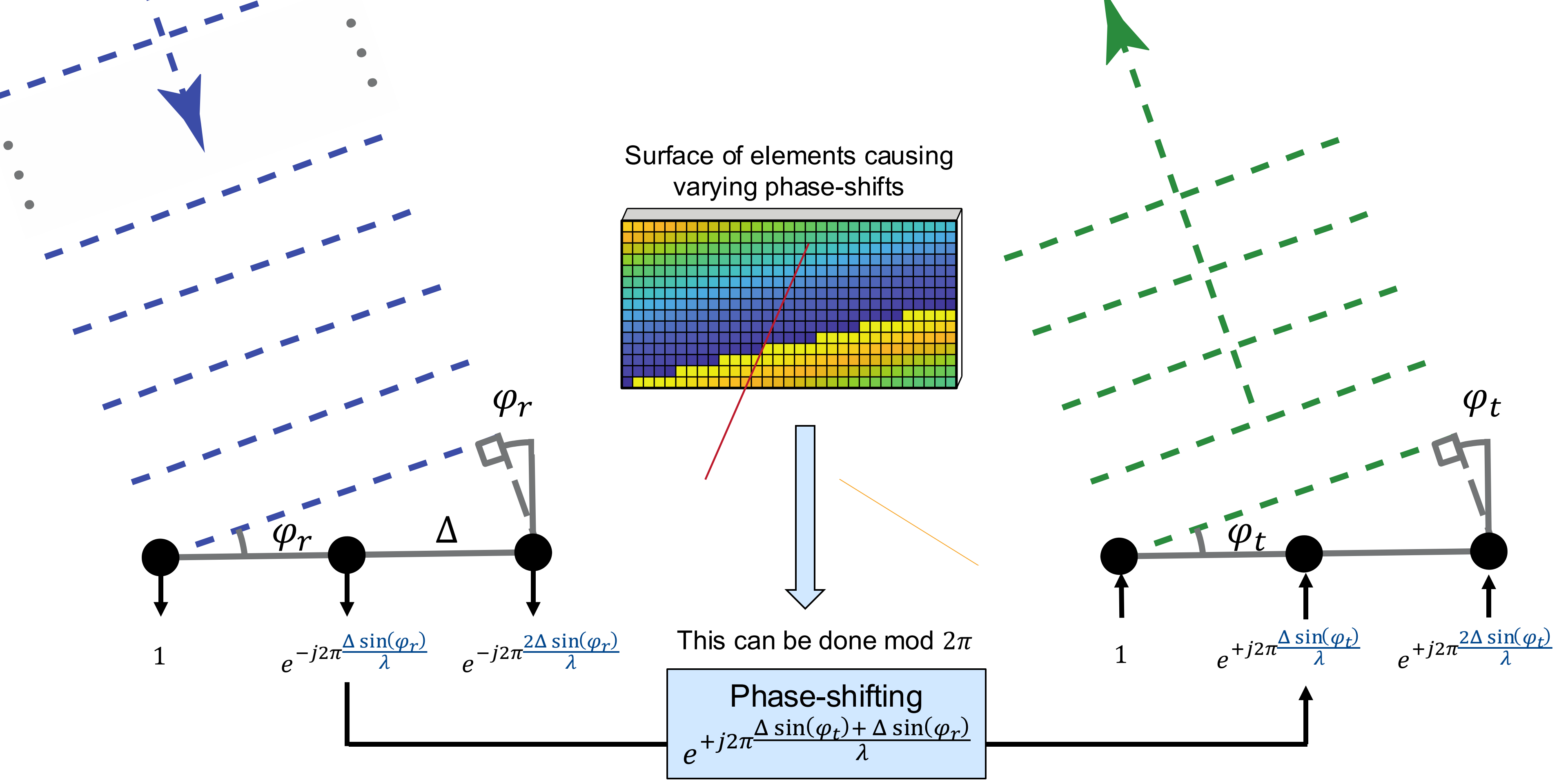
Array response vector:

$$\boldsymbol{r}(\varphi) = \begin{bmatrix} 1 \\ e^{-j2\pi\frac{\Delta\sin(\varphi)}{\lambda}} \\ e^{-j2\pi\frac{2\Delta\sin(\varphi)}{\lambda}} \end{bmatrix}$$

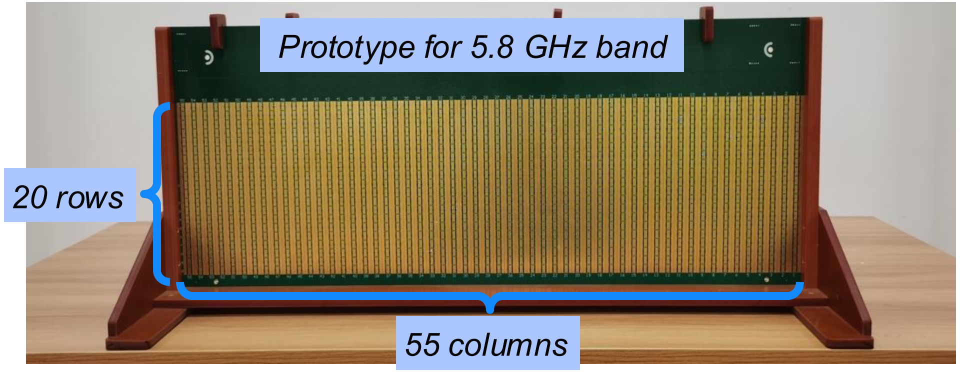


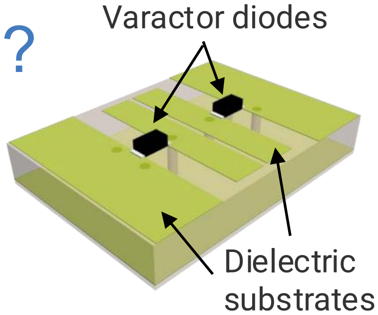


Controllable Reflection



How Does an Element Phase-Shift the Signal?



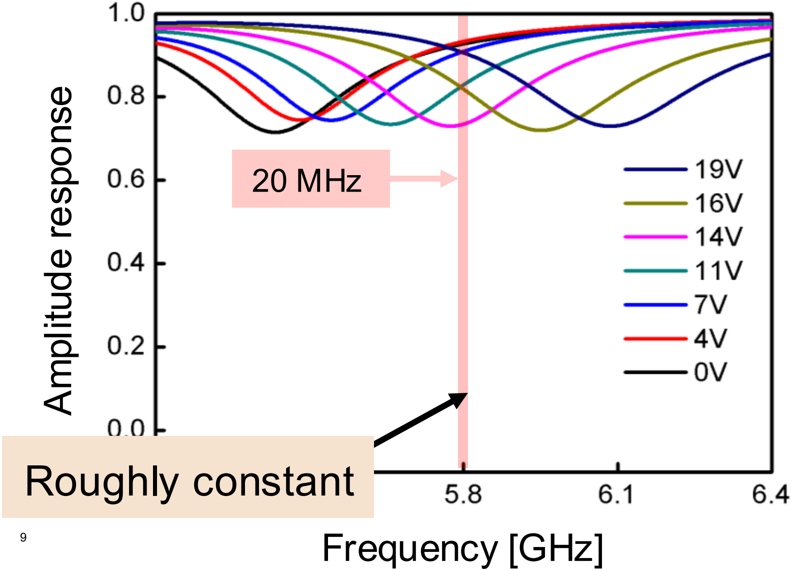


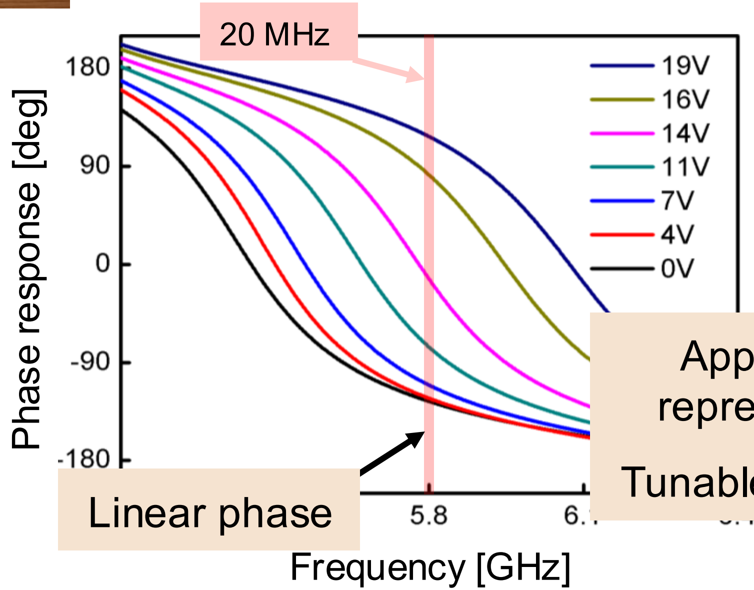
Example: Patch with bias voltage V

Reflection coefficient:

$$\frac{Z_n(V) - Z_0}{Z_n(V) + Z_0}$$

Reference: X. Pei, H. Yin, L. Tan, L. Cao, Z. Li, K. Wang, K. Zhang, E. Björnson, "RIS-Aided Wireless Communications: Prototyping, Adaptive Beamforming, and Indoor/Outdoor Field Trials," IEEE TCOM 2021.

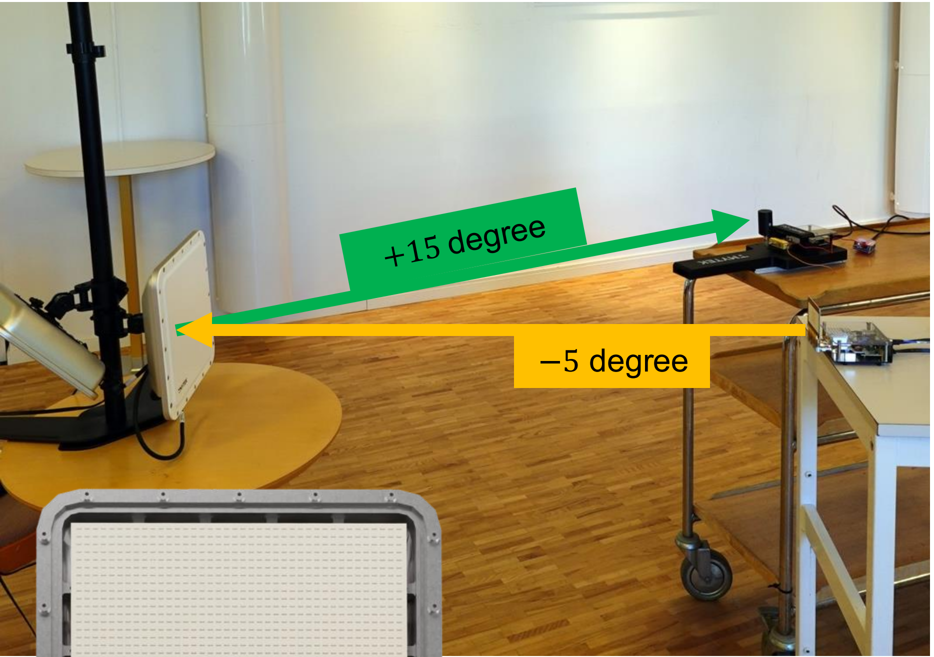




Approximate representation:

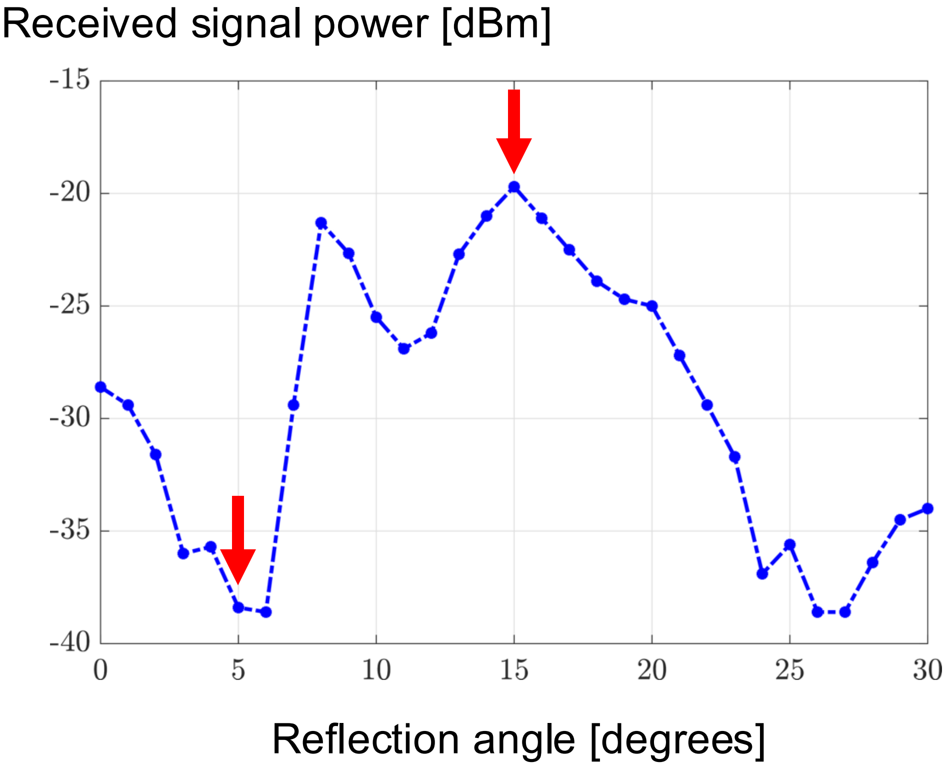
Tunable time delay

Recent Experiment at KTH

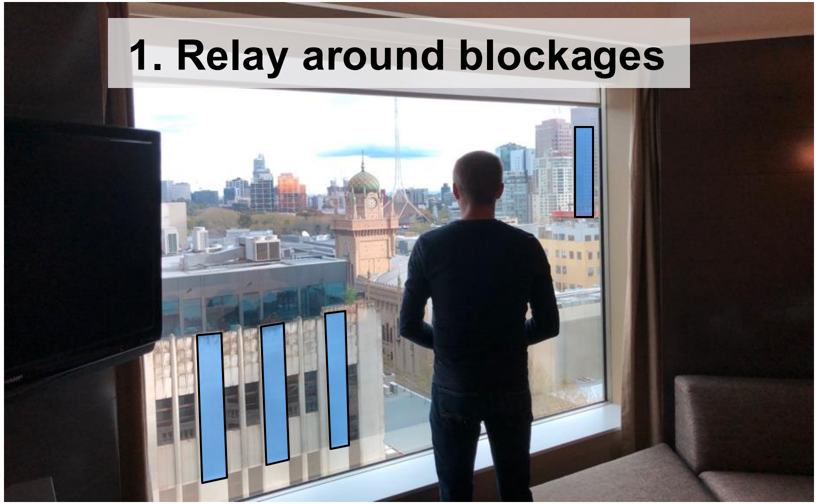


28 GHz RIS

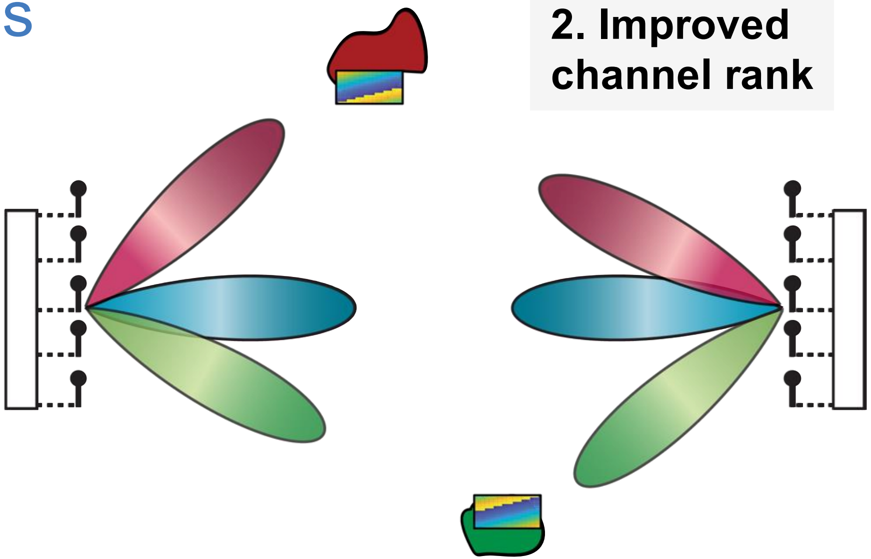
32 × 32 array



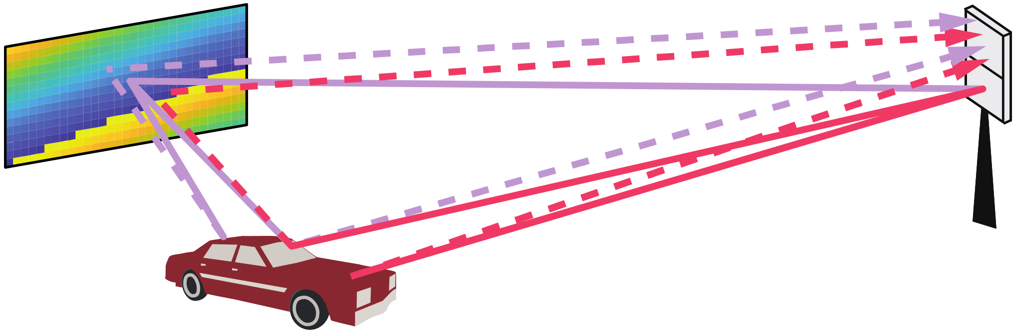
Many Possible RIS Use Cases



2. Improved channel rank

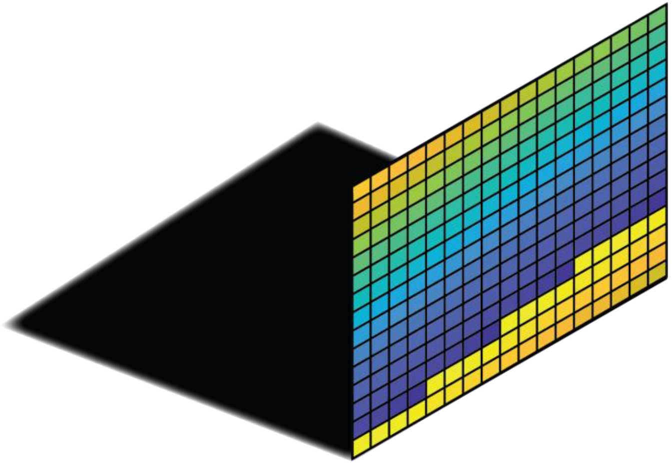


3. Improved localization and sensing

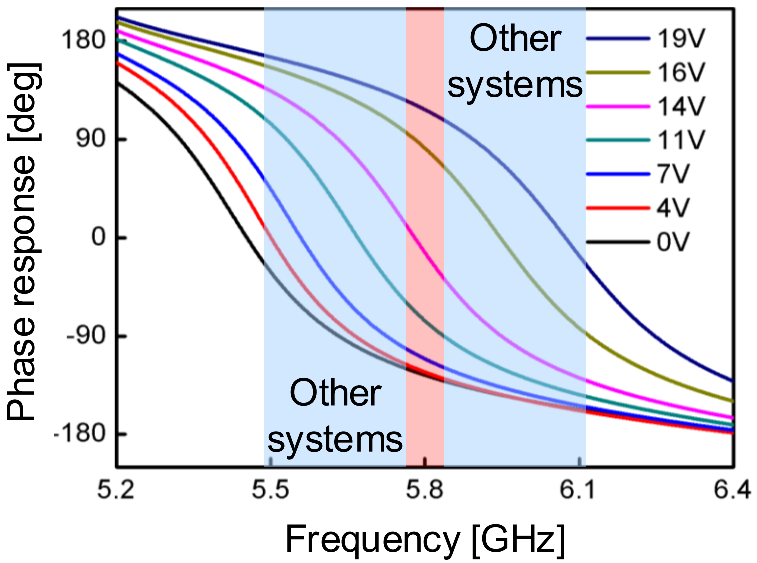


4. **Physical layer security**
5. **Wireless power transfer**
6. **…**

ISSUES WITH
UNCONTROLLED RIS



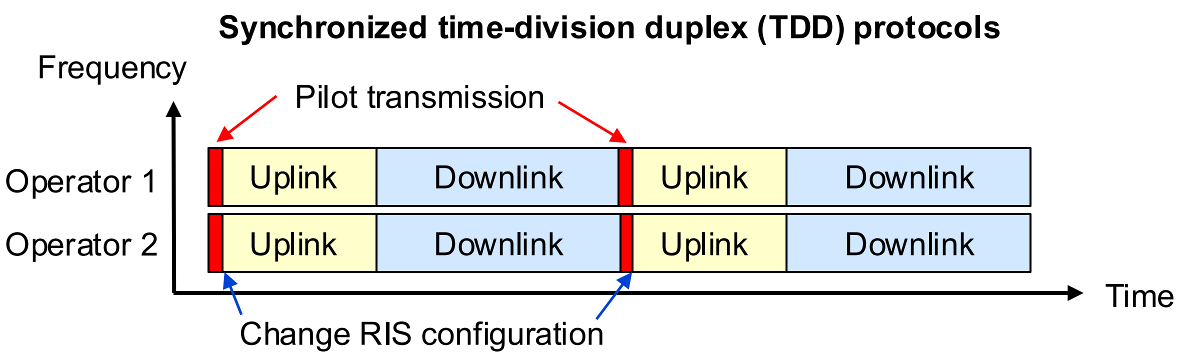
Reconfigurable Surfaces Affect Multiple Systems

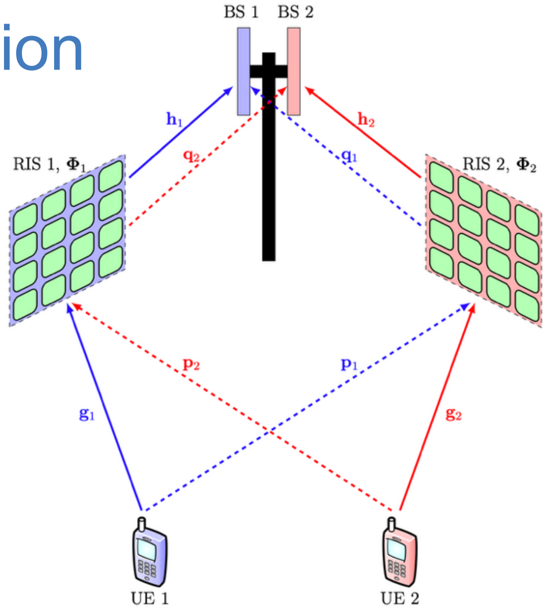


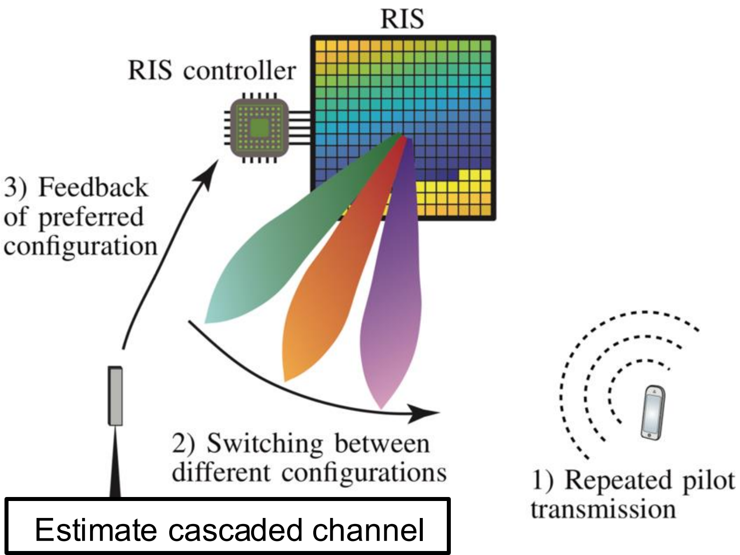
Best case scenario:
Increased small-scale fading

Nothing prevents you from waving a metal plate in front of a base station

Worst-Case: Inter-Operator Pilot Contamination







Both operators change both channel simultaneously

None of them gets the channel they wanted!

Reference: D. Gürgünoglu, E. Björnson, G. Fodor, "Combating Inter-Operator Pilot Contamination in Reconfigurable Intelligent Surfaces Assisted Multi-Operator Networks," IEEE Tran. Commun, 2024

Channel Estimation with Inter-Operator Pilot Contamination

Received signal at operator 1's base station (pilot $\sqrt{P_p}$):

$$y_{p1} = \underbrace{\sqrt{P_p}\phi_1^T \mathbf{D}_{\mathbf{h}_1}\mathbf{g}_1}_{\text{From own RIS}} + \underbrace{\sqrt{P_p}\phi_2^T \mathbf{D}_{\mathbf{q}_1}\mathbf{p}_1}_{\text{Via other RIS}} + w_{p1}$$

Repeat pilot with L different RIS configurations:

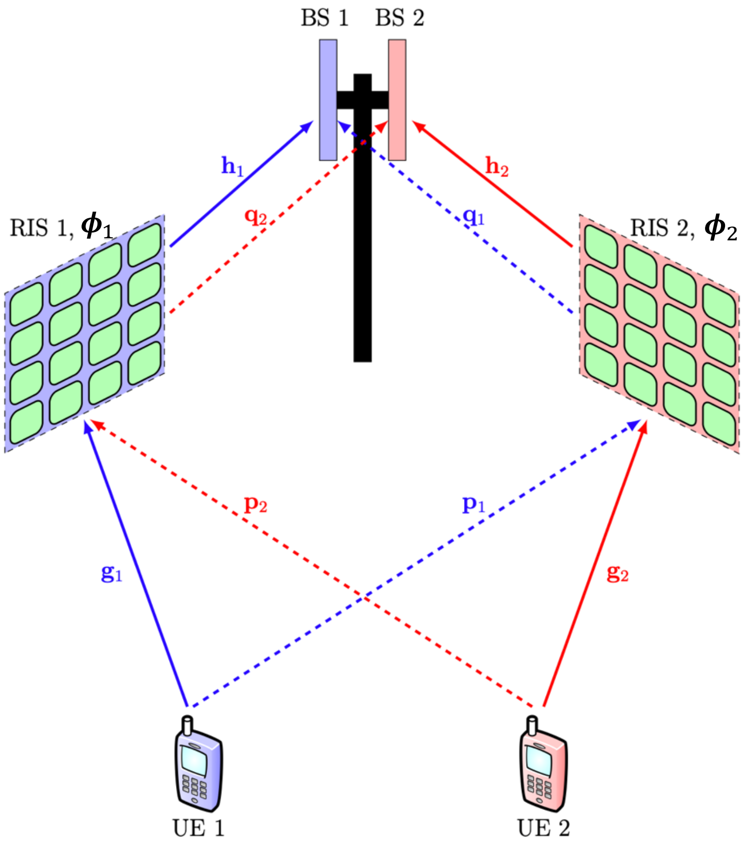
$$\mathbf{B}_k \triangleq [\phi_k[1] \quad \ldots \quad \phi_k[L]]^T \in \mathbb{C}^{L \times N}$$

Stack the received signals:

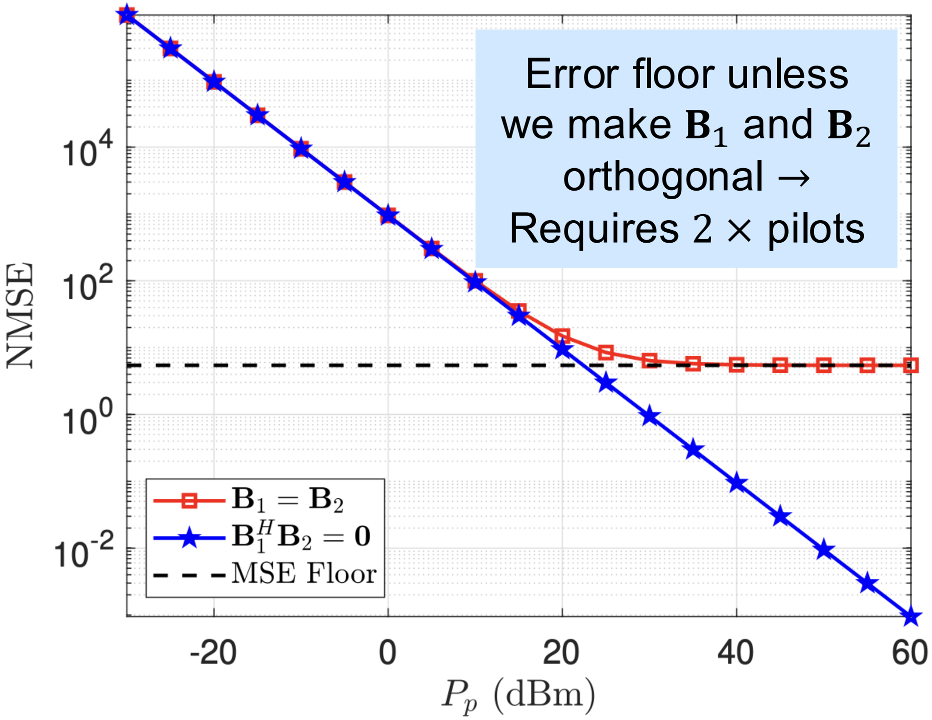
$$\mathbf{y}_{p1} = \sqrt{P_p}\mathbf{B}_1\mathbf{D}_{\mathbf{h}_1}\mathbf{g}_1 + \sqrt{P_p}\mathbf{B}_2\mathbf{D}_{\mathbf{q}_1}\mathbf{p}_1 + \mathbf{w}_{p1}$$

Least-squares estimator of $\mathbf{g}_1$:

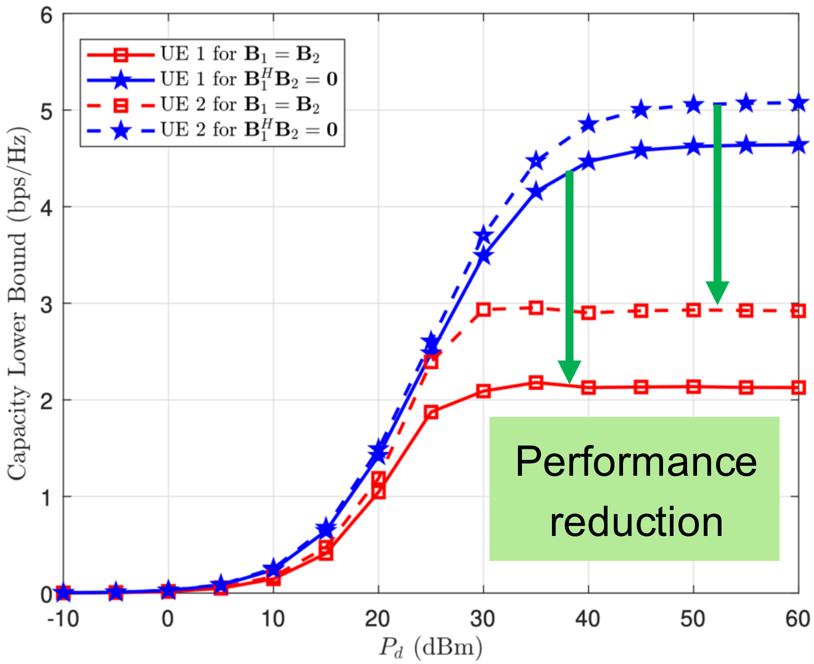
$$\hat{\mathbf{g}}_1 = \frac{\mathbf{D}_{\mathbf{h}_1}^{-1}\mathbf{B}_1^{\dagger}\mathbf{y}_{p1}}{\sqrt{P_p}} = \mathbf{g}_1 + \mathbf{D}_{\mathbf{h}_1}^{-1}\mathbf{B}_1^{\dagger}\mathbf{B}_2\mathbf{D}_{\mathbf{q}_1}\boldsymbol{p}_1 + \text{noise}$$



Consequences of Inter-Operator Pilot Contamination



Pilot transmission power versus the channel estimation normalized mean-squared error (NMSE)



Capacity with fixed pilot power

How to Combat Inter-Operator Pilot Contamination?

Receive Beamforming Schemes to Mitigate Inter-Operator Pilot Contamination in RIS-Aided MIMO Networks

Doğa Gürgünoğlu, *Student Member, IEEE*, Ziya Gülgün, Emil Björnson, *Fellow, IEEE*, Gabor Fodor, *Senior Member, IEEE*

***Abstract*—When reconfigurable intelligent surfaces (RISs) are integrated into cellular networks, they can give rise to inter-operator pilot contamination, severely degrading network performance. While combatting this effect is possible by orthogonalizing the RIS configurations, it requires inter-operator coordination and limits the degree of configuration freedom per RIS. Therefore, in this work, we explore the use of receive beamforming to mitigate inter-operator pilot contamination in RIS-aided multiple input multiple output (MIMO) systems, where two operators share infrastructure and deploy RISs to enhance network coverage. We focus on uplink channel estimation and data transmission and propose a method in which the base stations (BSs) apply a novel kind of receive beamforming to suppress ... posed met... and an a... contamina... BS beamf... interfering... pilot cont... channel, r... and halvi... BS uses ...**

[2]. As they became prevalent due to the large-scale deployments by multiple operators, they made a revolutionary impact on the achievable performance of mobile broadband services [3]. Thanks to the multiple antennas, wireless channels gained multiple spatial degrees-of-freedom allowing for spatial diversity and multiplexing schemes that improve signal quality and enable to serve multiple users using fewer resources over time and frequency [4]. In addition, the presence of multiple antennas gave rise to an effect called channel hardening, which made the channels with more antennas less random, resulting in lower outage probabilities and hence increased reliability ... changer in ... efficiency ... data-heavy ... streaming ... MIMO has ... antennas, ... capabilities

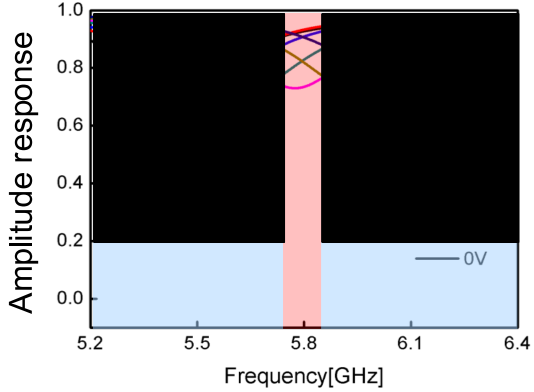
Multi-antenna signal processing

Identify other RIS presence

Spatial interference suppression

Improved hardware design

Sharper amplitude response

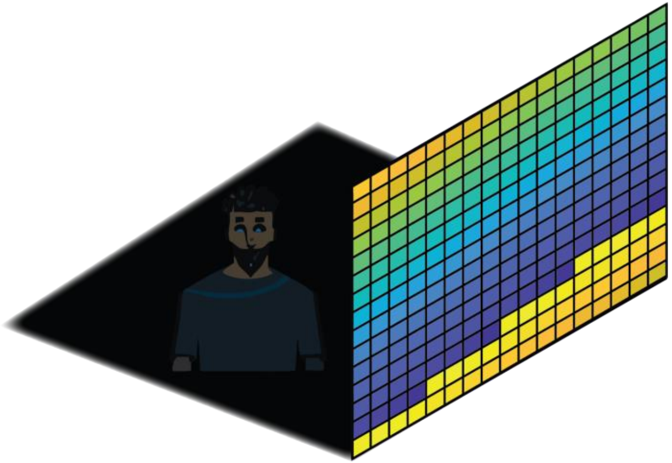


Policy making and standardization

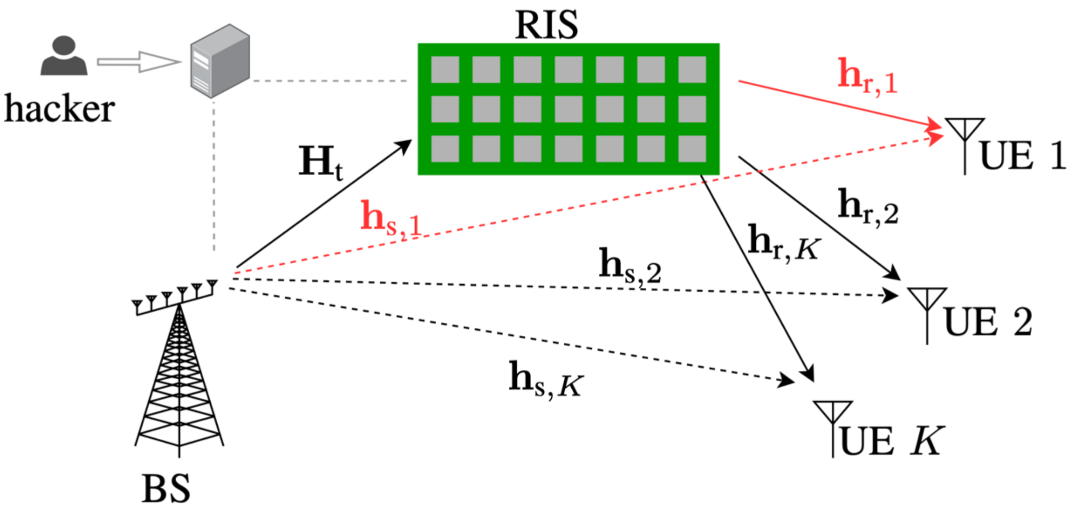
Who is allowed to use an RIS?

Do we need operational rules?

ISSUES WITH **MALICIOUS RIS**



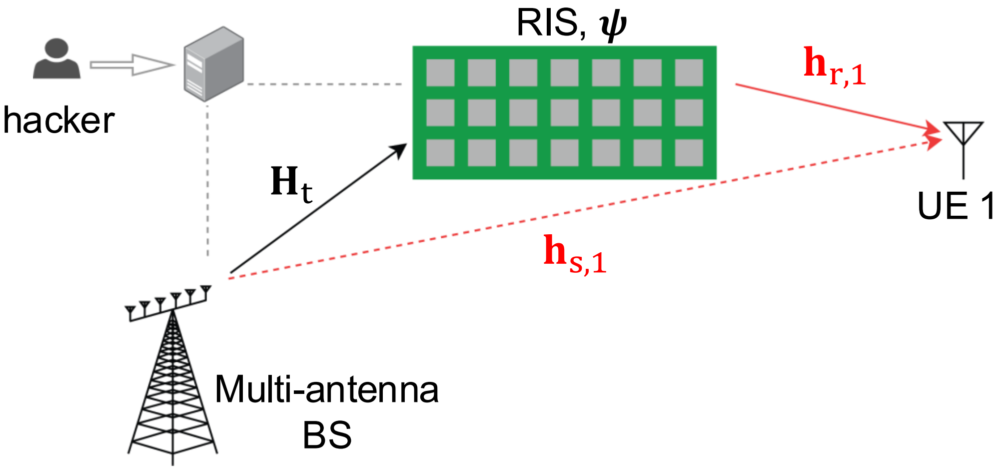
What if a Hacker Controls the RIS?



Goal: Remove one UE from service without being discovered (minimal effect on other users)

Reference: S. Rivetti, Ö. T. Demir, E. Björnson M. Skoglund, “Malicious Reconfigurable Intelligent Surfaces: How Impactful Can Destructive Beamforming be?,” IEEE Wireless Commun. Lett., 2024.

Single-User Case



Effective channel with precoder $\mathbf{p}_1$:

$$\left|\underbrace{\mathbf{p}_1^T \mathbf{h}_{s,1}}_{h_{s,1}} + \underbrace{\mathbf{p}_1^T \mathbf{H}_t \mathbf{D}_{\mathbf{h}_{r,1}}}_{\breve{\mathbf{h}}_1^H} \boldsymbol{\psi}\right|^2 = \widehat{\boldsymbol{\psi}}^H \mathbf{R}_1 \widehat{\boldsymbol{\psi}}$$

Define: $\hat{\boldsymbol{\psi}} = \left[\boldsymbol{\psi}^\top, 1\right]^\top, \quad \mathbf{R}_1 = \begin{bmatrix} \breve{\mathbf{h}}_1 \breve{\mathbf{h}}_1^H & \breve{\mathbf{h}}_1 h_{s,1} \\ h_{s,1}^* \breve{\mathbf{h}}_1^H & |h_{s,1}|^2 \end{bmatrix}$

P1: $\underset{\hat{\boldsymbol{\psi}}}{\text{minimize}} \ \hat{\boldsymbol{\psi}}^H \mathbf{R}_1 \hat{\boldsymbol{\psi}}$

subject to $\left|\hat{\psi}_n\right| = 1, \ n = 1, \ldots, N,$

$\hat{\psi}_{N+1} = 1,$

Constructive superposition:

Maximize $\left|\breve{\mathbf{h}}_1^H \boldsymbol{\psi}\right|^2$ and give phase $\arg(h_{s,1})$

Destructive superposition:

Maximize $\left|\breve{\mathbf{h}}_1^H \boldsymbol{\psi}\right|^2$ and give phase $-\arg(h_{s,1})$

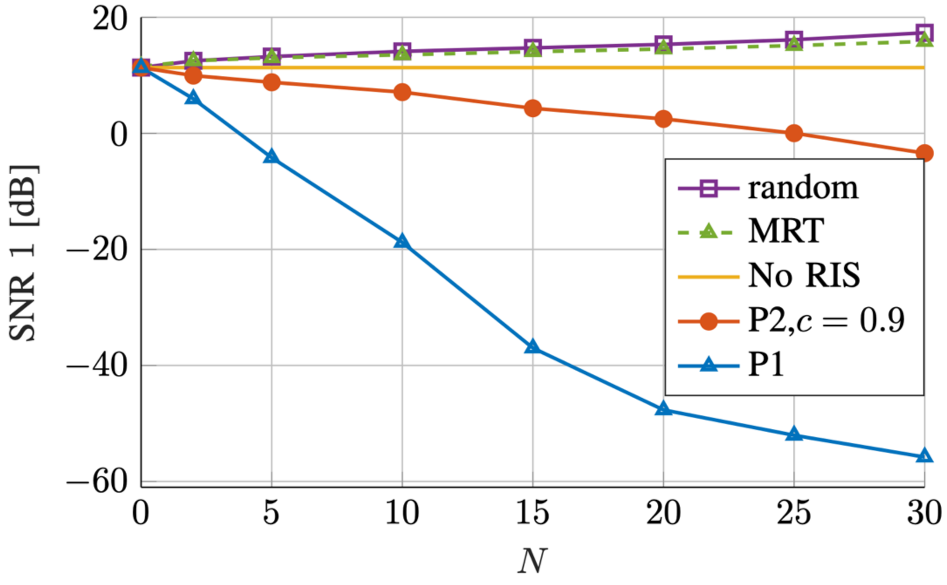
(Or make $\breve{\mathbf{h}}_1^H \boldsymbol{\psi} = -h_{s,1}$ if possible)

Multi-User Case

P2:

$$\begin{aligned} \underset{\hat{\psi}}{\text{minimize}} \quad & \hat{\psi}^{\mathsf{H}}\mathbf{R}_1\hat{\psi} \\ \text{subject to} \quad & \hat{\psi}^{\mathsf{H}}\mathbf{R}_k\hat{\psi} \geq \gamma_k\sigma^2, \; k = 2,\ldots,K, \\ & \left|\hat{\psi}_n\right| = 1, \; n = 1,\ldots,N, \\ & \hat{\psi}_{N+1} = 1, \end{aligned}$$

SNR constraints: Pick γ_k as fraction c of maximum SNR



Solution: Relax constraints to continuous high-rank $\mathbf{\Psi} = \boldsymbol{\psi}\boldsymbol{\psi}^{\mathrm{H}}$, then use randomization techniques.

Works also with imperfect CSI

Reference: S. Rivetti, Ö. T. Demir, E. Björnson M. Skoglund, "Malicious Reconfigurable Intelligent Surfaces: How Impactful Can Destructive Beamforming be?," IEEE Wireless Commun. Lett., 2024.

Another Example of a Malicious RIS

Destructive and Constructive RIS Beamforming in an ISAC Multi-User MIMO Network

Steven Rivetti[†], Özlem Tuğfe Demir[*], Emil Björnson[†], Mikael Skoglund[†]
[†]School of Electrical Engineering and Computer Science (EECS), KTH Royal Institute of Technology, Sweden
[*]Department of Electrical-Electronics Engineering, TOBB University of Economics and Technology, Ankara, Türkiye

Abstract—**Integrated sensing and communication (ISAC) has already established itself as a promising solution to the spectrum scarcity problem, even more so when paired with a reconfigurable intelligent surface (RIS), as RISs can shape the propagation environment by adjusting their phase-shift coefficients. Albeit the potential performance gain, a RIS is also a potential security threat to the system. In this paper, we explore both the positive and negative sides of having a RIS in a multi-user multiple-input multiple-output (MIMO) ISAC network. We first develop an alternating optimization algorithm, obtaining the active and passive beamforming vectors that maximize the sensing signal-to-noise ratio (SNR) under minimum signal-to-interference-plus-noise ratio (SINR) constraints for the communication users and finite power budget. We also investigate the destructive potential of the RIS by devising a RIS phase-shift optimization algorithm that minimizes the sensing SNR while preserving the same minimum ... system. V... element ... results sh... good as ... strategies**

Index T... failures

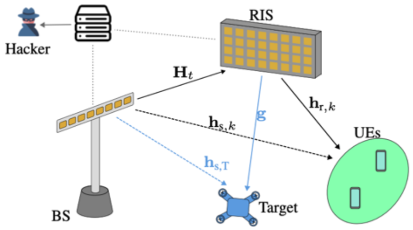


Fig. 1: A RIS-aided ISAC network where a hacker has hacked into the RIS's control circuit.

... as mali... tion and... possibl... r system... egitimat... erferenc... oise ont... to be a...

Premise: We use a BS array and RIS to

a) Communicate with users

b) Sense properties of a target

Constructive superposition:

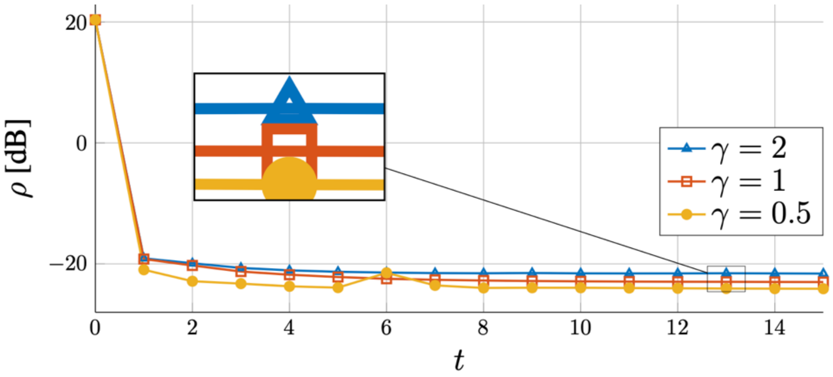
Maximize sensing SNR

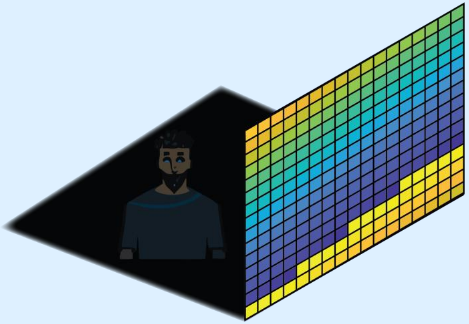
Deliver SINR γ to users

Destructive superposition:

Minimize sensing SNR instead

(Hide a trespasser)





Should We **Be Afraid** of **Uncontrolled** or **Malicious** Reconfigurable Surfaces?

Yes, we cannot add RIS into systems without defining rules for their use and adapting other algorithms to their existence

Yes, they can be used to turn off features or hide targets, while “flying under the radar”. The implementation must be secure.