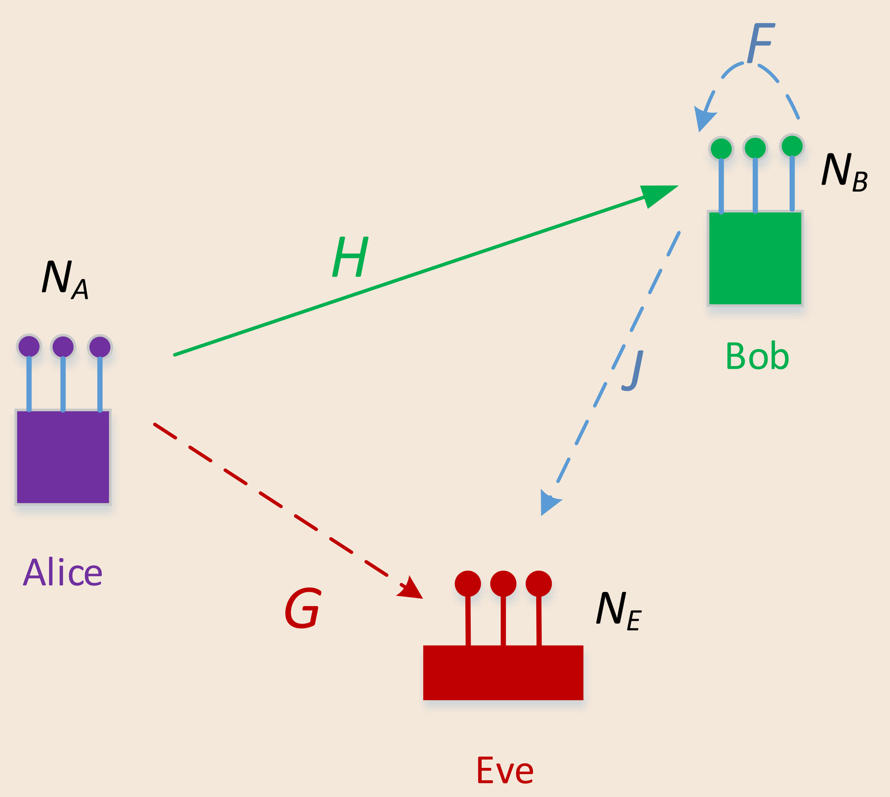
A MINORIZATION-MAXIMIZATION ALGORITHM FOR AN-BASED MIMOME SECRECY RATE MAXIMIZATION

Mudassir Masood (KFUPM), Ali Ghrayeb (TAMUQ), Prabhu Babu (IIT), Issa Khalil (QCRI), Mazen Hasna (QU)

1. What is this work about?

- ⋆ The problem of secrecy rate maximization in a multi-input multi-output multi-eavesdropper (MIMOME) wiretap channel is considered
- ⋆ An algorithm to achieve an exact solution is developed
- ⋆ Approach: Maximize achievable secrecy rate by performing joint-beamforming-and-artificial-noise optimization
- ⋆ Method: Develop a minorization-maximization algorithm to solve the difficult to optimize problem
- ⋆ The locally optimal solution allows us to benchmark existing methods

2. System Model



- ⋆ Alice, Bob and Eve are multi-antenna devices with N_A, N_B and N_E antennas respectively
- ⋆ Alice generates data ($\mathbf{s}$) and artificial noise ($\mathbf{z}$)
- ⋆ Bob is full-duplex - generates artificial noise ($\mathbf{w}$) while receiving data
- ⋆ Bob is equipped with self-interference cancellation (ρ)

$$\mathbf{x} = \mathbf{s} + \mathbf{z}$$
$$\mathbf{y}_{Bob} = \mathbf{H}\mathbf{x} + \sqrt{\rho}\mathbf{F}\mathbf{w} + \mathbf{n}_{Bob}$$
$$\mathbf{y}_{Eve} = \mathbf{G}\mathbf{x} + \mathbf{J}\mathbf{w} + \mathbf{n}_{Eve}$$
$$\mathbf{s} \sim \mathcal{CN}(\mathbf{0}, \mathbf{Q}), \mathbf{z} \sim \mathcal{CN}(\mathbf{0}, \mathbf{\Sigma}), \mathbf{w} \sim \mathcal{CN}(\mathbf{0}, \mathbf{W})$$

3. Secrecy Rate Maximization

We maximize the achievable secrecy rate as follows:

$$R_s^\star = \max_{\mathbf{Q},\mathbf{\Sigma},\mathbf{W}} \ \{C_b(\mathbf{Q},\mathbf{\Sigma},\mathbf{W}) - C_e(\mathbf{Q},\mathbf{\Sigma},\mathbf{W})\}$$
$$\text{s.t.} \quad \mathbf{Q} \succeq \mathbf{0}, \mathbf{\Sigma} \succeq \mathbf{0}, \mathbf{W} \succeq \mathbf{0},$$
$$\text{Tr}(\mathbf{Q}) \le P_s,\ \text{Tr}(\mathbf{\Sigma}) \le P_z,\ \text{Tr}(\mathbf{W}) \le P_b.$$

where

$C_b(\mathbf{Q},\mathbf{\Sigma},\mathbf{W}) \longleftarrow$ achievable rate at Bob

$C_e(\mathbf{Q},\mathbf{\Sigma},\mathbf{W}) \longleftarrow$ achievable rate at Eve

4. Minorization-Maximization Algorithm (MM)

- ⋆ In its original form, the secrecy rate maximization problem cannot be solved as it contains some convex terms.
- ⋆ We use MM to reformulate it into a sequence of simpler and easy to optimize cost (surrogate) functions.
- ⋆ These surrogate functions must minorize the original cost function at a given point to ensure tightness.
- ⋆ We use Lemma 1 to reformulate the secrecy rate maximization problem.

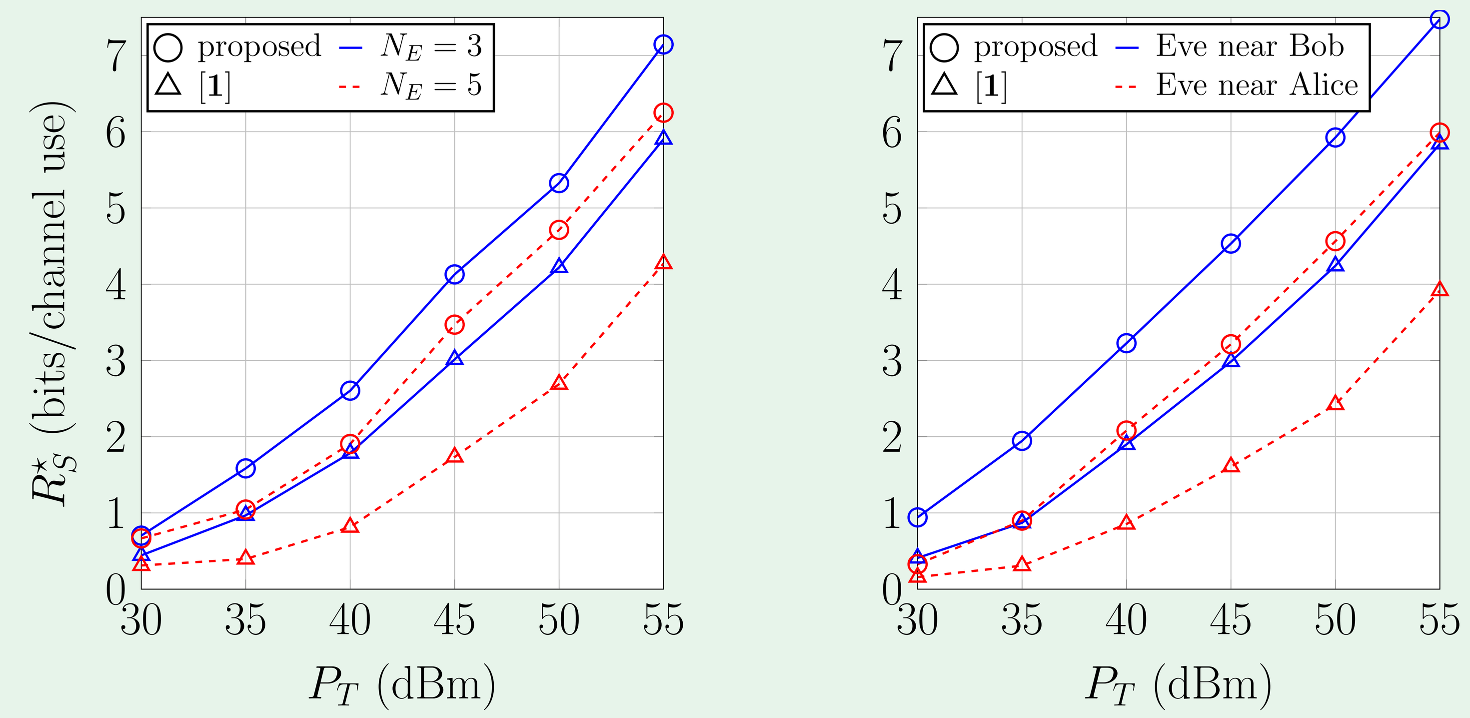
Lemma 1: For $f(\mathbf{X}) = -\log\det\mathbf{X}$, a function of square matrix $\mathbf{X}$, the minorizing function at $\mathbf{X} = \mathbf{X}_0$ is given by $\bar{f}(\mathbf{X},\mathbf{X}_0) = -\log\det\mathbf{X}_0 - \text{Tr}\left(\mathbf{X}_0^{-1}\mathbf{X}\right)$. Here $\bar{f}(\mathbf{X},\mathbf{X}_0)$ is the tangent plane of $f(\mathbf{X})$ which lower bounds it at $\mathbf{X} = \mathbf{X}_0$ while $\mathbf{X}_0^{-1}$ is the gradient of $\log\det\mathbf{X}$ evaluated at $\mathbf{X}_0$.

MM estimation of optimal $(\mathbf{Q}, \mathbf{\Sigma}, \mathbf{W})$

- ⋆ $k = 0$, Initialize $\mathbf{Q}^{(0)}, \mathbf{\Sigma}^{(0)}, \mathbf{W}^{(0)}$
- ⋆ **do**
  - $R_s^{(k)}$ = Solve reformulated problem using $\mathbf{Q}^{(k)}, \mathbf{\Sigma}^{(k)}, \mathbf{W}^{(k)}$
  - $k = k + 1$
  - $\mathbf{Q}^{(k)} = \mathbf{Q}^{(k-1)}$, $\mathbf{\Sigma}^{(k)} = \mathbf{\Sigma}^{(k-1)}$, $\mathbf{W}^{(k)} = \mathbf{W}^{(k-1)}$
- ⋆ **until** convergence
- ⋆ $\mathbf{Q}^\star = \mathbf{Q}^{(k)}$, $\mathbf{\Sigma}^\star = \mathbf{\Sigma}^{(k)}$, $\mathbf{W}^\star = \mathbf{W}^{(k)}$
- ⋆ Calculate secrecy rate $R_s^\star$ using $(\mathbf{Q}^\star, \mathbf{\Sigma}^\star, \mathbf{W}^\star)$

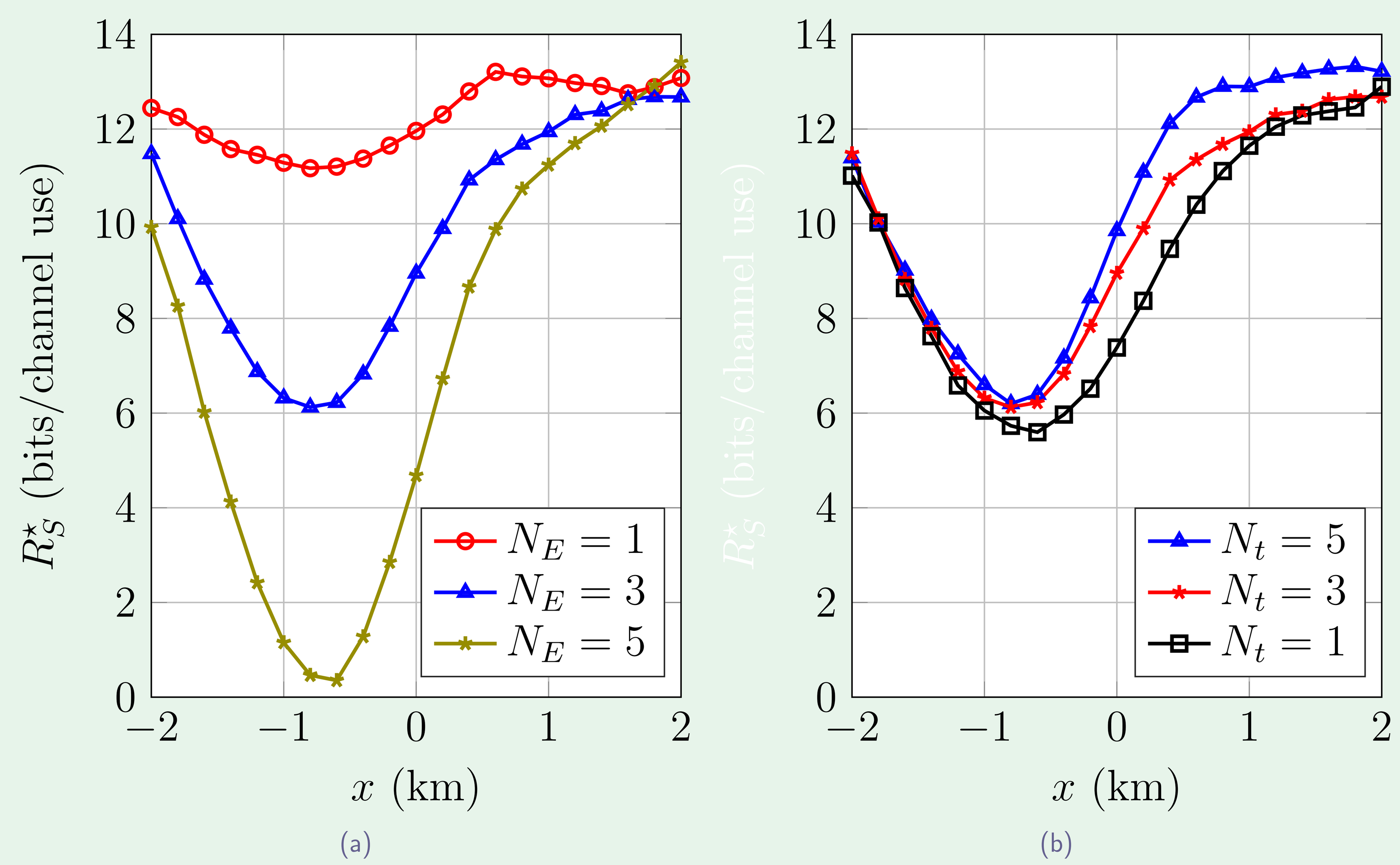
5. Experiments

Setup 1: No noise from Alice - effect of different system parameters



Effect of (a) N_E and (b) Eve's location, on $R_s^\star$

Setup 2: Alice and Bob are located one kilometer apart at (-0.5,0) and (0.5,0) respectively and Eve moves along the line $y = 0.5$ from (-2.0,0.5) to (2.0,0.5).



Variations in $R_s^\star$ as Eve moves on a line for various configurations of (a) N_E and (b) N_t, $P_z = 0, P_s = P_T$.

7. References

[1] G. Zheng, I. Krikidis, J. Li, A. Petropulu, and B. Ottersten, "Improving physical layer secrecy using full-duplex jamming receivers," *IEEE Trans. Sig. Proc.*, vol. 61, pp. 49624974, 2013.
[2] M. Masood, A. Ghrayeb, P. Babu, I. Khalil, and M. Hasna, "A Minorization-Maximization Algorithm for Maximizing the Secrecy Rate of the MIMOME Wiretap Channel," *IEEE Comm. Lett.*, 2017.

8. Acknowledgement

This work was made possible by NPRP grant NPRP 8-052-2-029 from the Qatar National Research Fund (a member of Qatar Foundation).

email: mudassir@kfupm.edu.sa, ali.ghrayeb@qatar.tamu.edu, prabhubabu@care.iitd.ernet.in, ikhalil@qf.org.qa, hasna@qu.edu.qa