Guaranteeing Secrecy using Artificial Noise

Emmanuel Obeng Frimpong

Intelligent Communication and Information Security Lab

8th December 2021

HANBAT NATIONAL UNIVERSITY

CONTENTS

- **Introduction**
- **System Model**
- **Simulation Results**

Introduction

- Consider the problem of secret communication from the transmitter to the receiver, over a wireless medium, where a passive eavesdropper may be present.

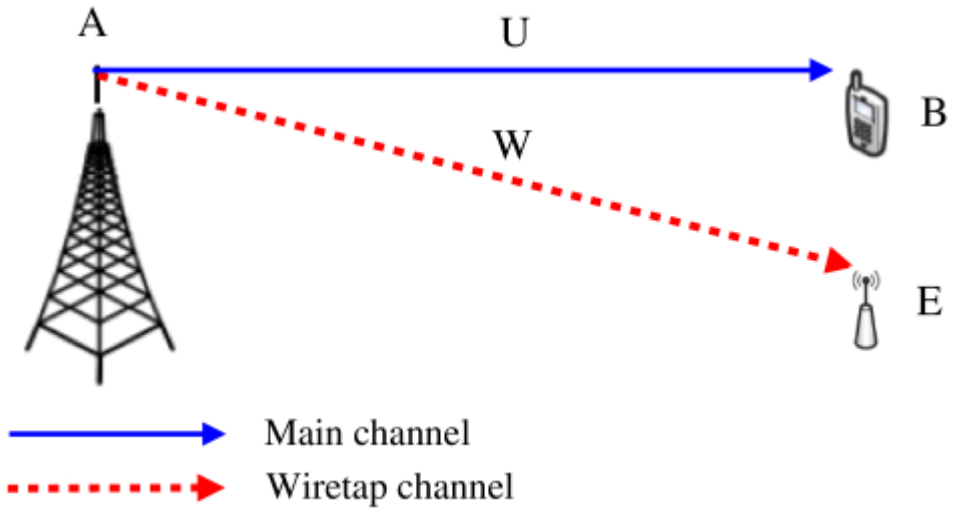


Figure 1

Any scheme that guarantees secrecy in such a scenario must do so regardless of the eavesdropper position.

Introduction

- Claude Shannon showed that perfect secrecy is achievable only if the secret key is at least as large as the secret message. He assumed that the eavesdropper has access to precisely the same information as the receiver, except the secret key.
- Other authors considered a scenario where the receiver and the eavesdropper have separate channels and showed that secret communication is possible if the eavesdropper's channel has a smaller capacity than the receiver's channel.

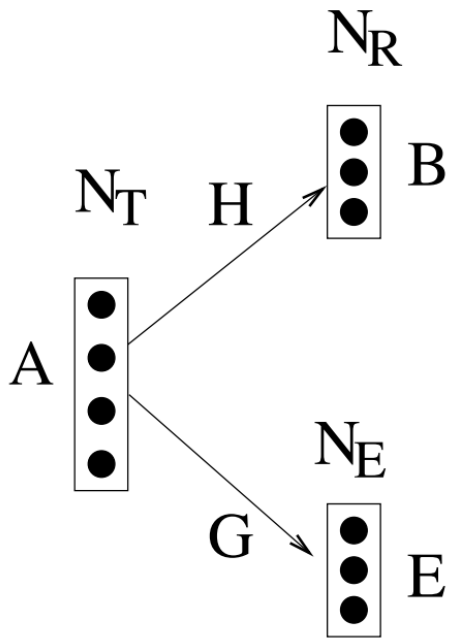
Introduction

- This paper presents a solution to this problem, where the transmitter can use some of the available power to transmit artificially generated noise.
- Since, this noise is generated by the transmitter, the transmitter can design it such that only the eavesdropper's channel is degraded.
- Thus, by selectively degrading the eavesdropper's channel, secret communication can be guaranteed.

System Model Discussion

- Authors consider two scenarios, which demonstrate different methods of generating artificial noise.
- Scenario 1: Multiple antennas
- Scenario 2: Multiple Amplifying relays
- The key idea is that a transmitter, perhaps in cooperation with the amplifying relays, can generate noise artificially to conceal the secret message that it is transmitting.

Scenario 1: Multiple antennas



(a) Scenario 1

If A transmits x_k at time k. B and E receive, respectively;

$$\boldsymbol{z}_k = \boldsymbol{H}_k x_k + \boldsymbol{n}_k$$

$$\boldsymbol{y}_k = \boldsymbol{G}_k x_k + \boldsymbol{e}_k$$

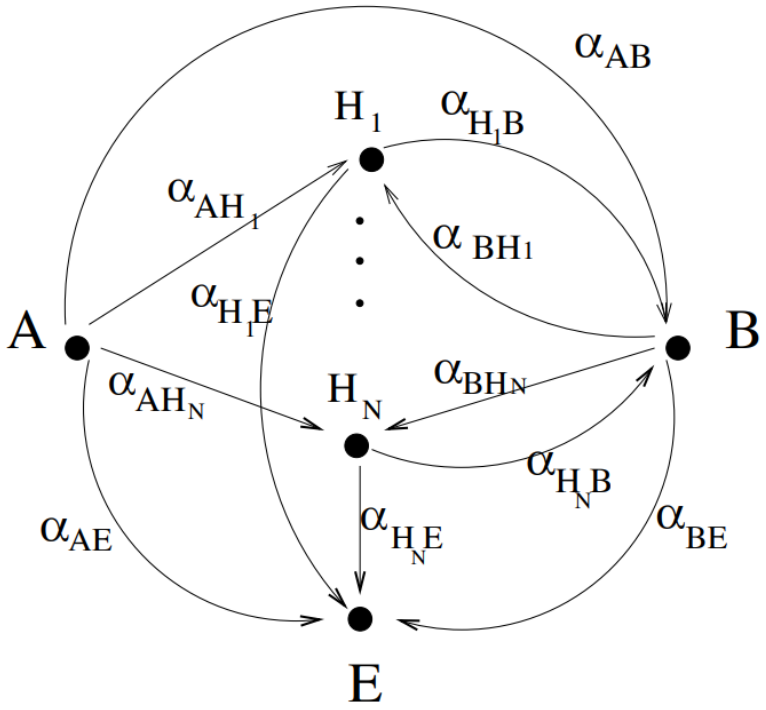
It is assumed that the receiver can estimate its channel $\boldsymbol{H}_k$ perfectly and feed it back to the transmitter noiselessly.

It is also assumed that the eavesdropper may know both the receiver's and its own channel.

$\boldsymbol{G}_k$ may not be known to the transmitter.

The secrecy of this scheme is not dependent on the secrecy of channel gains.

Scenario 2: Multiple Amplifying relays



(b) Scenario 2

- This scenario considers the case where the transmitter does not have multiple transmit antennas, but instead, has amplifying relays for cooperation.
- The channel gain from X to Y is denoted α_{XY}.
- Note that the channels are not necessarily reciprocal, i.e., in general $\alpha_{XY} \neq \alpha_{YX}$
- It is assumed that all the channel gains are known to all the nodes (possibly, even to the eavesdropper).

Artificial Noise Using Transmit Antennas

- Assume that both the receiver and the eavesdropper have a single antenna
- The artificial noise is produced such that it lies in the null space of the receiver's channel.
- Information signal is transmitted in the range space of the receiver's channel.
- The transmitter chooses $\boldsymbol{x}_k$ as the sum of information bearing signal s_k and the artificial noise signal $\boldsymbol{w}_k$;
  - $\boldsymbol{x}_k = \boldsymbol{s}_k + \boldsymbol{w}_k$
- Then, the signals received by the receiver and the eavesdropper are given by, respectively,
  - $z_k = \boldsymbol{H}_k \boldsymbol{s}_k + n_k$
  - $y_k = \boldsymbol{G}_k \boldsymbol{s}_k + \boldsymbol{G}_k \boldsymbol{w}_k + e_k$

Artificial Noise Using Transmit Antennas

- Transmitter chooses the information bearing signal as $\boldsymbol{s}_k = \boldsymbol{p}_k u_k$, where u_k is the information signal.
- Secrecy capacity is bounded below by :
  - $Secrecy\ Capacity \geq\ C_{sec}^{a} = I(Z;U) - I(Y;U)$
  - $= \log\left(1 + \frac{|\boldsymbol{H}_k \boldsymbol{p}_k|^2 \sigma_u^2}{\sigma_n^2}\right) - \log\left(1 + \frac{|\boldsymbol{G}_k \boldsymbol{p}_k|^2 \sigma_u^2}{\boldsymbol{E}|\boldsymbol{G}_k \boldsymbol{w}_k|^2 + \sigma_e^2}\right)$
- We assume that the total transmit power $f_1(\sigma_u^2, \sigma_v^2)$ is constraint to P_0.
- σ_u^2, σ_v^2 is chosen to maximize the lower bound on average secrecy capacity
  - $\overline{C_{sec}^{a}} = \max_{f_1(\sigma_u^2, \sigma_v^2) \leq P_0} \mathbf{E}_{\boldsymbol{H}_k, \boldsymbol{G}_k} [C_{sec}^{a}]$

Artificial Noise Using Transmit Antennas

- We study variation of $\overline{C_{sec}^{a}}$ with the eavesdropper's distance from the transmitter.
- The distance can be modeled as position dependent noise power σ_e^2 , instead of position dependent channel gains. The worst-case situation would occur if σ_e^2 approaches *0*.
- The minimum secrecy capacity that can be guaranteed, irrespective of the eavesdropper's position is given by

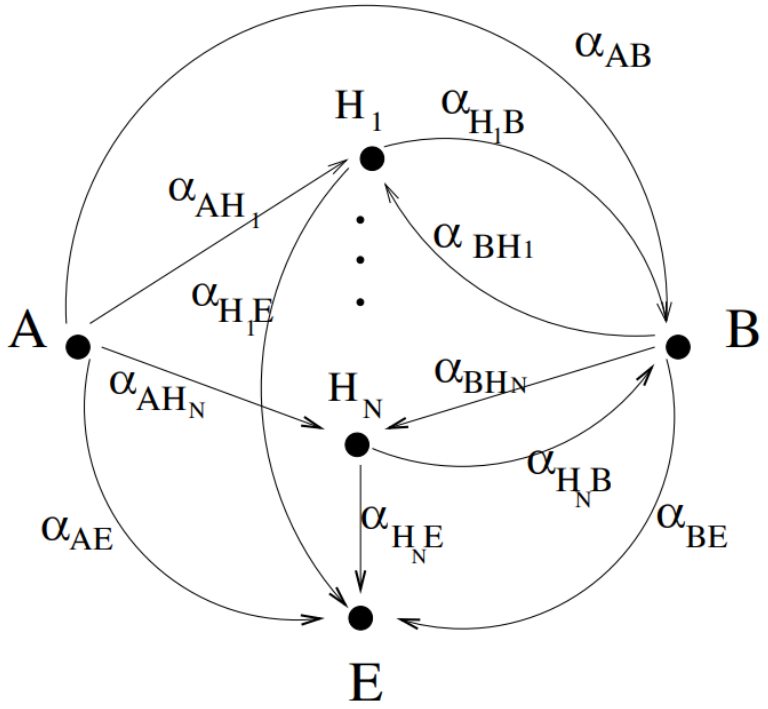
$$\overline{C_{sec}^{a}} \geq \overline{C_{sec,mg}^{a}} = \max_{f_1(\sigma_u^2,\sigma_v^2) \leq P_0} \mathbf{E}_{\boldsymbol{H}_k,\boldsymbol{G}_k} \log\left(1+\frac{|\boldsymbol{H}_k\boldsymbol{p}_k|^2\sigma_u^2}{\sigma_n^2}\right) - \log\left(1+\frac{|\boldsymbol{G}_k\boldsymbol{p}_k|^2\sigma_u^2}{\boldsymbol{E}|\boldsymbol{G}_k\boldsymbol{w}_k|^2}\right)$$

Artificial Noise Using Relays

- A novel 2-stage protocol that achieves this coordination amongst relays.
- In the first stage, the transmitter and the receiver both transmit independent artificial noise signals to the relays. The relays and the eavesdropper receive different linear combinations of these two signals.
- In the second stage, the relays simply replay a weighted version of the received signal, using a publicly available sequence of weights.
- At the same time, in this second stage, the transmitter transmits its secret message, along with a weighted version of its artificial noise, which was transmitted in the first stage.

Artificial Noise Using Relays

- Stage 1: A and B transmit $\alpha_{AB}x$ and y, respectively. H_i and E receive respectively,
  - $r_{H_i} = \alpha_{AH_i}\alpha_{AB}x + \alpha_{BH_i}y + n_i$
  - $r_{E,1} = \alpha_{AE}\alpha_{AB}x + \alpha_{BE}y + e_1$
- Stage 2: A and H_i transmit $-\sum_i \beta_i \alpha_{AH_i}\alpha_{BH_i}x + z$
- and $\beta_i r_{H_i}$ respectively.
- $r_B = \alpha_{AB}z + \sum_i \beta_i \alpha_{H_iB}(\alpha_{BH_i}y + n_i) + n_o$
- $r_{E,2} = \alpha_{AE}z + \sum_i \beta_i\alpha_{AH_i}(\alpha_{AB}\,\alpha_{H_iE} - \alpha_{AE}\alpha_{H_iB})x + \beta_i\alpha_{BH_i}\alpha_{H_iE}y + \beta_i\alpha_{H_iE}n_i + e_2$



(b) Scenario 2

Artificial Noise Using Relays

- Simplifying:
- The equivalent channel from A to B is given by
  - ✓$r_B = \alpha_{AB} z + n_B$
  - ✓Where $n_B = \sum_i \beta_i \alpha_{H_i B} \left(\alpha_{B H_i} y + n_i \right) + n_o$
- The channel from A to E can be written as

$$\mathbf{r}_E = \mathbf{h}_z z + \mathbf{H}_{xy} \begin{pmatrix} x \\ y \end{pmatrix} + \mathbf{n},$$

$$\mathbf{h}_z = \begin{pmatrix} 0 \\ \alpha_{AE} \end{pmatrix}, \mathbf{n} = \begin{pmatrix} e_1 \\ \sum_{i=1}^{N_H} \beta_i \; \alpha_{H_i E} \; n_i + e_2 \end{pmatrix},$$

$$\mathbf{H}_{xy} = \begin{pmatrix} \alpha_{AB} \; \alpha_{AE} & \alpha_{BE} \\ \gamma & \sum_{i=1}^{N_H} \beta_i \alpha_{B H_i} \; \alpha_{H_i E} \end{pmatrix},$$

where $\gamma = \alpha_{AB} \sum_{i=1}^{N_H} \beta_i \quad \alpha_{A H_i} \quad \alpha_{H_i E} \; - \; \alpha_{AE} \sum_{i=1}^{N_H} \beta_i \alpha_{A H_i} \alpha_{H_i B}.$

Artificial Noise Using Relays

- Capacity is given by:

$$C = \log|\mathbf{h}_z\mathbf{h}_z^{\dagger}\sigma_z^2 + \mathbf{K}| - \log|\mathbf{K}|$$

$$\mathbf{K} = \begin{pmatrix} |h_{11}|^2\sigma_x^2 + |h_{12}|^2\sigma_y^2 + \sigma_e^2 & 0 \\ 0 & \eta \end{pmatrix}$$

where h_{11}, h_{12}, h_{21}, h_{22} are the elements of $\mathbf{H}_{xy}$, and $\eta = |h_{21}|^2\sigma_x^2 + |h_{22}|^2\sigma_y^2 + \sum_{i=1}^{N_H}(|\alpha_{H_iE}|^2\sigma_{\beta_i}^2)\sigma_n^2 + \sigma_e^2$

- The lower bound on secrecy capacity is given by,

$$C_{sec}^h = I(Z;\tilde{R}_B) - I(Z;R_{E,1},R_{E,2})$$
$$= \log(1 + |\alpha_{AB}|^2\sigma_z^2/\sigma_{n_B}^2) - \log|\mathbf{h}_z\mathbf{h}_z^{\dagger}\sigma_z^2 + \mathbf{K}|/|\mathbf{K}|$$

where $\sigma_{n_B}^2 = \sum_{i=1}^{N_H}(|\alpha_{H_iB}|^2\sigma_{\beta_i}^2)\sigma_n^2 + \sigma_e^2$

Artificial Noise Using Relays

- The total power, transmitted by all nodes, in the two stages, is $f_2(\sigma_x^2, \sigma_y^2, \sigma_z^2, \sigma_{\beta_i}^2)$ and constrained by P_0. Let $\sigma_{\beta_i}^2 = \xi \ \forall i$.
- The combination of powers $(\sigma_x^2, \sigma_y^2, \sigma_z^2, \xi)$ is chosen to maximize the average C_{sec}^h:

$$\overline{C_{sec}^h} \doteq \max_{f_2(\sigma_x^2,\sigma_y^2,\sigma_z^2,\xi)\leq P_0} \mathbf{E}[\log(1+|\alpha_{AB}|^2\sigma_z^2/\sigma_{n_B}^2) - \log|\mathbf{h}_z\mathbf{h}_z^\dagger\sigma_z^2+\mathbf{K}|/|\mathbf{K}|]$$

Numerical Results

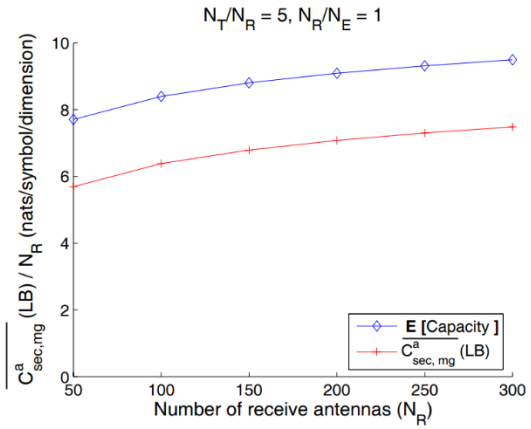


Fig. 2. $\overline{C^a_{sec,mg}}$: variation with N_R (N_T/N_R fixed).

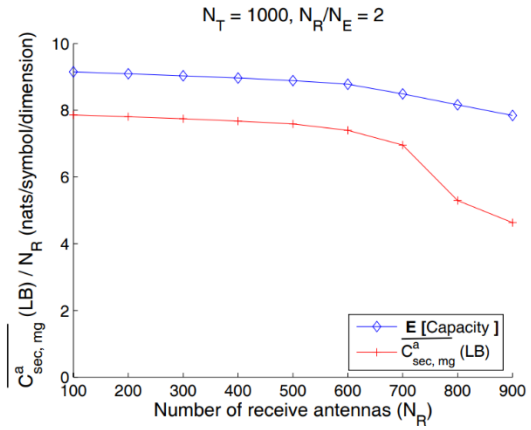


Fig. 3. $\overline{C^a_{sec,mg}}$: variation with N_R (N_T fixed).

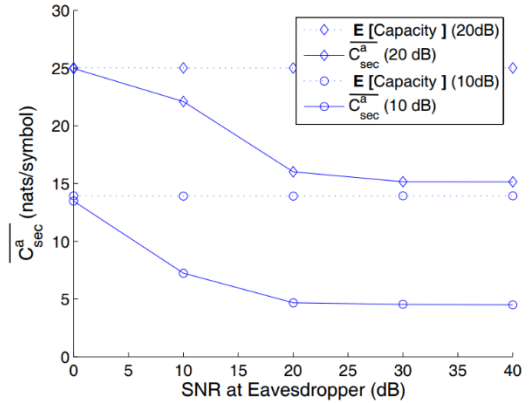


Fig. 4. $\overline{C^a_{sec,mg}}$: variation with distance.

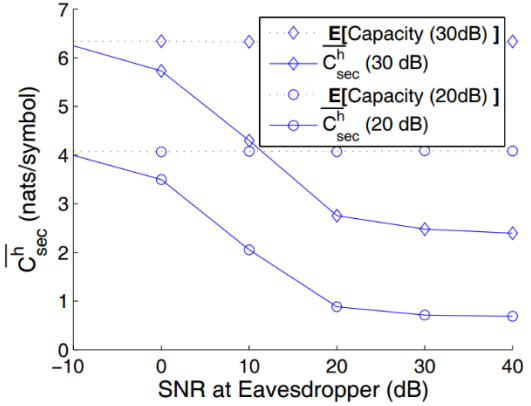


Fig. 5. $\overline{C^h_{sec,mg}}$: variation with distance.

Numerical Results

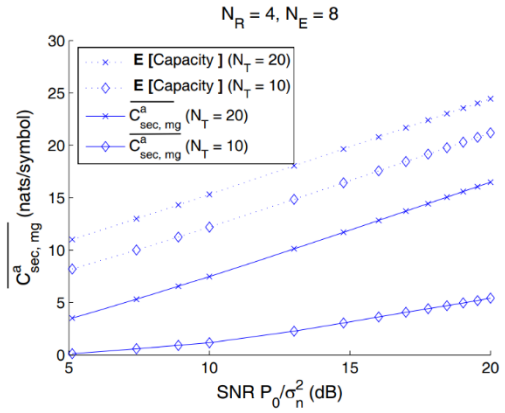


Fig. 6. $\overline{C^a_{sec,mg}}$: variation with P_0.

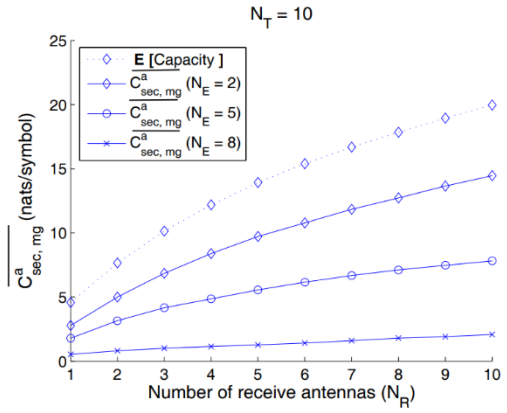


Fig. 8. $\overline{C^a_{sec,mg}}$: variation with N_E and N_R.

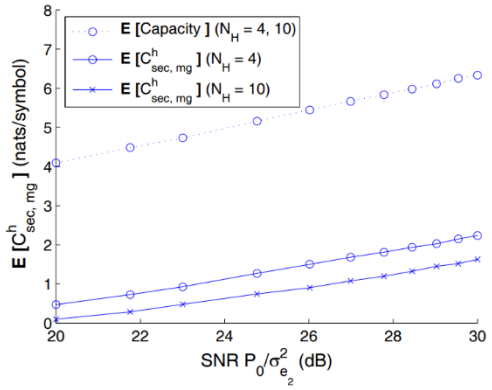


Fig. 7. $\overline{C^h_{sec,mg}}$: variation with P_0.

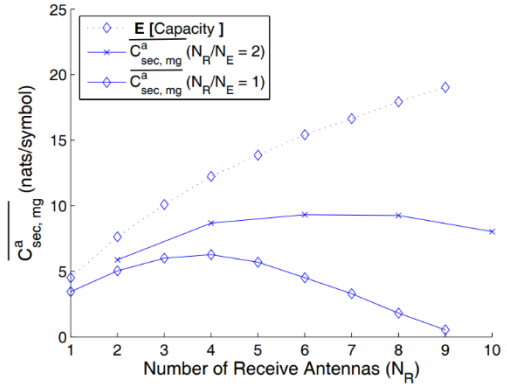
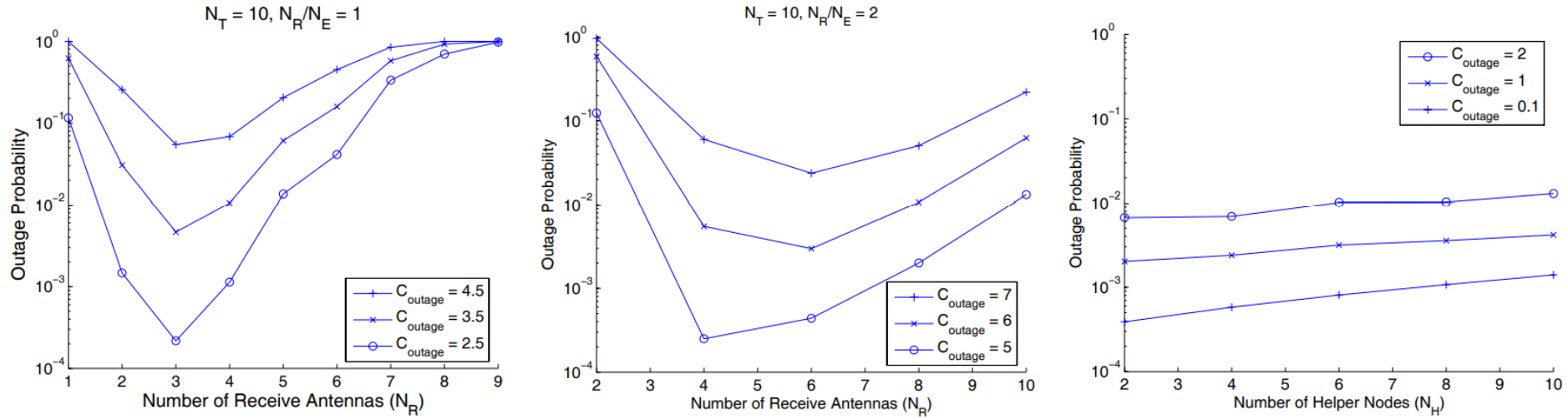


Fig. 9. $\overline{C^a_{sec,mg}}$: fixed ratio of N_E and N_R.

Numerical Results



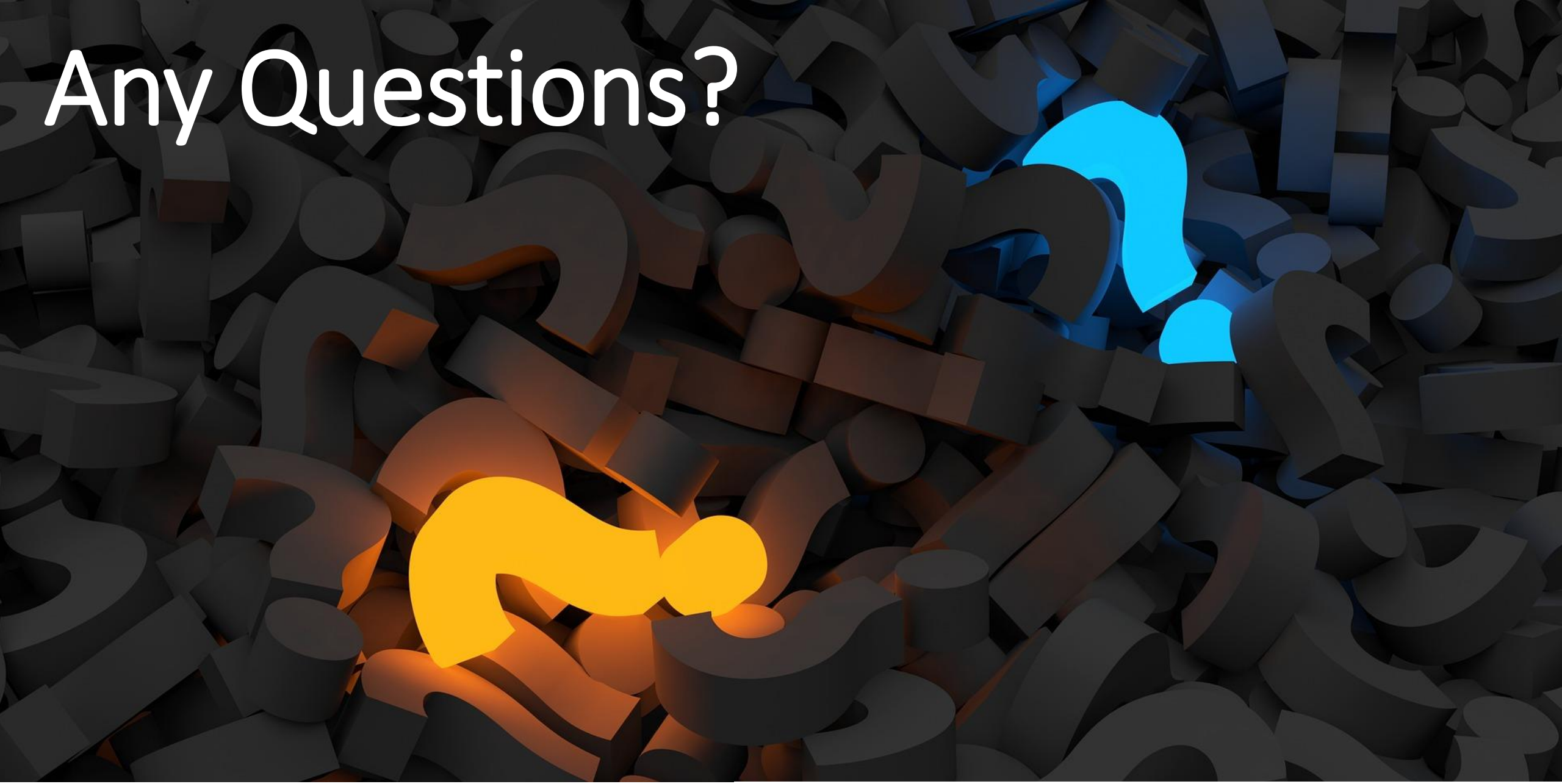
(a) Multiple antenna scenario ($N_R = N_E$) (b) Multiple antenna scenario ($N_R = 2N_E$) (c) Multiple relays scenario

Fig. 10. Outage Probability

REFERENCES

- Figure 1: https://deepai.org/publication/survey-on-physical-layer-security-for-5g-wireless-networks

Any Questions?



HANBAT NATIONAL UNIVERSITY

E-mail: frimpongemmanuelobeng@gmail.com