Physical Layer Security over Wireless Channels

Xiangyun (Sean) Zhou

UNIK - University Graduate Center
The University of Oslo, Norway

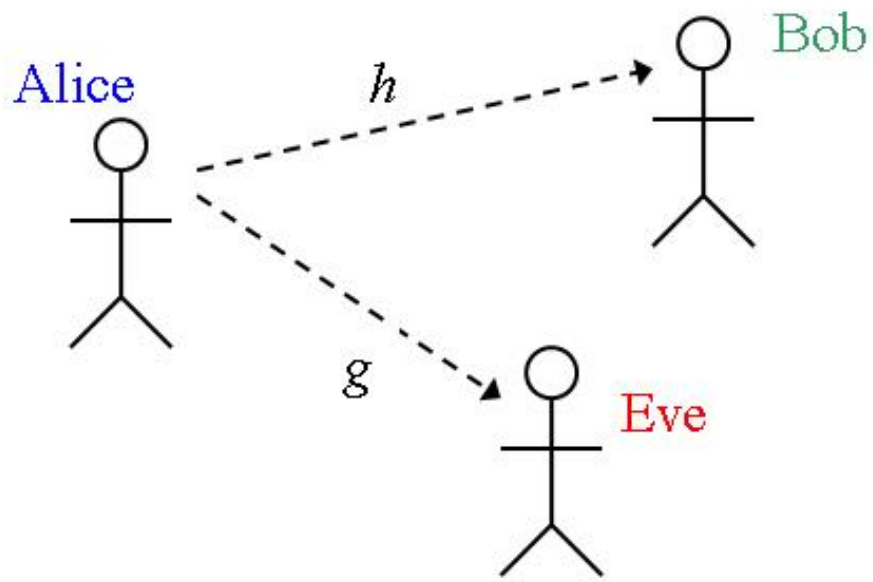
Research Collaborator: Prof. Matt McKay
Hong Kong University of Science and Technology, Hong Kong

26 August 2010

Outline

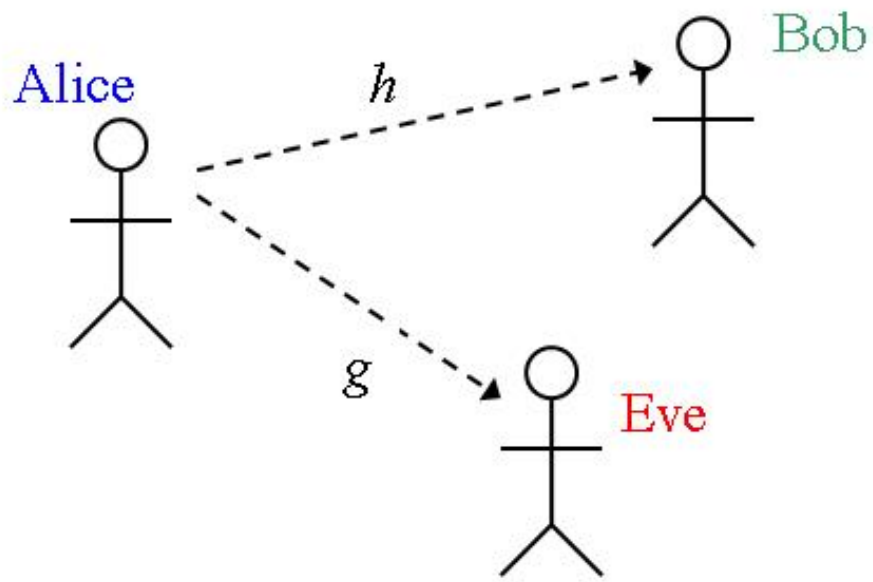
- Introduction to physical-layer security or information theoretic security.
- An example of using artificial noise to guarantee secrecy.

System Model



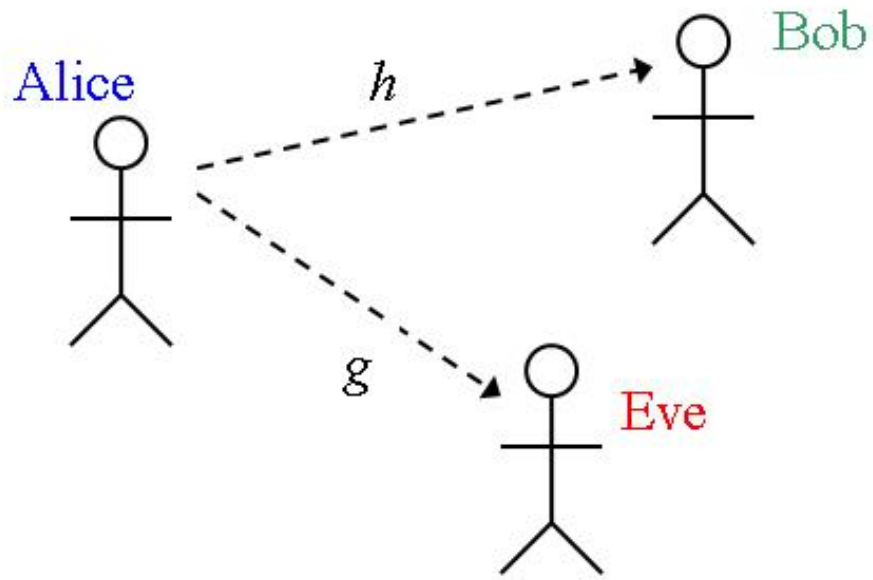
- Alice sends confidential information $\mathbf{x}$ to Bob.
- $y_B = \mathbf{h}\,\mathbf{x} + n_B$ is the received signal at Bob.
- $y_E = \mathbf{g}\,\mathbf{x} + n_E$ is the received signal at Eve.

System Model



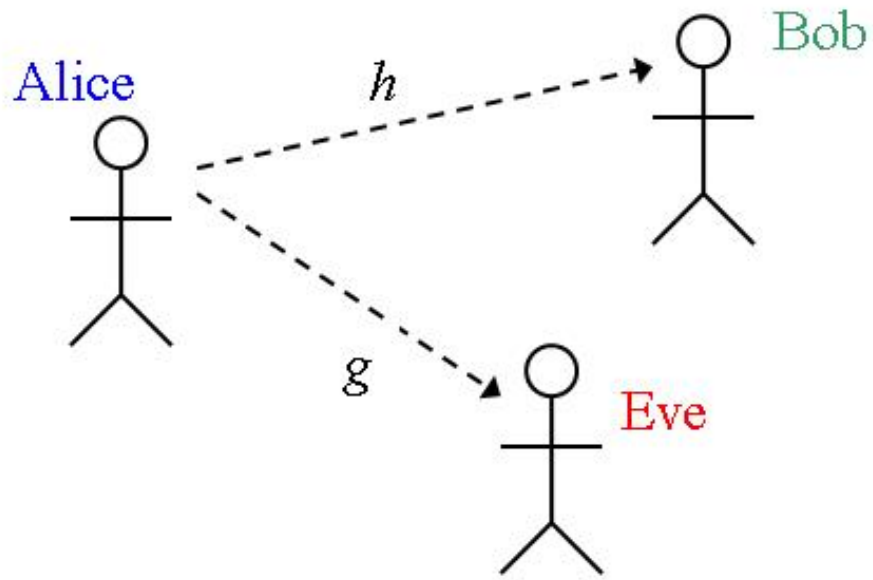
- Alice sends confidential information $\mathbf{x}$ to Bob.
- $y_B = \mathbf{h}\,\mathbf{x} + n_B$ is the received signal at Bob.
- $y_E = \mathbf{g}\,\mathbf{x} + n_E$ is the received signal at Eve.
- What is the maximum data rate for perfect secrecy without secret key?

Secrecy Capacity



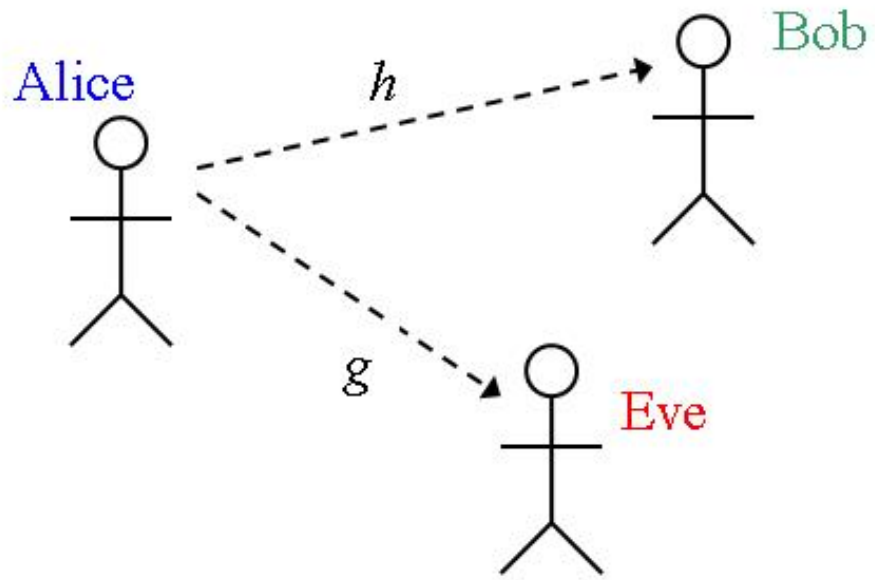
- $C(\mathbf{h})$ is the amount of information that can be transferred from Alice to Bob.
- $C(\mathbf{g})$ is the amount of information that can be transferred from Alice to Eve.

Secrecy Capacity



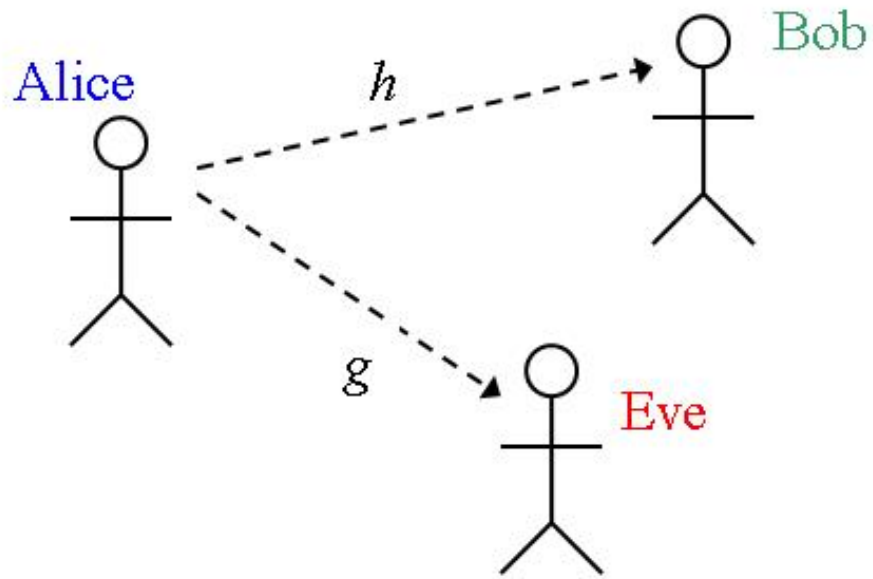
- $C(\mathbf{h})$ is the amount of information that can be transferred from Alice to Bob.
- $C(\mathbf{g})$ is the amount of information that can be transferred from Alice to Eve.
- Secrecy capacity: $C(\mathbf{h}) - C(\mathbf{g})$.
- Encoding scheme: Binning, requires knowledge of $\mathbf{h}$ and $\mathbf{g}$.

Type of Wireless Channel



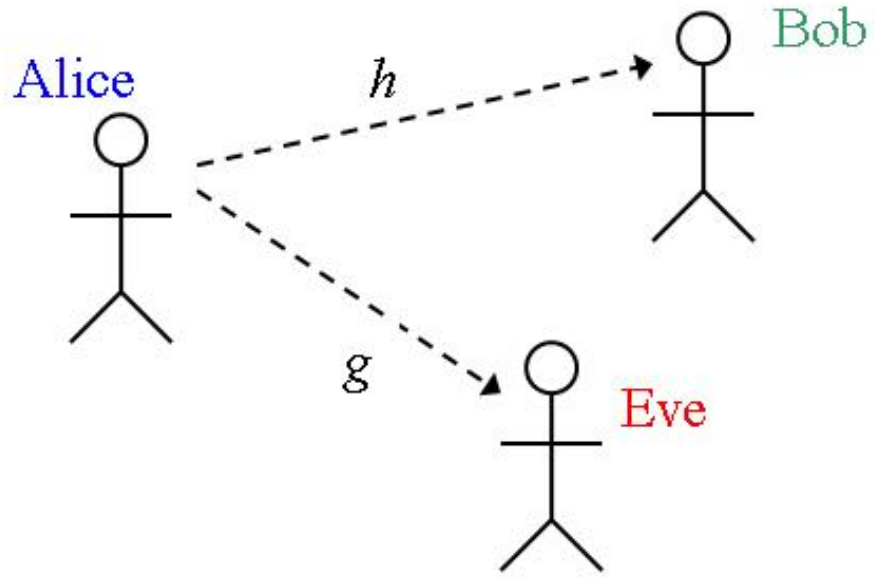
- Path loss channel: **h** and **g** are constant, e.g. line-of-sight.
- Fading channel: **h** and **g** are random, e.g. lots of scatterers and obstacles.

Type of Wireless Channel



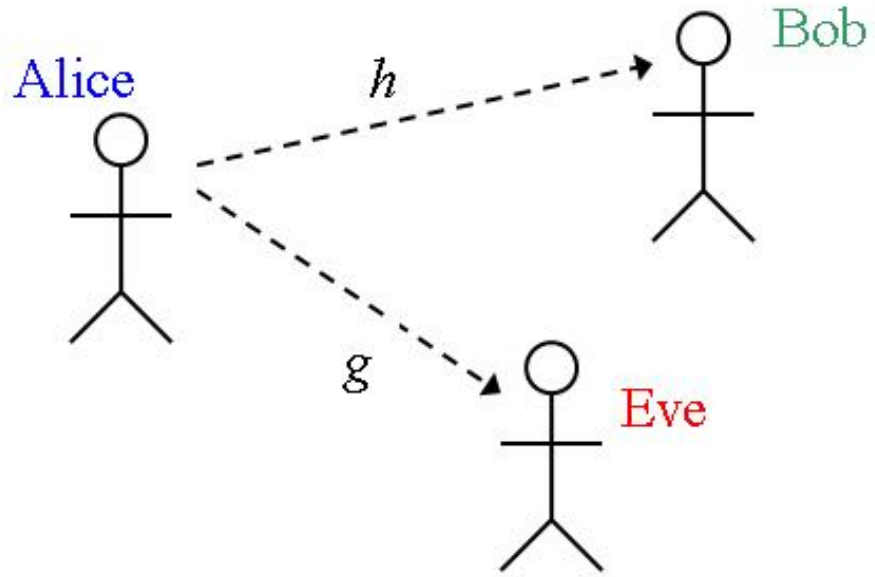
- Path loss channel: **h** and **g** are constant, e.g. line-of-sight.
- Fading channel: **h** and **g** are random, e.g. lots of scatterers and obstacles.
- Secret communication is possible if **h** is stronger than **g**: $C(\mathbf{h}) - C(\mathbf{g}) > 0$.
- The encoding requires knowledge of **h** and **g**.

Ergodic Secrecy Capacity for Fading Channels



What shall we do if we do not know the fading channel $\mathbf{g}$?

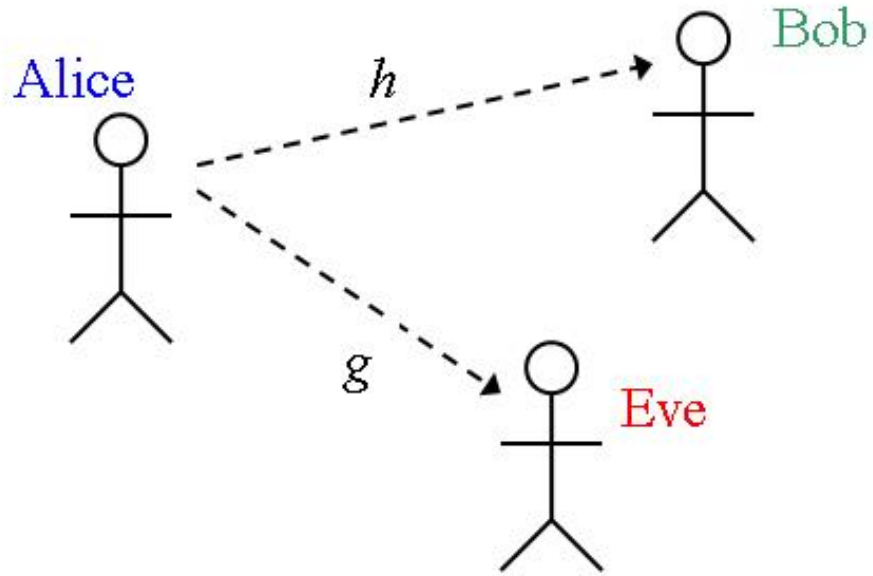
Ergodic Secrecy Capacity for Fading Channels



What shall we do if we do not know the fading channel $\mathbf{g}$?

- Instead of instantaneous secrecy capacity $C(\mathbf{h}) - C(\mathbf{g})$, we consider the ergodic secrecy capacity $\mathbb{E}_{\mathbf{h},\mathbf{g}}\{C(\mathbf{h}) - C(\mathbf{g})\}$.
- Note that it is easy for Alice to know $\mathbf{h}$.

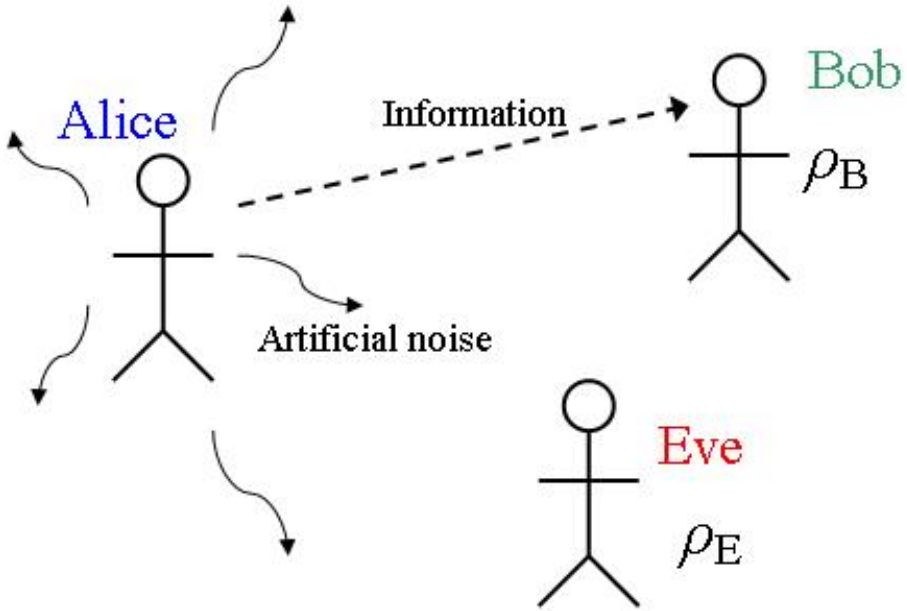
Ergodic Secrecy Capacity for Fading Channels



What shall we do if we do not know the fading channel $\mathbf{g}$?

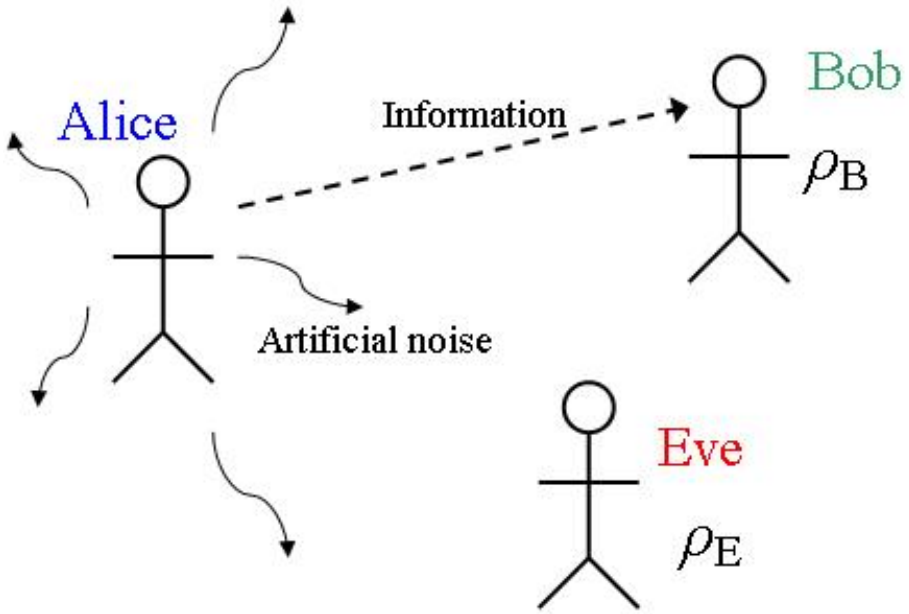
- Instead of instantaneous secrecy capacity $C(\mathbf{h}) - C(\mathbf{g})$, we consider the ergodic secrecy capacity $\mathbb{E}_{\mathbf{h},\mathbf{g}}\{C(\mathbf{h}) - C(\mathbf{g})\}$.
- Note that it is easy for Alice to know $\mathbf{h}$.
- How to simultaneously make $C(\mathbf{h})$ as large as possible and $C(\mathbf{g})$ as small as possible with the knowledge of $\mathbf{h}$ but not $\mathbf{g}$?

The Use of Artificial Noise



- Alice transmits useful information to Bob, at the same time producing artificial noise to confuse Eve.
- Specifically, the artificial noise is mapped onto the subspace orthogonal to **h**.
- Note that Alice needs multiple antennas.

The Optimization Problem: Power Allocation

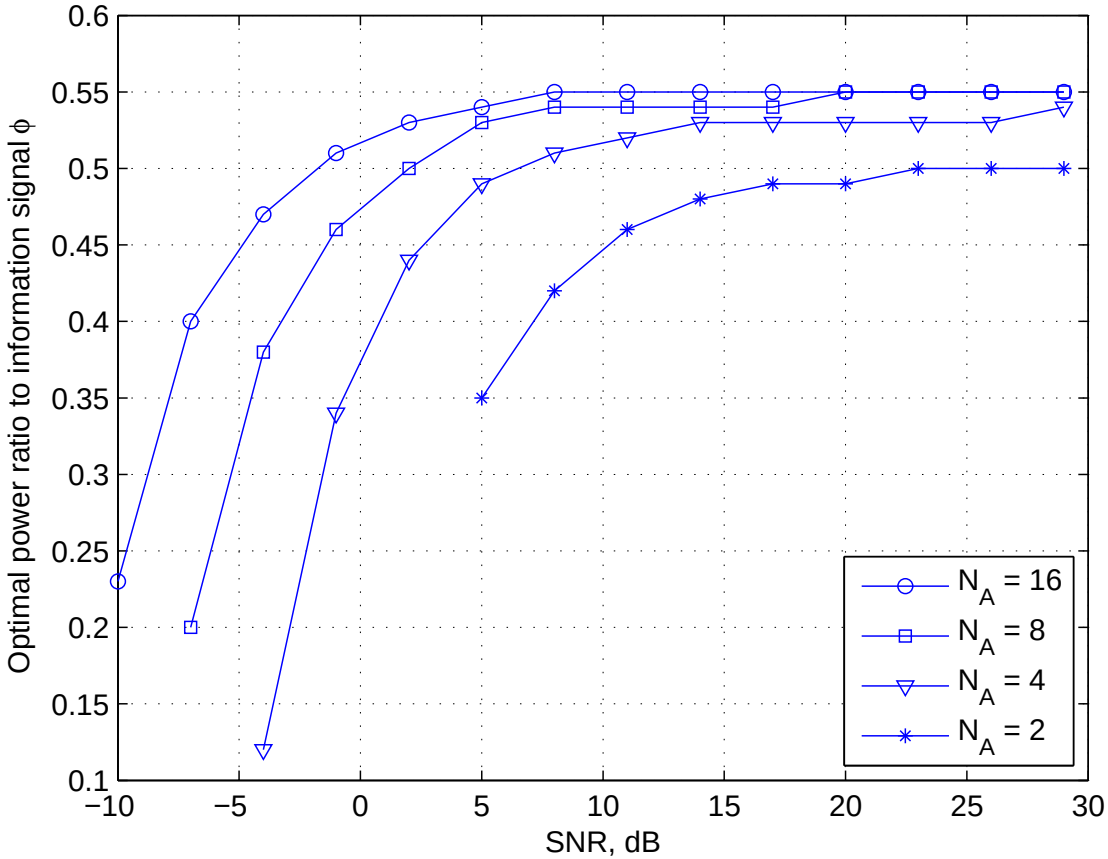


With a total transmit power constraint, what is the optimal power split between transmissions of information and artificial noise?

Power Allocation Parameters

- Alice has a total amount of transmit power budget P.
- A portion, denoted by ϕ, of P is allocated for information transmission.
- What is the optimal value of ϕ that maximizes the ergodic secrecy capacity $\mathbb{E}_{\mathbf{h},\mathbf{g}}\{C(\mathbf{h}) - C(\mathbf{g})\}$?
- How does the optimal value of ϕ changes with the number of antennas at Alice N_A?

Result: Optimal Power Allocation

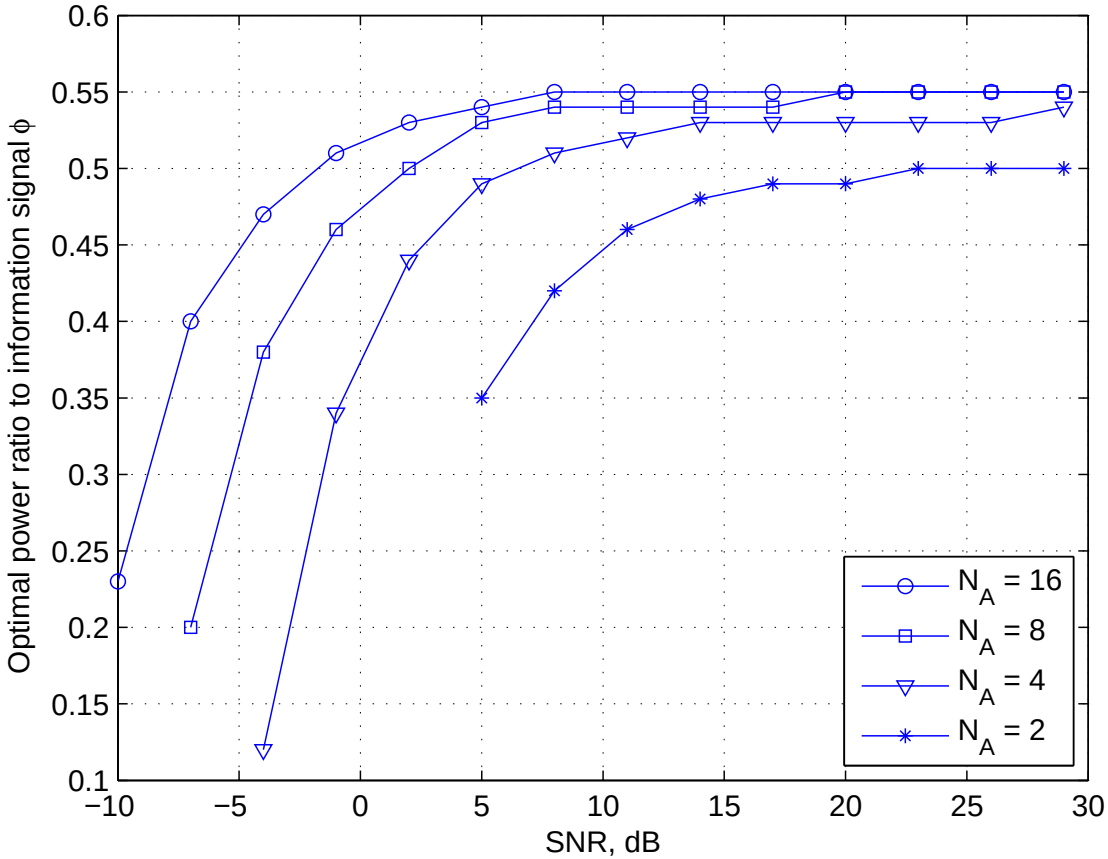


x-axis: power budget P. y-axis: optimal value of ϕ.

N_A: number of antennas at Alice.

- As P increases, more power should be allocated to information transmission.

Result: Optimal Power Allocation

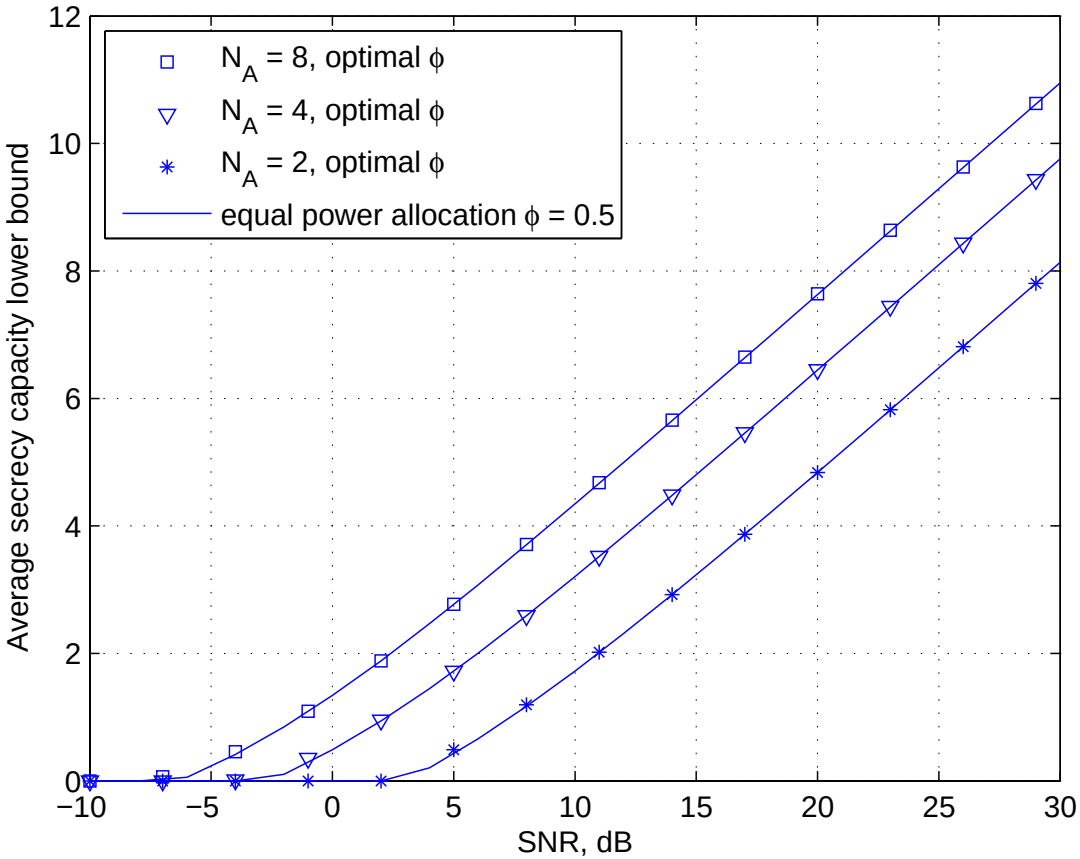


x-axis: power budget P. y-axis: optimal value of ϕ.

N_A: number of antennas at Alice.

- As N_A increases, more power should be allocated to information transmission.

Result: Ergodic Secrecy Capacity



x-axis: power budget P.

y-axis: secrecy capacity $\mathbb{E}_{\mathbf{h},\mathbf{g}}\{C(\mathbf{h}) - C(\mathbf{g})\}$.

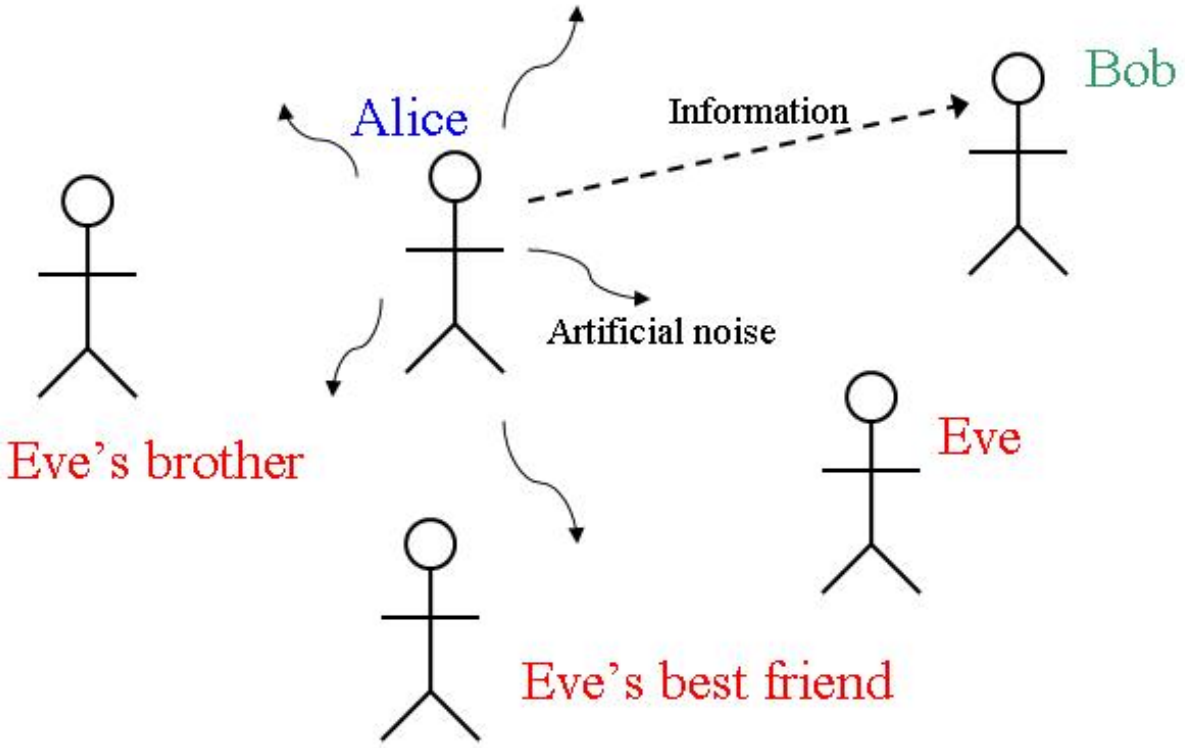
N_A: number of antennas at Alice.

- Equal power allocation works pretty well in all scenarios.

Extended Problems

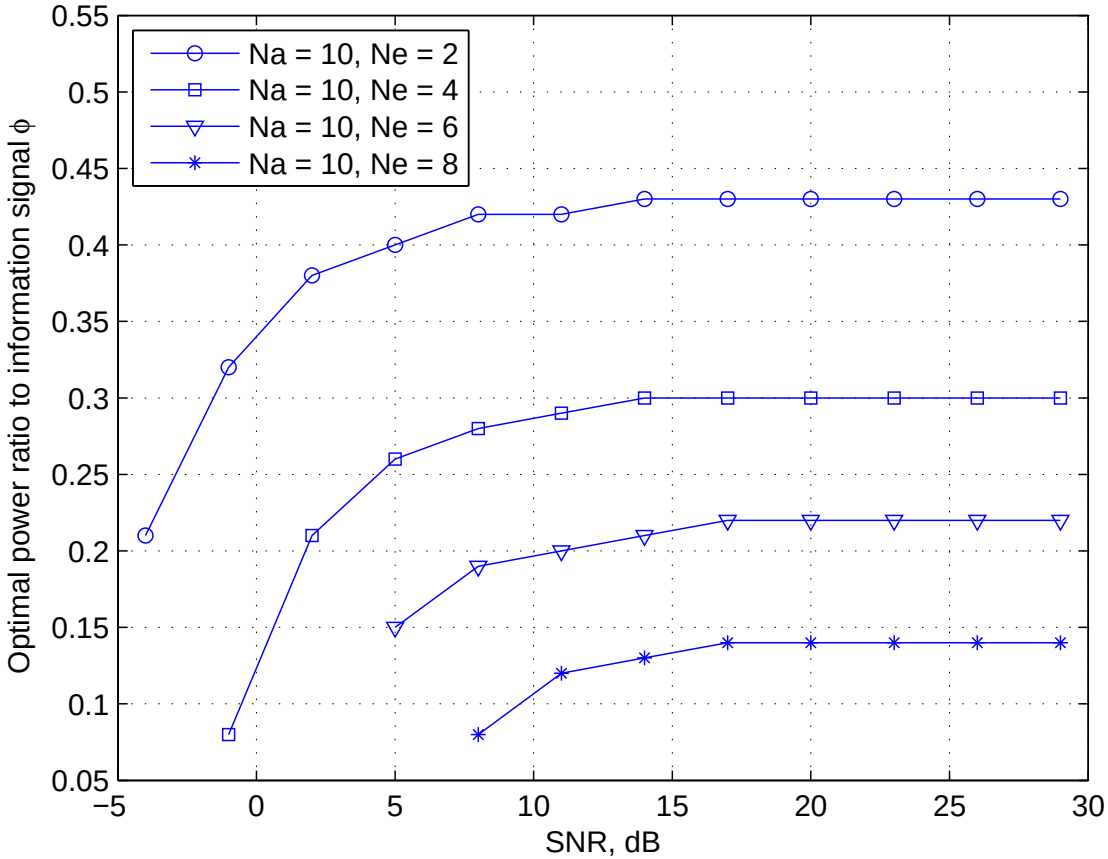
- Multiple Eves.
- Imperfect Channel Knowledge.

Multiple Colluding Eves



- N_E: the total number of "Eves".
- The number of antennas at Alice must be larger than the number of Eves.

Result: Optimal Power Allocation

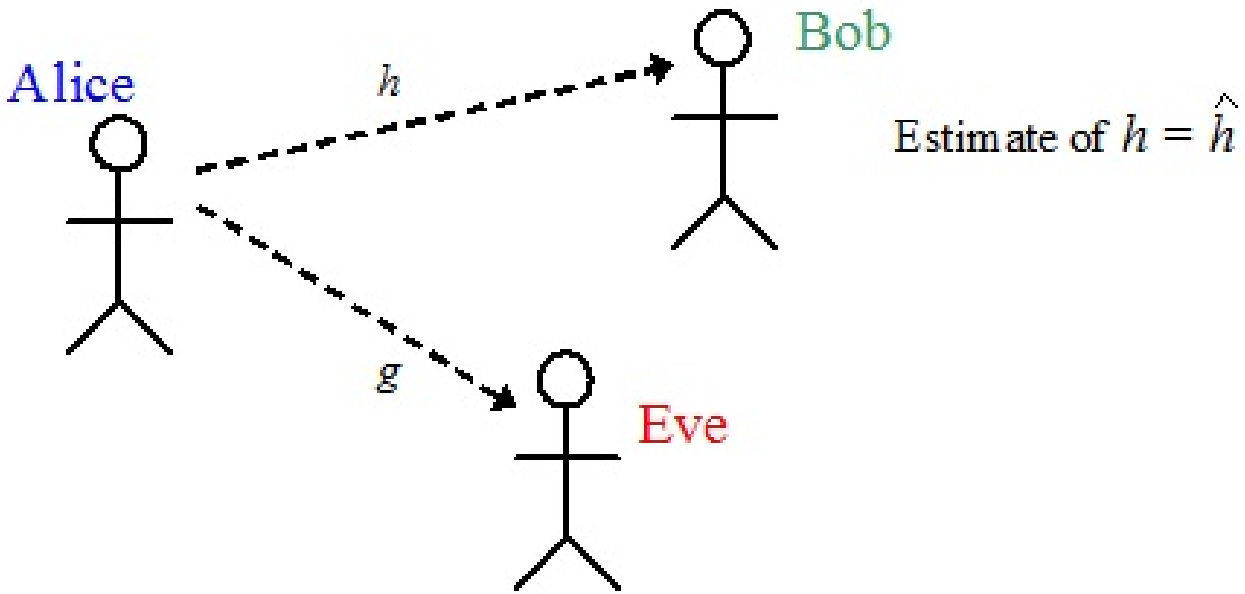


x-axis: power budget P. y-axis: optimal value of ϕ.

N_E: total number of Eves.

- As N_E increases, more power should be allocated to generate artificial noise.

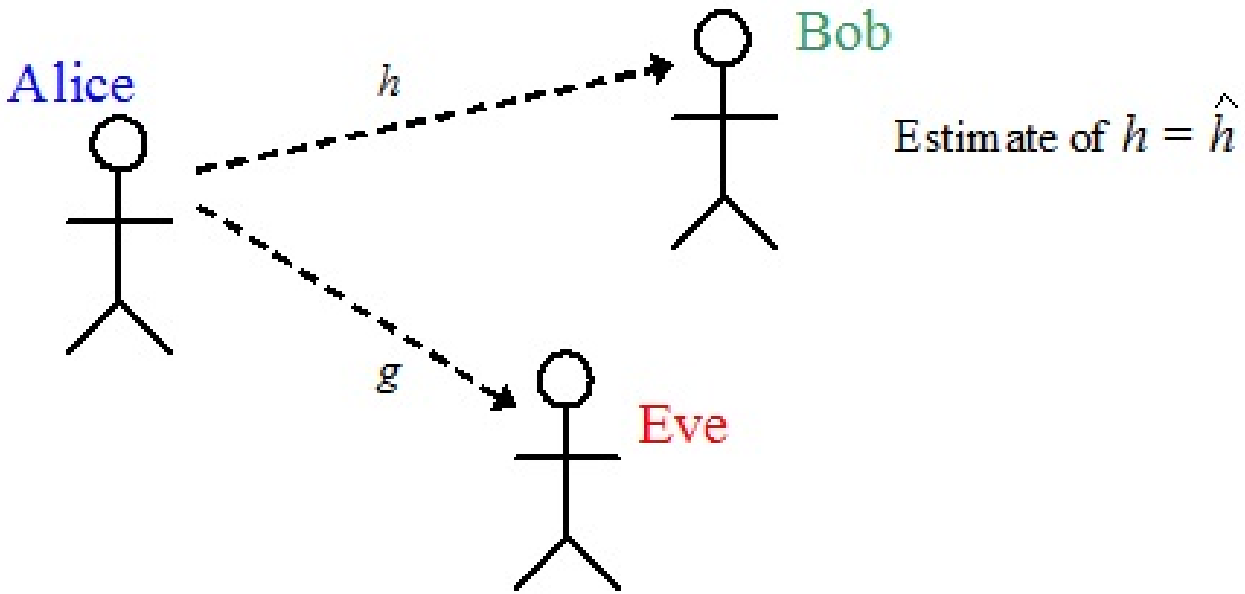
Imperfect Channel Estimation



In practice, Bob cannot estimate **h** with no error.

- $\mathbf{h} = \hat{\mathbf{h}} + \tilde{\mathbf{h}}$, where $\hat{\mathbf{h}}$ is the estimated channel at Bob.
- With a reliable feedback link, Alice also knows $\hat{\mathbf{h}}$.

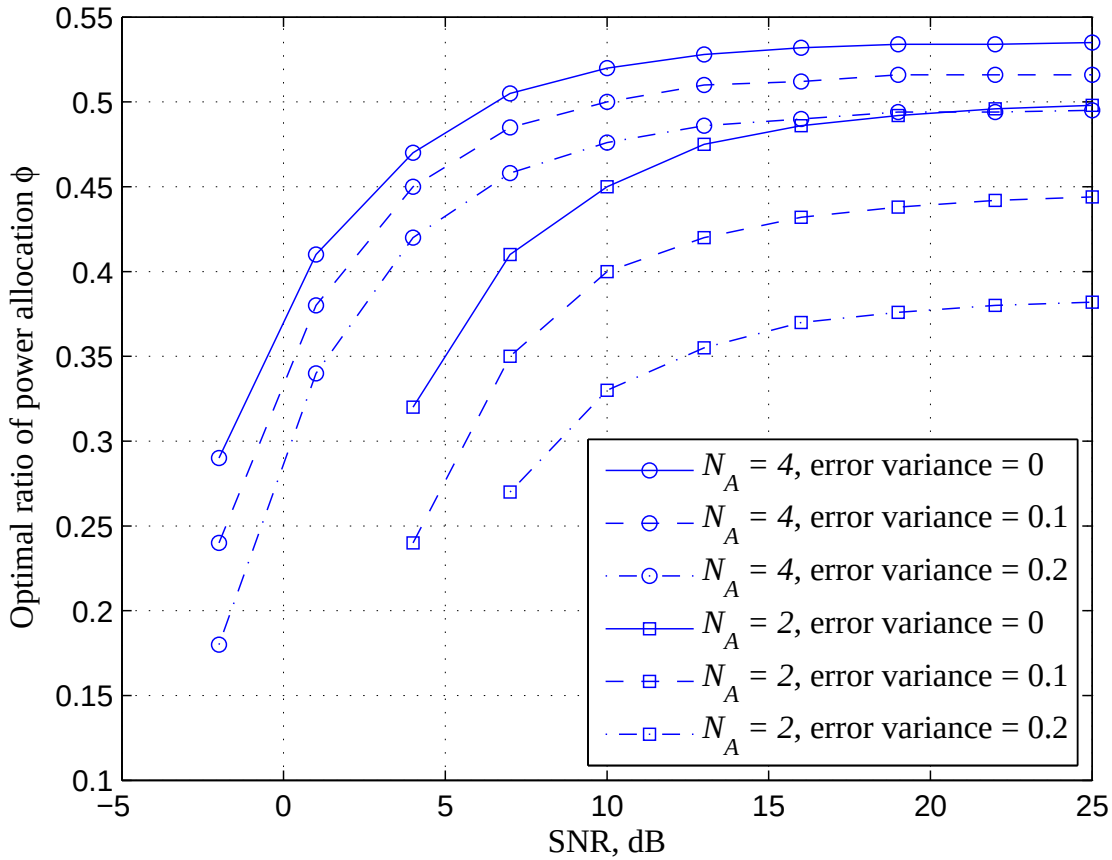
Imperfect Channel Estimation



In practice, Bob cannot estimate $\mathbf{h}$ with no error.

- $\mathbf{h} = \hat{\mathbf{h}} + \tilde{\mathbf{h}}$, where $\hat{\mathbf{h}}$ is the estimated channel at Bob.
- With a reliable feedback link, Alice also knows $\hat{\mathbf{h}}$.
- The information signal is transmitted into $\hat{\mathbf{h}}$ and the artificial noise is transmitted into the subspace orthogonal to $\hat{\mathbf{h}}$.

Result: Optimal Power Allocation



x-axis: power budget P. y-axis: optimal value of ϕ.

N_A: number of antennas at Alice.

- As the channel estimation error increases, more power should be allocated to generate artificial noise.

Conclusions

- The use of artificial noise by Alice makes secrecy communication possible even without the knowledge of Eve's channel.

Conclusions

- The use of artificial noise by Alice makes secrecy communication possible even without the knowledge of Eve's channel.
- For a single Eve, Alice should use equal amount of power for generating the artificial noise and transmitting the information.

Conclusions

- The use of artificial noise by Alice makes secrecy communication possible even without the knowledge of Eve's channel.
- For a single Eve, Alice should use equal amount of power for generating the artificial noise and transmitting the information.
- For multiple colluding Eves, Alice should use more power to generate the artificial noise and less power to transmit the information.

Conclusions

- The use of artificial noise by Alice makes secrecy communication possible even without the knowledge of Eve's channel.
- For a single Eve, Alice should use equal amount of power for generating the artificial noise and transmitting the information.
- For multiple colluding Eves, Alice should use more power to generate the artificial noise and less power to transmit the information.
- When practical channel estimation is considered, Alice should use more power to generate the artificial noise as the channel estimation error increases.

Key References

- The idea of using artificial noise for secret communication was proposed in
  S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *IEEE Trans. Wireless Commun.*, vol. 7, no. 6, pp. 2180–2189, June 2008.

- The results on the optimal power allocation will appear in
  X. Zhou and M. R. McKay, "Secure Transmission with Artificial Noise over Fading Channels: Achievable Rate and Optimal Power Allocation," *IEEE Trans. Veh. Tech.*, 2010.

Thank you very much for your attention!