Downlink Non-Orthogonal Multiple Access Systems With an Untrusted Relay

Ahmed Arafa [1], Wonjae Shin [2,1], Mojtaba Vaezi [3,1], and H. Vincent Poor [1]

[1]Electrical Engineering Department, Princeton University, Princeton, NJ 08544, USA
[2]Department of Electronics Engineering, Pusan National University, Busan 46241, South Korea
[3]Electrical and Computer Engineering Department, Villanova University, PA 19085, USA
Emails: *aarafa@princeton.edu, wjshin@pusan.ac.kr., mvaezi@villanova.edu, poor@princeton.edu*

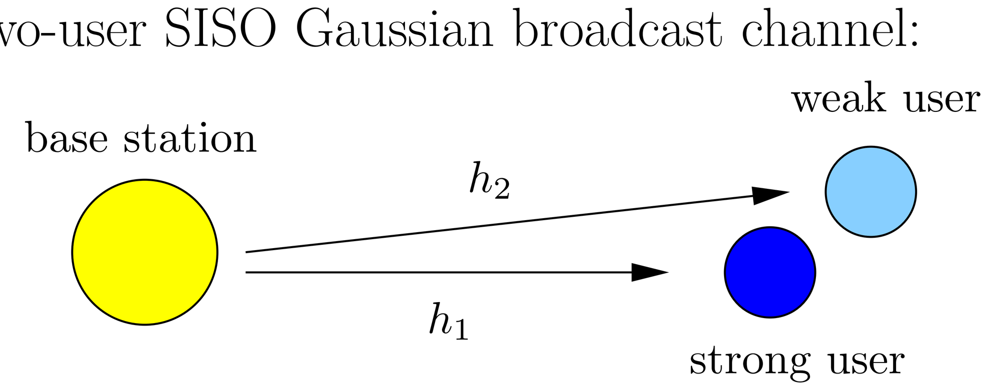
PRINCETON UNIVERSITY

Introduction

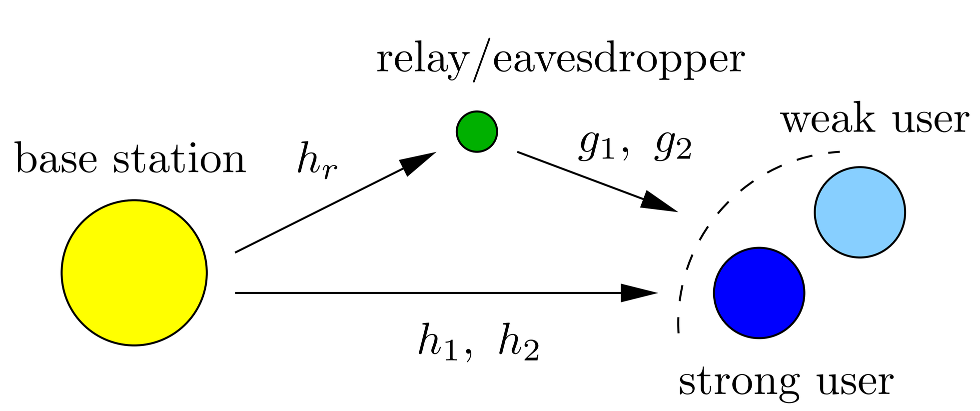
- NOMA techniques offer solutions to spectrum scarcity and congestion problems.
- *Key feature:* efficient utilization of available resources serving multiple users *simultaneously*.
- Using a relay node can generally boost up achievable rates in wireless communication systems.
- **What if the relay is untrusted?**
- Use physical layer security techniques to secure NOMA users' data from the relay, and still benefit from its presence.

System Model

- Two-user SISO Gaussian broadcast channel:



- An **untrusted** half-duplex relay assists the BS:



- BS uses superposition coding:

$$x=\sqrt{\alpha P}s_1+\sqrt{\bar{\alpha}P}s_2$$

where $0\le\alpha\le1$ and $\bar{\alpha}\triangleq1-\alpha$.

- Treating the relay as an eavesdropper achieves the following secrecy rates [1, Theorem 5]:

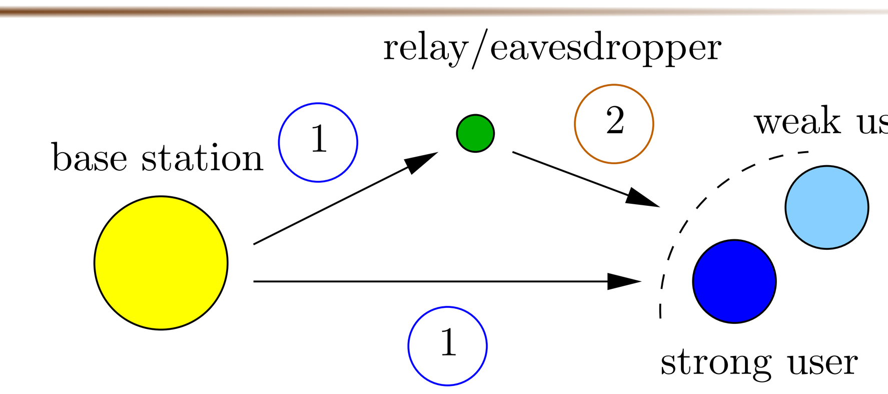
$$r_{s,1}=\left[\log\left(1+|h_1|^2\alpha P\right)-\log\left(1+|h_r|^2\alpha P\right)\right]^+$$

$$r_{s,2}=\left[\log\left(1+\frac{|h_2|^2\bar{\alpha}P}{1+|h_2|^2\alpha P}\right)-\log\left(1+\frac{|h_r|^2\bar{\alpha}P}{1+|h_r|^2\alpha P}\right)\right]^+$$

- **Can we achieve higher secrecy rates by employing the *untrusted* relay?**

Passive User Mode

- Communication occurs over two phases.
- Phase 1: BS broadcasts to users and relay.
- Phase 2: relay uses either *compress-and-forward* or *amplify-and-forward*.
- Both users *passively* listen to the communication.



Using *compress-and-forward*, the following secrecy rates are achievable with *passive users:*

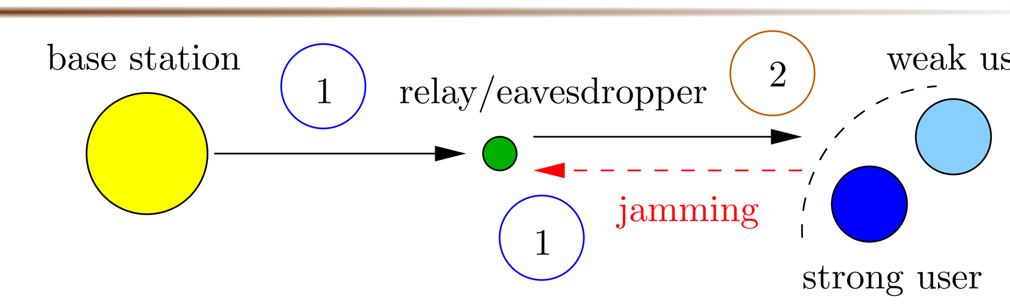
$$r_{s,1}^{CF,P}=\frac{1}{2}\left[\log\left(1+|h_1|^2\alpha\bar{P}+\frac{|h_r|^2\alpha\bar{P}}{1+\sigma_Q^2}\right)-\log\left(1+|h_r|^2\alpha\bar{P}\right)\right]^+$$

$$r_{s,2}^{CF,P}=\frac{1}{2}\left[\log\left(1+\frac{|h_2|^2\bar{\alpha}\bar{P}}{1+|h_2|^2\alpha\bar{P}}+\frac{|h_r|^2\bar{\alpha}\bar{P}}{1+|h_r|^2\alpha\bar{P}+\sigma_Q^2}\right)-\log\left(1+\frac{|h_r|^2\bar{\alpha}\bar{P}}{1+|h_r|^2\alpha\bar{P}}\right)\right]^+$$

$\bar{P}\le P$ is the *new* BS power, and σ_Q^2 is the quantization (compression) noise, whose value is such that decodability at *both* users is guaranteed (a function of $P-\bar{P}$).

Active User Mode

- Phase 1: BS broadcasts to users and relay; users transmit a jamming signal to confuse the relay.
- Nodes are half-duplex $\Rightarrow$ two-hop network.



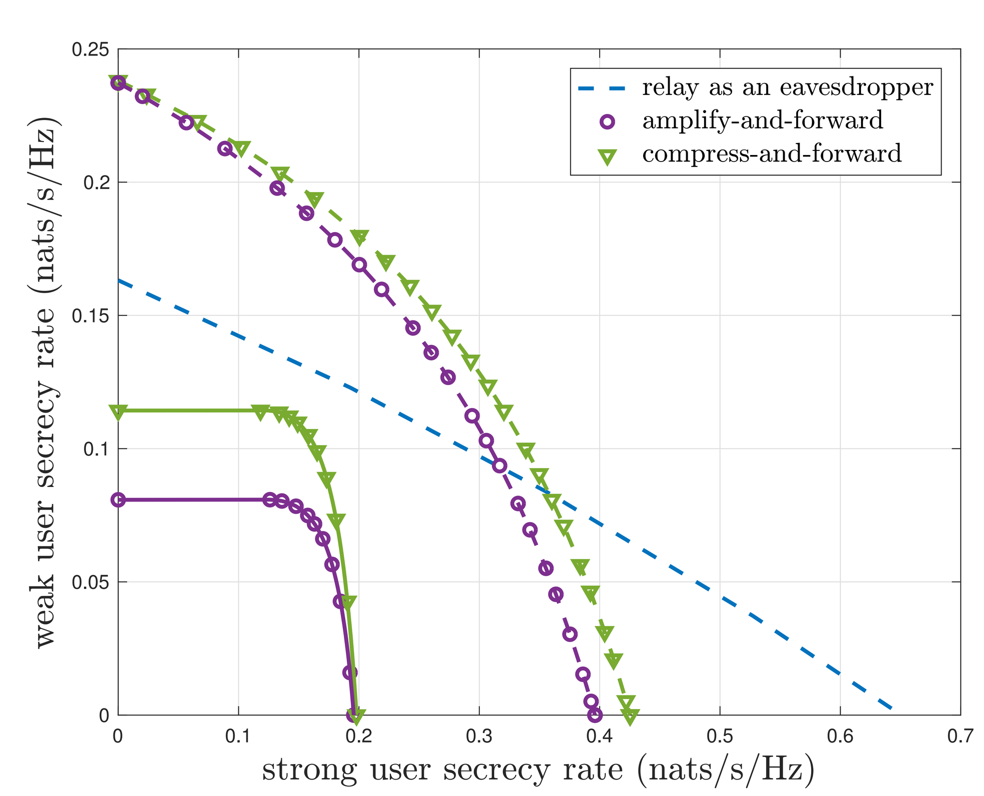
Using *compress-and-forward*, the following secrecy rates are achievable with *active users:*

$$r_{s,1}^{CF,A}=\frac{1}{2}\left[\log\left(1+\frac{|h_r|^2\alpha\bar{P}}{1+\sigma_Q^2}\right)-\log\left(1+\frac{|h_r|^2\alpha\bar{P}}{1+\|\boldsymbol{g}\|^2\delta}\right)\right]^+$$

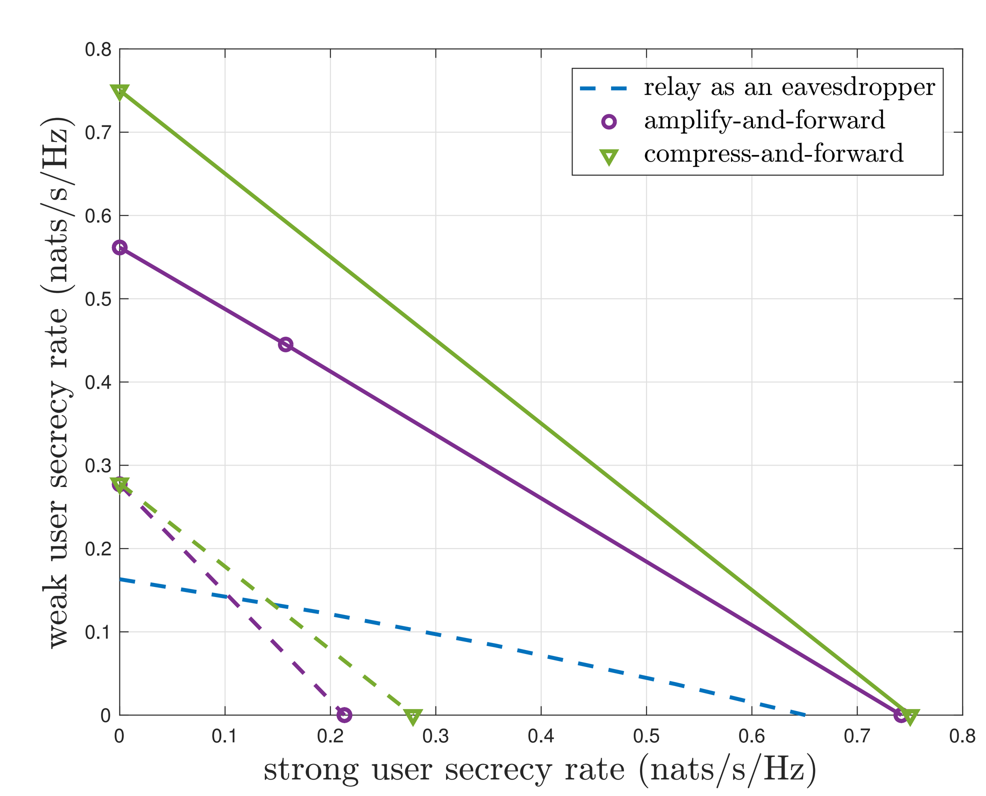
$$r_{s,2}^{CF,A}=\frac{1}{2}\left[\log\left(1+\frac{|h_r|^2\bar{\alpha}\bar{P}}{1+|h_r|^2\alpha\bar{P}+\sigma_Q^2}\right)-\log\left(1+\frac{|h_r|^2\bar{\alpha}\bar{P}}{1+\|\boldsymbol{g}\|^2\delta+|h_r|^2\alpha\bar{P}}\right)\right]^+$$

$\delta\le P-\bar{P}$ is the users' jamming power, and $\boldsymbol{g}\triangleq[g_1,\ g_2]$.

Passive User Mode

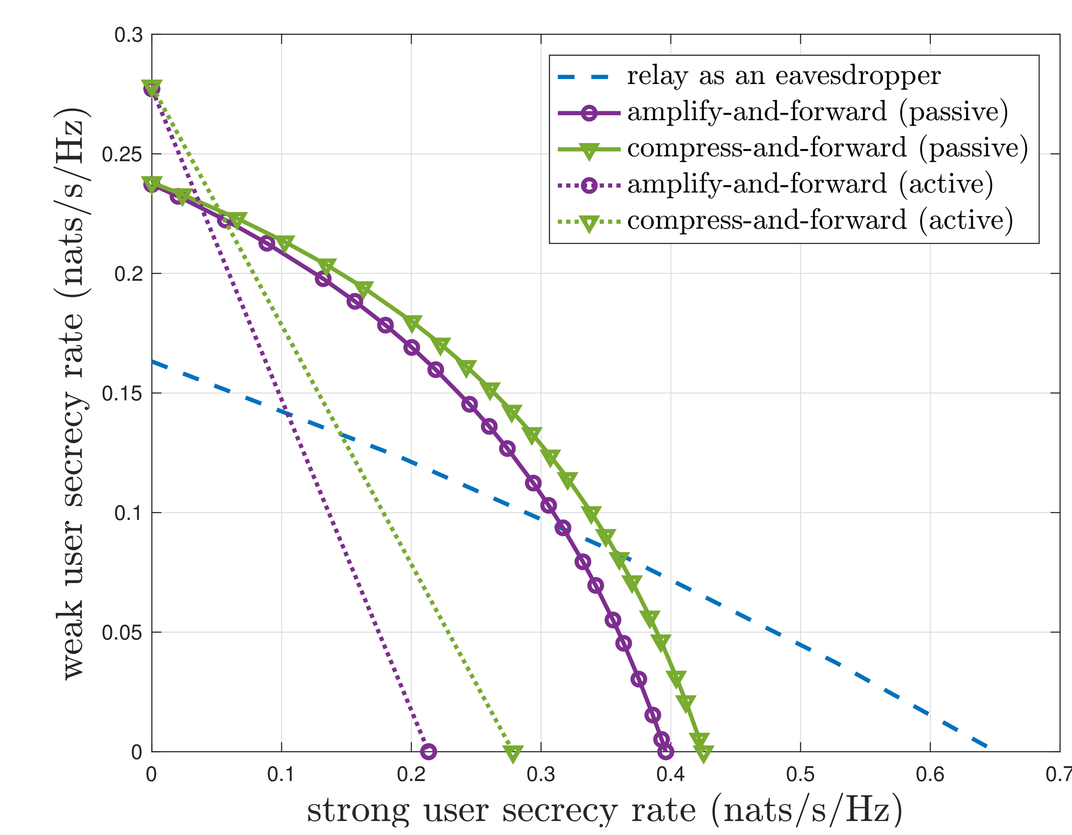


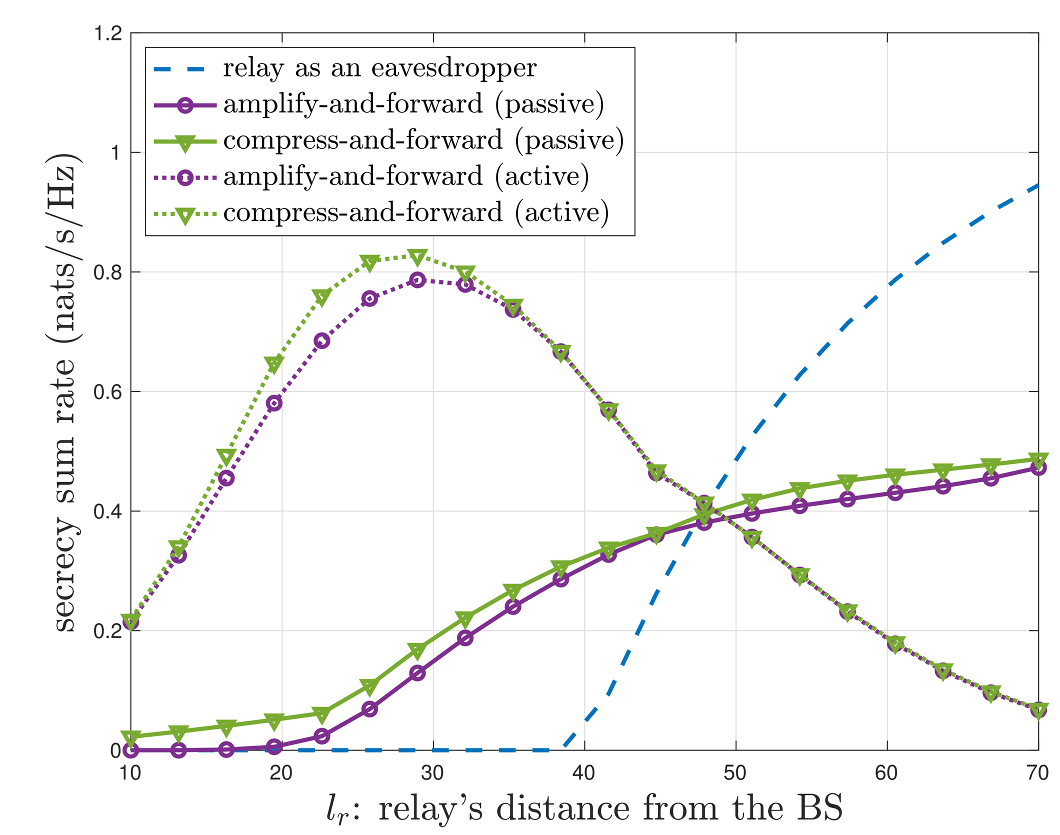
Active User Mode



Dashed lines are when relay is further than users from BS.

Passive vs. Active User Modes





Take away: best user mode and relaying scheme depends on system parameters, especially the relay's distance from BS and users.

References

[1] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, April 2011.

[2] X. He and A. Yener, "Cooperation with an untrusted relay: A secrecy perspective," *IEEE Trans. Inf. Theory*, vol. 56, no. 8, pp. 3807–3827, August 2010.

[3] A. Zewail and A. Yener, "Multi-terminal two-hop untrusted-relay networks with hierarchical security guarantees," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 9, pp. 2052–2066, September 2017.