Relay-Aided Secure Broadcasting for VLC

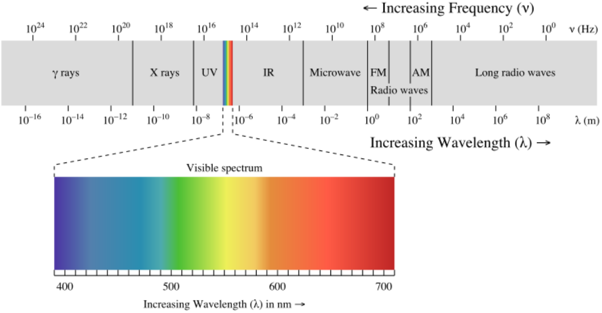
Ahmed Arafa[1] Erdal Panayirci[2] H. Vincent Poor[1]

[1]Electrical Engineering Department, Princeton University, USA

[2]Department of Electrical and Electronics Engineering, Kadir Has University, Istanbul, Turkey

11/27/2018

Visible Light Communications (VLC)

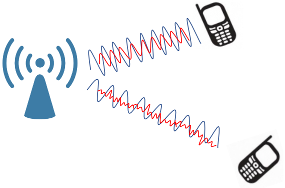


(ref. Wikipedia)

- Offers solutions to spectrum congestion issues by shifting communication frequencies to the visible light range, where much larger (unlicensed) spectrum is available.
- Transmit antennas become LED fixtures; receive antennas become photodetectors.
- Integrable with indoor lighting infrastructures in offices, malls, libraries...
- Relatively more secure than RF, yet still vulnerable to eavesdropping.

Security at the Physical Layer

- Traditionally a higher-layer issue: encryption, key distribution...
- Might be insufficient with the increasing computational powers of adversarial nodes/eavesdroppers.

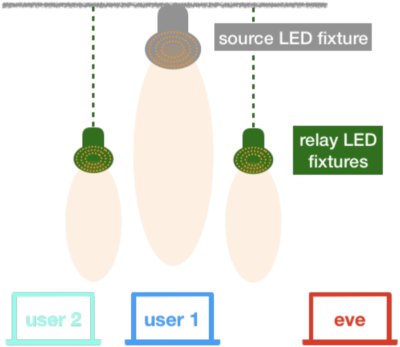


- Physical layer security provides security by exploiting the imperfections in the physical communication channel: noise, fading, interference...
- Joint encoding for security and reliability.

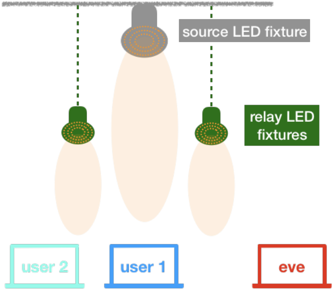
Physical Layer Security for VLC—Related Works

- Jamming for security: [**Mostafa-Lampe** '14], [**Zaid-Rezki-Chaaban-Alouini** '15]
- MISO settings: [**Mostafa-Lampe** '15 '16], [**Arfaoui-Rezki-Ghrayeb-Alouini** '16 '17]
- SISO with discrete signaling: [**Arfaoui-Ghrayeb-Assi** '18]
- MIMO settings: [**Arfaoui-Ghrayeb-Assi** '17]
- Secrecy outage: [**Pan-Ye-Ding** '17], [**Cho-Chen-Coon** '17 '18], [**Yin-Haas** '18]
- Hybrid RF/VLC: [**Marzban-Kashef-Abdallah-Khairy** '17], [**Pan-Ye-Ding** '17]
- BCCM: [**Pham-Pham** '16], [**Arfaoui-Ghrayeb-Assi** '17]
- ...

This Paper: Employing Relay LEDs to Secure a VLC Downlink...



- VLC broadcast channel with two legitimate users, and an external eavesdropper.
- K *Cooperative* half-duplex relay LED fixtures assist the source and offer security.
  - Relaying for single-user VLC w/o security was introduced in [**Kzilirimak-Narmanlioglu-Uysal** '15].
- Suitable model for *multi-layered* lighting systems in offices, airports and plants.
- Transmitters (receivers) are each equipped with a single LED fixture (photodetector).



- Intensity modulation is used to superimpose the source's data signal $x \in \mathbb{R}$ on top of a fixed positive bias current that drives its LEDs.
- Superposition coding is used to convey two messages (x_1, x_2) to the legitimate users:

$$x = \alpha x_1 + (1 - \alpha) x_2, \quad 0 \leq \alpha \leq 1$$

- Weak user decodes its message by treating interference as noise; strong user decodes its message via successive interference cancellation.
- Amplitude constraint imposed to maintain operation within LEDs' dynamic range:

$$\alpha |x_1| + (1 - \alpha) |x_2| \leq A \quad \text{a.s.}$$

- **For a given signaling scheme, what's an achievable secrecy rate region? How can invoking the relays improve it?**

Direct Transmission (Without Relays)

Theorem

The following secrecy rate pair is achievable via direct transmission for a given α*:*

$$r_{1,s} = \left[\frac{1}{2}\log\left(1+\frac{2{h_1}^2\alpha^2A^2}{\pi e}\right) - \frac{1}{2}\log\left(1+\frac{{h_e}^2\alpha^2A^2}{3}\right)\right]^+$$

$$r_{2,s} = \left[\frac{1}{2}\log\left(\frac{1+\frac{2{h_2}^2A^2}{\pi e}}{1+\frac{{h_2}^2\alpha^2A^2}{3}}\right) - \frac{1}{2}\log\left(\frac{1+\frac{{h_e}^2A^2}{3}}{1+\frac{2{h_e}^2\alpha^2A^2}{\pi e}}\right)\right]^+$$

- Source uses uniform signaling: x_1 and $x_2 \sim$ i.i.d. uniform random variables on [-A,A].
- Evaluate the capacity expressions of the multi receiver wiretap channel derived by [**Ekrem** - **Ulukus** '11]:

$$c_{1,s} = [\mathbb{I}(x; y_1|x_2) - \mathbb{I}(x; y_e|x_2)]^+$$
$$c_{2,s} = [\mathbb{I}(x_2; y_2) - \mathbb{I}(x_2; y_e)]^+$$

- Lower bounding via entropy power inequality and concavity of differential entropy.

Direct Transmission (Without Relays)

Theorem

The following secrecy rate pair is achievable via direct transmission for a given α*:*

$$r_{1,s} = \left[\frac{1}{2}\log\left(1+\frac{2{h_1}^2\alpha^2A^2}{\pi e}\right) - \frac{1}{2}\log\left(1+\frac{{h_e}^2\alpha^2A^2}{3}\right)\right]^+$$

$$r_{2,s} = \left[\frac{1}{2}\log\left(\frac{1+\frac{2{h_2}^2A^2}{\pi e}}{1+\frac{{h_2}^2\alpha^2A^2}{3}}\right) - \frac{1}{2}\log\left(\frac{1+\frac{{h_e}^2A^2}{3}}{1+\frac{2{h_e}^2\alpha^2A^2}{\pi e}}\right)\right]^+$$

- The strong user's achievable secrecy rate is positive iff

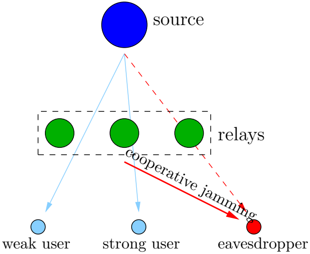
$$\frac{2}{\pi e}h_1^2 > \frac{1}{3}h_e^2$$

- The weak user's achievable secrecy rate is positive iff

$$\left(\frac{2}{\pi e}-\frac{\alpha^2}{3}\right)h_2^2 + \left(\frac{2\alpha^2}{\pi e}-\frac{1}{3}\right)h_e^2 > \left(\frac{1}{9}-\frac{4}{\pi^2e^2}\right)\alpha^2h_2^2h_e^2$$

- **Can we enhance these conditions by invoking the relays?**

Relay Scheme 1: Cooperative Jamming



- The relays cooperatively transmit a jamming signal $\boldsymbol{J}z$, *simultaneously* with the source's transmission.
- $\boldsymbol{J} \in \mathbb{R}^K$ is a beamforming vector and z is a random variable, both to be designed:

$$|z| \leq \bar{A} \quad \text{a.s.}$$
$$|\boldsymbol{J}| \preceq \mathbf{1}_K$$

  - $\bar{A}$: amplitude constraint imposed on each relay LED fixture.

- In order not to harm the legitimate users, the beamforming vector should satisfy:

$$\boldsymbol{g}_1^T \boldsymbol{J}_o = \boldsymbol{g}_2^T \boldsymbol{J}_o = 0$$

Relay Scheme 1: Cooperative Jamming

Theorem

The following secrecy rate pair is achievable via cooperative jamming for a given α:

$$r^J_{1,s} = \left[\frac{1}{2}\log\left(1 + \frac{2{h_1}^2\alpha^2 A^2}{\pi e}\right) - \frac{1}{2}\log\left(\frac{1 + \frac{{h_e}^2\alpha^2 A^2}{3} + \frac{\left({\boldsymbol{g}_e}^T \boldsymbol{J}_o\right)^2 \bar{A}^2}{3}}{1 + \frac{2\left({\boldsymbol{g}_e}^T \boldsymbol{J}_o\right)^2 \bar{A}^2}{\pi e}}\right)\right]^+$$

$$r^J_{2,s} = \left[\frac{1}{2}\log\left(\frac{1 + \frac{2{h_2}^2 A^2}{\pi e}}{1 + \frac{{h_2}^2\alpha^2 A^2}{3}}\right) - \frac{1}{2}\log\left(\frac{1 + \frac{{h_e}^2 A^2}{3} + \frac{\left({\boldsymbol{g}_e}^T \boldsymbol{J}_o\right)^2 \bar{A}^2}{3}}{1 + \frac{2{h_e}^2\alpha^2 A^2}{\pi e} + \frac{2\left({\boldsymbol{g}_e}^T \boldsymbol{J}_o\right)^2 \bar{A}^2}{\pi e}}\right)\right]^+$$

- The random variable z (relays' common signal) is chosen uniformly on $\left[-\bar{A}, \bar{A}\right]$.

- Best beamforming vector:

$$\max_{\boldsymbol{J}_o} \quad \left(\boldsymbol{g}_e^T \boldsymbol{J}_o\right)^2$$
$$\text{s.t.} \quad [\boldsymbol{g}_1\ \boldsymbol{g}_2]^T \boldsymbol{J}_o \triangleq \boldsymbol{G}^T \boldsymbol{J}_o = [0 \quad 0]$$
$$|\boldsymbol{J}_o| \preceq \boldsymbol{1}_K$$

- Unique solution:

$$\boldsymbol{J}_o^* = \frac{\mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{g}_e}{\max_i\left(|\mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{g}_e|\right)_i}$$

- $\mathcal{P}^\perp(\cdot)$ is a projection matrix:

$$\mathcal{P}^\perp(\boldsymbol{A}) \triangleq \boldsymbol{I}_K - \boldsymbol{A}\left(\boldsymbol{A}^T\boldsymbol{A}\right)^{-1}\boldsymbol{A}^T$$

Relay Scheme 1: Cooperative Jamming

Theorem

The following secrecy rate pair is achievable via cooperative jamming for a given α:

$$r_{1,s}^{J} = \left[\frac{1}{2}\log\left(1+\frac{2{h_1}^2\alpha^2A^2}{\pi e}\right)-\frac{1}{2}\log\left(\frac{1+\frac{{h_e}^2\alpha^2A^2}{3}+\frac{\left({\boldsymbol{g}_e}^T\boldsymbol{J}_o\right)^2\bar{A}^2}{3}}{1+\frac{2\left({\boldsymbol{g}_e}^T\boldsymbol{J}_o\right)^2\bar{A}^2}{\pi e}}\right)\right]^+$$

$$r_{2,s}^{J} = \left[\frac{1}{2}\log\left(\frac{1+\frac{2{h_2}^2A^2}{\pi e}}{1+\frac{{h_2}^2\alpha^2A^2}{3}}\right)-\frac{1}{2}\log\left(\frac{1+\frac{{h_e}^2A^2}{3}+\frac{\left({\boldsymbol{g}_e}^T\boldsymbol{J}_o\right)^2\bar{A}^2}{3}}{1+\frac{2{h_e}^2\alpha^2A^2}{\pi e}+\frac{2\left({\boldsymbol{g}_e}^T\boldsymbol{J}_o\right)^2\bar{A}^2}{\pi e}}\right)\right]^+$$

- The random variable z (relays' common signal) is chosen uniformly on $[-\bar{A}, \bar{A}]$.

- Best beamforming vector:

$$\max_{\boldsymbol{J}_o} \quad \left(\boldsymbol{g}_e^T\boldsymbol{J}_o\right)^2$$
$$\text{s.t.} \quad [\boldsymbol{g}_1 \ \boldsymbol{g}_2]^T\boldsymbol{J}_o \triangleq \boldsymbol{G}^T\boldsymbol{J}_o = [0 \quad 0]$$
$$|\boldsymbol{J}_o| \preceq \mathbf{1}_K$$

- Unique solution:

$$\boldsymbol{J}_o^* = \frac{\mathcal{P}^{\perp}(\boldsymbol{G})\,\boldsymbol{g}_e}{\max_i\left(|\mathcal{P}^{\perp}(\boldsymbol{G})\,\boldsymbol{g}_e|\right)_i}$$

- $\mathcal{P}^{\perp}(\cdot)$ is a projection matrix:

$$\mathcal{P}^{\perp}(\boldsymbol{A}) \triangleq \boldsymbol{I}_K - \boldsymbol{A}\left(\boldsymbol{A}^T\boldsymbol{A}\right)^{-1}\boldsymbol{A}^T$$

Relay Scheme 1: Cooperative Jamming

Theorem

The following secrecy rate pair is achievable via cooperative jamming for a given α:

$$r_{1,s}^J = \left[\frac{1}{2}\log\left(1+\frac{2{h_1}^2\alpha^2A^2}{\pi e}\right) - \frac{1}{2}\log\left(\frac{1+\frac{{h_e}^2\alpha^2A^2}{3}+\frac{\left({\boldsymbol{g}_e}^T\boldsymbol{J}_o\right)^2\bar{A}^2}{3}}{1+\frac{2\left({\boldsymbol{g}_e}^T\boldsymbol{J}_o\right)^2\bar{A}^2}{\pi e}}\right)\right]^+$$

$$r_{2,s}^J = \left[\frac{1}{2}\log\left(\frac{1+\frac{2{h_2}^2A^2}{\pi e}}{1+\frac{{h_2}^2\alpha^2A^2}{3}}\right) - \frac{1}{2}\log\left(\frac{1+\frac{{h_e}^2A^2}{3}+\frac{\left({\boldsymbol{g}_e}^T\boldsymbol{J}_o\right)^2\bar{A}^2}{3}}{1+\frac{2{h_e}^2\alpha^2A^2}{\pi e}+\frac{2\left({\boldsymbol{g}_e}^T\boldsymbol{J}_o\right)^2\bar{A}^2}{\pi e}}\right)\right]^+$$

- The random variable z (relays' common signal) is chosen uniformly on $\left[-\bar{A},\bar{A}\right]$.

- Best beamforming vector:

$$\max_{\boldsymbol{J}_o} \quad \left(\boldsymbol{g}_e^T\boldsymbol{J}_o\right)^2$$
$$\text{s.t.} \quad [\boldsymbol{g}_1 \ \boldsymbol{g}_2]^T\boldsymbol{J}_o \triangleq \boldsymbol{G}^T\boldsymbol{J}_o = [0 \quad 0]$$
$$|\boldsymbol{J}_o| \preceq \boldsymbol{1}_K$$

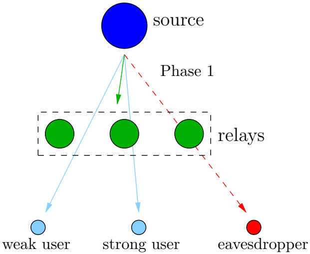
- Unique solution:

$$\boxed{\boldsymbol{J}_o^* = \frac{\mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{g}_e}{\max_i\left(|\mathcal{P}^\perp(\boldsymbol{G})\,\boldsymbol{g}_e|\right)_i}}$$

- $\mathcal{P}^\perp(\cdot)$ is a projection matrix:

$$\mathcal{P}^\perp(\boldsymbol{A}) \triangleq \boldsymbol{I}_K - \boldsymbol{A}\left(\boldsymbol{A}^T\boldsymbol{A}\right)^{-1}\boldsymbol{A}^T$$

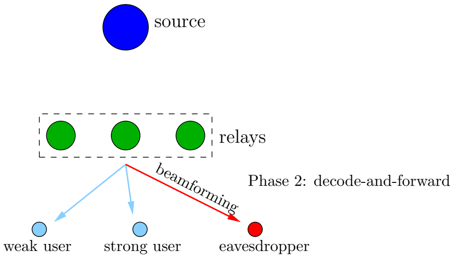
Relay Scheme 2: Decode-and-Forward



- Communication occurs over two phases.
- **Phase 1:** source broadcasts to both the relays and the legitimate users.
- **Phase 2:** relays decode their received signals, and forward toward the users using superposition coding after multiplying by a beamforming vector $\boldsymbol{d} \in \mathbb{R}^K$.
- Eavesdropper overhears communication in the two phases.
- To eliminate the eavesdropping benefit in the second phase, we set:

$$\boldsymbol{g}_e^T \boldsymbol{d}_o = 0$$

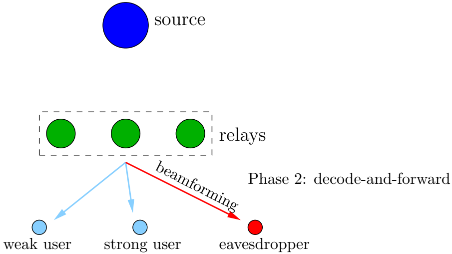
Relay Scheme 2: Decode-and-Forward



- Communication occurs over two phases.
- **Phase 1:** source broadcasts to both the relays and the legitimate users.
- **Phase 2:** relays decode their received signals, and forward toward the users using superposition coding after multiplying by a beamforming vector $\boldsymbol{d} \in \mathbb{R}^K$.
- Eavesdropper overhears communication in the two phases.
- To eliminate the eavesdropping benefit in the second phase, we set:

$$\boldsymbol{g}_e^T \boldsymbol{d}_o = 0$$

Relay Scheme 2: Decode-and-Forward



- Communication occurs over two phases.
- **Phase 1:** source broadcasts to both the relays and the legitimate users.
- **Phase 2:** relays decode their received signals, and forward toward the users using superposition coding after multiplying by a beamforming vector $\boldsymbol{d} \in \mathbb{R}^K$.
- Eavesdropper overhears communication in the two phases.
- To eliminate the eavesdropping benefit in the second phase, we set:

$$\boldsymbol{g}_e^T \boldsymbol{d}_o = 0$$

Relay Scheme 2: Decode-and-Forward

Theorem

The following secrecy rate pair is achievable via decode-and-forward for a given α:

$$r_{1,s}^{DF} = \frac{1}{2}\left[r_1^{DF} - \frac{1}{2}\log\left(1 + \frac{h_e^2\alpha^2 A^2}{3}\right)\right]^+$$

$$r_{2,s}^{DF} = \frac{1}{2}\left[r_2^{DF} - \frac{1}{2}\log\left(\frac{1 + \frac{h_e^2 A^2}{3}}{1 + \frac{2h_e^2\alpha^2 A^2}{\pi e}}\right)\right]^+$$

where

$$r_1^{DF} = \min\left\{\frac{1}{2}\log\left(1 + \frac{2h_1^2\alpha^2 A^2}{\pi e}\right) + \frac{1}{2}\log\left(1 + \frac{2\left(\boldsymbol{g}_1^T\boldsymbol{d}_o\right)^2\alpha^2\bar{A}^2}{\pi e}\right), \frac{1}{2}\log\left(1 + \min_{1\le i\le K}\frac{2h_{r,i}^2\alpha^2 A^2}{\pi e}\right)\right\}$$

$$r_2^{DF} = \min\left\{\frac{1}{2}\log\left(\frac{1 + \frac{2h_2^2 A^2}{\pi e}}{1 + \frac{h_2^2\alpha^2 A^2}{3}}\right) + \frac{1}{2}\log\left(\frac{1 + \frac{2\left(\boldsymbol{g}_2^T\boldsymbol{d}_o\right)^2\bar{A}^2}{\pi e}}{1 + \frac{\left(\boldsymbol{g}_2^T\boldsymbol{d}_o\right)^2\alpha^2\bar{A}^2}{3}}\right), \frac{1}{2}\log\left(\min_{1\le i\le K}\frac{1 + \frac{2h_{r,i}^2 A^2}{\pi e}}{1 + \frac{h_{r,i}^2\alpha^2 A^2}{3}}\right)\right\}$$

- i.i.d. uniform signaling over $\left[-\bar{A}, \bar{A}\right]$ is used at the relays.
- Extra $\frac{1}{2}$ terms are due to sending same information over two phases.

Relay Scheme 2: Decode-and-Forward

- Best beamforming vector:

$$\begin{aligned} \max_{\boldsymbol{d}_o} \quad & \alpha \left(\boldsymbol{g}_1^T \boldsymbol{d}_o \right)^2 + (1-\alpha) \left(\boldsymbol{g}_2^T \boldsymbol{d}_o \right)^2 \\ \text{s.t.} \quad & \boldsymbol{g}_e^T \boldsymbol{d}_o = 0 \\ & |\boldsymbol{d}_o| \preceq \mathbf{1}_K \end{aligned}$$

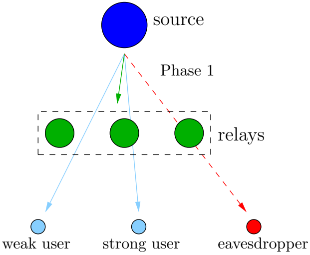
- Unique solution:

$$\boxed{\boldsymbol{d}_o^* = \mathcal{P}^{\perp}(\boldsymbol{g}_e) \frac{\boldsymbol{v}_d}{\max_i \left(|\boldsymbol{v}_d| \right)_i}}$$

with $\boldsymbol{v}_d$ being the leading eigenvector of the matrix:

$$\mathcal{P}^{\perp}(\boldsymbol{g}_e) \left(\alpha \boldsymbol{g}_1 \boldsymbol{g}_1^T + (1-\alpha) \boldsymbol{g}_2 \boldsymbol{g}_2^T \right) \mathcal{P}^{\perp}(\boldsymbol{g}_e)$$

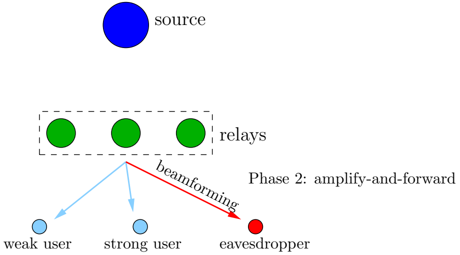
Relay Scheme 3: Amplify-and-Forward



- Communication also occurs over two phases.
- **Phase 2:** relays multiply their received signals $\boldsymbol{y}_r$ by a beamforming vector $\boldsymbol{a} \in \mathbb{R}^K$.
- To eliminate the eavesdropping benefit in the second phase, we set:

$$\boldsymbol{g}_e^T \mathtt{diag}(\boldsymbol{h}_r)\, \boldsymbol{a}_o = 0$$

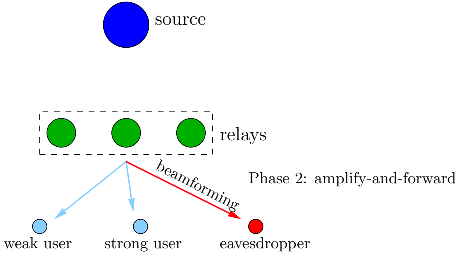
Relay Scheme 3: Amplify-and-Forward



- Communication also occurs over two phases.
- **Phase 2:** relays multiply their received signals $\boldsymbol{y}_r$ by a beamforming vector $\boldsymbol{a} \in \mathbb{R}^K$.
- To eliminate the eavesdropping benefit in the second phase, we set:

$$\boldsymbol{g}_e^T \mathtt{diag}(\boldsymbol{h}_r)\, \boldsymbol{a}_o = 0$$

Relay Scheme 3: Amplify-and-Forward



- Communication also occurs over two phases.
- **Phase 2:** relays multiply their received signals $\boldsymbol{y}_r$ by a beamforming vector $\boldsymbol{a} \in \mathbb{R}^K$.
- To eliminate the eavesdropping benefit in the second phase, we set:

$$\boldsymbol{g}_e^T \mathtt{diag}(\boldsymbol{h}_r)\, \boldsymbol{a}_o = 0$$

Relay Scheme 3: Amplify-and-Forward

Theorem

The following secrecy rate pair is achievable via amplify-and-forward for a given α:

$$r_{1,s}^{AF} = \frac{1}{2}\left[\frac{1}{2}\log\left(1+\frac{2{\kappa_1}^2\alpha^2A^2}{\pi e}\right)-\frac{1}{2}\log\left(1+\frac{{h_e}^2\alpha^2A^2}{3}\right)\right]^+$$

$$r_{2,s}^{AF} = \frac{1}{2}\left[\frac{1}{2}\log\left(\frac{1+\frac{2{\kappa_2}^2A^2}{\pi e}}{1+\frac{{\kappa_2}^2\alpha^2A^2}{3}}\right)-\frac{1}{2}\log\left(\frac{1+\frac{{h_e}^2A^2}{3}}{1+\frac{2{h_e}^2\alpha^2A^2}{\pi e}}\right)\right]^+$$

where

$$\kappa_j^2 \triangleq h_j^2 + \frac{\left(\mathbf{g}_j^T\, diag\left(\mathbf{h}_r\right)\mathbf{a}_o\right)^2}{1+\left(\mathbf{g}_j^T\mathbf{a}_o\right)^2}, \quad j=1,2$$

- Extra $\frac{1}{2}$ terms are due to sending same information over two phases.

Relay Scheme 3: Amplify-and-Forward

- Best beamforming vector for the jth user:

$$\begin{aligned} \max_{\boldsymbol{a}_o} \quad & \frac{\left(\boldsymbol{g}_j^T \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o\right)^2}{1 + \left(\boldsymbol{g}_j^T \boldsymbol{a}_o\right)^2} \\ \text{s.t.} \quad & \boldsymbol{g}_e^T \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o = 0 \\ & \left|\mathtt{diag}\left(\boldsymbol{y}_r\right) \boldsymbol{a}_o\right| \preceq \mathbf{1}_K \bar{A} \end{aligned}$$

Relay Scheme 3: Amplify-and-Forward

- Auxiliary parameterized problem:

$$
\begin{aligned}
p_j^{AF}(\lambda) \triangleq \max_{\boldsymbol{a}_o} \quad & \left(\boldsymbol{g}_j^T \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o\right)^2 - \lambda \left(1 + \left(\boldsymbol{g}_j^T \boldsymbol{a}_o\right)^2\right) \\
\text{s.t.} \quad & \boldsymbol{g}_e^T \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o = 0 \\
& \left|\mathtt{diag}\left(\boldsymbol{y}_r\right) \boldsymbol{a}_o\right| \preceq \mathbf{1}_K \bar{A}
\end{aligned}
$$

- Unique solution for every λ:

$$
\boxed{\boldsymbol{a}_o = \mathcal{P}^{\perp}\left(\mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{g}_e\right) \frac{\boldsymbol{v}_a}{\max_i \left(\left|\mathtt{diag}\left(\boldsymbol{y}_r\right) \boldsymbol{v}_a\right|\right)_i} \bar{A}}
$$

  with $\boldsymbol{v}_a$ being the leading eigenvector of the matrix:

$$
\mathcal{P}^{\perp}\left(\mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{g}_e\right) \left(\mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{g}_j \boldsymbol{g}_j^T \mathtt{diag}\left(\boldsymbol{h}_r\right) - \lambda \boldsymbol{g}_j \boldsymbol{g}_j^T\right) \mathcal{P}^{\perp}\left(\mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{g}_e\right)
$$

- Use bisection search to find the optimal λ^* : $p_j^{AF}\left(\lambda^*\right) = 0$.
- Finally, we set:

$$
\boxed{\boldsymbol{a}_o^* = \alpha \boldsymbol{a}_o^{(1)} + (1-\alpha) \boldsymbol{a}_o^{(2)}}
$$

Relay Scheme 3: Amplify-and-Forward

- Auxiliary parameterized problem:

$$\begin{aligned} p_j^{AF}(\lambda) \triangleq \max_{\boldsymbol{a}_o} \quad & \left(\boldsymbol{g}_j^T \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o\right)^2 - \lambda \left(1 + \left(\boldsymbol{g}_j^T \boldsymbol{a}_o\right)^2\right) \\ \text{s.t.} \quad & \boldsymbol{g}_e^T \mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{a}_o = 0 \\ & \left|\mathtt{diag}\left(\boldsymbol{y}_r\right) \boldsymbol{a}_o\right| \preceq \boldsymbol{1}_K \bar{A} \end{aligned}$$

- Unique solution for every λ:

$$\boxed{\boldsymbol{a}_o = \mathcal{P}^{\perp}(\mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{g}_e) \frac{\boldsymbol{v}_a}{\max_i \left(\left|\mathtt{diag}\left(\boldsymbol{y}_r\right) \boldsymbol{v}_a\right|\right)_i} \bar{A}}$$

with $\boldsymbol{v}_a$ being the leading eigenvector of the matrix:

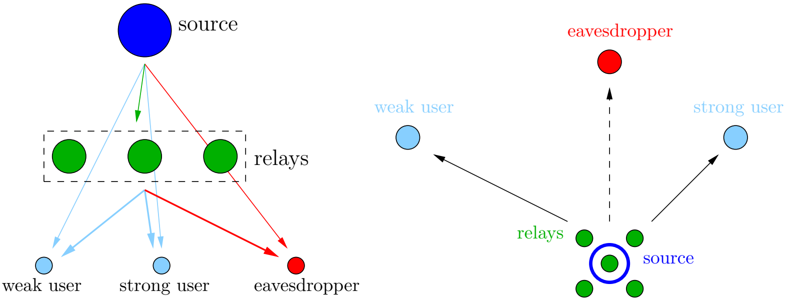
$$\mathcal{P}^{\perp}(\mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{g}_e) \left(\mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{g}_j \boldsymbol{g}_j^T \mathtt{diag}\left(\boldsymbol{h}_r\right) - \lambda \boldsymbol{g}_j \boldsymbol{g}_j^T\right) \mathcal{P}^{\perp}(\mathtt{diag}\left(\boldsymbol{h}_r\right) \boldsymbol{g}_e)$$

- Use bisection search to find the optimal λ^* : $p_j^{AF}\left(\lambda^*\right) = 0$.

- Finally, we set:

$$\boxed{\boldsymbol{a}_o^* = \alpha \boldsymbol{a}_o^{(1)} + (1-\alpha) \boldsymbol{a}_o^{(2)}}$$

Numerical Results

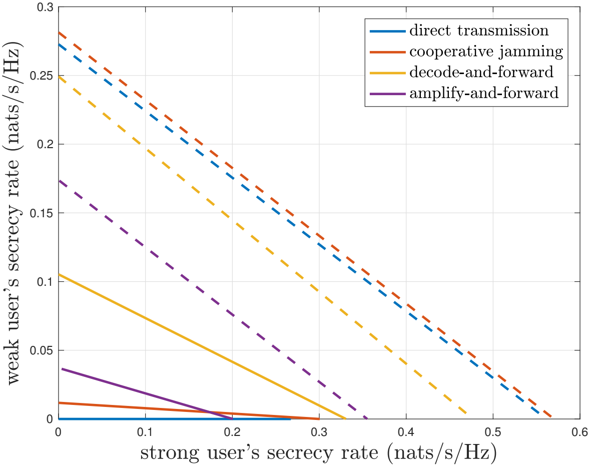


- $K = 5$ relays.
- Channel gain between two nodes q_1 and q_2:

$$\frac{A_{det}(m+1)}{2\pi l_{q_1,q_2}^2}\left(\frac{|z_{q_1}-z_{q_2}|}{l_{q_1,q_2}}\right)^{m+1}$$

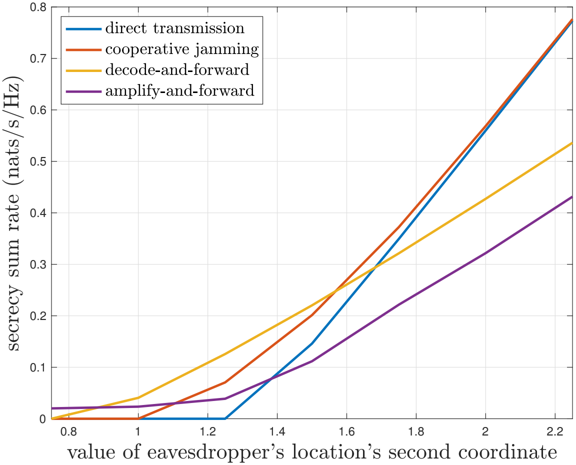
  - A_{det}: photodetector's area.
  - m: order of Lambertian emission.
  - z_q: elevation of node q from the ground.
  - l_{q_1,q_2}: distance between nodes q_1 and q_2.

Numerical Results—Secrecy Rate Regions



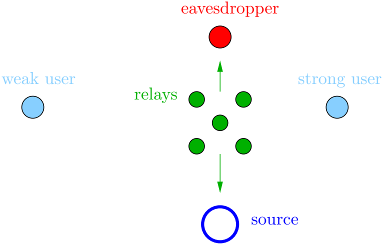
- Solid lines: eavesdropper at $(0, 1.75, 0.7)$; dashed lines: at $(0, 2, 0.7)$.

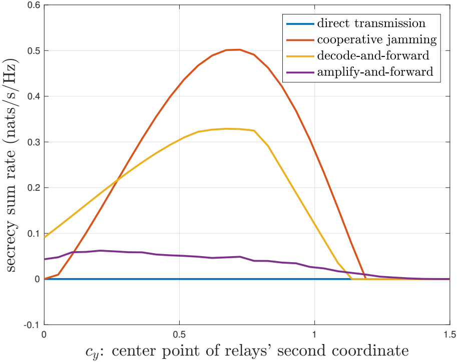
Numerical Results—Secrecy Sum Rates



- Second coordinate of eavesdropper's location is varied; first is at 0 and third at 0.7.
- $\alpha = 0.8$ is fixed.

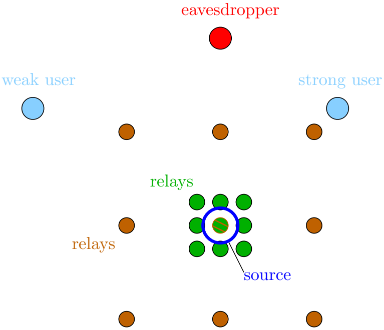
Numerical Results—Relays Center Position

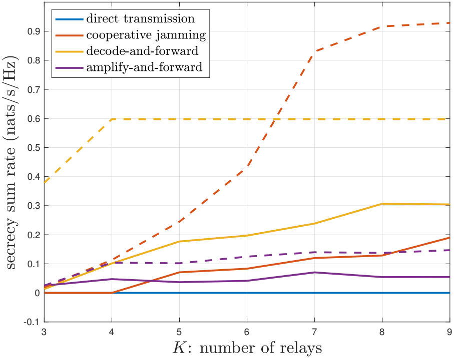




- Eavesdropper's position is fixed at $(0, 1, 0.7)$.

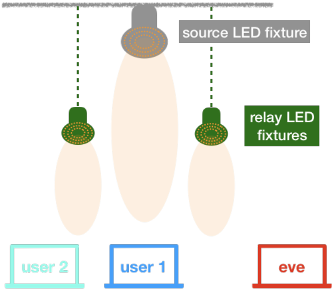
Numerical Results—Number of Relays and Their Relative Distances





- Relays are scattered along a square of side length 2ℓ.
- green: $\ell = 0.1$; brown: $\ell = 0.5$.
- Eavesdropper is at $(0, 1.25, 0.7)$.
- Solid lines are for the green layout; dashed are for brown.

Conclusions



- Considered the security benefits of employing relays in multiuser VLC with an external eavesdropper.
- Achievable secrecy rate regions for direct transmission, and for three relaying schemes: cooperative jamming, decode-and-forward and amplify-and-forward:
  - Uniform signaling + secure beamforming subject to amplitude constraints.
- Best relaying scheme depends on **relative locations** of users and eavesdropper.

- Possible future extensions:
  - MIMO settings.
  - Achievable secrecy rates based on signaling other than uniform: discrete, truncated generalized normal, . . .
  - Unknown eavesdropper's location: secrecy outage probabilities and robust beamforming.