可視光通信における物理層セキュリティの基本的な分析

代表研究者　　PHAM VAN THANH　静岡大学　工学部　助教

1 はじめに

過去 10 年間で、モバイルデバイスの爆発的な成長と、データ集約型のマルチメディアアプリケーションの数の増加が見られた. Cisco System Inc.によると、2016 年から 2021 年までの期間中、グローバルデータトラフィックは 1 か月あたり 7 エクサバイトから 49 エクサバイトに増加していた[1]. データトラフィックに対するこの途方もない需要は、現在の無線技術に深刻な負担をかけ、通信目的で新しい電磁スペクトルの使用を促している. データ伝送に可視スペクトルを使用する可視光通信（Visible Light Communication-VLC）は、既存の RF 技術の代替または補完的なソリューションとして注目を集めている[2][3]. VLC の研究開発は、高速無線接続の必要性の高まり、RF スペクトルの不足、および照明に発光ダイオード（LED）を使用することの普及により推進されてきた.

新興技術として、研究作業の大部分は、VLC システムのパフォーマンスと実用性の向上に注目している[4]-[7]. 可視光のブロードキャストの性質により、VLC チャネルが悪意のあるユーザーによる盗聴に対して脆弱になるため、セキュリティとプライバシーも VLC の設計における重要な懸念事項である. 現在のセキュリティ対策は、OSI モデルの上位層で実行される従来の鍵ベースの暗号化技術が多用されている. これらの手法の機密性は、主に秘密鍵の導出の複雑さに依存し、現在の計算能力では、この鍵導出問題を妥当な時間で解決することは不可能であると考えられている. それにもかかわらず、ハードウェアの急速な進歩（例えば、量子コンピューティングの開発）は、近い将来、いくつかの暗号化アルゴリズムのセキュリティを脅かすと予想される. これにより、物理層でのセキュリティ（物理層セキュリティ（Physical Layer Security - PLS）とも呼ばれる）に関する多くの研究が動機付けられた[8]-[10]. これは、伝送メディアの固有の不確実性を利用して、許可されていないユーザーによる盗聴に対処する.

最近、温室効果ガス排出量を削減するための世界的な取り組みにより、エネルギー効率も通信システムの設計において重要な側面と見なされている. そのため、この研究の目的は、エネルギー効率の観点から VLC の物理層のセキュリティを研究することである.

2 研究背景と目的

2-1 背景

PLS は RF システムの文脈で広く研究されてきたが、ごく最近、VLC への採用が注目されている. まず、単一の送信機のシナリオで、[11]の著者は、1 人の正当なユーザー（Bob と呼ばれる）と一人の盗聴者（Eve と呼ばれる）を含む従来の盗聴チャネルを調べ、単一入力単一出力 VLC チャネルの下限と上限の機密容量を包括的に分析した. 十分な照明を提供するには複数の LED 照明器具を配置する必要があるため、実際には図 1 に示すようなマルチ送信機 VLC システムの方が適切であると考えられている. マルチトランスミッター構成では、空間の自由度を用いて機密性のパフォーマンスを向上させるプリコーディングおよび人工ノイズ（Artificial Noise -AN）技術の使用も可能になる. この点で、VLC システムにプリコーディングと AN を利用することについて多くの研究が行われてきた. ただし、これらの研究は、主に PLS のパフォーマンスを向上させるための最適な設計に重点を置いていた[12]-[15]. エネルギー効率の視点からの最適な設計はよく理解されていないので、本研究では、このギャップを埋めようとしている.

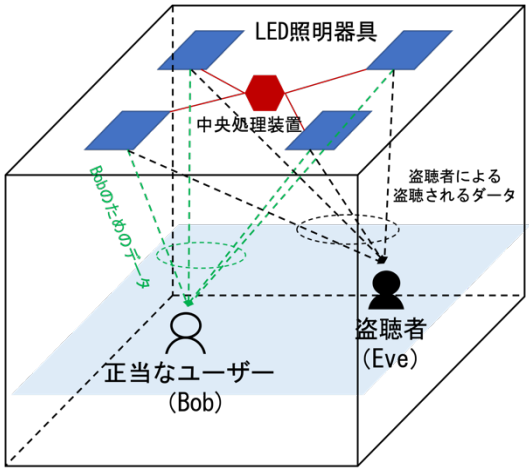

図 1：VLC セキュリティリスクの例

公益財団法人電気通信普及財団
研究調査助成報告書　第37号　2022年度

2-1 目的

この研究は、PLS 性能の制約要件を考慮した VLC システムのエネルギー効率を最適化することを目的としている．具体的には、Bob と Eves の信号対干渉電力と雑音比（Signal-to-interference-plus-noise ratio-SINRs）を機密性のパフォーマンスの尺度として使用し、本研究の最初の目的は、総送信電力を最小化するための AN 設計を研究することである． 送信機での Eves のチャネル状態情報（Channel State Information-CSI）の可用性に応じて、2 つの異なるアプローチが検討される．不明な Eves'CSI の場合、AN は Bob のチャネルの零空間上にあるように生成される． そうすることで、Bob を対象とした情報伝達信号に干渉することはないが、Eves のチャネルの品質を低下させる可能性がある． この設計では、AN サイズ（AN シンボルベクトルのサイズとして定義）と AN 調整電力パラメーターが合計送信電力と Eves の SINR に与える影響に関心がある． Eves の CSI が送信機でわかっている場合は、Eves の SINRs に特定の制約を課すことができるように、より適切な設計が調査される．さらに、ユーザーの CSI が送信機によって正確に推定されているという仮定は、実際にはかなり非現実的なので、チャネル推定の不確実性を考慮した堅牢な設計も検討する．

3 研究成果

A. ユーザーの CSI が送信機によって正確に推定されている場合

1. 送信機が Eves'CSI をわかっていない場合

多くの場合、Eves は受動的な悪意のあるユーザーであり、CSI を送信機にフィードバックしない。その結果、瞬間的な Eves の SINR に特定の制約要件を課すことは不可能である． ただし、AN の使用は、Bob の送信をできるだけ妨害せずに、Eves のチャネル品質を低下させる可能性があるため、依然として有益である。 簡単に言えば、N_t個 LED 送信機を持つ V L C シズテムのための設計問題は数学的に次のように定式化できる．

$$\begin{aligned} \mathcal{P}\mathbf{1}: \ \underset{\mathbf{v},\mathbf{W}}{\text{minimize}} \quad & \|\mathbf{v}\|_2^2 + \|\mathbf{W}\|_2^2 \\ \text{subject to} \quad & \mathrm{SINR}_0 \geq \gamma_0, \\ & \left|[\mathbf{v}]_n\right| + \left\|[\mathbf{W}]_{n,:}\right\|_1 \leq \Delta_n, \ \ n = 1, 2, ..., N_t. \end{aligned}$$

$\mathbf{v}$と$\mathbf{W}$はそれぞれ情報伝達信号プリコーダーと AN であり、$\mathbf{SINR_0}$は Bob の SINR である．さらに、γ_0は Bob の SINR の最小事前定義したしきい値であり、Δ_nは情報伝達信号と AN の振幅制約を表す定数である．AN の利点を活用するために、$\mathbf{W}$は Bob のチャネルベクトル$\mathbf{h}_0^T$の零空間上にある非ゼロ行列になるように選択される．具体的には、$\overline{\mathbf{W}}$を$\mathbb{R}^{N_t \times N_s}$行列とし、その$N_s$列は AN サイズと呼ばれ、$\mathbf{h}_0^T$の零空間の正規直交基底の$(N_t - 1)$ベクトルから選択され、$\mathbf{W}$は以下のように与えることができる．

$$\mathbf{W} = \rho \frac{\min\limits_n \Delta_n}{\max\limits_n \left\| [\overline{\mathbf{W}}]_{n,:} \right\|_1} \overline{\mathbf{W}},$$

ここで、$\rho \in (0, 1]$は、$\mathbf{W}$のパワーを制御する AN パワー調整パラメーターと呼ばれる．次に、$\mathbf{v}$は次のように設計される．

$$\begin{aligned} \mathcal{P}\mathbf{2}(\rho): \ \underset{\mathbf{v}}{\text{minimize}} \quad & \|\mathbf{v}\|_2^2 \\ \text{subject to} \quad & \frac{\left|\mathbf{h}_0^T \mathbf{v}\right|^2}{\tilde{\sigma}_0^2} \geq \gamma_0, \\ & \left|[\mathbf{v}]_n\right| \leq \Delta_n - \rho \frac{\min\limits_n \Delta_n}{\max\limits_n \left\| [\overline{\mathbf{W}}]_{n,:} \right\|_1} \left\| [\overline{\mathbf{W}}]_{n,:} \right\|_1, \ \ n = 1, 2, ..., N_t. \end{aligned}$$

2. 送信機が Eves'CSI をわかっている場合

K人の Eves がアクティブである（つまり、送信機が Eves の CSI を知っている）場合では、Eves の SINR に対する特定の制約を設計で考慮に入れることができるため、次の設計課題を検討する．

公益財団法人電気通信普及財団
研究調査助成報告書 第37号 2022年度

$$\mathcal{P}\mathbf{4}: \underset{\mathbf{v},\mathbf{W}}{\text{minimize}} \quad \|\mathbf{v}\|_2^2 + \|\mathbf{W}\|_2^2$$
$$\text{subject to} \quad \text{SINR}_0 \geq \gamma_0,$$
$$\text{SINR}_k \leq \gamma_k, \;\; k = 1, 2, ..., K,$$
$$\left|[\mathbf{v}]_n\right| + \left\|[\mathbf{W}]_{n,:}\right\|_1 \leq \Delta_n, \;\; n = 1, 2, ..., N_t.$$

SINR_kはk番目 Eve の SINR である．Bob の SINR 制約要件は、次のように凸型に変換できるが

$$\frac{1}{\gamma_0}\mathbf{h}_0^T\mathbf{v} \geq \sqrt{\left\|\mathbf{h}_0^T\mathbf{W}\right\|_2^2 + \tilde{\sigma}_0^2},$$

Eves の SINR に対する制約要件は当てはまらないので、上記の設計課題は一般的に取り組みが困難である．そのため、本研究では、計算コストがかかる可能性のある最適な解を見つけるのではなく、2 つの異なる準最適でありながら複雑性の低い解決アプローチを調査することを目的としている．具体的に、設計課題の解決に (Convex-Concave Procedure – CCP) [16]と (Semidefinite Relaxation – SDR) [17]の手法を使用することに焦点を当てている．

2.1 CCP

CCP は反復手順であり、収束が保証された一連の代理凸最適化問題を解決する．まず、Eves の SINR の制約条件は、次のように書き直す．

$$\frac{1}{\gamma_k}\left(\mathbf{h}_k^T\mathbf{v}\right)^2 \leq \left\|\mathbf{h}_k^T\mathbf{W}\right\|_2^2 + \tilde{\sigma}_k^2, \;\; k = 1, 2, ..., K,$$

次に、テイラー展開を使用して、右辺を凸項に近似する．具体的に、CCP の i 番目の反復では、次の下限が使用される．

$$\left\|\mathbf{h}_k^T\mathbf{W}^{(i-1)}\right\|_2^2 + 2\left[\mathbf{W}^{(i-1)}\right]^T\mathbf{h}_k\mathbf{h}_k^T\left(\mathbf{W}^{(i)} - \mathbf{W}^{(i-1)}\right) + \tilde{\sigma}_k^2 \leq \left\|\mathbf{h}_k^T\mathbf{W}^{(i)}\right\|_2^2 + \tilde{\sigma}_k^2, \;\; k = 1, 2, ..., K,$$

ここで、$\mathbf{W}^{(i-1)}$は前の反復から得られた最適解である．次に、以下の凸最適化問題のシーケンスを解くことにより、P4 の局所解を見つけることができる．

$$\mathcal{P}\mathbf{5}: \underset{\mathbf{v},\mathbf{W}^{(i)}}{\text{minimize}} \;\; \|\mathbf{v}\|_2^2 + \left\|\mathbf{W}^{(i)}\right\|_2^2$$
$$\text{subject to}$$
$$\frac{1}{\gamma_0}\mathbf{h}_0^T\mathbf{v} \geq \sqrt{\left\|\mathbf{h}_0^T\mathbf{W}^{(i)}\right\|_2^2 + \tilde{\sigma}_0^2},$$
$$\frac{1}{\gamma_k}\left(\mathbf{h}_k^T\mathbf{v}\right)^2 \leq \left\|\mathbf{h}_k^T\mathbf{W}^{(i-1)}\right\|_2^2 + 2\left[\mathbf{W}^{(i-1)}\right]^T\mathbf{h}_k\mathbf{h}_k^T\left(\mathbf{W}^{(i)} - \mathbf{W}^{(i-1)}\right) + \tilde{\sigma}_k^2, \;\; k = 1, 2, ..., K,$$
$$\left|[\mathbf{v}]_n\right| + \left\|\left[\mathbf{W}^{(i)}\right]_{n,:}\right\|_1 \leq \Delta_n, \;\; n = 1, 2, ..., N_t.$$

2.2 SDR

提示された CCP アプローチの欠点は、その反復性であり、収束点に到達するために多数の反復が必要になる場合がある．この問題に対処するために、SDR の使用について調査する． SDR は、二次制約の有無にかかわらず、非凸二次計画法を処理するための効率的な近似アプローチである．このテクニックを利用するために、P4 を次のように書き直してみましょう．

$$\mathcal{P}6: \quad \underset{\mathbf{v},\mathbf{W}}{\text{minimize}} \quad \text{Tr}\left(\mathbf{v}\mathbf{v}^T\right) + \text{Tr}\left(\mathbf{W}\mathbf{W}^T\right)$$
$$\text{subject to} \quad \frac{\mathbf{h}_0^T\mathbf{v}\mathbf{v}^T\mathbf{h}_0}{\mathbf{h}_0^T\mathbf{W}\mathbf{W}^T\mathbf{h}_0 + \tilde{\sigma}_0^2} \geq \gamma_0,$$
$$\frac{\mathbf{h}_k^T\mathbf{v}\mathbf{v}^T\mathbf{h}_k}{\mathbf{h}_k^T\mathbf{W}\mathbf{W}^T\mathbf{h}_k + \tilde{\sigma}_k^2} \leq \gamma_k, \;\; k = 1, 2, ..., K,$$
$$\left|[\mathbf{v}]_n\right| + \left\|[\mathbf{W}]_{n,:}\right\|_1 \leq \Delta_n, \;\; n = 1, 2, ..., N_t.$$

次に、新しい変数$\mathbf{V}=\mathbf{v}\mathbf{v}^T$及び$\widetilde{\mathbf{W}}=\mathbf{W}\mathbf{W}^T$を導入する．これらの変数変換は$\text{rank}(\mathbf{V})=1$と$\text{rank}\left(\widetilde{\mathbf{W}}\right)=\text{rank}(\mathbf{W})$と同等する．そして、上記の課題の三番目の条約要件を$\mathbf{V}$と$\mathbf{W}$で表すためには、以下の不等式を用いる．

$$\frac{\left(|[\mathbf{v}]_n|+\left\|[\mathbf{W}]_{n,:}\right\|_1\right)^2}{2}\leq[\mathbf{V}]_{n,n}+\left[\widetilde{\mathbf{W}}\right]_{n,n},\ \ n=1,2,...,N_t.$$

そのため、以下の問題はP5の上限の解を与える．

$$\begin{aligned}\mathcal{P}\mathbf{7}:\quad &\underset{\mathbf{V},\widetilde{\mathbf{W}}}{\text{minimize}} && \text{Tr}\left(\mathbf{V}\right)+\text{Tr}\left(\widetilde{\mathbf{W}}\right)\\ &\text{subject to} && \frac{\mathbf{h}_0^T\mathbf{V}\mathbf{h}_0}{\mathbf{h}_0^T\widetilde{\mathbf{W}}\mathbf{h}_0+\tilde{\sigma}_0^2}\geq\gamma_0,\\ & && \frac{\mathbf{h}_k^T\mathbf{V}\mathbf{h}_k}{\mathbf{h}_k^T\widetilde{\mathbf{W}}\mathbf{h}_k+\tilde{\sigma}_k^2}\leq\gamma_k,\ \ k=1,2,..,K,\\ & && \left[\mathbf{V}\right]_{n,n}+\left[\widetilde{\mathbf{W}}\right]_{n,n}\leq\frac{\Delta_n^2}{2},\ \ n=1,2,..,N_t,\\ & && \mathbf{V}\succeq\mathbf{0},\ \widetilde{\mathbf{W}}\succeq\mathbf{0},\\ & && \text{rank}\left(\mathbf{V}\right)=\ 1,\\ & && \text{rank}\left(\widetilde{\mathbf{W}}\right)=\text{rank}\left(\mathbf{W}\right),\end{aligned}$$

ただし、上記の問題の最後の２つの要約条件は凸状ではないので、それを省略して、以下の問題を検討する．

$$\begin{aligned}\mathcal{P}\mathbf{8}:\quad &\underset{\mathbf{V},\widetilde{\mathbf{W}}}{\text{minimize}} && \text{Tr}\left(\mathbf{V}\right)+\text{Tr}\left(\widetilde{\mathbf{W}}\right)\\ &\text{subject to} && \frac{\mathbf{h}_0^T\mathbf{V}\mathbf{h}_0}{\mathbf{h}_0^T\widetilde{\mathbf{W}}\mathbf{h}_0+\tilde{\sigma}_0^2}\geq\gamma_0,\\ & && \frac{\mathbf{h}_k^T\mathbf{V}\mathbf{h}_k}{\mathbf{h}_k^T\widetilde{\mathbf{W}}\mathbf{h}_k+\tilde{\sigma}_k^2}\leq\gamma_k,\ \ k=1,2,..,K,\\ & && \left[\mathbf{V}\right]_{n,n}+\left[\widetilde{\mathbf{W}}\right]_{n,n}\leq\frac{\Delta_n^2}{2},\ \ n=1,2,..,N_t,\\ & && \mathbf{V}\succeq\mathbf{0},\ \widetilde{\mathbf{W}}\succeq\mathbf{0},\end{aligned}$$

P8は半正定値計画法（Semidefinite Programming－SDP）であり、効率的に解ける．そして、P8 に対する最適な解$\mathbf{V}^*$と$\widetilde{\mathbf{W}}^*$が常に$\text{rank}(\mathbf{V}^*)=1$と$\text{rank}(\widetilde{\mathbf{W}})\leq1$を満たしていることを証明した。$\text{rank}\left(\widetilde{\mathbf{W}}\right)=0$の場合、$\widetilde{\mathbf{W}}=\mathbf{0}$と$\mathbf{W}=\mathbf{0}$となる．それは AN なしの設計と同等である．$\text{rank}\left(\widetilde{\mathbf{W}}\right)=1$の場合、最適な設計には AN サイズ$N_s=1$を選択するだけで十分であることを意味し、$\text{rank}\left(\widetilde{\mathbf{W}}\right)=\text{rank}(\mathbf{W})=1$につながる．従って、$\text{rank}\left(\widetilde{\mathbf{W}}\right)=\text{rank}(\mathbf{W})$は常に成立し、P7 とP8 が同等であることがわかった．

B. ユーザーの CSI が送信機によって不正確に推定されている場合

Bob と Eves の CSI が送信機で完全に知られているという仮定は、特に移動するユーザーの場合、かなり非現実的である．アップリンクとダウンリンクの相互関係を用いて送信機で CSI 推定を実行できる RF 通信とは異なり、VLC の場合の CSI は受信機で推定してから、RF 又は赤外線アップリンクを用いて送信機にフィードバックする必要がある．結果として、ユーザーの移動により、時代遅れの CSI 推定は避けらず、チャネルモデルの不確実性を考慮した堅牢な AN 設計が必要だと考えられる．

1. チャネルの不確実性モデル

以下のような相加的な不確実性を持つチャネルモデルを考慮する．

$$\mathbf{h}_k=\hat{\mathbf{h}}_k+\mathbf{u}_k,$$

ここで、$\hat{\mathbf{h}}_k$は実際のチャネル$\mathbf{h}_k$の推定値であり、$\mathbf{u}_k$は推定誤差ベクトルを表す．ユーザーの移動

によって引き起こされた古い CSI の場合、推定誤差は次のように制限される

$$\|\mathbf{u}_k\|_2 \le \delta_k,$$

δ_kは CSI 推定とフィードバックの間のチャネルゲインの最大変化に依存する．簡単にするために、$\delta_k = \alpha\|\hat{\mathbf{h}}_k\|_2$とし、$\alpha \in [0,1)$ は CSI の不確実性の大きさを測定する要素である．

2. 送信機が Eves' CSI をわかっていない場合

このシナリオでは、堅牢な設計は、最小の（つまり、最悪の場合の）Bob の SINR が特定のしきい値を超えていることを保証することを目的としている．最悪の場合の Bob の SINR は

$$\mathrm{SINR}_0^{\text{worst-case}} = \min_{\|\mathbf{u}_0\|_2\le\delta_0} \frac{\left|\left(\hat{\mathbf{h}}_0^T+\mathbf{u}_0^T\right)\mathbf{v}\right|^2}{\left(\rho\frac{\min\limits_n \Delta_n}{\max\limits_n \left\|[\overline{\mathbf{W}}]_{n,:}\right\|_1}\right)^2 \left\|\mathbf{u}_0^T\overline{\mathbf{W}}\right\|_2^2+\tilde{\sigma}_0^2} \ge \frac{\min\limits_{\|\mathbf{u}_0\|_2\le\delta_0}\left|\left(\hat{\mathbf{h}}_0^T+\mathbf{u}_0^T\right)\mathbf{v}\right|^2}{\left(\rho\frac{\min\limits_n \Delta_n}{\max\limits_n \left\|[\overline{\mathbf{W}}]_{n,:}\right\|_1}\right)^2 \max\limits_{\|\mathbf{u}_0\|_2\le\delta_0}\left\|\mathbf{u}_0^T\overline{\mathbf{W}}\right\|_2^2+\tilde{\sigma}_0^2}$$

によって与えられる．

次に、堅牢な AN 設計を次のように定式化できる．

$$\begin{aligned}
\mathcal{P}\mathbf{9}:\ \underset{\mathbf{v}}{\text{minimize}} \quad & \|\mathbf{v}\|_2^2 \\
\text{subject to} \quad & \frac{\min\limits_{\|\mathbf{u}_0\|_2\le\delta_0}\left|\left(\hat{\mathbf{h}}_0^T+\mathbf{u}_0^T\right)\mathbf{v}\right|^2}{\left(\rho\frac{\min\limits_n \Delta_n}{\max\limits_n \left\|[\overline{\mathbf{W}}]_{n,:}\right\|_1}\right)^2 \max\limits_{\|\mathbf{u}_0\|_2\le\delta_0}\left\|\mathbf{u}_0^T\overline{\mathbf{W}}\right\|_2^2+\tilde{\sigma}_0^2} \ge \gamma_0, \\
& \left|[\mathbf{v}]_n\right| \le \Delta_n - \rho\frac{\min\limits_n \Delta_n}{\max\limits_n \left\|[\overline{\mathbf{W}}]_{n,:}\right\|_1}\left\|[\overline{\mathbf{W}}]_{n,:}\right\|_1, \quad n=1,2,...,N_t.
\end{aligned}$$

上記の問題の 2 番目の制約条件は非凸のため、P9 は凸最適化の問題ではないことがわかった．それを凸状にするために、最初に、$\mathbf{V}_{\mathrm{rb}} = \mathbf{v}\mathbf{v}^T$を定義することにより、前述した SDR 手法を再び使用する．そして、S-Procedure[18]と$\mathrm{rank}(\mathbf{V}_{\mathrm{rb}}) = 1$の制約条件を省略することによって、P9 を次のように再定式化できる．

$$\begin{aligned}
\mathcal{P}\mathbf{10}:\ \underset{\substack{\mathbf{V}_{\mathrm{rb}},\tau_0,\omega_0,\\ \lambda_0,\xi_0}}{\text{minimize}} \quad & \mathrm{Tr}\left(\mathbf{V}_{\mathrm{rb}}\right) \\
\text{subject to} \quad & \\
& \begin{bmatrix} \lambda_0\mathbf{I}_{N_t}+\mathbf{V}_{\mathrm{rb}} & \mathbf{V}_{\mathrm{rb}}\hat{\mathbf{h}}_0 \\ \hat{\mathbf{h}}_0^T\mathbf{V}_{\mathrm{rb}} & -\lambda_0\delta_0^2+\hat{\mathbf{h}}_0^T\mathbf{V}_{\mathrm{rb}}\hat{\mathbf{h}}_0-\tau_0 \end{bmatrix} \succeq 0, \\
& \begin{bmatrix} \xi_0\mathbf{I}_{N_t}-\overline{\mathbf{W}}\,\overline{\mathbf{W}}^T & \mathbf{0}_{N_t} \\ \mathbf{0}_{N_t}^T & -\xi_0\delta_0^2+\omega_0 \end{bmatrix} \succeq 0, \\
& \mathbf{V}_{\mathrm{rb}} \succeq 0 \\
& [\mathbf{V}_{\mathrm{rb}}]_{n,n} \le \left(\Delta_n - \rho\frac{\min\limits_n \Delta_n}{\max\limits_n \left\|[\overline{\mathbf{W}}]_{n,:}\right\|_1}\left\|[\overline{\mathbf{W}}]_{n,:}\right\|_1\right)^2, \quad n=1,2,...,N_t, \\
& \tau_0 - \gamma_0\left(\left(\rho\frac{\min\limits_n \Delta_n}{\max\limits_n \left\|[\overline{\mathbf{W}}]_{n,:}\right\|_1}\right)^2\omega_0+\tilde{\sigma}_0^2\right) \ge 0, \\
& \lambda_0 \ge 0, \xi_0 \ge 0.
\end{aligned}$$

ここで、

$$\tau_0 = \min_{\|\mathbf{u}_0\|_2\le\delta_0}\left(\hat{\mathbf{h}}_0^T+\mathbf{u}_0^T\right)\mathbf{V}_{\mathrm{rb}}\left(\hat{\mathbf{h}}_0+\mathbf{u}_0\right)$$

$$\omega_0 = \max_{\|\mathbf{u}_0\|_2 \le \delta_0} \left\| \mathbf{u}_0^T \overline{\mathbf{W}} \right\|_2^2$$

を定義する.

次に、P10 の最適解$\mathbf{V}_{\mathrm{rb}}^*$が常に$\mathrm{rank}(\mathbf{V}_{\mathrm{rb}}^*) = 1$を満たすことを証明したので、P9 と P10 は同等であることがわかった.

3. **送信機が Eves' CSI をわかっている場合**

この場合、最悪の場合の Bob と Eves の SINR は次の式で与えられる.

$$\mathrm{SINR}_0^{\text{worst-case}} = \min_{\|\mathbf{u}_0\|_2 \le \delta_0} \frac{\left| \left(\hat{\mathbf{h}}_0^T + \mathbf{u}_0^T \right) \mathbf{v} \right|^2}{\left\| \left(\hat{\mathbf{h}}_0^T + \mathbf{u}_0^T \right) \mathbf{W} \right\|_2^2 + \tilde{\sigma}_0^2} \ge \frac{\min\limits_{\|\mathbf{u}_0\|_2 \le \delta_0} \left| \left(\hat{\mathbf{h}}_0^T + \mathbf{u}_0^T \right) \mathbf{v} \right|^2}{\max\limits_{\|\mathbf{u}_0\|_2 \le \delta_0} \left\| \left(\hat{\mathbf{h}}_0^T + \mathbf{u}_0^T \right) \mathbf{W} \right\|_2^2 + \tilde{\sigma}_0^2},$$

$$\mathrm{SINR}_k^{\text{worst-case}} = \max_{\|\mathbf{u}_k\|_2 \le \delta_k} \frac{\left| \left(\hat{\mathbf{h}}_k^T + \mathbf{u}_k^T \right) \mathbf{v} \right|^2}{\left\| \left(\hat{\mathbf{h}}_k^T + \mathbf{u}_k^T \right) \mathbf{W} \right\|_2^2 + \tilde{\sigma}_k^2} \le \frac{\max\limits_{\|\mathbf{u}_k\|_2 \le \delta_k} \left| \left(\hat{\mathbf{h}}_k^T + \mathbf{u}_k^T \right) \mathbf{v} \right|^2}{\min\limits_{\|\mathbf{u}_k\|_2 \le \delta_k} \left\| \left(\hat{\mathbf{h}}_k^T + \mathbf{u}_k^T \right) \mathbf{W} \right\|_2^2 + \tilde{\sigma}_k^2}, \quad k = 1, ..., K.$$

SDR 手法を用いて、$\mathbf{V}_{\mathrm{rb}} = \mathbf{v}\mathbf{v}^T$と$\widetilde{\mathbf{W}}_{rb} = \mathbf{W}\mathbf{W}^T$にする. そして、S-Procedure、$\mathrm{rank}(\mathbf{V}_{\mathrm{rb}}) = 1$と$\mathrm{rank}\left(\widetilde{\mathbf{W}}_{rb}\right) = \mathrm{rank}(\mathbf{W})$の制約条件を省略することによって、この場合の AN 設計は以下のように与えられる.

$$\begin{aligned}
\mathcal{P}\mathbf{11}: \ & \underset{\substack{\mathbf{V}_{\mathrm{rb}}, \widetilde{\mathbf{W}}_{\mathrm{rb}}, \\ \tau_0, \kappa_0, \lambda_0, \zeta_0 \\ \upsilon_k, \varphi_k, \varrho_k, \varsigma_k}}{\text{minimize}} \quad \mathrm{Tr}\left(\mathbf{V}_{\mathrm{rb}}\right) + \mathrm{Tr}\left(\widetilde{\mathbf{W}}_{\mathrm{rb}}\right) \\
& \text{subject to} \\
& \begin{bmatrix} \lambda_0 \mathbf{I}_{N_t} + \mathbf{V}_{\mathrm{rb}} & \mathbf{V}_{\mathrm{rb}} \hat{\mathbf{h}}_0 \\ \hat{\mathbf{h}}_0^T \mathbf{V}_{\mathrm{rb}} & -\lambda_0 \delta_0^2 + \hat{\mathbf{h}}_0^T \mathbf{V}_{\mathrm{rb}} \hat{\mathbf{h}}_0 - \tau_0 \end{bmatrix} \succeq 0, \\
& \begin{bmatrix} \zeta_0 \mathbf{I}_{N_t} - \widetilde{\mathbf{W}}_{\mathrm{rb}} & -\widetilde{\mathbf{W}}_{\mathrm{rb}} \hat{\mathbf{h}}_0 \\ -\hat{\mathbf{h}}_0^T \widetilde{\mathbf{W}}_{\mathrm{rb}} & -\zeta_0 \delta_0^2 - \hat{\mathbf{h}}_0^T \widetilde{\mathbf{W}}_{\mathrm{rb}} \hat{\mathbf{h}}_0 + \kappa_0 \end{bmatrix} \succeq 0, \\
& \begin{bmatrix} \varrho_k \mathbf{I}_{N_t} + \widetilde{\mathbf{W}}_{\mathrm{rb}} & \widetilde{\mathbf{W}}_{\mathrm{rb}} \hat{\mathbf{h}}_k \\ \hat{\mathbf{h}}_k^T \widetilde{\mathbf{W}}_{\mathrm{rb}} & -\varrho_k \delta_k^2 + \hat{\mathbf{h}}_k^T \widetilde{\mathbf{W}}_{\mathrm{rb}} \hat{\mathbf{h}}_k - \upsilon_k \end{bmatrix} \succeq 0, \quad k = 1, 2, ..., K, \\
& \begin{bmatrix} \varsigma_k \mathbf{I}_{N_t} - \mathbf{V}_{\mathrm{rb}} & -\mathbf{V}_{\mathrm{rb}} \hat{\mathbf{h}}_k \\ -\hat{\mathbf{h}}_k^T \mathbf{V}_{\mathrm{rb}} & -\varsigma_k \delta_k^2 - \hat{\mathbf{h}}_k^T \mathbf{V}_{\mathrm{rb}} \hat{\mathbf{h}}_k + \varphi_k \end{bmatrix} \succeq 0, \quad k = 1, 2, ..., K, \\
& \mathbf{V}_{\mathrm{rb}} \succeq 0, \widetilde{\mathbf{W}}_{\mathrm{rb}} \succeq 0, \\
& \left[\mathbf{V}_{\mathrm{rb}}\right]_{n,n} + \left[\widetilde{\mathbf{W}}_{\mathrm{rb}}\right]_{n,n} \le \frac{\Delta_n^2}{2}, \quad n = 1, 2, ..., N_t, \\
& \tau_0 - \gamma_0(\kappa_0 + \tilde{\sigma}_0^2) \ge 0, \\
& -\varphi_k + \gamma_k(\upsilon_k + \tilde{\sigma}_k^2) \ge 0, \quad k = 1, 2, ..., K, \\
& \lambda_0 \ge 0, \zeta_0 \ge 0, \varrho_k \ge 0, \varsigma_k \ge 0.
\end{aligned}$$

ここで、

$$\kappa_0 = \max_{\|\mathbf{u}_0\|_2 \le \delta_0} \left(\hat{\mathbf{h}}_0^T + \mathbf{u}_0^T \right) \widetilde{\mathbf{W}}_{\mathrm{rb}} \left(\hat{\mathbf{h}}_0 + \mathbf{u}_0 \right)$$

$$\upsilon_k = \min_{\|\mathbf{u}_k\|_2 \le \delta_k} \left(\hat{\mathbf{h}}_k^T + \mathbf{u}_k^T \right) \widetilde{\mathbf{W}}_{\mathrm{rb}} \left(\hat{\mathbf{h}}_k + \mathbf{u}_k \right)$$

$$\varphi_k = \max_{\|\mathbf{u}_k\|_2 \le \delta_k} \left(\hat{\mathbf{h}}_k^T + \mathbf{u}_k^T \right) \mathbf{V}_{\mathrm{rb}} \left(\hat{\mathbf{h}}_k + \mathbf{u}_k \right)$$

を定義する. 最後に、P11 の最適解$\mathbf{V}_{\mathrm{rb}}^*$と$\widetilde{\mathbf{W}}_{\mathrm{rb}}^*$が$\mathrm{rank}(\mathbf{V}_{\mathrm{rb}}^*) = 1$と$\mathrm{rank}\left(\widetilde{\mathbf{W}}_{\mathrm{rb}}^*\right) \le 1$を満たすことを証明した.

C. シミュレーション結果

シミュレーションのため、LED 照明器具の数は$N_t = 4$、各 LED 照明器具の平均光パワーは 35dBm に設定されている．これは 3.16 ワットにほぼ相当する．さらに、すべてのシミュレーションは、Bob と Eves の 10,000 のランダムに分散された位置による結果を平均することによって取得される．

1. 送信機が Eves' CSI をわかっていない場合

図 2 には、さまざまな AN サイズを考慮してρに関する合計送信電力と Eves の SINR が示されている．Bob の SINR のしきい値は$\gamma_0 = 30$dB に設定されている．正確な CSI 設計と不確実な CSI 設計の結果が比較され、不確実性の大きさ$\alpha = 0.01$が選択されている．正確な CSI 設計の場合、Bob の SINR はγ_0に等しくなる．ただし、これは、ρが増加するにつれて Bob の SINR が増加する堅牢な設計の場合には当てはまらない．Bob の SINR のこれらの望ましくない増加は、CSI が不確実な場合に、より高い送信電力をもたらす．両方の設計で AN を使用すると、Bob と Eve の SINR の間に大きなギャップが生じる可能性があることがわかった．具体的には、ρ=0.1 とN_s =1, 2, 3 の場合、これらはそれぞれ約 15、20、および 21dB である．

Eves の SINR は、N_s又はρのいずれかを増やすことで低下する可能性があるが、AN サイズを増やす方が有益である可能性があることに気付くことができる．たとえば、正確な CSI 設計の場合、Eves の SINR を 0dB でターゲットにするには、N_s = 1、2、および 3 に対してそれぞれρ=0.75、0.35、および 0.3 が必要である．これらのρの値により、送信電力は 41.14、37、36.53dBm になる．これは、ρが AN 振幅に与える影響が乗法的であるのに対し、AN サイズの場合は加法的であるためである．結果として、ρの増加によるプリコーダー$\mathbf{v}$の選択の自由度の低下は、AN サイズの増加によって引き起こされるものよりも深刻である．

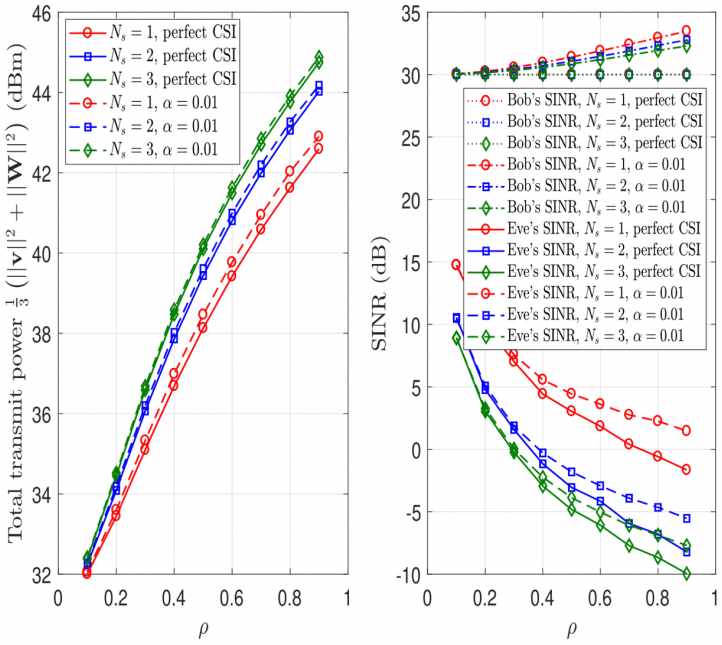

図 2：総送信電力対ρ

2. 送信機が Eves' CSI をわかっている場合

さまざまな数の Eves に対する総送信電力と Bob の SINR しきい値の関係を図 3 に示す．Eves の SINR のしきい値は、$\gamma_k = 0$dB に設定されている．AN を使用しない設計よりも、AN を使用した設計の利点を確認した．たとえば、γ_0 =30 dB で正確な CSI の場合、AN の使用による省電力は K=1、2 の場合にそれぞれ 3.16dB と 4dB である．さらに、チャネルの不確実性によって引き起こされる電力ペナルティは、γ_0に対して増加することがわかった．また、CCP と SDR 手法は K = 1 の場合に同じ解を提供するが、CCP は K=2 の場合に送信電力を少し高くする．これは、K が増加すると CCP が返した解の品質が低下していることを意味すると考える．

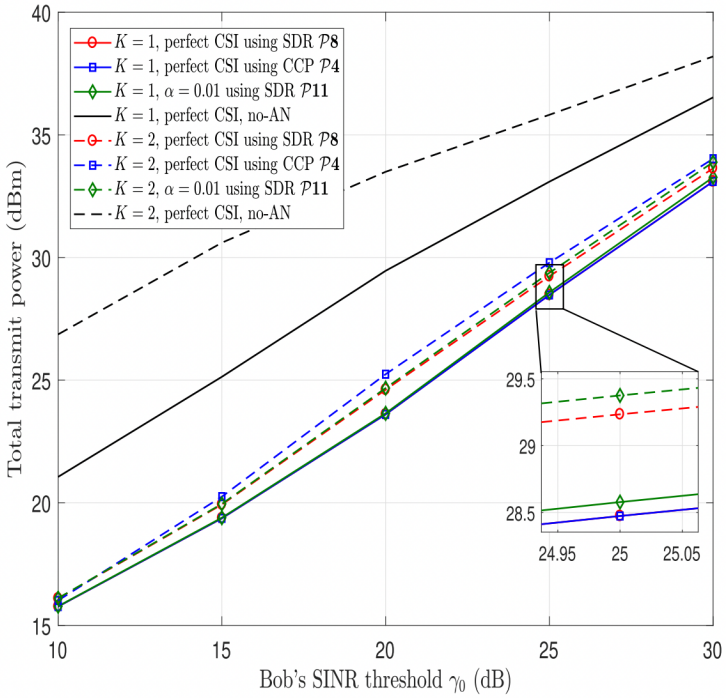

図 3：総送信電力対 Bob の SINR の閾値

【参考文献】

[1] Cisco Systems Inc., Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2017-2022 White Paper. [Online]. Available: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.html

[2] A. Jovicic, J. Li, and T. Richardson, "Visible light communication: Opportunities, challenges and the path to market," *IEEE Commun. Mag.*, vol. 51, no. 12, pp. 26-32, Dec. 2013.

[3] P. H. Pathak, X. Feng, P. Hu, and P. Mohapatra, "Visible light communication, networking, and sensing: A survey, potential and chal- lenges," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2047-2077, 4th Quart., 2015.

[4] L. Zeng et al., "High data rate multiple input multiple output (MIMO) optical wireless communications using white led lighting," *IEEE J. Sel. Areas Commun.*, vol. 27, no. 9, pp. 1654-1662, Dec. 2009.

[5] A. H. Azhar, T.-A. Tran, and D. O'Brien, "A gigabit/s indoor wireless transmission using MIMO-OFDM visible-light communications," *IEEE Photon. Technol. Lett.*, vol. 25, no. 2, pp. 171-174, Jan. 2013.

[6] D. Tsonev et al., "A 3-Gb/s single-LED OFDM-based wireless VLC link using a gallium nitride μLED," *IEEE Photon. Technol. Lett.*, vol. 26, no. 7, pp. 637-640, Apr. 2014.

[7] A. Nuwanpriya, S.-W. Ho, and C. S. Chen, "Indoor MIMO visible light communications: Novel angle diversity receivers for mobile users," *IEEE J. Sel. Areas Commun.*, vol. 33, no. 9, pp. 1780-1792, Sep. 2015.

[8] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355-1387, Oct. 1975.

[9] M. A. Arfaoui *et al.*, "Physical Layer Security for Visible Light Communication Systems: A Survey," in *IEEE Commun. Surv. Tutor.*, vol. 22, no. 3, pp. 1887-1908, thirdquarter 2020.

[10] Cho, S.; Chen, G.; Coon, J.P.; Xiao, P. “Challenges in Physical Layer Security for Visible Light Communication Systems”, *Network*, 2, pp. 53-65, 2022.
[11] J.-Y. Wang, C. Liu, J.-B. Wang, Y. Wu, M. Lin, and J. Cheng, “Physical- layer security for indoor visible light communications: Secrecy capacity analysis,” *IEEE Trans. Commun.*, vol. 66, no. 12, pp. 6423-6436, Dec. 2018.
[12] A. Mostafa and L. Lampe, “Optimal and robust beamforming for secure transmission in MISO visible-light communication links,” *IEEE Trans. Signal Process.*, vol. 64, no. 24, pp. 6501-6516, Dec. 2016.
[13] S. Ma, Z.-L. Dong, H. Li, Z. Lu, and S. Li, “Optimal and robust secure beamformer for indoor MISO visible light communication,” *J. Lightw. Technol.*, vol. 34, no. 21, pp. 4988-4998, Nov. 1, 2016.
[14] T. V. Pham and A. T. Pham, “Secrecy sum-rate of multi-user MISO visible light communication systems with confidential messages,” *Optik*, vol. 151, pp. 65-76, Dec. 2017.
[15] M. A. Arfaoui, A. Ghrayeb, and C. M. Assi, “Secrecy performance of multi-user MISO VLC broadcast channels with confidential mes- sages,” *IEEE Trans. Wireless Commun.*, vol. 17, no. 11, pp. 7789-7800, Nov. 2018.
[16] A. L. Yuille and A. Rangarajan, “The concave-convex procedure (CCCP),” *Neural Comput.*, vol. 15, no. 4, pp. 915-936, Apr. 2003.
[17] Z.-Q. Luo, W.-K. Ma, A. So, Y. Ye, and S. Zhang, “Semidefinite relaxation of quadratic optimization problems,” *IEEE Signal Process. Mag.*, vol. 27, no. 3, pp. 20-34, May 2010.
[18] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
Energy Efficient Artificial Noise-Aided Precoding Designs for Secured Visible Light Communication Systems	IEEE Transactions on Wireless Communications	1月 2021年
Energy-Efficient Precoding for Multi-User Visible Light Communication with Confidential Messages	2021 IEEE 93rd Vehicular Technology Conference (VTC2021-Spring)	4月 2021年
Energy-Efficient Friendly Jamming for Physical Layer Security in Visible Light Communication	2021 IEEE International Conference on Communications Workshops (ICC Workshops)	6月 2021年
Energy-Efficient Precoding Designs for Multi-User Visible Light Communication Systems with Confidential Messages	IEEE Transactions on Green Communications and Networking	12月 2021年