第 35 回助成研究完了報告書

西暦　2024 年　4　月 20　日

一般財団法人 東海産業技術振興財団　御中

申込者の所属機関・
学部名・職名・氏名　静岡大学・工学部・助教・PHAM VAN THANH
又は団体・代表者名　　印
住所又は所在地　（〒432-8018）静岡県浜松市中区蜆塚４－１－１０
ビューしじみの森２C

連絡責任者氏名
電　話 090-9220-9562

一般財団法人 東海産業技術振興財団の西暦 2023 年度採択の助成による研究調査を下記のとおり実施しましたので、報告します。

記

テーマと研究期間

テ　ー　マ	可視光通信における物理層セキュリティ改善のための強化学習を用いた最適な適応変調方式の設計
研究期間　西暦	２０２３　年　４月　～　２０２４　年　３月

研究実績の概要

1. はじめに

従来の暗号化と比較して、盗聴者に対する情報の機密性を保証する強力なアプローチを提供する物理層セキュリティ（Physical Layer Security - PLS）への関心が高まっている［１］。本研究では、可視光通信（Visible Light Communications）チャネルの秘密レートとビット誤り率（Bit-error rate - BER）を最適化することを目的とした M 値適応多値パルス振幅変調(M-PAM)とプリコーディングの共同設計を研究する。具体的には、提案された設計は正規ユーザー（i.e., Bob）のチャネルの通信の信頼性と盗聴者（i.e., Eve）のチャネルの通信の信頼性の低さをそれぞれ保証しながら、多値パルス振幅変調 M-PAM の秘密レートを最大化することを目的としている。この目的のために、VLC 信号の振幅の制約を考慮した M-PAM の機密性、Bob および Eve のチャネルの BER の間のトレードオフを捉える報酬関数が導入され、最大化される。ただし、このような最適化問題は PAM の秘密レートの非閉形式式と BER の複雑な非線形式のため、古典的な最適化手法を使用して解決するのは困難である。したがって、強化学習アプローチを用いて設計課題に取り組む。本研究の主な成果は次のとおりである。

a. VLC チャネルの適応 M-PAM 変調とプリコーディングの共同設計を提案した。提案した設計は秘密レートを向上させながら Bob のチャネルの信頼性を確保し同時に Eve のチャネルの信頼性を低下させる。
b. Q 学習と深層 Q 学習に基づいた強化学習アプローチを用いた変調次数と送信プリコーダーを共同最適化する。この目的のために、秘密レートや Bob と Eve のチャネルの BER を組み合わせた報酬関数が導入される。
c. M-PAM の正確な秘密レートの式は積分形式で導出されるが、これは特に変調次数が高い場合に計算コストが高くなる可能性がある。 これは提案した学習アプローチのトレーニング時間の増加に繋がる。 トレーニング時間を短縮するために、秘密レートの近似式を導出する。 その後、正確な式と近似式の間で精度と計算時間の比較を実施する。

2. 信号モデル

送信側では、**図 1** に示すように、入力ビットが M-PAM 変調器に入力されて、d で示されるバイポーラ PAM シンボルが生成される。n 番目の照明器具では、まずプリコーダ w_n を使用して PAM シンボルがプリコードされる。LED の入力信号は非負でなければならないため、DC バイアス電流 I_{DC} をプリコードされた信号に追加する必要がある。DC バイアスの追加は、LED の照明レベルを調整するためでもある(VLC システムの場合、依然として照明が主な目的であり、適切な照明設定の下で通信面のパフォーマンスを調査する必要があることに注意すべきである)。したがって、LED の駆動電流は次のように表される。

$$x_n = w_n d + I_{\mathrm{DC}}$$

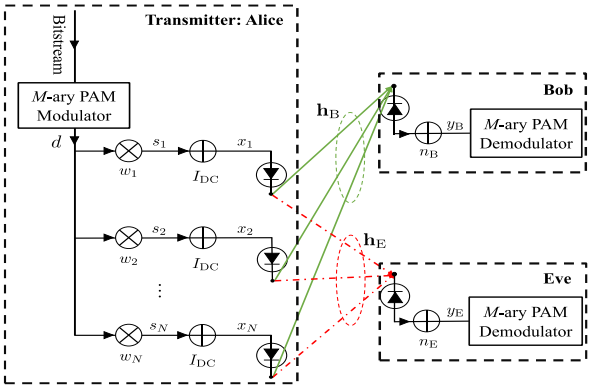


図 1．システムモデル

LED には、放射される光パワーが駆動電流の振幅に比例する特定の線形範囲があるので、この線形変換を維持するには（LED の適切な動作とエネルギー効率のため）、x_n を $I_{\mathrm{DC}} \pm \alpha I_{\mathrm{DC}}$ の範囲内に制限する必要がある。ここで、$\alpha \in [0,\ 1]$ は変調指数を示す。この制約を満たすには $|w_n| \le 1$ と $|d| \le \alpha I_{\mathrm{DC}}$ を課す必要がある。γ をフォトダイオード（PD）の応答性、η を LED の電気から光への変換効率として表すと、PD の出力の信号は次のように書き込まれる

$$\bar{y}_{\mathrm{R}} = \gamma\eta \mathbf{h}_{\mathrm{R}}^T \mathbf{w} d + n_{\mathrm{R}}$$

ここでは、$h_R^T = [h_R^1\ h_R^2 \dots h_R^N]^T$ はチャネルベクトルであり、$w = [w_1\ w_2 \dots w_N]^T$ は送信プリコーダである。また、n_{R} は分散 σ_R^2 を持つゼロ平均加算性白色ガウス雑音である。

3. 秘密レート

考慮されている盗聴チャネルの機密容量 C_s は、Bob のチャネル C_B と Eve のチャネル C_e の容量の差として与えられる。

$$C_s = [C_{\mathrm{B}} - C_{\mathrm{E}}]^+$$

ただし、$[x]^+ \triangleq \max(x, 0)$ である。また、C_B と C_e はチャネル入力 d とチャネル出力 $\bar{y}_{\mathrm{R}}$ 間の相互情報量として定義される。

$$\begin{aligned} C_{\mathrm{R}} &= I(d; \bar{y}_{\mathrm{R}}) = h(\bar{y}_{\mathrm{R}}) - h(\bar{y}_{\mathrm{R}}|d) = h(\bar{y}_{\mathrm{R}}) - h(n_{\mathrm{B}}) \\ &= -\int_{-\infty}^{+\infty} p(\bar{y}_{\mathrm{R}}) \log_2 p(\bar{y}_{\mathrm{R}}) \mathrm{d}\bar{y}_{\mathrm{R}} - \frac{1}{2}\log_2\left(\pi e \sigma_{\mathrm{R}}^2\right) \end{aligned}$$

$d_i\ (i = 0, 1, \dots, M-1)$ を PAM コンスタレーションの M 個シンボルとし、すべてのシンボルが等しい確率で送信されると仮定する（つまり、$p(d_i) = \frac{1}{M}, \forall i$）。また、$n_{\mathrm{R}}$ はゼロ平均と分散 σ_{R}^2 のガウス分布であるため、$p(\bar{y}_{\mathrm{R}})$ は以下のように与えられる。

$$\begin{aligned} p(\bar{y}_{\mathrm{R}}) &= \sum_{i=0}^{M-1} p(\bar{y}_{\mathrm{R}}|d = d_i) p(d_i) \\ &= \frac{1}{M} \sum_{i=0}^{M-1} \frac{1}{\sqrt{2\pi}\sigma_{\mathrm{R}}} \exp\left(-\frac{\left|\bar{y}_{\mathrm{R}} - \gamma\eta \mathbf{h}_{\mathrm{R}}^T \mathbf{w} d_i\right|^2}{2\sigma_{\mathrm{R}}^2}\right) \end{aligned}$$

上記の分析から、秘密レートの計算には、2 つの積分演算が含まれることがわかるが、これは一般に計算量が多いと考えられる。その結果、強化学習アルゴリズムは収束するまでに多数の反復が必要となるため、上記の秘密レートの正確な式を使用すると、長いトレーニング時間がかかる可能性がある。トレーニング時間を短縮するために、積分を必要としない秘密レートの近似式を提案する。この目的のために、$p(\bar{y}_{\mathrm{R}})$ は次のように書き換えられる。

$$p(\bar{y}_{\mathrm{R}}) = \frac{1}{M} \sum_{i=0}^{M-1} \mathcal{N}(\bar{y}_{\mathrm{R}}, \mu_i, \sigma_{\mathrm{R}})$$

ここでは、$\mu_i = \gamma\eta \mathbf{h}_{\mathrm{R}}^T \mathbf{w} d$ であり、$\mathcal{N}(x, \mu, \sigma)$ は平均 μ と標準偏差 σ をもつガウス変数 x の確率密度関数(PDF)を示す。$p(\bar{y}_{\mathrm{R}})$ の対数のテイラー展開は次のようになる。

$$\log_2 p(\bar{y}_\mathrm{R}) = \sum_{k=0}^{\infty} \frac{1}{k!} (\bar{y}_\mathrm{R} - \mu_i)^k \frac{d^k \log_2 p(\bar{y}_\mathrm{R})}{d\bar{y}_\mathrm{R}{}^k} \Big|_{\bar{y}_\mathrm{R}=\mu_i}$$

上記の式を用いて、$h(\bar{y}_\mathrm{R})$ は次のように書くことができる。

$$h(\bar{y}_\mathrm{R}) = \frac{-1}{M} \sum_{i=0}^{M-1} \int_{-\infty}^{+\infty} \mathcal{N}(\bar{y}_\mathrm{R}, \mu_i, \sigma_R) \times \left(\sum_{k=0}^{\infty} \frac{1}{k!} (\bar{y}_\mathrm{R} - \mu_i)^k \frac{d^k \log_2 p(\bar{y}_\mathrm{R})}{d\bar{y}_\mathrm{R}{}^k} \Big|_{\bar{y}_\mathrm{R}=\mu_i} \right) \mathrm{d}\bar{y}_\mathrm{R}$$

$$= \frac{-1}{M} \sum_{i=0}^{M-1} \sum_{k=0}^{\infty} \frac{\rho_{i,k}}{k!} \frac{d^k \log_2 p(\bar{y}_\mathrm{R})}{d\bar{y}_\mathrm{R}{}^k} \Big|_{\bar{y}_\mathrm{R}=\mu_i}$$

ただし、$\rho_{i,k}$はガウスのk番目の中心モーメントであり、次の式で与えられる。

$$\rho_{i,k} = \begin{cases} 0 & \text{if } n \text{ is odd} \\ \sigma_\mathrm{R}^k (k-1)!! & \text{if } n \text{ is even,} \end{cases}$$

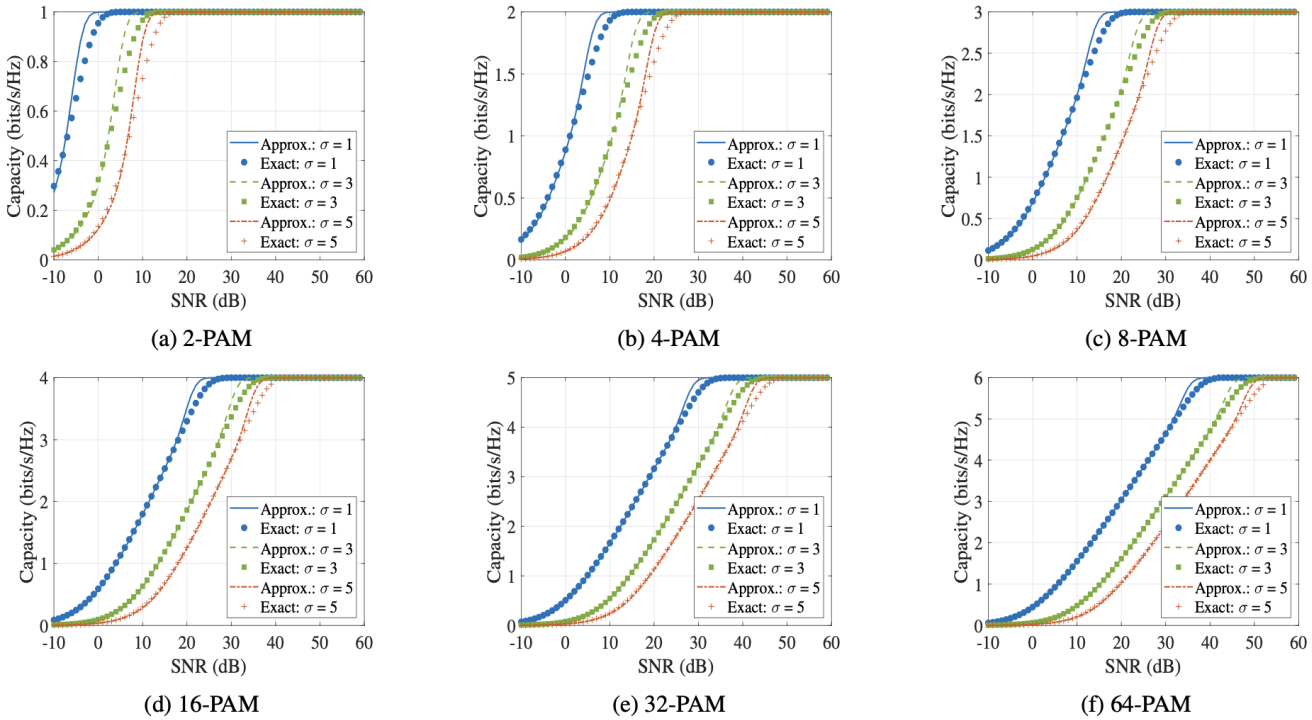
上記の無限和の最初の 3 つの項を使用すると、近似値は次のように求められる。

$$h(\bar{y}_\mathrm{R}) \approx \frac{-1}{M} \sum_{i=0}^{M-1} \sum_{k=0}^{2} \frac{\rho_{i,k}}{k!} \frac{d^k \log_2 p(\bar{y}_\mathrm{R})}{d\bar{y}_\mathrm{R}{}^k} \Big|_{\bar{y}_\mathrm{R}=\mu_i}$$

また、$\rho_{i,0} = 1$, $\rho_{i,1} = 0$と $\rho_{i,2} = \sigma_\mathrm{R}^2$であるため、上記の式は以下のようになる。

$$h(\bar{y}_\mathrm{R}) \approx \frac{-1}{M} \sum_{i=0}^{M-1} \left(\log_2 p(\mu_i) + \frac{\sigma_\mathrm{R}^2}{2} \frac{d^k \log_2 p(\bar{y}_\mathrm{R})}{d\bar{y}_\mathrm{R}{}^k} \Big|_{\bar{y}_\mathrm{R}=\mu_i} \right)$$

提示された近似式の精度は、信号対雑音比(SNR)の広い範囲にわたるさまざまな変調次数と雑音の電力に対して**図 2** に数値的に示されている。近似値が正確な値と十分に一致していることが観察される。



(a) 2-PAM　(b) 4-PAM　(c) 8-PAM

(d) 16-PAM　(e) 32-PAM　(f) 64-PAM

図 2. 正確な式と近似式との比較

また、近似式と正確な式の計算の複雑さに関する比較も**表 1** にまとめられている。ここでは、SNR = 20dB およびσ_R=3 での 100 回の評価にわたる実行時間の平均が示されている。計算は Intel® Xeon® プロセッサー 2.30GHz と 12GB RAM を搭載した Windows11 デスクトップ コンピューターで実装した。近似式の計算時間は正

確な式の実行時間よりも大幅に高速であることが明確に示されている。

Modulation order M / Execution time, (seconds)	2	4	8	16	32	64
Approximate expression in (20)	0.06	0.26	0.53	1.79	6.70	24.87
Exact expression in (10)	0.89	0.95	3.07	4.91	13.91	30.32

表 1. 正確な式と近似式の計算時間（秒）

4. ビット誤り率

グレイコーディングを仮定すると、M-PAM の BER は次のように求められる［2］。

$$p_{\mathrm{e,R}}=\sum_{k=1}^{\log_2 M}\sum_{i=0}^{M(1-2^{-k})-1}(-1)^{\left\lfloor \frac{i2^{k-1}}{M}\right\rfloor}\left(2^{k-1}-\left\lfloor\frac{i2^{k-1}}{M}+\frac{1}{2}\right\rfloor\right)\times\frac{1}{M\log_2 M}\mathrm{erfc}\left((2i+1)\sqrt{\frac{3\left(\gamma\eta\mathbf{h}_{\mathrm{R}}^{T}\mathbf{w}/\sigma_{\mathrm{R}}\right)^{2}E_s}{M^2-1}}\right)$$

5. 提案共同設計

本研究は Bob のチャネルの信頼性を保証し、Eve のチャネルの信頼性を低下させながら秘密レートを最大化する適応変調とプリコーディングの共同設計を目的としている。変調次数を増やすと秘密保持能力が向上することが示されている［3］。それにもかかわらず、変調が高くなると、（シンボル間の距離が短くなるために）シンボルがノイズの影響を受けやすくなり、その結果、BER が高くなり、したがって信頼性が低下する。一方で、以前の研究では、プリコーディング設計により秘密レートが向上することも示されていが、チャネルの信頼性の問題を考慮しなかった。主な理由としては、BER の式が多くの場合非線形、非凸で、非常に複雑であるためである。秘密レートとチャネル信頼性に対する変調次数の対照的な影響、および BER の式の非凸性と高度な複雑さのため、提案した共同設計は古典的な最適化手法を使用して明示的に解決できないと考えられる。厳密な数学的解決の難しさは機械学習ベースの技術の使用を調査する動機になり、特に、本研究では Q 学習と深層 Q 学習に基づく強化学習(RL)アプローチを考慮する。

a. Q 学習に基づいた共同設計

Q 学習は報酬関数を最大化することで環境と対話するエージェントに最適な行動ポリシーを達成することを目的としたモデルフリーの強化学習アルゴリズムである。提案共同設計の文脈では、エージェント、環境、状態、アクション、および報酬関数が次のように指定される。

1) **エージェント**: 変調次数 M とプリコーダ**w**の最適化を担当する送信機の中央処理装置(CPU)である。
2) **環境**: CPU を除くシステム全体である。たとえば、LED 照明器具の光パワー、Bob と Eve の位置、Bob と Eve のチャネルの BER である。
3) **状態**: エージェントが適切なアクションを選択するための入力となる、システムのパラメーターのサブセットである。 特に提案共同設計では、状態**s**は、前の状態での Bob と Eve のチャネルの BER と、現在の状態での Bob と Eve のチャネルの CSI で構成される。 また、Λをすべての可能な状態のセットとする。
4) **アクション**: a で示されるアクションは変調次数 M とプリコーダー**w**の選択である。さらに、$\mathbb{A}$をすべての可能なアクションのセットとする。
5) **報酬関数**: 通信チャネルの信頼性は BER パフォーマンスによって判定されるため、秘密レート、Bob と Eve のチャネルの BER を取得する以下のようなの報酬関数を考慮する。

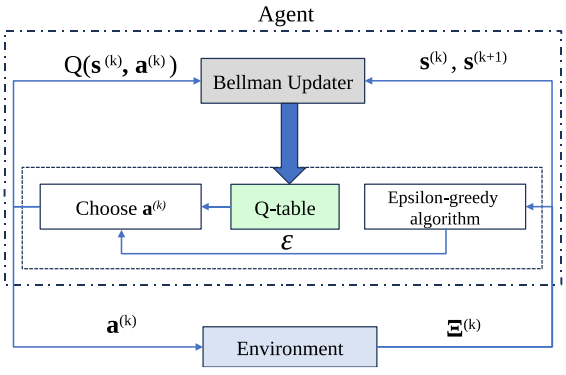


図 3. 提案 Q 学習に基づいた共同設計

$$u=C_s-\delta p_{e,\mathrm{B}}+\zeta p_{e,\mathrm{E}}$$

ここでは、δとζはそれぞれ Bob と Eve のチャネルの BER の報酬値への寄与に影響を与える選択された係数である。

提案した Q 学習に基づいた共同設計の全体的な概略図は**図 3** に示されている。ここでは、状態とアクションのペアの値を保存するために Q テーブルが使用される。

b.　深層 Q 学習に基づいた共同設計

前のセクションで提案した Q 学習に基づいた共同設計では、有限のアクション空間が必要である。この要件を達成するために、プリコーダ**w**が離散値に量子化され、アクションポリシーが最適化されなくなった。 量子化解像度を増やすことで、より良いアクションポリシーを実現できるが、これによりトレーニング時間も増加する。この問題に対処するために、actor-critic のネットワークフレームワークを利用して継続的なアクション空間に取り組む深層 Q 学習モデルを用いる。

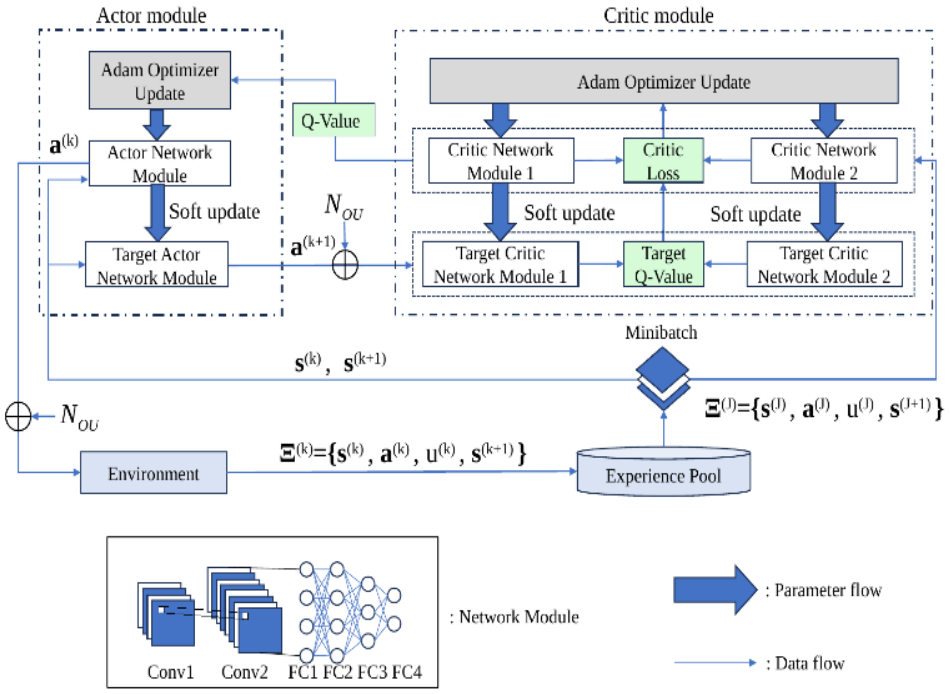


図 4.　提案深層 Q 学習に基づいた共同設計

図 4 に示すように、すべてのネットワークモジュールは、2 つの畳み込みニューラルネットワーク(CNN)と 4 つの完全接続(FC)層で構成される同じアーキテクチャを持っている。 この構成は設計課題の多次元の性質に関連する特定の目的に役立つ。通常のニューラルネットワークはデータを順次処理できるが、空間データの処理には制限があるが、CNN は Bob と Eve の位置によって影響を受けるデータポイント間の空間階層と関係を効率的にキャプチャできる。

6.　シミュレーション結果と観察

提案共同設計の有効性がシミュレーション結果を通じて示されている。床の中心を原点とする 3D デカルト座標系を使用して、LED 照明器具、Bob と Eve の位置を指定する。 部屋の寸法は$d_L \times d_W \times d_H$として示され、床に対する受信機の高さは$d_R$として設定される。**図 5** は有線接続を介して中央処理装置(CPU)に接続された 4 つの LED 照明器具がある部屋の一般的なレイアウトを示している。

提案共同設計の有効性を強調するために、以下で説明する 4 つの異なるベースラインを比較する。

1) **ベースライン 1**：変調は最低次の 2-PAM に固定される。 このベースライン設計は秘密レートの低下を犠牲にして、低い BER(つまり、高いチャネル信頼性)を優先する。
2) **ベースライン 2**：変調は高次の 64-PAM に固定される。 **ベースライン 1** とは対照的に、このベ

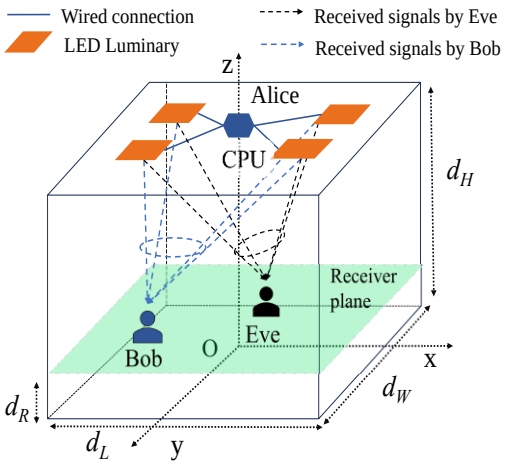


図 5.　システム構成

ースラインは、高い BER(つまり、低いチャネル信頼性）を犠牲にして、高い秘密レートを実現することを目的としている。

3) **ベースライン 3**：プリコーダ$\mathbf{w}$は$\mathbf{h}_E^T$のヌル空間上にあることにする（つまり、$\mathbf{h}_E^T\mathbf{w}=0$)。 このベースラインの設計原則は、Eve が信号を受信できないようにすることである。したがって、秘密レートは Bob のチャネルの容量になる。

4) **ベースライン 4**:提案共同設計を変調に依存しない下限秘密容量式[4]で与えられる）と近似 4PAM BER 式が使用された［5］で提案した共同設計と比較する。

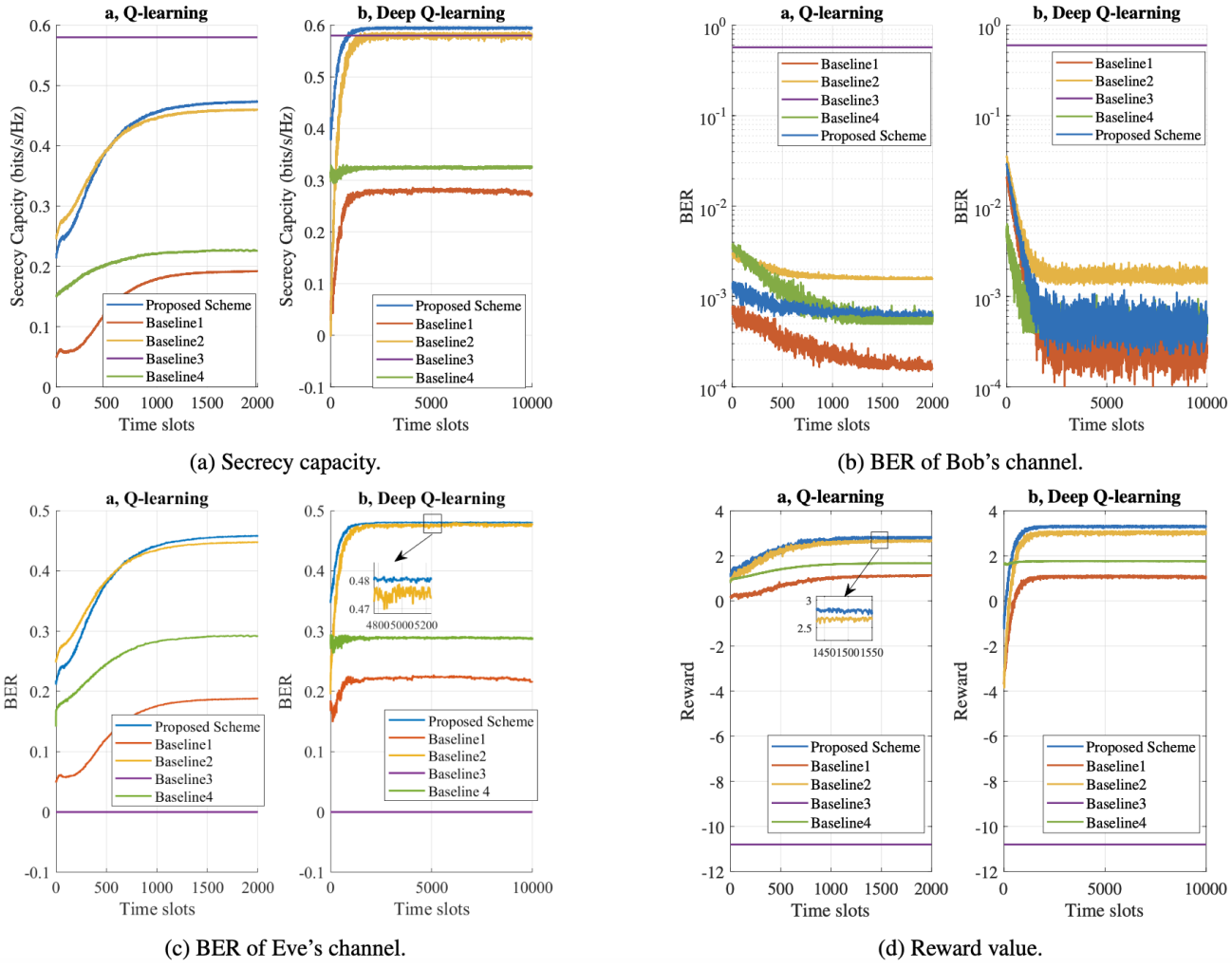


図 6. 提案共同設計とベースラインの比較

秘密レート、Bob と Eve のチャネルの BER、報酬のパフォーマンスをそれぞれ**図 6a**，**6b**，**6c**，**6d** に示す。ここでは、Q 学習と深層 Q 学習に基づいたアプローチの比較も示されている。秘密レートに関しては、提案した真相 Q 学習に基づいた共同設計が最高のパフォーマンスを達成する。これは**ベースライン 1** 及び**ベースライン 4** の 2 倍であり、**ベースライン 2** および**ベースライン 3** のパフォーマンスよりわずかに優れている。ただし、Q 学習ベースの共同設計の場合、**ベースライン 3** のパフォーマンスは提案された共同設計のパフォーマンスよりもかなり優れているが Bob のチャネルの BER は非常に高くなった。 これは、FEC（Forward Error Correction）前の BER しきい値を大幅に上回っている。また、提案共同設計**ベースライン 1**、**2** 及び **4** がすべて、Bob のチャネルの FEC 前の BER しきい値を満たしていることが検証される （つまり、Bob のチャネルの BER は3.8×10^{-3}未満）。全体として、Bob と Eve のチャネルの機密性と BER を考慮すると、**図 6d** に表示される報酬値は、提案された共同設計が 4 つのベースラインよりも優れていることを明らかにした。

7. 参考文献

[1] M. A. Arfaoui, M. D. Soltani, I. Tavakkolnia, A. Ghrayeb, M. Safari, C. M. Assi, and H. Haas, “Physical layer security for visible light communication systems: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1887-1908, 2020.

[2] K. Cho and D. Yoon, “On the general ber expression of one- and two- dimensional amplitude modulations,” *IEEE Transactions on Communications*, vol. 50, no. 7, pp. 1074-1080, 2002.

[3] S. Rezaei Aghdam, A. Nooraiepour, and T. M. Duman, “An overview of physical layer security with finite-alphabet signaling,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1829-1850, 2019.

[4] A. Mostafa and L. Lampe, “Physical-layer security for MISO visible light communication channels,” *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 9, pp. 1806-1818, 2015.

[5] L. Xiao, G. Sheng, S. Liu, H. Dai, M. Peng, and J. Song, “Deep reinforcement learning-enabled secure visible light communication against eavesdropping,” *IEEE transactions on communications*, vol. 67, no. 10, pp. 6994-7005, 2019.

研究成果の発表　---　計画・形式等

1. Duc M. T. Hoang, Thanh V. Pham, Anh T. Pham, Chuyen T. Nguyen, “Q-learning-based Joint Design of Adaptive Modulation and Precoding for Physical Layer Security in Visible Light Communications,” in Proc. of *the 2023 IEEE 97th Vehicular Technology Conference: VTC2023-Spring*, Florence, Italy, June 2023.
2. Duc M. T. Hoang, Thanh V. Pham, Anh T. Pham, Chuyen T. Nguyen, “Joint Design of Adaptive Modulation and Precoding for Physical Layer Security in Visible Light Communications using Reinforcement Learning,” *IEEE Access* （審査中）, April 2024.