

xASK を用いるしきい値秘密分散法を融合する VN-CodeSK 照明光通信方式

VN-CodeSK Illumination Light Communications System Using Secret Sharing Scheme with xASK

谷田 潤哉¹
Junya Yada

羽瀨 裕真¹
Hiromasa Habuchi

茨城大学工学部情報工学科¹

Department of Computer and Information Science, College of Engineering, Ibaraki University

1 まえがき

照明光通信において照明機能を維持しつつ通信を行う方式として、可変 N 並列符号多値変調法 (VN-CodeSK) が提案されている [1]。また照明光が重なるエリアでの情報量を増加させるために、VN-CodeSK 方式に (2,2) しきい値秘密分散 (VSS) 法 [2] の考え方を取り入れる拡張 VN-CodeSK 方式が提案されている [3]。しかし、この方式では、VSS の Share が "0" のとき VN-CodeSK データ伝送が行われなため、CodeSK データの情報伝送速度は [1] の方式の 1/2 になってしまう。

本稿では、xASK により 0.1 を表現する (2,2) しきい値秘密分散法を VN-CodeSK 方式に融合させることで、VSS による情報伝送速度の劣化を防ぐ方式を提案する。

2 システム構成

図 1 に提案方式のシステムモデルを示す。本システムでは、CodeSK データの信号強度は "0", "1" でなく、"x" ($0 \leq x < 1$), "1" とする。

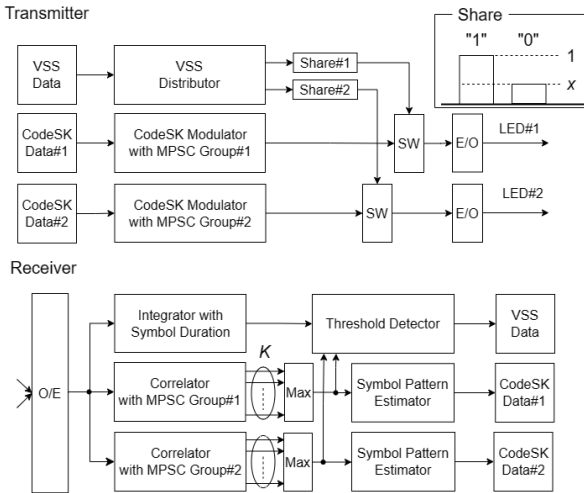


図 1: システムモデル

送信機側では、2 値の VSS データから (2,2) VSS の原理により、2 個の Share を生成する。VSS データが "0" の場合は、(Share#1, Share#2) = (x, x), (1, 1) をランダムに選択する。VSS データが "1" の場合は、(Share#1, Share#2) = (x, 1), (1, x) をランダムに選択する。CodeSK データは、それぞれ割り当てられた MPSC をもとに生成する。

受信機側では、CodeSK データと VSS データをそれぞれ復号する。CodeSK データ復号器では、受信信号と割り当てられた K 個の MPSC との相関値から、N 個の大きい

相関値を求め、その組み合わせにより CodeSK データを復調する。VSS データ復号器では、受信信号を 1 シンボル区間積分した値 V を 2 個のしきい値 ($Th_1 < Th_2$) と比較し、VSS データを復号する。 $Th_1 > V$ または $Th_2 \leq V$ の場合、VSS データは "0" と推定され、 $Th_1 \leq V < Th_2$ の場合、VSS データは "1" と推定される。

3 性能評価

図 2 に提案方式の情報伝送速度 (η_p) と従来方式の情報伝送速度 (η_c) の比 (η_p/η_c) を示す。

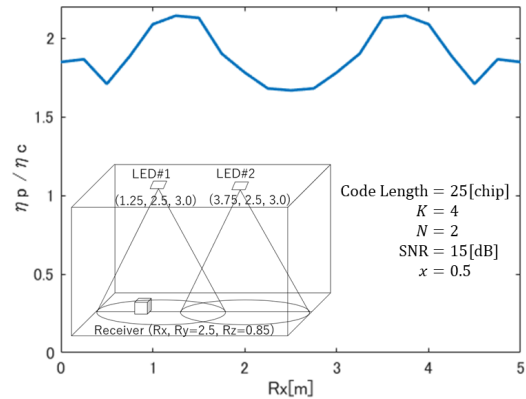


図 2: 提案方式と従来方式の情報伝送速度の比

図 2 より、提案方式は従来方式よりも受信機の座標に関係なく情報伝送速度が向上できることが分かった。また、提案方式は従来方式よりも本質的に情報伝送速度を 5/3 倍向上でき、 $R_x = 1.25, 3.75$ [m] において最大で 2.1 倍を達成できることが分かった。

4 むすび

本稿では、xASK を用いるしきい値秘密分散法を融合する VN-CodeSK 照明光通信方式を提案した。

参考文献

- [1] K.Osawa, et.al, "Theoretical analysis on bit error rate of visible-light variable N-parallel code-shift-keying," IEICE Trans. Fundamentals, vol.E101-A, no.12, pp.2352-2358, Dec. 2018
- [2] M.Naor and A.Shamir, "Visual Cryptograph", Advances in Cryptology-EUROCRYPT'94, vol.950, pp.1-12, May 1994
- [3] 幡豆ら, "(2, 2) しきい値秘密分散法を用いる拡張 VN-CodeSK 照明光通信方式", 信学論 B, vol.J106, No.8, pp.594-602, 2023-8