Chiffrement par Précodage Spatial de la Couche Physique sous Contrainte d'Enveloppe Constante

Clément LEROY[1] Tarak ARBI[1] Oudomsack Pierre PASQUERO[2] Benoît GELLER[1]

[1]Laboratoire U2IS, ENSTA, Institut Polytechnique de Paris, France

[2]DGA-MI, Ministère des armées, 35998 Rennes cedex 9, France

Résumé – Les systèmes de communication à entrées multiples ont de nombreux avantages comparés aux systèmes avec une seule antenne à l'émission comme une meilleure efficacité énergétique et une confidentialité améliorée en dirigeant le signal vers son récepteur légitime. Toutefois, les signaux qui souffrent d'un rapport élevé de puissance crête sur puissance moyenne nuisent considérablement à l'efficacité énergétique de l'émetteur. Dans ce papier, nous proposons un précodeur à enveloppe constante qui permet de chiffrer spatialement l'information pour des systèmes à entrée multiple et à sortie unique (MISO). Notre méthode permet de bruiter les canaux des récepteurs illégitimes en introduisant de l'aléa dans la façon de précoder l'information, sans que cela ne dégrade le canal du récepteur légitime. Notre méthode de transmission n'est ni plus coûteuse énergétiquement, ni plus complexe algorithmiquement que les autres précodeurs de la littérature ; en revanche, elle permet un gain de confidentialité important ainsi qu'un PAPR optimum, comme le montrent nos simulations.

Abstract – Multiple-input communication systems offer numerous advantages compared to single-antenna transmission systems, such as improved energy efficiency and enhanced confidentiality by directing the signal toward its legitimate receiver. However, signals with a high peak-to-average power ratio significantly reduce the energy efficiency of the transmitter. In this paper, we propose a constant-envelope precoder that enables information encryption for multiple-input single-output (MISO) systems. Our method degrades the channels of illegitimate receivers by introducing randomness in the precoding process, without affecting the legitimate receiver's channel. Our transmission method is neither more energy-consuming nor more algorithmically complex than other precoders in the literature; yet, it allows for a considerable gain in confidentiality and an optimal PAPR, as demonstrated by our simulations.

1 Introduction [1]

La confidentialité des télécommunications sans fils est généralement assurée par des algorithmes de chiffrement classique qui encodent l'information pour la rendre indécryptable par un récepteur non légitime. Cependant, ces méthodes nécessitent une coordination entre l'émetteur et le récepteur qui peut être trop contraignante dans certains cas d'utilisation, notamment pour les communications militaires et pour les objets des nouvelles générations de radio mobiles. Afin de pallier ce problème, des algorithmes de chiffrement de la couche physique tirant profit de la connaissance du canal du récepteur légitime ont été proposés dans la littérature. Ils sont basés sur les travaux fondateurs de Wyner [8] qui a prouvé qu'il était possible d'assurer une confidentialité parfaite au niveau de la couche physique grâce à un simple codage canal. Ses travaux ont par la suite été généralisés pour les canaux de diffusion [3] et puis spécifiquement pour les résaux sans fils.

Ces dernières années, des méthodes de chiffrement ont été proposées dans la littérature pour le cas où l'émetteur dispose de plusieurs antennes. Un tel réseau d'antennes permet d'optimiser l'efficacité énergétique de la transmission en concentrant la puissance du signal vers le récepteur légitime (formation de faisceaux). Ces méthodes visent à dégrader le canal du récepteur illégitime sans perturber le canal légitime en émettant un signal de masquage en plus du signal utile. Le signal de masquage est ainsi généré dans le noyau du canal légitime, ce qui n'est possible que lorsque le nombre d'antennes à l'émission est supérieur au nombre d'antennes du récepteur légitime [4].

L'efficacité de ces réseaux d'antennes est toutefois considérablement amoindrie lorsque les signaux à transmettre souffrent d'un rapport de puissance crête à puissance moyenne (PAPR) élevé. Ainsi, plusieurs études ont analysé les communications à entrées mutliples et à sortie unique (MISO) et à enveloppe constante [5, 6]. Dans [5], les auteurs ont démontré que lorsque la transmission était à enveloppe constante, le canal de communication était équivalent à un canal gaussien à entrée et sortie uniques pour lequel l'entrée était restreinte dans le plan complexe à un ensemble ayant la forme d'un anneau, d'où le nom de $doughnut\ channel$. Les auteurs de [6] ont par la suite proposé des méthodes explicites de génération des signaux à enveloppe constante à émettre par chaque antenne afin de transmettre un symbole d'information donné. Cependant, ces approches ne prennent pas en compte la problématique de la confidentialité de la transmission et ne s'intéressent qu'au lien entre l'émetteur et le récepteur légitime. Dans la littérature, seule la méthode OPALS [7] décrit explicitement une façon de générer les signaux à enveloppe constante à émettre par chaque antenne pour garantir une forme de confidentialité. Cette méthode ne peut toutefois être utilisée que dans le cas marginal des communications avec ligne de vue directe et la confidentialité y repose sur un nombre limité de variables aléatoires binaires, ce qui la laisse particulièrement vulnérables aux attaques par force brute.

Dans ce papier, nous proposons un nouvel algorithme de génération des signaux dans le cas de la transmission à en-

[1]Cette étude a été financée par le projet AID CIEDS SEPHYTEL.

veloppe constante par un réseau d'antennes. En s'inspirant des travaux qui introduisent un bruit artificiel en direction des espions potentiels [4], nous introduisons une part d'aléa dans la transmission du signal, ce qui permet de dégrader le signal reçu par les récepteurs non légitimes sans impacter le signal légitime. Notre proposition atteint les mêmes performances que les précédentes propositions de la littérature en terme de qualité de signal pour le récepteur légitime et dégrade considérablement le canal illégitime. Ce gain de confidentialité est totalement gratuit : notre méthode ne consomme pas davantage d'énergie que les autres méthodes à enveloppe constante précédemment proposées et la complexité de notre algorithme est également linéaire en L_A, le nombre d'antennes émettrices.

Dans la suite de l'article, la section 2 détaille notre modèle de système de communication. La génération des signaux proposée est décrite dans la section 3. Les résultats de cette méthode en terme de rapport signal sur bruit sont présentés dans la section 4. Enfin, la section 5 conclut l'article.

2 Modèle du système

2.1 Transmission à enveloppe constante

On considère un système de communication où l'émetteur (Alice) a L_A antennes tandis que le récepteur légitime (Bob) n'a qu'une seule antenne. Le canal entre Alice et Bob est modelisé par le vecteur : $\mathbf{h} = (h_1 \dots h_{L_A})^T$. Un récepteur illégitime (Ève) avec L_E antennes tente d'intercepter la communication et de décoder l'information. Le canal entre Alice et Ève est modélisé par la matrice $\mathbf{G}$. À l'instant t, Alice émet le signal $\mathbf{x}(t) = (x_1(t) \dots x_{L_A}(t))^T$ (où $x_k(t)$ est le signal émis par l'antenne k). Bob reçoit :

$$y_B(t) = \mathbf{h}^T \mathbf{x}(t) + n_B(t) = \sum_{k=1}^{L_A} h_k x_k(t) + n_B(t), \quad (1)$$

tandis qu'Ève reçoit :

$$\mathbf{y}_E(t) = \mathbf{G}\mathbf{x}(t) + \mathbf{n}_E(t), \quad (2)$$

où n_B et $\mathbf{n}_E$ sont des bruits blancs gaussiens de puissances respectives σ_B^2 et σ_E^2. Par soucis de clarté, on omettra la mention de l'instant t dans la suite de ce papier.

On suppose une synchronisation parfaite entre Alice et tous les récepteurs. Le canal légitime $\mathbf{h}$ est supposé connu de tous les acteurs de la communication tandis que le canal non légitime $\mathbf{G}$ est supposé parfaitement connu d'Ève seulement, $\mathbf{G}$ est complètement inconnu d'Alice et de Bob.

Avec la méthode de formation de faisceaux (beamforming), l'émetteur maximise le rapport signal sur bruit (RSB) de Bob en précodant un symbole d'information u par le vecteur $\sqrt{P_T}\frac{\mathbf{h}^\dagger}{\|\mathbf{h}\|}u$, où P_T est la puissance totale de transmission et $.^\dagger$ est l'hermitien.

Dans ce papier, on s'intéresse non seulement à optimiser le RSB de Bob, mais aussi à réduire celui d'Ève, tout en se limitant à l'émission de signaux à enveloppe constante (EC). Avec cette dernière contrainte, pour tout k, on a : $|x_k|^2 = \frac{P_T}{L_A}$. Donc x_k s'écrit :

$$x_k = \sqrt{\frac{P_T}{L_A}} e^{j\theta_k}. \quad (3)$$

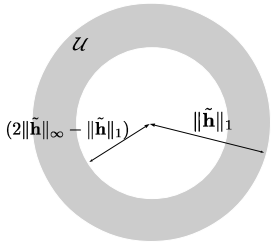

FIGURE 1 : Illustration de l'ensemble $\mathcal{U}$ (partie grisée) dans le plan complexe $\mathbb{C}$.

Le signal reçu par Bob peut donc s'écrire :

$$y_B = \sqrt{\frac{P_T}{L_A}} \sum_{k=1}^{L_A} h_k e^{j\theta_k} + n_B. \quad (4)$$

2.2 Système SISO équivalent

En posant $u = \sum_{k=1}^{L_A} h_k e^{j\theta_k}$, on obtient un canal gaussien équivalent à entrée et sortie uniques (SISO) où Alice envoie u et Bob reçoit :

$$y_B = \sqrt{\frac{P_T}{L_A}} u + n_B. \quad (5)$$

L'ensemble $\mathcal{U}$ des valeurs possibles de u a la forme d'un anneau dans le plan complexe (c.f. figure 1), il est défini par [5, 6] :

$$\mathcal{U} = \{u \in \mathbb{C} : (2\|\mathbf{h}\|_\infty - \|\mathbf{h}\|_1) \leq |u| \leq \|\mathbf{h}\|_1\}. \quad (6)$$

Dans un premier temps, l'émetteur et le récepteur conviennent d'une constellation de symboles d'information $\mathcal{C}$ telle que $\mathcal{C} \subset \mathcal{U}$. On suppose dans cet article que la synchronisation entre Alice et Bob est faite et on s'intéresse aux façons de choisir les signaux qu'émettent chaque antenne afin que Bob reçoive bien le bon symbole d'information u.

2.3 Analyse du modèle du système

À symbole d'information u fixé, on note :

$$\Theta(u) = \left\{ \boldsymbol{\theta} = (\theta_1, \dots, \theta_{L_A}) : \sum_{k=1}^{L_A} h_k e^{j\theta_k} = u \right\}. \quad (7)$$

Dans le cas classique (i.e. sans Ève) largement étudié [5] où seuls Alice et Bob sont considérés, le choix des phases $\boldsymbol{\theta}$ pour transmettre le symbole d'information u n'a pas d'importance, à condition que les phases sont bien dans $\Theta(u)$. Ainsi, des constructions déterministes ont été proposées [6], mais la prise en compte d'Ève rend ces précodeurs insatisfaisants puisque les diagrammes I/Q de réception pour Ève ne sont alors que de simples déformations facilement prévisibles des diagrammes I/Q de Bob. Au lieu de cela, on propose de choisir $\boldsymbol{\theta}$ aléatoirement dans $\Theta(u)$. On peut décomposer le signal x_k à envoyer par la k^{ieme} antenne en deux composantes, une déterministe ($x_k^{(det)}$) et une aléatoire de moyenne nulle (b_k) :

$$x_k = x_k^{(det)} + b_k = \sqrt{\frac{P_T}{L_A}} e^{j\theta_k}. \quad (8)$$

Comme mentionné précedemment, dès lors que $\boldsymbol{\theta}$ est dans $\Theta(u)$, Bob reçoit le symbole u. Alice est la seule à connaitre quelles sont les phases $\boldsymbol{\theta}$ qui ont effectivement été choisies pour la transmission. Ainsi, le canal entre Alice et Bob ne dépend pas de la variable aléatoire $\mathbf{b} = (b_1 \dots b_{L_A})^T$ qui traduit le choix de $\boldsymbol{\theta}$ dans $\Theta(u)$. Cette variable impacte toutefois Ève en agissant comme un bruit supplémentaire qui dégrade son canal. En effet, elle reçoit :

$$\mathbf{y}_E = \mathbf{G}\mathbf{x}^{(det)} + \mathbf{G}\mathbf{b} + \mathbf{n}_E. \tag{9}$$

On définit alors le RSB moyen pour Ève par :

$$RSB_{Eve} = \frac{\mathbb{E}\left[\|\mathbf{G}\mathbf{x}^{(det)}\|^2\right]}{\mathbb{E}\left[\|\mathbf{G}\mathbf{b}\|^2\right] + \sigma_E^2}, \tag{10}$$

et le RSB moyen pour Bob par :

$$RSB_{Bob} = \frac{\mathbb{E}\left[|\mathbf{h}^T\mathbf{x}|^2\right]}{\mathbb{E}\left[|n_B|^2\right]} = \frac{\frac{P_T}{L_A}\mathbb{E}\left[|u|^2\right]}{\sigma_B^2}. \tag{11}$$

La variable aléatoire $\mathbf{b}$ est nécessaire pour assurer l'envoi de signaux à enveloppe constante. Choisir $\mathbf{b}$ de façon aléatoire n'impacte nullement Bob mais offre, sans aucune perte en efficacité énergétique, un gain de confidentialité en dégradant le canal d'Ève.

3 Précodeur à enveloppe constante

3.1 Caractérisation de $\Theta(u)$

On peut caractériser $\Theta(u)$ en établissant une relation entre les phases $\theta_1, \theta_2, \dots, \theta_{L_A}$.

Lemme : Soient n un entier entre 0 et $L_A - 1$ et $(\theta_1, \dots, \theta_n)$ une famille de n phases (si $n = 0$, alors la famille est vide). La famille peut être complétée par $\theta_{n+1}, \dots, \theta_{L_A}$ de telle façon que $\boldsymbol{\theta} = (\theta_1, \dots, \theta_{L_A})$ est dans $\Theta(u)$ si et seulement si :

$$\rho_n^{(in)} \leq \left| \sum_{k=1}^{n} h_k e^{j\theta_k} - u \right| \leq \rho_n^{(out)}, \tag{12}$$

où :

$$\begin{aligned} \rho_n^{(in)} &= \left(2 \max_{n+1 \leq k} |h_k| - \sum_{k=n+1}^{L_A} |h_k| \right), \\ \rho_n^{(out)} &= \sum_{k=n+1}^{L_A} |h_k|. \end{aligned} \tag{13}$$

Démonstration. Lorsque $\theta_1, \dots, \theta_n$ sont fixés, pour que $(\theta_1, \dots, \theta_{L_A})$ soit dans $\Theta(u)$, il faut que $\theta_{n+1}, \dots, \theta_{L_A}$ vérifient :

$$\sum_{k=n+1}^{L_A} h_k e^{j\theta_k} = u - \sum_{k=1}^{n} h_k e^{j\theta_k}. \tag{14}$$

Ainsi, en posant $\tilde{u} = u - \sum_{k=1}^{n} h_k e^{j\theta_k}$, on obtient par application de (6) au canal modelisé par $\tilde{\mathbf{h}} = (h_{n+1} \dots h_{L_A})$ que des phases $\theta_{n+1}, \dots, \theta_{L_A}$ convenables existent si et seulement si $\tilde{u}$ est dans l'ensemble défini par :

$$(2\|\tilde{\mathbf{h}}\|_\infty - \|\tilde{\mathbf{h}}\|_1) \leq |\tilde{u}| \leq \|\tilde{\mathbf{h}}\|_1, \tag{15}$$

ce qui finalise la preuve. □

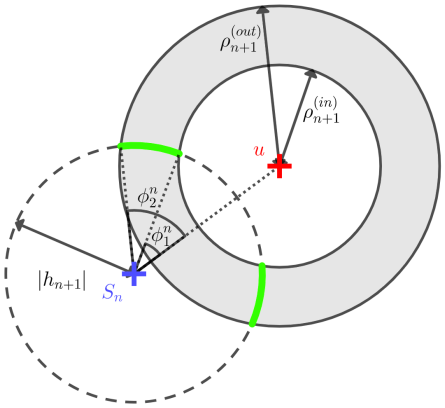

FIGURE 2 : Illustration du théorème.

Théorème : Si $\theta_1, \dots, \theta_n$ sont fixés vérifiant les inéquations (12), θ_{n+1} peut être choisi dans l'ensemble $\Theta_{n+1}(u)$ défini par :

$$\Theta_{n+1}(u) = arg\left(\frac{u - S_n}{h_{n+1}}\right) + [-\phi_2^n; -\phi_1^n] \cup [\phi_1^n; \phi_2^n], \tag{16}$$

où :

$$S_n = \sum_{k=1}^{n} h_k e^{j\theta_k}, \tag{17}$$

$$\phi_1^n = \begin{cases} \arccos\left(\frac{|h_{n+1}|^2 + (\rho_{n+1}^{(in)})^2 - |u - S_n|^2}{2\rho_{n+1}^{(in)}|h_{n+1}|}\right), & \text{si } c_1 \geq 0 \\ 0, & \text{si } c_1 < 0 \end{cases} \tag{18}$$

$$\phi_2^n = \begin{cases} \arccos\left(\frac{|h_{n+1}|^2 + (\rho_{n+1}^{(out)})^2 - |u - S_n|^2}{2\rho_{n+1}^{(out)}|h_{n+1}|}\right), & \text{si } c_2 \geq 0 \\ \pi, & \text{si } c_2 < 0 \end{cases} \tag{19}$$

avec :

$$c_1 = |S_n - u| - |h_{n+1}| - \rho_{n+1}^{(in)}, \tag{20}$$

$$c_2 = |S_n - u| + |h_{n+1}| - \rho_{n+1}^{(out)}. \tag{21}$$

La figure 2 illustre comment on peut déduire le théorème grâce au lemme et au théorème d'Al-Kashi. Les arcs en vert correspondent aux phases possibles θ_{n+1}, après avoir choisi $\theta_1, \dots, \theta_n$ pour qu'il existe une famille $(\theta_1, ..., \theta_{L_A})$ dans $\Theta(u)$.

3.2 Algorithme de génération des phases

Afin de maximiser le caractère aléatoire du bruit artificiel $\mathbf{b}$, on décide de maximiser l'entropie différentielle conditionnelle $H(\mathbf{b}|u)$ qui peut se décomposer comme suit :

$$H(\mathbf{b}|u) = H(b_1, \dots, b_{L_A}|u) = H(\theta_1, \dots, \theta_{L_A}|u) \tag{22}$$

$$= \sum_{k=1}^{L_A} H(\theta_k | u, \theta_1, \dots, \theta_{k-1}). \tag{23}$$

Donc $H(\mathbf{b}|u)$ est maximisée lorsque chaque θ_n est tiré uniformément dans l'ensemble $\Theta_n(u)$ défini par (16).

Grâce aux résultats précédents, nous pouvons désormais proposer l'Algorithme 1 pour la génération des phases. On remarquera que cet algorithme est de complexité faible (linéraire en L_A) similaire à [6].

Algorithme 1 : Génération des phases

Entrée : u, P_T, $\mathbf{h} = (h_1, \ldots, h_{L_A})$.
$S = 0$
pour $k = 1 \ldots L_A$ **faire**
  ψ prend une valeur aléatoire dans $[\phi_1^n; \phi_2^n]$
  e prend une valeur aléatoire dans $\{-1, 1\}$
  $\theta_k \leftarrow arg(u - S) - arg(h_k) + \psi e$
  $S \leftarrow S + h_k e^{j\theta_k}$
fin
Sortie : $(\theta_1, \ldots, \theta_{L_A})$

4 Résultats numériques

Nous présentons ici les performances de notre proposition de méthode. Elles sont évaluées à l'aide du RSB en fonction du rapport puissance émise P_T sur variance du bruit (on suppose ici que $\sigma_B^2 = \sigma_E^2$). Nous simulons quatre méthodes sur des canaux de Rayleigh : notre proposition, le beamforming, le précodeur de [6], et de la méthode de masquage par bruit artificiel gaussien (BAG) proposée par [4]. Enfin, on fixe $L_A = 64$ et $L_E = 2$. La puissance du masque pour le BAG est choisie pour que le RSB de Bob soit similaire à notre méthode.

Le RSB de Bob est optimal lorsque la méthode du beamforming est utilisée mais les amplificateurs sont ici supposés parfaits. L'utilisation des méthodes déterministes (celle issue de [6] et le beamforming) conduit à un haut RSB pour Ève, et l'information est donc faiblement protégée. Les deux méthodes non déterministes (notre proposition et le BAG) permettent de réduire considérablement le RSB de Ève, et donc d'améliorer la sécurité de la communication. En effet, lorsque notre méthode est utilisée, le RSB d'Ève est réduit d'environ 5 dB par rapport au RSB induit par [6].

La figure 4 illustre l'avantage de notre proposition par rapport au BAG. Elle présente la fonction de répartition complémentaire (FRC) du PAPR des signaux émis par notre méthode, par le beamforming et par le BAG. Le PAPR y est calculé sur des trames de 1000 symboles. Le PAPR pour notre méthode est optimal grâce à la contrainte de l'enveloppe constante, alors qu'il est très élevé pour les deux autres méthodes, ce qui réduit considérablement leur efficacité énergétique.

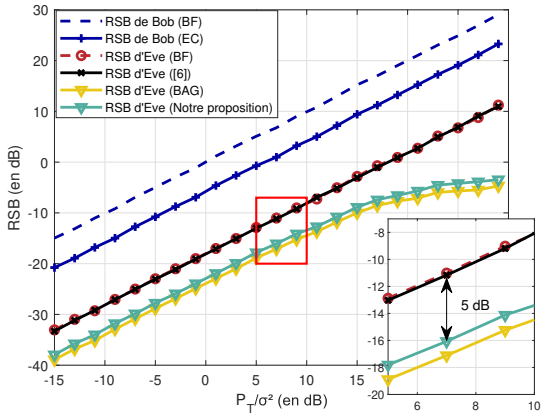

FIGURE 3 : RSB en fonction du rapport de puissance $\frac{P_T}{\sigma^2}$.

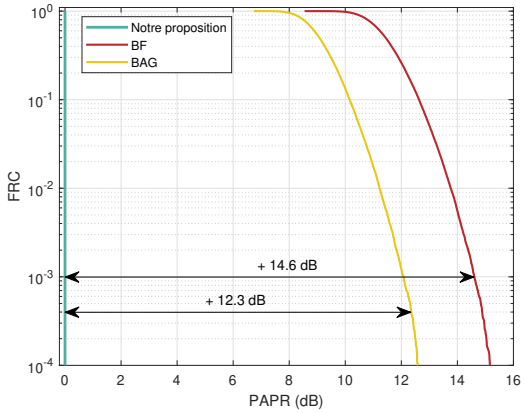

FIGURE 4 : FRC du PAPR pour différentes méthodes.

5 Conclusion

Dans ce papier, nous avons proposé un nouveau précodeur à enveloppe constante qui permet sans aucune perte énergétique de dégrader le canal des récepteurs illégitimes. Nos simulations du RSB et les comparaisons avec les méthodes de référence de précodage et de chiffrement soulignent l'efficacité de notre méthode. Notre méthode de chiffrement pourrait à l'avenir être associée aux constellations tournées, pour leur résistance au brouillage et leur capacité à opérer à PAPR limité en modulations multi-porteuses [2, 1].

Références

[1] Tarak ARBI, Benoît GELLER, Jianxiao YANG, Charbel ABDEL NOUR et Olivier RIOUL : Uniformly projected rcqd qam : A low-complexity signal space diversity solution over fading channels with or without erasures. *IEEE Transactions on Broadcasting*, 64(4):803–815, 2018.

[2] Tarak ARBI, Zi YE et Benoît GELLER : Low-complexity blind papr reduction for ofdm systems with rotated constellations. *IEEE Trans. on Broadcast.*, 67(2):491–499, 2021.

[3] I. CSISZAR et J. KORNER : Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978.

[4] S. GOEL et R. NEGI : Guaranteeing secrecy using artificial noise. *IEEE Trans. Wirel. Commun.*, 7(6), 2008.

[5] S.K. MOHAMMED et E.G. LARSSON : Single-user beamforming in large-scale miso systems with per-antenna constant-envelope constraints : The doughnut channel. *IEEE Trans. Wirel. Commun.*, 11(11):3992–4005, 2012.

[6] J. PAN et W.K. MA : Constant envelope precoding for single-user large-scale miso channels : Efficient precoding and optimal designs. *IEEE Journal of Selected Topics in Signal Processing*, 8(5):982–995, 2014.

[7] E. TOLLEFSON, B.R. JORDAN et J.D. GAEDDERT : Outphased array linearized signaling (opals) : A practical approach to physical layer encryption. *In 2015 IEEE Military Comm. Conference*, pages 294–299, 2015.

[8] A. D. WYNER : The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, 1975.