Analyse de la vulnérabilité d'un schéma de sécurité basé sur le bruit artificiel face à un espion multi-récepteurs

Jules BURGAT[1,2] Jean-Baptiste DORÉ[1] Joumana FARAH[2] Matthieu CRUSSIÈRE[2]

[1]CEA-Leti, Univ. Grenoble Alpes, Grenoble, France,

[2]Univ Rennes, INSA Rennes, CNRS, IETR-UMR 6164, F-35000 Rennes, France.

Résumé – Ce travail analyse la vulnérabilité des schémas de sécurité basés sur le bruit artificiel face à un espion utilisant plusieurs récepteurs. Nous étudions deux attaques et évaluons leurs performances en termes d'erreur quadratique moyenne (mean squared error (MSE)), à la fois théoriquement et par simulations. La première attaque, reposant sur une approche de système linéaire, est efficace lorsque le nombre d'interceptions dépasse celui des antennes d'émission. La seconde, basée sur le principe de la combinaison à rapport maximal (maximal ratio combining (MRC)), est novatrice et reste performante même avec moins d'interceptions que d'antennes émettrices. Les résultats théoriques sont formulés et confirmés par des simulations. Ce travail analyse aussi la robustesse aux erreurs d'estimation des schémas proposés. Les résultats de notre étude soulignent la nécessité d'une sélection rigoureuse des paramètres pour réduire les risques d'interception.

Abstract – This work analyzes the vulnerability of artificial noise-based security schemes to multi-sensor eavesdropping. We investigate two attacks and evaluate their performance in terms of MSE, both theoretically and through simulations. The first attack, relying on a linear system approach, is effective when the number of wiretaps exceeds the number of transmitting antennas. The second, based on MRC, is novel and remains effective even with fewer wiretaps than tranmitting antennas. Theoretical results are formulated and validated through simulations. We also highlight the impact of the estimation errors on eavesdropping performance. Our findings emphasize the need for careful parameter selection to mitigate eavesdropping risks.

1 Introduction

Dans les systèmes de communication sans fil modernes, garantir une transmission sécurisée est un défi majeur, en particulier en présence d'espions. Une approche largement étudiée pour renforcer la sécurité au niveau physique consiste à utiliser le bruit artificiel [1] afin de dégrader la capacité d'un espion à intercepter les messages transmis. Bien que le bruit artificiel perturbe efficacement la réception non autorisée, son efficacité dépend de plusieurs paramètres, notamment du nombre d'antennes de l'espion et de la puissance allouée au bruit artificiel [2].

Ce travail examine la vulnérabilité des schémas de bruit artificiel face à deux types d'attaques distinctes menées par un espion. La première attaque, appelée attaque par résolution de système, exploite la structure linéaire du signal reçu, comme proposé dans [2] et [3], et s'appuie sur des techniques d'estimation classiques telles que l'estimation par moindres carrés (least squares estimator (LSE)) et l'estimation du minimum de variance sans biais (minimum mean square error (MMSE)). Cette méthode est particulièrement efficace lorsque l'espion dispose d'un nombre suffisant d'antennes et d'une connaissance du canal entre l'émetteur et le récepteur légitime (channel state information (CSI)), lui permettant ainsi d'éliminer le bruit artificiel et de reconstruire avec précision le message transmis. La seconde attaque, appelée attaque par MRC, est introduite comme une nouvelle méthode permettant de reconstruire le message même lorsque le nombre d'antennes de l'espion est limité. Cette approche repose sur la combinaison de plusieurs signaux reçus afin de maximiser le rapport signal sur bruit (signal to noise ratio (SNR)). Cela rend possible la récupération du message original malgré la présence de bruit artificiel. Contrairement à l'attaque par résolution de système, l'attaque par MRC ne nécessite pas de connaître le CSI entre l'émetteur et le récepteur légitime, mais elle exige une connaissance *a priori* ou une estimation du vecteur de précodage.

À travers une analyse théorique et des simulations numériques, nous évaluons la performance en termes de MSE de ces deux attaques dans différentes conditions. Une analyse de la robustesse est également menée pour étudier l'impact des erreurs d'estimation sur les connaissances de l'espion. Nos résultats montrent que si l'attaque par résolution de système offre de meilleures performances lorsque l'espion dispose d'un grand nombre d'antennes, l'attaque par MRC reste efficace avec un plus petit nombre d'antennes, à condition que le niveau de bruit artificiel ne soit pas trop élevé. Ce travail est organisé de la manière suivante : la modélisation du système est introduite dans la section II. La description des attaques et l'analyse théorique sont réalisées dans la section III. La section IV est dédiée à l'évaluation des approches, et la dernière section conclut et propose des perspectives.

2 Modélisation du système

Nous nous intéressons à un système général de bruit artificiel tel que présenté dans [1]. Supposons que l'émetteur, équipé d'un réseau d'antennes de taille N, cherche à envoyer un message à un récepteur unique muni d'une seule antenne. La distance entre antennes, notée d, est fixée à $\frac{\lambda}{2}$, où λ est la longueur d'onde du signal transmis. Soit $\mathbf{h_0} \in \mathbb{C}^{1\times N}$ l'effet du canal pour le récepteur légitime, et $\mathbf{h_m} \in \mathbb{C}^{1\times N}$, pour $m > 0$, l'effet du canal pour l'espion m. Ces canaux sont supposés indépendants de l'indice temporel noté k. Ainsi, si $\mathbf{x}[k] \in \mathbb{C}^{N\times 1}$ est le vecteur traité par le réseau d'antennes émettrices à l'instant k, le message reçu par la $m^{\text{ème}}$ antenne de l'espion, noté $r_m[k]$, s'exprime par :

$$r_m[k] = \mathbf{h_m}\mathbf{x}[k] \ + \eta_m[k], \tag{1}$$

où $\eta_m[k]$ est un bruit additif blanc gaussien (additive white gaussian noise (AWGN)) dont la puissance, notée σ^2_{noise}, est supposée indépendante du récepteur $m \in [\![1, M]\!]$.

Soit $a[k]$ le symbole de données transmis à l'instant k, appartenant à une constellation K-quadrature amplitude modulation (QAM) ou à toute autre modulation, et supposé inconnu de l'espion. La suite des symboles $(a[k])_{k\in\mathbb{N}}$ est supposée indépendante et identiquement distribuées (i.i.d). Dans le schéma de bruit artificiel, $\mathbf{x}[k]$ est choisi comme suit :

$$\mathbf{x}[k] := a[k]\mathbf{w} + \boldsymbol{\mu}[k]. \tag{2}$$

On notera $\mathbf{w} \in \mathbb{C}^{N\times 1}$ le vecteur de précodage dont les composantes sont appelées poids de formation de faisceau.

Le vecteur $\boldsymbol{\mu}[k] \in \mathbb{C}^{N\times 1}$ représente un bruit artificiel aléatoire et est conçu pour satisfaire $\mathbf{h}_0\boldsymbol{\mu}[k] = 0$, garantissant ainsi qu'il n'affecte pas le récepteur légitime. Une manière de construire $\boldsymbol{\mu}[k]$ consiste à trouver une base orthonormée de l'espace nul de $\mathbf{h_0}$, qui est de dimension $N-1$, puis de concaténer ces vecteurs pour former la matrice $\mathbf{V} \in \mathbb{C}^{N\times(N-1)}$ telle que $\mathbf{h_0V} = \mathbf{0}_{\mathbb{C}^{N-1}}$ et $\mathbf{V}^H\mathbf{V} = \mathbf{I}_{N-1}$. Ensuite, on définit :

$$\boldsymbol{\mu}[k] := \mathbf{V}\mathbf{n}[k], \tag{3}$$

où $\mathbf{n}[k]$ suit une loi gaussienne centrée de matrice de covariance $\sigma^2_{an}\mathbf{I}_{N-1}$, soit $\mathbf{n}[k] \sim \mathcal{N}(0, \sigma^2_{an}\mathbf{I}_{N-1})$ avec $\sigma_{an} \in [0, 1]$. Considérant que la puissance émise par chaque antenne vaut 1, il est nécessaire de normaliser $a[k]$ et $\boldsymbol{\mu}[k]$. On définit alors :

$$\tilde{\mathbf{x}}[k] := \sqrt{1-\sigma^2_{an}}a[k]\mathbf{w} + \sqrt{\frac{N}{N-1}}\boldsymbol{\mu}[k]. \tag{4}$$

Si $\tilde{x}_n$ désigne la $n^{\text{ème}}$ composante du vecteur $\tilde{\mathbf{x}}$, on peut vérifier que $\mathbb{E}\left[|\tilde{x}_n|^2\right] = 1, \forall n \in [\![1, N]\!]$, si $\mathbb{E}\left[|a|^2\right] = 1$.

Comme expliqué dans [1], l'intérêt principal de cette approche est de dégrader l'information mutuelle entre l'émetteur et l'espion lorsque le canal de l'espion est différent de $\mathbf{h_0}$[1]. En effet, d'après l'équation (1), le message reçu par un espion s'écrit :

$$\begin{aligned} r_m[k] &= \mathbf{h_m}\tilde{\mathbf{x}}[k] \ + \eta_m[k] \\ &= \sqrt{1-\sigma^2_{an}}a[k]\mathbf{h}_m\mathbf{w} \ + \sqrt{\frac{N}{N-1}}\mathbf{h}_m\boldsymbol{\mu}[k] \ + \eta_m[k]. \end{aligned} \tag{5}$$

Ainsi, la sécurité de ce schéma repose sur le terme $\mathbf{h_m}\boldsymbol{\mu}[k]$ dans (5), qui entraîne un niveau d'interférence significatif lorsque $\mathbf{h}_m \neq \mathbf{h}_0$. Pour le récepteur légitime, on a :

$$\begin{aligned} r_0[k] &= \sqrt{1-\sigma^2_{an}}a[k]\mathbf{h_0w} \ + \sqrt{\frac{N}{N-1}}\underbrace{\mathbf{h_0}\boldsymbol{\mu}[\mathbf{k}]}_{=0} + \eta_0[k] \\ &= \mathbf{h_0w}\sqrt{1-\sigma^2_{an}}a[k] + \eta_0[k]. \end{aligned} \tag{6}$$

Ainsi, le message est amplifié pour le récepteur légitime.

3 Description des attaques et résultats théoriques

Dans cette étude, nous supposons que l'espion peut librement déployer un certain nombre d'antennes, noté M, à divers emplacements. Nous supposons également qu'il connaît parfaitement les canaux d'écoute $\mathbf{h}_1, \ldots, \mathbf{h}_M$. Une synchronisation parfaite en temps et en fréquence est aussi supposée. Dans ce qui suit, l'indice temporel k est omis pour simplifier les expressions. À partir de l'équation (1), le vecteur reçu par l'espion est :

$$\begin{aligned} \mathbf{r} &= \mathbf{H}\tilde{\mathbf{x}} + \boldsymbol{\eta} \\ &= \mathbf{Hw}\sqrt{1-\sigma^2_{an}}a + \sqrt{\frac{N}{N-1}}\boldsymbol{HVn} + \boldsymbol{\eta}, \end{aligned} \tag{7}$$

où $\mathbf{H}$ représente la matrice de canal et $\boldsymbol{\eta}$ le bruit. Nous présentons deux méthodes pour estimer a.

3.1 Attaque par résolution de système

Cette attaque peut être vue comme une adaptation des idées présentées dans [3]. Étroitement liée à ce travail, l'étude [2] propose une analyse générale des performances du taux d'erreur binaire (bit error rate (BER)) et de la capacité de confidentialité de cette attaque. Nous rappellerons brièvement le principe de cette attaque et donnerons notre principale contribution de cette section : le calcul de l'expression théorique de la MSE entre le message estimé et le message original.

En utilisant le système linéaire bruité (7), la première étape pour l'intercepteur est d'estimer le vecteur $\tilde{\mathbf{x}}$ par $\widehat{\tilde{\mathbf{x}}} := \mathbf{Tr} \in \mathbb{C}^N$. Dans notre cas, $\mathbf{T}$ sera exprimée soit par $\mathbf{T} = \left(\boldsymbol{H}^{\boldsymbol{H}}\boldsymbol{H}\right)^{-1}\boldsymbol{H}^{\boldsymbol{H}} \in \mathcal{M}_{N,M}(\mathbb{C})$ pour le cas d'un estimateur LSE, soit par $\mathbf{T} = \boldsymbol{\Gamma}_{\tilde{\boldsymbol{x}}}\mathbf{H}^{\mathbf{H}}\left(\mathbf{V}\boldsymbol{\Gamma}_{\tilde{\boldsymbol{x}}}\mathbf{H}^{\mathbf{H}} + \boldsymbol{\Gamma}_{\boldsymbol{\eta}}\right)^{-1} \in \mathcal{M}_{N,M}(\mathbb{C})$ pour le cas d'un estimateur MMSE, voir [4], avec $\boldsymbol{\Gamma}_{\mathbf{z}}$ la matrice de covariance de la variable aléatoire $\mathbf{z} \in \mathbb{C}^N$: $\boldsymbol{\Gamma}_{\mathbf{z}} = (\mathbb{E}[z_i\bar{z}_j])_{1\leq i,j\leq N} \in \mathcal{M}_{N\times N}(\mathbb{C})$. Il est important de noté que dans le cas d'un estimateur MMSE, une connaissance de la statistique du message émis est nécéssaire à l'espion. A noter que dans [2], seul l'estimateur LSE est considéré. Ensuite, d'après l'équation (6), afin d'annuler le bruit artificiel, l'espion réplique l'effet du canal légitime en estimant r_0 par :

$$\widehat{r_0} := \mathbf{h}_0\widehat{\tilde{\mathbf{x}}} = \mathbf{h}_0\mathbf{Tr}. \tag{8}$$

Selon la contrainte de puissance d'émission par antenne (voir l'équation (4)), le message reçu est pondéré par un facteur $\mathbf{h_0w}\sqrt{1-\sigma^2_{an}}$. Ainsi, a peut être estimée par :

$$\hat{a} := \left(\mathbf{h_0w}\sqrt{1-\sigma^2_{an}}\right)^{-1}\widehat{r_0}. \tag{9}$$

Nous sommes maintenant en mesure de déterminer théoriquement l'erreur entre le message d'intérêt a et l'estimation $\hat{a}$, ce qui constitue la principale contribution de cette section.

Théorème 1. *Pour tout estimateur $\widehat{\tilde{\boldsymbol{x}}} := \mathbf{Tr}$ de $\tilde{\boldsymbol{x}}$ avec $\mathbf{T} \in \mathcal{M}_{N\times M}(\mathbb{C})$, l'espion peut estimer un message, noté $\hat{a}$, tel que :*

$$MSE(\hat{a}, a) = \frac{C(\mathbf{h}_1, \cdots, \mathbf{h}_M, \sigma_{noise})}{(\mathbf{h_0w})^2(1-\sigma^2_{an})}, \tag{10}$$

où C est une constante qui dépend du canal de l'intercepteur et de σ_{noise}.

Du point de vue de la sécurité, il est important de remarquer que cette erreur augmente lorsque σ^2_{an} augmente.

Démonstration. Nous donnons quelques étapes pour montrer ce résultat. Soit $\boldsymbol{\eta}' := \sqrt{1-\sigma^2_{an}}a\mathbf{h_0} \odot \mathbf{w} - \mathbf{h_0} \odot \mathbf{Tr} \in \mathbb{C}^N$,

[1] Implicitement, si la position de l'espion est suffisamment éloignée du récepteur légitime, on peut supposer que cette condition est vérifiée.

où $\mathbf{x} \odot \mathbf{y}$ est le produit terme à terme définit par $\mathbf{x} \odot \mathbf{y} = (x_n y_n)_{1 \leq n \leq N} \in \mathbb{C}^N$. On peut alors montrer que

$$|a - \hat{a}|^2 = \frac{1}{(\mathbf{h_0 w})^2 (1 - \sigma_{an}^2)} |\mathbf{h_0 w} \sqrt{1 - \sigma_{an}^2} a - \mathbf{h_0 T r}|^2,$$

et donc

$$\begin{aligned} \mathbb{E}\left[|a - \hat{a}|^2\right] &= \frac{1}{(\mathbf{h_0 w})^2 (1 - \sigma_{an}^2)} \mathbb{E}\left[\left|\sum_{n=1}^{N} \eta'_n\right|^2\right] \\ &= \frac{1}{(\mathbf{h_0 w})^2 (1 - \sigma_{an}^2)} \sum_{1 \leq p,q \leq N} \left(\mathbf{\Gamma}_{\boldsymbol{\eta'}}\right)_{p,q}. \end{aligned}$$

Enfin, la constante définie dans le Théorème 1 est $\sum_{1 \leq p,q \leq N} \left(\mathbf{\Gamma}_{\boldsymbol{\eta'}}\right)_{p,q}$. □

Le choix de l'estimateur dépend fortement du nombre de récepteurs espions M, c'est-à-dire de la nature du système linéaire bruité (7). En effet, pour un système sous-déterminé ($M < N$), seul l'estimateur MMSE peut être considéré et les performances seront largement impactées puisque l'intercepteur tente de résoudre un système avec plus d'inconnues que d'observations. L'intérêt de la méthode suivante est de se débarrasser de cette contrainte concernant la nature du système linéaire (7).

3.2 Attaque du schéma basé sur le bruit artificiel utilisant l'estimateur MRC

L'utilisation de cette attaque ne nécessite pas la connaissance parfaite du canal légitime $\mathbf{h}_0$ mais seulement celle du précodeur $\mathbf{w}$. Plusieurs attaques sur bruit artificiel ont déjà été proposées lorsque le CSI légitime est indisponible pour l'intercepteur, [5, 6]. Cependant, des hypothèses fortes ont été faites concernant la faisabilité de ces attaques, notamment sur la constellation utilisée ou le nombre d'antennes de transmission. L'intuition de cette attaque est que lorsque le niveau du bruit artificiel est suffisamment bas, il est encore possible pour l'intercepteur de décoder le message. Ainsi, en combinant plusieurs récepteurs, on peut réduire le niveau du bruit artificiel, permettant ainsi de décoder le message. Le système linéaire bruité (7) peut se réécrire comme

$$\mathbf{r} = \mathbf{Hw} \sqrt{1 - \sigma_{an}^2} a + \boldsymbol{\mu'}, \tag{11}$$

où $\mathbf{Hw} \in \mathbb{C}^M$ et $\boldsymbol{\mu'} := [\mu'_1, \cdots, \mu'_M]^T \in \mathbb{C}^M$, avec $\mu'_m := \mathbf{h}_m \sqrt{\frac{N}{N-1}} \boldsymbol{\mu} + \boldsymbol{\eta}_m \in \mathbb{C}$ qui est un bruit gaussien complexe à moyenne nulle. L'estimation MRC $\hat{a}_{\text{MRC}}$ est donnée par :

$$\hat{a}_{\text{MRC}} = \frac{1}{\sqrt{1 - \sigma_{an}^2}} \frac{\mathbf{w}^H \mathbf{H}^H \mathbf{r}}{||\mathbf{Hw}||_2^2}. \tag{12}$$

avec $||\mathbf{y}||_2 = \left(\mathbf{y}^H \mathbf{y}\right)^{\frac{1}{2}} \ \forall \mathbf{y} \in \mathbb{C}^N$, selon [4]. Nous exprimons maintenant la principale contribution de cette section.

Théorème 2. *L'erreur quadratique moyenne (MSE) de l'estimation MRC est donnée par :*

$$MSE(\hat{a}_{MRC}, a) = \frac{1}{(1 - \sigma_{an}^2)||\mathbf{Hw}||_2^4} \mathbf{w}^H \mathbf{H}^H \mathbb{E}\left[\boldsymbol{\mu'}^H \boldsymbol{\mu'}\right] \mathbf{Hw} \tag{13}$$

Démonstration. En substituant $\mathbf{r}$ exprimée par (11) dans l'estimateur MRC et après simplification, on obtient :

$$\hat{a}_{\text{MRC}} = a + \frac{1}{\sqrt{1 - \sigma_{an}^2}} \frac{\mathbf{w}^H \mathbf{H}^H \boldsymbol{\mu'}}{||\mathbf{Hw}||_2^2}.$$

La formule théorique de la MSE peut ensuite être trouvée à partir de l'égalité précédente. □

Il est important de noter que l'estimation MRC dépend uniquement du vecteur de précodage $\mathbf{w}$ et ne nécessite pas la connaissance de $\mathbf{h}_0$. De plus, une estimation du facteur de mise à l'échelle et de rotation de la constellation $\sqrt{1 - \sigma_{an}^2} \mathbf{h}_m \mathbf{w}$ dans chaque position d'écoute suffit pour utiliser cette attaque. D'autre part une large diversité spatiale des mesures n'est pas nécessaire contrairement à l'estimation LSE, pourvu que les écoutes soient indépendantes. Ces deux points réduisent ainsi considérablement les difficultés d'implantation de cette attaque.

4 Évaluations numériques

Sans perte de généralité, bien que l'algorithme soit conçu pour un canal général, nous analysons les attaques pour le cas d'un canal en ligne de vue directe (line-of-sight (LoS)), représentatif d'une application de type communications par satellites. Ainsi, l'effet du canal dépend uniquement de la position du récepteur. L'hypothèse du champ lointain suggère que, dans une direction θ, le signal émis est déphasé de $2\pi\alpha \sin\theta$ entre deux antennes successives, où $\alpha = d/\lambda$. Ainsi, le canal dans la direction θ est $\mathbf{h}_\theta = \left[1, \ldots, e^{-2j\pi(N-1)\alpha \sin\theta}\right]$.

Nous considérons une constellation 16-QAM sur un canal LoS, où θ_0, l'angle de visée (Direction of Departure (DoD)) du récepteur légitime, est estimé pour trouver le précodage correspondant $\mathbf{w}$. On considèrera que $\mathbf{w} = \left(e^{-jArg(h_{0,1})}, \cdots, e^{-jArg(h_{0,N})}\right)$, où $Arg(z)$ dénote l'argument d'un nombre complexe $z \in \mathbb{C}$, n'affecte que la phase du signal. Les simulations suivantes comparent les performances de LSE et MRC et analysent leur robustesse face aux erreurs d'estimation. Les résultats de l'estimateur MMSE ne sont pas présentés, car ils sont similaires à ceux de LSE pour $M \geq N$ aux niveaux de bruit artificiel étudiés, et peu performants pour $M \leq N$.

4.1 Comparaison de performances

Le rapport entre la puissance allouée au message d'intérêt a et la puissance allouée au bruit artificiel (signal to artificial noise ratio (SANR)) est déterminante pour évaluer les performances des attaques proposées. La figure 1 présente la MSE en fonction du SANR, définie comme $\frac{1-\sigma_{an}^2}{\sigma_{an}^2}$, pour un espion muni de M antennes, réparties en dehors du lobe principal du diagramme de rayonnement de l'émetteur. Les écoutes sont effectuées de manière équi-réparties dans les intervalles $]-\pi/3, -0{,}2[\cup]0{,}2, \pi/3[$ où l'on suppose que le recepteur légitime est positionné en $\theta_0 = 0$. Cette figure illustre les Théorèmes 1 et 2 où les valeurs théoriques et empiriques coïncident.

Comme prévu, l'estimation LSE surpasse l'estimation MRC, car la première annule complètement le bruit artificiel, tandis que la seconde ne fait que maximiser le SNR, où le bruit est composé à la fois de bruit artificiel et thermique. Cependant, l'avantage clé du MRC réside dans sa capacité à fournir une estimation fiable du message transmis, même

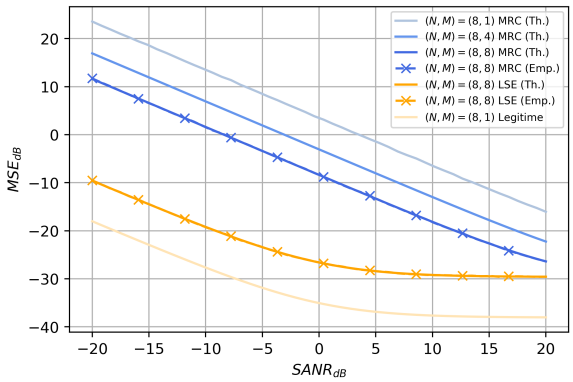

FIGURE 1 : MSE des estimateurs MRC et LSE pour $(N, \sigma_{\text{noise}}) = (8, 0{,}05)$ en fonction du $SANR_{\text{dB}}$, dans le cas d'un espion déployant des antennes équi-réparties dans les intervalles $]-\pi/3, -0{,}2[\cup]0{,}2, \pi/3[$.

lorsque l'espion dispose de la moitié du nombre d'antennes utilisé par l'émetteur. Plus précisément, pour une SANR supérieure à 5 dB, la MSE tombe en dessous de -10 dB lorsque l'estimateur MRC utilise 4 capteurs, tandis que 8 antennes sont utilisées au niveau de l'émetteur.

Il est également important de noter qu'à mesure que le SANR approche de $-\infty$, c'est-à-dire lorsque σ_{an} tend vers 1, la performance du récepteur légitime se détériore également. Plus précisément, la MSE atteint -20 dB pour un SANR de -20 dB, tandis qu'elle atteint -35 dB pour SANR égal à 0 dB. En observant (4), cela s'explique par le fait que la puissance du message d'intérêt diminue à mesure que le SANR diminue. Un niveau élevé de bruit artificiel augmente la sécurité, mais réduit la performance du récepteur légitime.

4.2 Influence de l'erreur d'estimation de l'angle de visée (DoD)

L'estimation de l'angle θ_0 définissant la DoD est essentiel pour l'utilisation de ces deux attaques. En effet, pour l'estimation LSE, la valeur de cet angle détermine entièrement $\mathbf{h}_{\theta_0}$ dans le cadre d'un canal LoS. Pour l'estimation MRC, le facteur d'échelle et de rotation de la constellation dans la direction θ_m, $\mathbf{h}_{\theta_m}\mathbf{w}$ est entièrement déterminé par θ_0, étant donné que l'espion connaît parfaitement le canal $\mathbf{h}_{\theta_m}$. Il est donc nécessaire d'évaluer la robustesse de ces attaques à une erreur d'estimation de θ_0. La figure 2 évalue l'impact d'une erreur d'estimation dans la DoD θ_0. Si $\mathbf{w}$, $\mathbf{h}_0$ et $\mathbf{H}$ dans les équations (8) et (12) sont estimés en fonctions de $\theta_0 + \epsilon$, le graphique illustre la dégradation de la MSE pour les estimations MRC et LSE en fonction de ϵ.

Pour $\epsilon > 1.5°$, les estimateurs MRC et LSE présentent des performances pratiquement identiques. Cela indique qu'au-delà d'un certain seuil d'erreur d'estimation, l'avantage d'utiliser LSE plutôt que MRC diminue considérablement. Dans ces conditions, pour les deux estimateurs, la démodulation devient quasi-impossible lorsque $\epsilon \geq 3°$ car la MSE est supérieure à -5 dB. Par conséquent, l'impact de l'erreur d'estimation de la DoD, ϵ, devient un facteur dominant, conduisant les deux estimateurs à converger en termes de performance MSE.

5 Conclusion et perspectives

Dans ce travail, nous avons étudié deux attaques contre le schéma de bruit artificiel et évalué leurs performances en terme

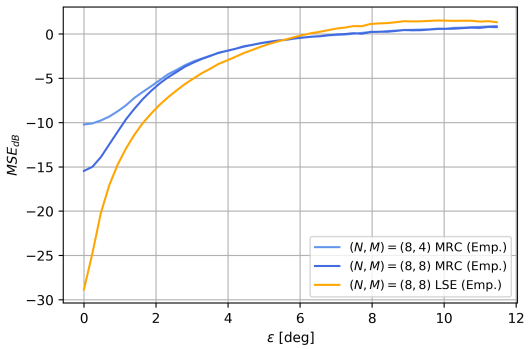

FIGURE 2 : MSE des estimations MRC et LSE pour $(N, \sigma_{noise}, SANR_{dB}) = (8, 0.05, 7)$ en fonction de l'erreur d'estimation ϵ exprimée en degré [deg].

de MSE à l'aide de résultats théoriques et de simulations. La première, issue de la littérature (section 3.1), a été re-visitée sous l'angle de la MSE avec divers estimateurs. Elle est efficace lorsque le nombre de points d'écoute dépasse celui des antennes d'émission et suppose la connaissance de la CSI, une hypothèse forte sur les capacités de l'espion. La seconde attaque, introduite dans 3.2, fonctionne même avec un nombre réduit d'écoutes même si les récepteurs sont très proches ce qui facilite son implantation. La limite de cette attaque impose que le bruit artificiel reste modéré. Pour les deux attaques, l'erreur d'estimation de la DoD impacte fortement les performances.

L'efficacité des attaques dépend aussi de la position des points d'écoute, un espion pouvant les optimiser. Enfin, les résultats de la seconde attaque soulignent qu'une forte allocation de puissance au bruit artificiel est nécessaire même contre un espion faiblement équipé, au détriment de l'efficacité énergétique. Une comparaison avec d'autres méthodes de sécurité physique constituerait une perspective intéressante.

Références

[1] Rohit NEGI et Satashu GOEL : Secret communication using artificial noise. *In VTC-2005-Fall. 2005 IEEE 62nd Vehicular Technology Conference, 2005.*, 2005.

[2] Hong NIU et AL : Artificial Noise Elimination : From the Perspective of Eavesdroppers. *IEEE Transactions on Communications*, 2022.

[3] Jules BURGAT et AL : Vulnerability Analysis of Dynamic Directional Modulations : a Multi-Sensor Receiver Attack. *In MILCOM 2024 - 2024 IEEE Military Communications Conference (MILCOM)*, 2024.

[4] Tse et VISWANATH : *Fundamentals of Wireless Communication*. Cambridge University Press, New York, NY, USA, 2004.

[5] Hong NIU et AL : Artificial Noise Elimination Without the Transmitter–Receiver Link CSI. *IEEE Transactions on Vehicular Technology*, 2024.

[6] Hong NIU et AL : When the CSI from Alice to Bob is Unavailable : What Can Eve Do to Eliminate the Artificial Noise ? *In 2022 IEEE 96th Vehicular Technology Conference (VTC2022-Fall)*, 2022.