Table des matières

Liste des tableaux

Liste des figures

Notation et symboles

Notation mathématique

x	scalaire
X	variable aléatoire
$\mathbf{x}$	vecteur
$\mathbf{X}$	matrice
$\mathcal{X}$	ensemble (ou alphabet)
$\|\mathcal{X}\|$	cardinalité de l'ensemble $\mathcal{X}$

Symboles

a_i	$i^{\text{ème}}$ bit dans la séquence binaire de longueur n
B	récepteur (Bob)
$B^{(i)}$	$i^{\text{ème}}$ récepteur
C	capacité d'un canal
$\mathcal{C}$	code (ensemble des mot-codes)
C_e	capacité du canal de l'espion
C_m	capacité du canal légitime
C_s	capacité secrète d'un canal
d	distance entre deux points
D	bande passante du canal)
E	espion (Eve)
E_b	énergie par bit
$E^{(i)}$	$i^{\text{ème}}$ espion
f_c	fréquence porteuse du signal émis
f_d	fréquence Doppler pour le modèle de canal à évanouissement de Rayleigh
g	temps discret
h	gain associé au canal

$\mathbf{h}$	gains complexes du canal de diffusion dégradé SIMO [1]
$\mathbf{H}$	gains complexes du canal de diffusion dégradé SIMO [1]
$\mathbb{H}_b(p)$	entropie binaire de la probabilité p
$\mathbb{H}(X)$	entropie de la variable aléatoire X
$\mathbb{H}(X\|Y)$	entropie conditionnelle de X étant donné Y (équivocation)
$\mathbb{H}(X;Y)$	entropie mutuelle entre X et Y
$\mathbb{I}(X;Y)$	information mutuelle entre X et Y
$\mathbb{I}(X;Y\|Z)$	information mutuelle conditionnelle entre X et Y étant donné Z
J	relais brouilleur (Charlie)
$J^{(i)}$	$i^{\text{ème}}$ relais brouilleur
$\mathbf{k}$	clé secrète de chiffrement
$\mathcal{K}$	ensemble des clés secrètes)
$L(\mathcal{C}_n)$	fuite d'information du code $\mathcal{C}_n$
$\mathbf{m}$	message source
n	longueur d'un vecteur (ou séquence binaire)
N_B	nombre de récepteurs
N_E	nombre d'espions
N_J	nombre de relais brouilleurs
N_S	nombre de sources
N_0	densité spectrale de bruit
p	probabilité de transition
P_e	probabilité d'erreur
P_J	puissance allouée au brouillage
$P_{J^{(i)}}$	puissance allouée au $i^{\text{ème}}$ relais brouilleur
$P_r(X)$	Probabilité de X
P_S	puissance allouée à la source d'émission
$P_{S^{(i)}}$	puissance allouée à la $i^{\text{ème}}$ source d'émission
P_{TOT}	puissance totale allouée au réseau sans fil : $P = P_S + P_J$
$P_{(Y\|X)}$	probabilité d'obtenir Y à la sortie du canal sachant que l'entrée était X
P_η	puissance du bruit blanc Gaussien au niveau du récepteur
P_0	puissance totale consommée au temps discret g
q	probabilité de croisement
r	rayon d'un terminal par rapport à la position de référence
R	taux de transmission d'un canal
R_e	taux d'erreur résiduel d'un canal

R_L	taux de fuite de l'information vers l'espion
s	surface en m^2
S	source d'émission (Alice)
$S^{(i)}$	$i^{\text{ème}}$ source d'émission
$S(\nu)$	densité spectrale de puissance Doppler pour un canal de Rayleigh
t	temps continu
v	vitesse de déplacement
x	symbole source
x_S	signal émis par la source
x_J	signal de brouillage
y_B	signal reçu par le récepteur légitime
y_E	signal reçu par l'espion
σ	écart type
ν	décalage de fréquence Doopler
$(.)^\dagger$	transposé hermitienne
$\sum$	matrice de covariance
λ	longueur d'onde du signal émis par une source
θ	angle d'une direction par rapport à une direction de référence
η	bruit blanc gaussien au niveau du récepteur
θ_i	angle du $i^{\text{ème}}$ direction par rapport à une direction de référence
ρ	coordonnée radiale dans le plan polaire
δ	coefficient de partage de puissance
ϕ	angle de déplacement sur la surface circulaire
$\prod$	matrice stochastique du canal binaire symétrique
ε	probabilité d'effacement
?	symbole d'effacement
α	coefficient d'atténuation linéique du signal dans l'air
τ	retard dans le temps
$\sum$	matrice de covariance

Fonctions

d_k	fonction de décodage cryptographique en utilisant la clé k
$f_X(x)$	fonction de densité de probabilité de X
erf(z)	fonction d'erreur (aussi appelée fonction d'erreur de Gauss)
erfc(z)	fonction d'erreur complémentaire notée de la fonction erf(z)
$F_X(x)$	fonction de répartition de X
$log_b(X)$	logarithme dans la base b de X
w_k	fonction de codage cryptographique en utilisant la clé k
$\oplus$	addition binaire bit à bit

Constantes

e	2,718281828...(Constante de Néper)
π	3,141592653...

Ensembles

$\mathbb{C}$	ensemble des nombres complexes
$\mathbb{R}$	ensemble des nombres réels

Liste des abréviations

AWGN	*Additive White Gaussian Noise* / Bruit Additif Blanc Gaussien
BC	*Broadcast Channel* / Canal de diffusion
BCC	*Broadcast Channel with Confidential messages* / Canal de diffusion avec messages confidentiels
BEC	*Binary Erasure Channel* / Canal binaire à effacement
BER	*Bit Error Rate* / Taux d'erreur de bits
BPSK	*Binary Phase-Shift Keying*/ Modulation numérique par changement de phase à deux phases
BSC	*Binary Symmetric Channel* / Canal binaire symétrique
CSI	*Channel state information* / Informations d'état de canal
DMC	*Discrete Memoryless Channel* / Canal discret sans mémoire
DMS	*Discrete Memoryless Source* / Source discrète sans mémoire
DWTC	*Degraded Wiretap Channel* / Canal dégradé sous écoute
GSM	*Global System for Mobile Communications* / Système global des communications mobiles
ISI	*InterSymbol Interference* / Interférence inter-symbole
i.i.d.	*Independent and Identically Distributed* / Indépendant et identiquement distribué
LRTS	*Radiocommunications and Signal Processing Laboratory* / Laboratoire de Radiocommunications et de Traitement du Signal
LOS	*Line-of-sight* / Ligne-de-vue
LDPC	*Low Density Parity Check* / Contrôle de parité de faible densité
SNR	*Signal-to-Noise Ratio*/ Rapport signal sur bruit
SIMO	*Single-Input Multiple-Outputs channel*/ canal à entrée-unique sorties-multiples
WTC	*Wiretap Channel* / Canal sous écoute

Remerciements

Je tiens tout d'abord à remercier vivement, mon directeur de recherche, le professeur Jean-Yves Chouinard. Malgré un emploi de temps fort chargé, sa disponibilité et ses orientations pertinentes ont sagement guidé le déroulement de mon projet de recherche, le long de mon séjour au Laboratoire de Radiocommunications et de Traitement du Signal (LRTS), où il a su combiner sympathie et sérieux afin de me faire profiter de son expertise pour évaluer mes travaux de recherche et de ses conseils enrichissants, pour diriger l'évolution de mon cursus académique et celle de mon projet de recherche.

Sans oublier d'exprimer ma gratitude au professeur Mohamed Mejri pour son soutien et les connaissances acquises grâce à sa longue expérience dans le domaine de la sécurité informatique.

Je tiens à remercier spécialement le docteur Berdai Abdallah et le chercheur postdoctoral Mohamed Haj Taieb, de m'avoir orienté, aidé et conseillé. Mohammed Haj Taieb, qui n'a jamais hésité à consacrer son temps pour se pencher pleinement avec moi sur les questions liées à mes travaux de recherches et à me faire part de toute son expertise.

J'adresse mes plus sincères remerciements à ma très chère épouse, qui m'a soutenue et encouragé, pour la patience qu'elle m'a accordée et les énormes sacrifices qu'elle a fait pour que je sois là où je n'aurais jamais pu être sans elle. Je lui souhaite la réussite dans ses études dans le domaine de la finance à l'université Sherbrooke. Sans oublier les membres de ma famille qui m'ont aussi encouragés tout au long de ma formation.

Je tiens à exprimer ma sincère gratitude à mon pays, l'Algérie, et surtout mon organisme employeur, qui m'a donné la chance de venir à l'Université Laval et développer mes connaissances dans le domaine de la sécurité des télécommunications.

Enfin, j'adresse mes remerciements à tous les étudiants et amis du Laboratoire de Radiocommunication et de Traitement de Signal et tout le corps enseignant et administratif qui ont fait en sorte que l'environnement de travail soit instructif, propice et agréable.

...pour toutes ces personnes, je dédie ce travail

Chapitre 1

Introduction

1.1 Mise en contexte et problématique

La demande accrue des applications de communication sans fil a généré un développement significatif des réseaux de télécommunications sans fil, qui interconnectent des applications et des terminaux gourmands en ressources de voix et de données. La plupart des informations échangées ou traitées par les terminaux sont de nature confidentielle, d'où la nécessité d'assurer leur protection face aux accès illégitimes par espionnage, vol d'identité ou intrusion.

La méthode classique pour assurer la sécurité est l'utilisation d'une clé de chiffrement secrète partagée entre l'émetteur et le récepteur et éventuellement les nœuds impliqués dans la communication. Shannon [2] a prouvé que l'utilisation d'un masque jetable (one-time-pad) d'une clé $\mathbf{k}$ uniformément répartie sur l'ensemble $\mathcal{K}$ des clés de chiffrement, avec le message source $\mathbf{m}$, garantit une transmission sécurisée. Dans ce cas, aucune fuite d'information n'est faite au profit de l'espion. L'inconvénient majeur est que la longueur de la clé doit être aussi grande que la taille du message émis, ce qui est souvent trop coûteux à mettre en œuvre efficacement. Ceci a conduit à la naissance de la cryptographie à clé publique, qui repose sur les problèmes mathématiques difficiles. Cela empêche les espions de trouver la clé de chiffrement en un temps raisonnable pour déchiffrer la communication légitime.

Néanmoins, avec le développement de la recherche, en particulier la publication des travaux de Wyner [3] et l'introduction de la notion de canal sous écoute, une communication sécurisée entre les utilisateurs légitimes est possible sans nécessairement avoir recours à une clé secrète de chiffrement partagée entre les parties légitimes du réseau de communication.

Les travaux de Wyner ont été développés et généralisés par Csiszàr et Korner [4] et ont donné naissance au concept de brouillage coopératif qui se base sur l'exploitation de la couche physique du canal de communication. Il consiste à confondre les espions par la génération d'un bruit artificiel qui est injecté dans le réseau avec le signal d'information via un ou plusieurs relais, sans toutefois nuire à la fiabilité des communications légitimes : cela est possible par la coopération des utilisateurs légitimes du réseau. Plusieurs méthodes ont été proposées pour réaliser le brouillage coopératif, en prenant en

considération plusieurs contraintes : énergie allouée au réseau, fiabilité des communications légitimes, optimisation des coûts, etc.

Dans ce travail, on analyse plusieurs méthodes de brouillage coopératif dans les réseaux sans fil soumis à l'écoute clandestine impliquant plusieurs terminaux légitimes. Pour chaque méthode, on identifie les limites d'utilisation pour pouvoir proposer un scénario plus performant qui répond au mieux aux contraintes citées supra. Pour cela, on considère tout au long de ce travail, des canaux sans fil gaussien soumis à l'écoute.

Le but de ce travail est d'étudier, de programmer et d'analyser les performances du brouillage coopératif pour la sécurité des communications sans fil. Entre autres, on vérifie par simulation les résultats de divers travaux sur le brouillage coopératif, et on propose des améliorations pour améliorer au maximum le rendement du brouillage coopératif pour un réseau sans fil, en terme de fiabilité de liaison entre les communicants légitimes et en terme de perturbation de l'espion présent.

1.2 Organisation du mémoire

A cet effet, on détaille, dans le deuxième chapitre les principales notions de la théorie de l'information, pour expliquer comment elles ont été exploitées dans le déploiement du concept de brouillage coopératif et l'utilisation de ce dernier dans le but de sécuriser les communications légitimes sur des canaux soumis à l'écoute.

On présente, au chapitre 3, le principe de fonctionnement du brouillage coopératif ainsi que les paramètres à prendre en considération. Il existe plusieurs méthodes de brouillage coopératif et chaque méthode a ses domaines d'applications. Dans ce travail, on considère le brouillage coopératif par du bruit gaussien qui consiste en l'injection de ce bruit généré par un ou plusieurs relais avec le signal d'information émis par la source d'émission. On donne un exemple d'utilisation du brouillage coopératif par du bruit gaussien pour la sécurité des communications légitimes dans les réseaux sans fil soumis à une écoute clandestine.

Au chapitre 4, on étudie le concept de brouillage coopératif dans l'environnement de canaux de communication à affaiblissement. Le support du canal sans fil rencontre toujours des obstacles pendant l'acheminement du signal d'information depuis une source d'émission vers le récepteur correspondant. Ces obstacles vont atténuer, réfléchir, réfracter, et diffracter le signal. Ainsi, le récepteur reçoit une multitude de signaux qui diffèrent dans la phase et la fréquence. Plusieurs stratégies pour la sécurité des communications dans les environnements sans fil à affaiblissement ont été proposés, et un état de l'art est fait. Le modèle de Rayleigh est appliqué aux canaux soumis à l'écoute dans un environnement affecté par du bruit blanc gaussien. On effectue une recherche séquentielle de la configuration garantissant la plus grande fiabilité de la communication légitime, tout en limitant la fuite d'informations quelle que soit sa position dans la surface du réseau de communication.

Après la simulation du concept de brouillage coopératif au chapitre 3, via des stratégies simples à

un seul relais brouilleur, on présente au chapitre 5, plusieurs stratégies plus complexes. Le but est d'étudier l'effet des paramètres suivants sur l'efficacité du brouillage coopératif qui sont le mode d'allocation de puissance entre la source d'émission et les relais brouilleurs ainsi que le nombre de relais brouilleurs. Chaque stratégie proposée est une amélioration de la stratégie qui la précède, après détermination de la limite d'efficacité de cette dernière.

Au chapitre 6, on vérifie premièrement par simulation les résultats des travaux présentées par Dong et al. [5] sur l'application du brouillage coopératif dans un réseau linéaire simple avec un seul relais brouilleur. On propose par la suite un algorithme automatisé et on présente une analyse des résultats obtenus avec cet algorithme qui sert à chercher à améliorer les résultats du du brouillage coopératif obtenus au cinquième chapitre. Cela par l'implantation des N_J relais de la façon la plus rentable pour un réseau bidimensionnels à 3 relais brouilleurs et la détermination de la meilleure allocation de puissance entre la source d'émission et ces relais brouilleurs. On présente des conclusions sur les résultats obtenus avec une configuration à relais unique et à 3 relais.

Nous présentons au chapitre 7 une conclusion générale récapitulant les travaux effectués dans ce mémoire de maîtrise. Nous y indiquons les contributions du mémoire et on propose quelques directives pour des investigations futures pouvant améliorer l'algorithme d'optimisation proposé.

Chapitre 2

Théorie de l'information : fiabilité et sécurité des communications

2.1 Introduction

La théorie des communications est la science qui s'intéresse aux moyens utilisés pour la transmission de l'information depuis une source d'information jusqu'à un utilisateur dit récepteur légitime, d'une façon efficace, fiable et au moindre coût possible. C'est dans ce contexte que s'inscrivent les travaux de Claude E. Shannon, considéré comme le pionnier de la théorie de l'information qui en 1948, a fait de la théorie de l'information un domaine scientifique, en publiant un article [2] qui donna naissance au domaine de la théorie de l'information. Shannon démontra que pour n'importe quel canal de transmission, il était possible de transmettre sur celui-ci avec un taux d'erreur arbitrairement faible tant que le débit de transmission de codage était inférieur à un seuil appelé capacité du canal.

2.2 Architecture d'un système de communications

Dans sa publication de 1948 [2], Shannon a proposé un modèle bloc de communication, comme illustré à la figure 2.1. Un canal de transmission peut être modélisé comme une entrée à valeurs dans un alphabet $\mathcal{X}$, une sortie à valeurs dans un alphabet $\mathcal{Y}$, ainsi qu'une loi de transition qui détermine la probabilité d'obtenir Y à la sortie du canal sachant que l'entrée était X : cette probabilité est notée $P_r(Y|X)$. La connaissance du canal nous donne ainsi la loi de transition définie par la probabilité de chaque couple de valeurs d'entrée et de sortie X et Y.

2.3 Mesure de l'information

Après avoir définit la composition d'un système de communication, on présente dans ce qui suit, les paramètres de mesure de l'information qui est transportée dans ce canal de communication.

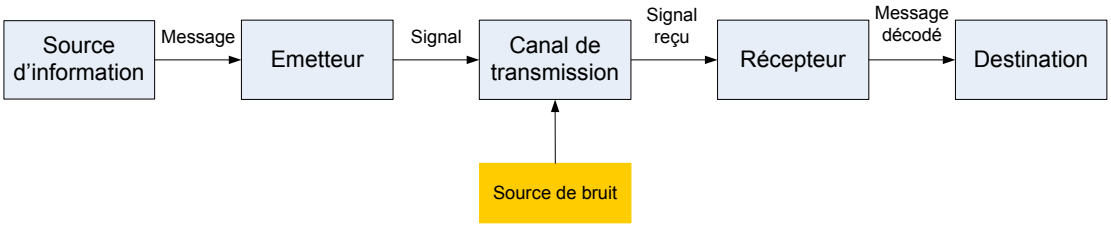


FIGURE 2.1 – *Schéma bloc de Shannon d'un système générique de communication.*

2.3.1 Entropie

Selon Shannon, l'entropie (ou l'incertitude) associée à une variable aléatoire discrète X d'alphabet $\mathcal{X} = \{\mathbf{x}_1,\mathbf{x}_2,.....,\mathbf{x}_z\}$ avec $z = |\mathcal{X}|$ est donnée par [6] :

$$\mathbb{H}(X) = -\sum_{x\in\mathcal{X}} P_r(x)\cdot\log_b P_r(x) \tag{2.1}$$

Cette quantité est par définition non-négative : $\mathbb{H}(X) \geq 0$. La borne supérieure de l'entropie : $\mathbb{H}(X) \leq \log_b|\mathcal{X}|$, est atteinte pour une distribution uniforme des probabilités. On définit l'entropie conditionnelle comme étant l'incertitude d'une variable aléatoire discrète X sachant une autre variable aléatoire discrète Y. L'entropie conditionnelle est définie par :

$$\mathbb{H}(X|Y) = -\sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P_r(x,y)\cdot\log_b P_r(x|y) \tag{2.2}$$

Si X et Y sont indépendantes, alors : $\mathbb{H}(X|Y) = \mathbb{H}(X)$. Le conditionnement réduit l'incertitude : on a toujours $\mathbb{H}(X|Y) \leq \mathbb{H}(X)$.

2.3.2 Information mutuelle

L'information mutuelle entre deux variables aléatoires discrètes X et Y est :

$$\mathbb{I}(X;Y) = \sum_{(x,y)\in\mathcal{X}\times\mathcal{Y}} P_r(x,y)\cdot\log_b\left[\frac{P_r(x,y)}{P_r(x)\cdot P_r(y)}\right] \tag{2.3}$$

Dans le diagramme de "Venn" illustré à la figure 2.2, on montre quelques propriétés de l'entropie et de l'information mutuelle :

– Lien entre l'entropie et l'information mutuelle :

$$\begin{aligned}\mathbb{I}(X;Y) &= \mathbb{H}(X) - \mathbb{H}(X|Y) &(2.4)\\ &= \mathbb{H}(Y) - \mathbb{H}(Y|X) &(2.5)\\ &= \mathbb{H}(X) + \mathbb{H}(Y) - \mathbb{H}(X,Y) &(2.6)\end{aligned}$$

– Si X et Y sont deux variables aléatoires indépendantes alors $\mathbb{I}(X;Y) = 0$.

– Si X et Y sont deux variables aléatoires tel que $Y = X$ alors $\mathbb{I}(X;Y) = \mathbb{H}(X) = \mathbb{H}(Y)$.

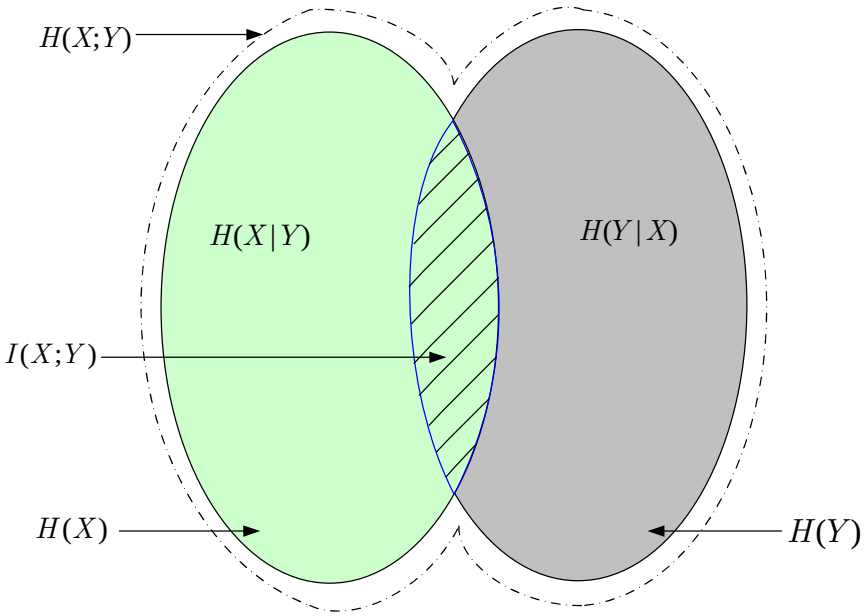


FIGURE 2.2 – *Diagramme de Venn pour l'entropie et l'information mutuelle.*

2.3.3 Capacité de canal

Soit un canal de transmission dont l'entrée est la variable aléatoire X de réalisation $x \in X$ et la sortie est représentée par la variable aléatoire Y de réalisation $y \in Y$. La matrice des probabilités de transition $P_r(y|x)$ exprime la probabilité que l'on observe y sachant que le symbole x a été transmis. Le canal est l'ensemble formé par le triplet $(X,Y,P_r(y,x))$.

La capacité de canal, C, est définie comme étant la quantité maximale d'information mesurée en une unité donnée (par exemple : bit) par unité de temps (par exemple : seconde) qui peut être transmise dans un canal généralement bruité, tel montré à l'équation (2.7).

$$C = \max_{\mathcal{S}(P_r(X))} \mathbb{I}(X;Y) \tag{2.7}$$

où $\mathcal{S}(P_r(X))$ est l'ensemble de toutes les distributions à l'entrée du canal.

Considérons un canal de capacité C bits/s. Si on veut transmettre une quantité d'information à un taux de transmission R bits/s tel que $R < C$, alors il existe une procédure de codage et une procédure de décodage tel que le taux d'erreur résiduel R_e soit arbitrairement faible [7]. Dans ce cas, il existe un codage qui permet d'avoir une probabilité d'erreur de décodage lorsque la longueur n de la séquence envoyée tend vers l'infini. Inversement, s'il existe un code dont la probabilité d'erreur de décodage est évanescente alors nécessairement on a $R \leq C$. En l'absence de bruit, la capacité C d'un canal est

le maximum de l'information moyenne de ce canal. La présence du bruit conditionne la capacité de canal (par symbole ou par unité de temps), imposant ainsi une limite supérieure au débit d'information possible. Si l'alphabet d'entrée du canal est fini et de taille q, alors la capacité en présence de bruit a pour limite supérieure la capacité sans bruit $\log q$, atteinte quand le bruit devient négligeable [8].

Dans ce cadre, on considère à la figure 2.3a, le modèle de canal composé de l'entrée X et de la sortie Y seulement et à la figure 2.3b, le modèle de canal où l'entrée du canal est précédé d'un codeur et suivi d'un décodeur.

En désignant par U et V les variables aléatoires à la sortie du codeur et à l'entrée du décodeur, l'information mutuelle du système s'écrit comme suit :

$$\mathbb{I}(U;V) = \mathbb{H}(U) - \mathbb{H}(U|V) \tag{2.8}$$

L'équation (2.8) peut être reliée avec l'entropie du canal sans *codeur/décodeur* par l'équation (2.9).

$$\mathbb{I}(U;V) \geq \mathbb{I}(X;Y) \tag{2.9}$$

Cette inégalité est dû au fait que le codeur et le décodeur ne créent pas d'information.

(a) Canal de transmission sans codeur et décodeur.

(b) Canal de transmission avec codeur et décodeur.

FIGURE 2.3 – *Principe de base du codage de canal.*

2.4 Sécurité des communications dans les canaux bruités

La confidentialité des informations est un facteur clé pour l'établissement d'une communication sécurisée entre un émetteur et un récepteur légitimes. On peut se poser les questions suivantes :

Comment l'information peut-elle être communiquer de manière fiable pour les utilisateurs légitimes, tout en la gardant secrète à l'espion ?

Comment une telle contrainte de secret sur la communication va-t-elle influer sur les limites et le flux de l'information dans le réseau ?

La théorie de l'information du secret répond à ces préoccupations en cherchant les moyens et les techniques de chiffrement robustes pour lutter contre les actes d'intrusion qui essayent d'extraire de l'information à partir des séquences qu'ils captent d'une communication légitime.

On peut modéliser un système de communication soumis à l'écoute de l'espion comme illustré à la figure 2.4. On prend comme exemple de canal, le canal binaire à effacement soumis à l'écoute (BEC), avec une probabilité d'effacement ε [7].

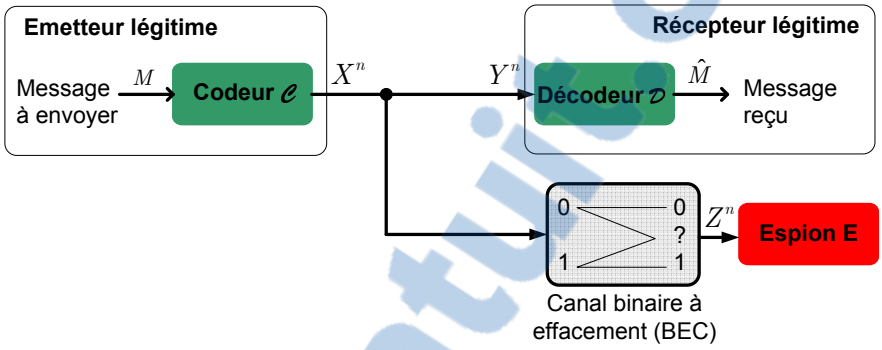


FIGURE 2.4 – *Communication sur un canal binaire à effacement (BEC) soumis à l'écoute.*

Dans ce système, on définit deux interlocuteurs. L'émetteur légitime, Alice, envoie au récepteur légitime, Bob, des mots-codes de longueur n sur ce canal. Une tierce personne, l'espion Eve, observe une version corrompue de ces mots-codes à la sortie du canal avec une probabilité d'effacement $\varepsilon \in [0,1]$. Les messages sont choisis dans l'ensemble $\mathcal{X} \in \{0,1\}$ uniformément distribués. Les mots-codes sont désignés par la variable aléatoire $X^n \in \{0,1\}^n$. On note l'observation de l'espion comme étant $Z^n \in \{0,1,?\}^n$, où le symbole ? est un symbole d'effacement. On dit que la communication entre l'émetteur et le récepteur légitimes est sécurisée si [7] :

$$\lim_{n\to\infty} = \mathbb{I}(X^n;Z^n) = 0 \tag{2.10}$$

On cherche à minimiser au maximum la quantité $\mathbb{I}(X^n;Z^n)$ que l'on considère comme étant la fuite d'informations vers l'espion. On présente dans ce qui suit, quelques théories visant à satisfaire l'équation 2.10.

2.4.1 Modèle de chiffrement de Shannon

Considérons le schéma d'un réseau de communication soumis à l'écoute clandestine par l'espion, illustré à la figure 2.5 [7]. Pour lutter contre cet espionnage, l'émetteur chiffre les communications avec un crypto-système en utilisant une clé secrète de chiffrement K, qui modifie la forme initiale du message à envoyer pour qu'il soit illisible par les espions. Ces fonctions cryptographiques sont en général basées sur des problèmes mathématiques difficiles à résoudre : sans connaître la clé de déchiffrement K, il est difficile, voir impossible, de déchiffrer un message, et ce, tant qu'il n'existe

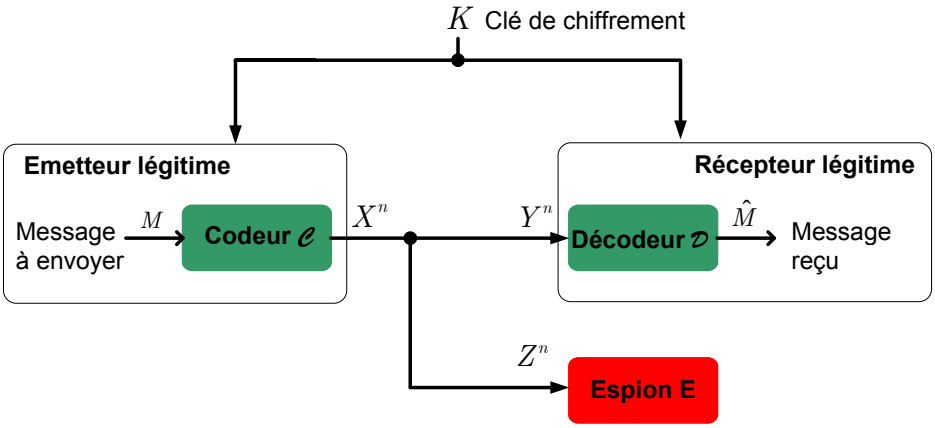


FIGURE 2.5 – *Principe du système de chiffrement de Shannon par l'utilisation d'une clé secrète de chiffrement partagée entre l'émetteur et le récepteurs légitimes.*

pas de moyen de résoudre le problème difficile. Dans [9], Rivest, Shamir et Adleman ont proposé une méthode pour obtenir une signature électronique et une clé publique de chiffrement, en se basant sur les calculs mathématiques difficiles et les nombres premiers [10].

D'une façon plus détaillée, un crypto-système, tel illustré à la figure 2.6, est un quintuple ($\mathcal{M}$, $\mathcal{X}$, $\mathcal{K}$, $\mathcal{W}$, $\mathcal{D}$), composé des cinq éléments suivants :

$$\begin{aligned}
\mathcal{M} &= \text{ensemble des messages clairs,} \\
\mathcal{X} &= \text{ensembles des messages chiffrés,} \\
\mathcal{K} &= \text{ensemble des clés secrètes,} \\
\mathcal{W} &= \text{fonction de chiffrement : } \{w_k : \mathcal{M} \to \mathcal{X} | k \in \mathcal{K}\}, \\
\mathcal{D} &= \text{fonction de déchiffrement : } \{d_k : \mathcal{X} \to \mathcal{M} | k \in \mathcal{K}\}.
\end{aligned}$$

tel que : $\forall\, k \in \mathcal{K}, \forall\, m \in \mathcal{M}, \exists\, k^{-1} \in \mathcal{K} \mid d_{k^{-1}}(w_k(m)) = m$.

Les messages sources m sont supposés aléatoires et tirés de l'ensemble des messages possibles $\mathcal{M}$. Les clés de chiffrement doivent être le plus aléatoire possible : elles sont tirées de l'ensemble $\mathcal{K}$ des clés de chiffrement possibles, où $\mathcal{K}$ est indépendant de $\mathcal{M}$. On parle de communication fiable si le récepteur légitime restitue sans erreur le message original : $m = d_k(x,k)$ avec $x = w_k(m,k)$. L'espion ne connaît généralement pas la valeur de la clé secrète k, mais il est susceptible de connaître la fonction de chiffrement w et la fonction de déchiffrement d. La mesure de l'entropie conditionnelle $\mathbb{H}(M|X)$ nous renseigne sur la quantité d'information que l'espion peut intercepter, ou équivocation . Elle peut être interprétée comme étant l'incertitude de l'espion sur les messages après avoir intercepté les mots-codes.

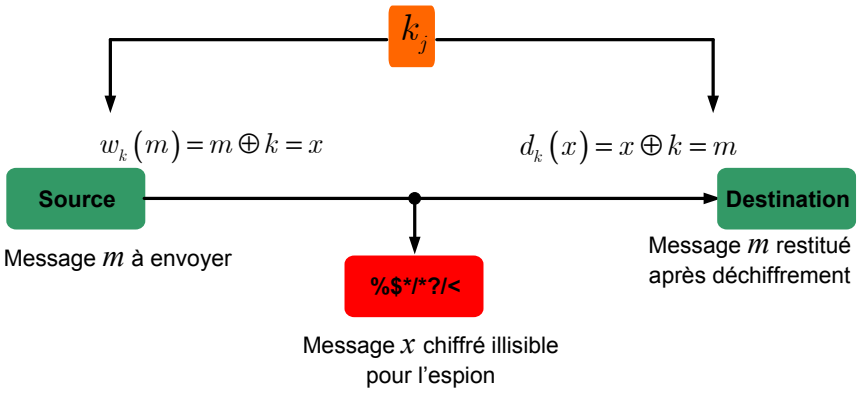


FIGURE 2.6 – *Fonctionnement d'un quintuple cryptographique* $(\mathcal{M}, \mathcal{X}, \mathcal{K}, \mathcal{W}, \mathcal{D})$.

2.4.2 Chiffrement de Vernam

On dit qu'un système de codage pour le système de chiffrement de Shannon atteint le secret parfait, si : $\mathbb{H}(K) \geq \mathbb{H}(M)$. Dans le cas particulier où on a : $|\mathcal{M}| = |\mathcal{X}| = |\mathcal{K}|$, on parle d'un *chiffrement de Vernam*, comme illustré à la figure 2.7. Dans ce cas, la condition pour avoir le secret parfait est donnée

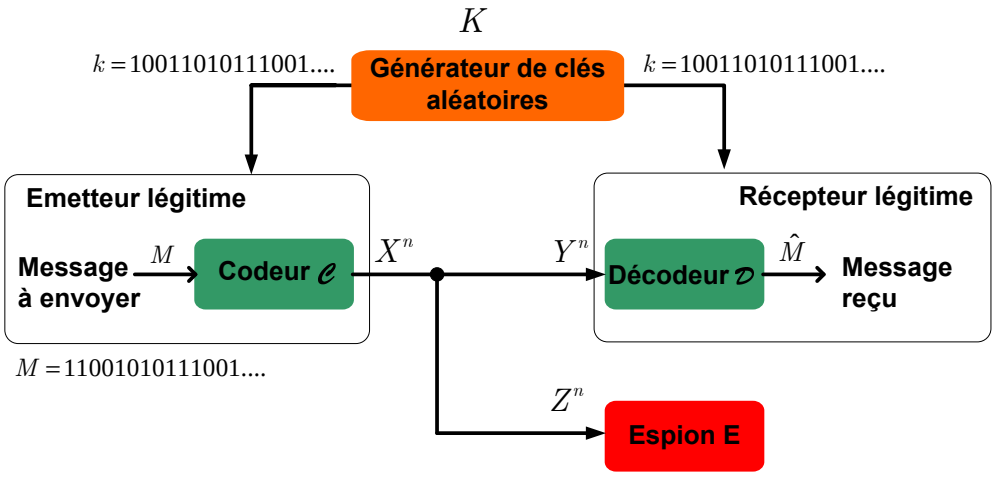


FIGURE 2.7 – *Chiffrement de Vernam utilisant un masque jetable (one-time-pad).*

par les deux conditions suivantes :

- pour chaque paire $(m,x) \in \mathcal{M} \times \mathcal{X}$, il existe une clé unique $k \in \mathcal{K}$ tel que $x = w(m,k)$,
- la clé k est uniformément distribuée dans l'ensemble $\mathcal{K}$.

Dans le système de codage de Vernam de la figure 2.7, pour envoyer un message $m \in \mathcal{M}$, l'émetteur légitime procède tout d'abord à son chiffrement par l'opération suivante : $x = m \oplus k$, (la clé de chiffrement $k \in \mathcal{K}$ est indépendante des messages m et uniformément distribuée sur $\mathcal{M}$). Pour restituer

le message m original du mot-code x sans erreur à la réception, on procède à l'opération suivante : $m = x \oplus k = (m \oplus k) \oplus k$.

En résonnant du point de vue entropie et information mutuelle, on a [7] :

$$\mathbb{I}(M;X) = \mathbb{H}(X) - \mathbb{H}(X|M) \tag{2.11}$$

Puisqu'on a un chiffrement avec masque jetable, l'équation (2.11) peut être écrite comme suit :

$$\mathbb{I}(M;X) = \mathbb{H}(X) - \mathbb{H}(K|M) \tag{2.12}$$

Avec K et M indépendants, l'équation (2.12) peut être écrite comme suit :

$$\mathbb{I}(M;X) = \mathbb{H}(X) - \mathbb{H}(K) = \log|\mathcal{X}| - \log|\mathcal{K}| = 0 \tag{2.13}$$

2.4.3 Modèle de canal sous écoute de Wyner : capacité secrète

La capacité secrète a été étudiée en [3] pour le canal discret sans mémoire sous écoute et dans [11] pour le canal gaussien sous écoute. Wyner [3] fut le premier à introduire la notion de capacité secrète par le biais d'un modèle de canal appelé canal dégradé sous écoute (DWTC) [12]. Le canal DWTC est le cas de canal dans lequel, on distingue deux interlocuteurs légitimes, soit Alice et Bob : Alice tente d'envoyer des informations à Bob tandis qu'une l'espion Eve observe une version du signal reçu par le récepteur légitime.

Deux canaux constituent le canal (DWTC) tel indiqué à la figure 2.8 : le premier est un canal discret sans mémoire (DMC) $(\mathcal{X}, P_r(Y|X), \mathcal{Y})$ caractérisé par la probabilité de transition $P_r(Y|X)$ et considéré comme le canal principal, tandis que le second canal (DMC) $(\mathcal{X}, P_r(Z|X), \mathcal{Z})$ de probabilité de transition $P_r(Z|X)$ est considéré comme le canal de l'espion.

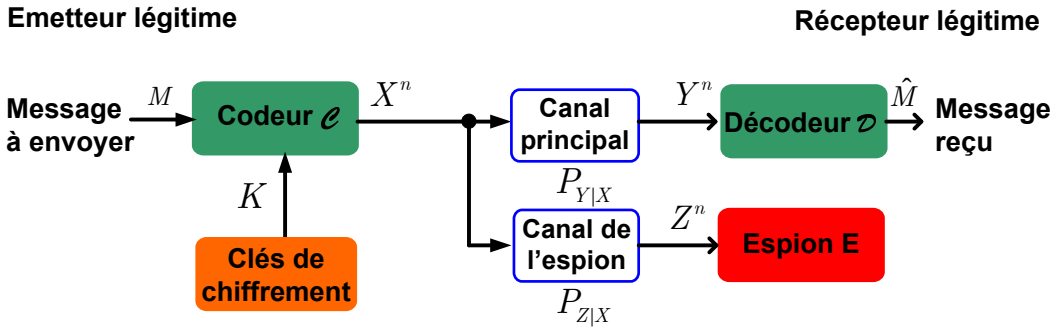


FIGURE 2.8 – *Schéma de principe d'un canal dégradé sous écoute (DWTC).*

La capacité secrète du canal (DWTC) $(\mathcal{X}, P_r(Y|X), \mathcal{Y}, \mathcal{Z})$ est donnée en fonction de l'information mutuelle :

$$C_s = \max_{P_r(x)} \mathbb{I}(X;Y|Z) = \max_{P_r(x)} (\mathbb{I}(X;Y) - \mathbb{I}(X;Z)) = C_m - C_e \tag{2.14}$$

Exemple de calcul de la capacité secrète : Pour mieux comprendre l'équation (2.14), considérons le canal (DWTC) $(\mathcal{X}, P_r(Y|X), \mathcal{Y}, \mathcal{Z})$ illustré à la figure 2.9, dans lequel, le canal principal est un canal en "Z" avec le paramètre p et le canal de l'espion est un canal binaire symétrique (BSC) avec une probabilité de croisement q. On a alors :

$$C_m = \max_{q\in[0,1]} \left(\mathbb{H}_b(q(1-p)) - q\cdot\mathbb{H}_b(p)\right) \tag{2.15}$$

$$C_e = 1-\mathbb{H}_b(p) \tag{2.16}$$

$$C_s = \max_{q\in[0,1]} \left(\mathbb{H}_b(q(1-p)) + (1-q)\cdot\mathbb{H}_b(p) - \mathbb{H}_b(p+q-2\cdot p\cdot q)\right) \tag{2.17}$$

La capacité secrète est au moins égale à la différence entre la capacité du canal principal et celle du canal de l'espion. Si on a le cas où $Y = Z$, cela veut dire que l'information captée par l'espion est la même que celle reçue par le récepteur légitime, on a donc $\mathbb{I}(X,Y|Z) = 0$ et par suite la capacité $C_s = 0$. La valeur de la capacité secrète est relative et dépend des débits d'information vers Bob et vers Eve.

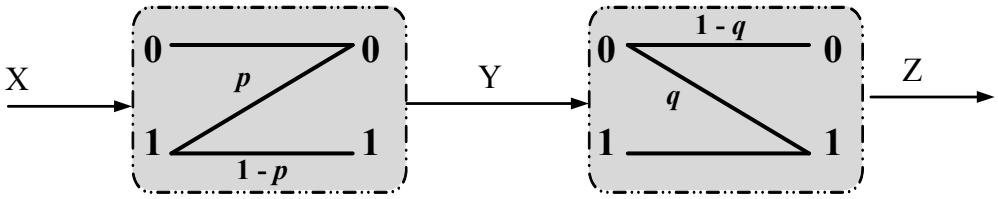


FIGURE 2.9 – *Exemple de canal DWTC avec canaux non symétrique.*

2.4.4 Capacité secrète des canaux gaussiens

Pour un canal gaussien, la capacité secrète C_s s'écrit comme suit [13] :

$$C_s = C_m - C_e = \frac{1}{2}\log\left(1+\frac{P}{\sigma_B^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_E^2}\right) \tag{2.18}$$

où P est la puissance du signal, σ_B et σ_E sont la variance des signaux de Bob et Eve respectivement, C_B et C_E sont respectivement la capacité du canal principal *Alice - Bob* et la capacité du canal de l'espion *Alice - Eve*.

2.4.5 Mesure du taux d'erreur au récepteur

On peut aussi mesurer le taux du secret d'un système de communication soumis à l'écoute clandestine par la mesure du taux d'erreur au niveau du récepteur légitime et de l'espion.

Dans les simulations, l'évaluation du taux d'erreur au niveau du récepteur légitime nous renseigne sur la fiabilité de la liaison légitime entre ce récepteur et la source d'émission. Tant que ce taux

d'erreur est au plus égal à une valeur seuil, la liaison reste fiable. L'évaluation du taux d'erreur au niveau de l'espion nous renseigne sur le taux de sécurité dans le système de communication (fuite d'informations vers l'espion). Plus ce taux d'erreur est élevé, plus sécurisé est le réseau. Cela dans le cas où on connaît la position de l'espion. Par contre, si la position de l'espion est inconnue, le cas le plus général, la sécurité du réseau dépend de la valeur moyenne du taux d'erreur de l'espion sur toute la surface du réseau de communication.

On évalue le taux d'erreur au niveau d'un récepteur en comparant le signal y reçu par ce même récepteur avec le signal x émis par la source d'information et calculer le nombre de bits erronés. La probabilité d'erreur de décodage au niveau du récepteur est :

$$P_e = \frac{\sum a_i \left\{ \begin{array}{l} a_i = 1 \text{ si } x(i) \neq y(i) \\ a_i = 0 \text{ si } x(i) = y(i) \end{array} \right\} i = 1,...,n}{n} \tag{2.19}$$

où a_i est le $i^{\text{ème}}$ bit de la séquence reçue et n est la longueur des séquences émises et reçus. Au niveau de la réception, on fait la somme des tensions des bits de même ordre dans le signal émis et le signal reçu. La valeur de chaque a_i se détermine par décision ferme : si cette somme de tension est positive alors $a_i = 1$ et si cette somme est négative alors $a_i = 0$.

2.5 Conclusion

Dans ce chapitre, on a présenté les principaux travaux et résultats de la théorie d'information qui ont menés par la suite à la mise en place du concept de brouillage coopératif, comme on va le voir au chapitre 3. On a commencé par présenter à la section 2.2, l'architecture générale d'un système de communication, tel définit par Shannon et à la section 2.3 les principales mesures qu'on peut faire, en particulier la mesure de l'information mutuelle, essentielle pour mesurer la capacité secrète. A la section 2.4, on a discuté sur la sécurité des communications dans les canaux bruités en commençant par le modèle de Shannon pour la sécurisation des communications légitimes, via l'utilisation d'une clé secrète de chiffrement et le cas particulier qui en découle à savoir le chiffrement de Vernam. On a montré que la principale inconvénient du chiffrement parfait de Vernam est que la clé de chiffrement doit être aussi longue que le message à chiffrer, cela a motivé les chercheurs à trouver les meilleurs moyens pour sécuriser les communications sans fil à moindre coût possible et de la façon la plus fiable. Ainsi, Wyner était parmi les premiers à introduire la notion de capacité secrète dans le domaine de la théorie de l'information, en utilisant son modèle de canal sous écoute. Il a défini la capacité secrète d'un système de communication comme étant la différence entre la capacité du canal légitime et la capacité du canal de l'espion. Ces résultats ont été développés par Csiszár et Körner qui ont montré que l'utilisation de codage de canal et de traitement de signal assurent une communication sécurisée sans avoir recours à une clé de chiffrement, même en présence d'espions dans le réseau sans fil de communication.

La connaissance des statistiques du canal principal et du canal de l'espion est importante pour garantir une communication sécurisée. Néanmoins, la connaissance des statistiques du canal de l'espion n'est pas aussi facile à déterminer que celles du canal principal puisque les deux interlocuteurs peuvent coopérer pour caractériser leur canal.

Chapitre 3

Sécurité du réseau - brouillage coopératif

3.1 Introduction

Contrairement aux méthodes de sécurité basées sur l'utilisation d'algorithmes cryptographiques au niveau des couches réseaux supérieures pour encrypter les informations échangées, la sécurité de la couche physique repose sur l'exploitation des caractéristiques physiques du canal sans fil (initialement introduite par Wyner [3]). On distingue alors deux situations :

1. Les réseaux sans fil classiques sans contrainte du secret, i.e absence d'espion, où la stratégie la plus courante pour la coopération de l'utilisateur est le relais de coopération pour l'amplification et la retransmission du signal reçu.
2. Les réseaux sans fil avec la contrainte de communication secrète, i.e présence d'un ou de plusieurs espions. On peut recourir au brouillage coopératif pour confondre l'espion. Cela est possible si le canal de l'espion est une version dégradée du canal principal et à un débit secret non nul sans que l'espion en tire profit de ses observations. Ce débit secret est généralement nul si les conditions du canal principal sont mauvaises c'est à dire pire que celles du canal de l'espion [14]. Une solution pour contourner le cas non souhaitable d'une dégradation du canal principal par rapport au canal de l'espion est le recours à la coopération des autres utilisateurs du réseau.

La première approche de la théorie de la sécurité de l'information remonte aux publications de Shannon [2] où il décrit une situation dans laquelle deux interlocuteurs veulent communiquer d'une façon sécurisée sur un canal bruité en présence d'un ou de plusieurs espions. Dans ce chapitre nous présentons le brouillage coopératif comme étant un moyen pour le renforcement de la sécurité de la couche physique des réseaux de communications sans fil. À la section 3.2, on décrit le principe de base du brouillage coopératif pour le renforcement de la sécurité des réseaux sans fil et nous présentons à la section 3.3, une stratégie simple de brouillage coopératif pour la sécurité des canaux gaussiens soumis à l'écoute dans un réseau simple linéaire où la position de l'espion est connue. À la section 3.4, on généralise le cas de la disposition linéaire des terminaux en un réseau sans fil à deux dimensions, pour évaluer les facteurs influant sur l'efficacité du brouillage coopératif où la position de l'espion est

aléatoire. On étudie ainsi l'effet de l'allocation de puissance entre la source d'information et le relais sur les taux d'erreur au niveau des récepteurs.

3.2 Principe du brouillage coopératif

3.2.1 Introduction

Le développement de l'exploitation du principe du canal sous écoute décrit à la section 2.4.3 mène à la naissance du concept de brouillage coopératif pour la sécurité des communications dans les réseaux multi-utilisateurs par l'exploitation des caractéristiques physiques du canal sans fil. Alors que la source transmet son message à sa destination, un relais brouilleur transmet un signal de brouillage afin de confondre l'espion. Ce concept s'inscrit dans la coopération entre les utilisateurs légitimes [15].

Dans ce cadre, considérons un réseau de communication composé de plusieurs émetteurs et récepteurs. Si la fiabilité de la liaison légitime est la seule préoccupation, alors pour maximiser le débit fiable possible d'une paire *émetteur - récepteur* donnée, tous les autres émetteurs ou relais indépendants doivent demeurer en silence puisque les signaux qu'ils transmettent ne feront que provoquer des interférences au niveau du récepteur légitime. Toutefois, lorsque la sécurité est une préoccupation supplémentaire, les émetteurs indépendants peuvent améliorer le débit secret d'une paire *émetteur - récepteur* par la transmission de signaux interférants. C'est grâce aux travaux de Tekin et Yener [16], [17] que ce phénomène a été découvert et publié en 2006 [18].

Lorsqu'un émetteur émet des signaux indépendants du message, ces signaux créent des interférences à la fois pour le récepteur légitime et pour l'espion diminuant ainsi leur capacité de décodage ainsi que leur taux de décodage fiable. Toutefois, l'effet net de ce brouillage peut être une augmentation de la différence des débits du récepteur légitime et de l'espion d'où une augmentation du débit secret atteignable entre les deux interlocuteurs légitimes. Le brouillage coopératif a été initialement proposé pour un canal sous écoute à accès multiple, où plusieurs utilisateurs légitimes souhaitent avoir des communications sécurisées simultanées avec un récepteur prévu en présence d'un espion.

3.2.2 Fonctionnement de base du brouillage coopératif

Considérons la figure 3.1 dans laquelle on illustre le principe du brouillage coopératif : deux sources d'émission discrètes sans mémoire (DMS) Alice et Charlie veulent communiquer simultanément avec un récepteur commun, Bob, via un canal de transmission à accès multiple soumis à une écoute clandestine par l'espion, Eve.

Si la position de l'espion est connue et si le canal entre le brouilleur et cet espion est de meilleure qualité qu'entre ce même relais et le récepteur légitime (par exemple si le relais est plus proche de l'espion que du récepteur légitime) et qu'au même moment le canal entre la source d'émission et le récepteur légitime est plus fiable que celui entre cette source et l'espion, alors le relais brouilleur peut contribuer à renforcer la capacité secrète entre la source et le récepteur légitime en cessant d'envoyer

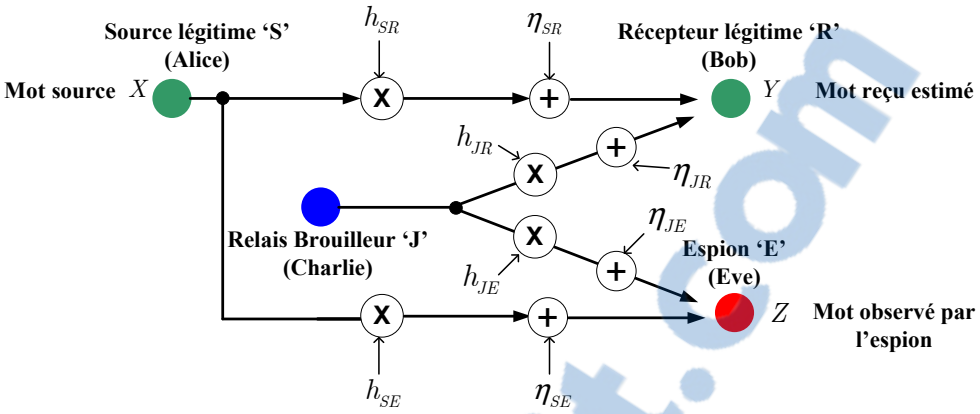


FIGURE 3.1 – *Principe du brouillage coopératif pour un canal sous écoute à accès multiple, constitué d'un émetteur, Alice, d'un récepteur, Bob, d'un espion, Eve et d'un relais brouilleur, Charlie.*

de l'information utile au récepteur légitime et en envoyant des signaux interférants (e.g. du bruit gaussien indépendant) au récepteur légitime et à l'espion simultanément. Étant donné que le canal entre le relais et l'espion est fiable, cela augmente davantage la quantité d'interférence vers l'espion que vers le récepteur légitime : ainsi le relais contribue à l'augmentation du taux secret de liaison entre la source et le récepteur légitime.

Généralement, la position de l'espion est inconnue (position aléatoire dans la surface du réseau). L'objectif est alors d'augmenter au maximum la surface de la zone brouillée par le relais sans nuire à la fiabilité des liaisons légitimes du réseau. Si le réseau dispose de N_J relais, alors leur positionnement idéal sur la surface du réseau garantit la fiabilité et la sécurité des canaux légitimes.

Dans [15], pour que l'espion ne soit pas en mesure de décoder les messages qu'il observe de la communication légitime entre la source d'émission Alice et le récepteur légitime Bob, on propose deux scénarios pour ajouter du bruit généré artificiellement afin de sécuriser les communications à la couche physique de telle sorte que la réception de Bob ne soit pas dégradée ; soit par l'utilisation d'une source multi-antennes, soit par l'utilisation de plusieurs relais brouilleurs mono-antenne. Dans les deux scénarios, on maintient une capacité secrète acceptable qui permet une communication sécurisée entre les interlocuteurs légitimes.

3.3 Simulation du brouillage coopératif dans un réseau sans fil sous écoute : cas d'un espion de position fixe

Dans cette section, on présente la méthodologie et les résultats de simulations obtenus de l'application du brouillage coopératif pour une disposition linéaire des terminaux légitimes et de l'espion. On évalue l'effet de l'emplacement du relais sur le taux d'erreur au récepteur légitime et à l'espion dont sa position est connue.

3.3.1 Description du réseau de communication simulé

Dans le schéma du réseau de communication sans fil illustré à la figure 3.2, on montre le principe de base du brouillage coopératif utilisé pour l'augmentation de la confusion de l'espion et ainsi donner un avantage pour le récepteur légitime. Le dit réseau de communication est constitué d'une source d'émission, Alice, d'un récepteur, Bob, d'un relais brouilleur, Charlie et d'un espion, Eve. Alice est placée au début d'une ligne droite alors que Bob est placé à une distance $d_{SB} = 25$ m de Alice. Charlie est placé à une distance $d_{SJ} = 5$ m et Eve est placé à une distance $d_{SE} = 15$ m. Si on considère la position de Alice comme étant l'origine de début de la ligne droite, on peut classer les différentes distances entre les terminaux comme suit : $d_{SJ} < d_{JE} < d_{SE} < d_{JB} < d_{SB}$.

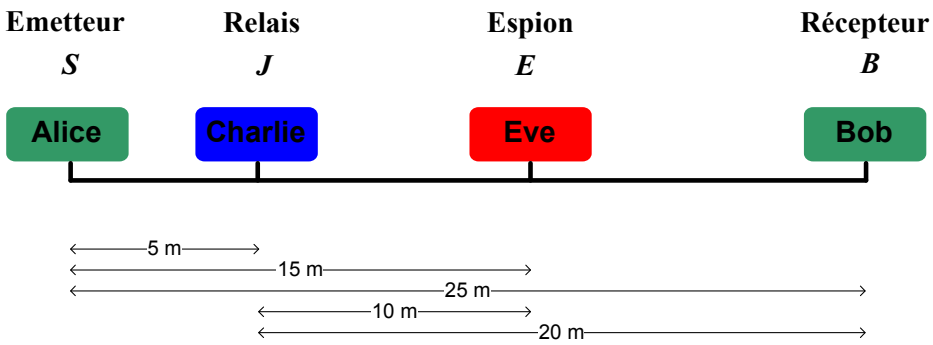


FIGURE 3.2 – *Position des différents terminaux dans le réseau sans fil sous écoute de la simulation [5].*

On définit quatre canaux de communications sans fil dans le système comme illustré au schéma explicatif 3.3 : le premier canal entre la source d'émission Alice et le récepteur Bob, le deuxième canal entre la source d'émission Alice et l'espion Eve, le troisième canal entre le relais brouilleur Charlie et le récepteur Bob et le quatrième canal entre le relais brouilleur Charlie et l'espion Eve. Chaque canal du réseau a un gain h qui dépend de la distance qui sépare les deux extrémités du canal de communication et de l'affaiblissement linéique de coefficient α. Le réseau est soumis à une contrainte de puissance. Un bruit blanc gaussien η est ajouté au signal reçu au niveau de chaque récepteur.

3.3.2 Déroulement des simulations et résultats obtenus

La contrainte de puissance totale allouée au système est $P_{TOT} = -10$ dBm avec $P_{TOT} = P_S + P_J$ à tout temps discret g. La source d'émission Alice émet un signal binaire aléatoire x_S de longueur $n = 1\,000\,000$ bits modulé en BPSK à deux phases $\{-1, 1\}$ à une puissance initiale égale à : $P_S(0)$. Le relais brouilleur Charlie émet au même moment un signal de brouillage aléatoire binaire x_J de même longueur modulé également en BPSK à une puissance initiale : $P_J(0) = P_{TOT} - P_S(0)$. Le bruit blanc gaussien (AWGN) reçu par chaque récepteur a une puissance $P_\eta = -70$ dBm.

Un autre paramètre utilisé dans la simulation est l'atténuation du signal émis exprimée en décibels par kilomètre. Cette atténuation est caractérisée par l'indice d'affaiblissement linéique α définit comme

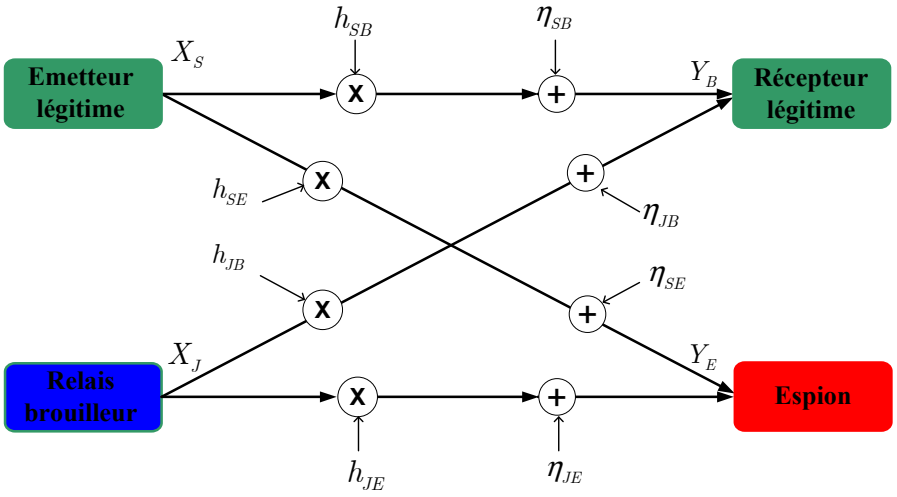


FIGURE 3.3 – *Modèle à quatre canaux de communication dans le réseau sans fil sous écoute.*

étant le taux de diminution d'un signal par unité de distance dont sa valeur dépend du milieu de propagation de ce signal émit par la source :

$$\text{atténuation} = d^{-\alpha} \tag{3.1}$$

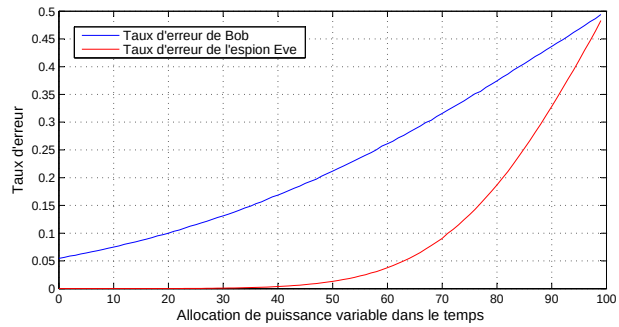
où α est l'indice d'affaiblissement par unité de longueur et d la distance en mètres. Dans cette simulation, on considère deux milieux de propagation : l'espace libre pour lequel $\alpha = 2$ et le milieu urbain pour lequel $\alpha = 3{,}5$, afin de comparer les résultats obtenus pour les deux milieux de propagation. On réalise la simulation en trois étapes :

Première étape des simulations : on alloue au temps discret initial g_0 toute la puissance P_{TOT} à la source Alice pour l'émission de son signal au récepteur Bob via un canal gaussien. Le bruit blanc gaussien s'additionne au signal de Alice au moment de sa réception par les récepteurs Bob et Eve. Les deux séquences reçues y_B et y_E sont de la forme :

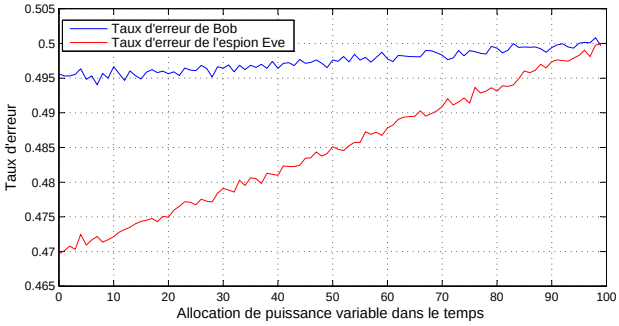
$$\begin{aligned} y_B(g) &= h_{SB} \cdot P_S(g) \cdot x_S + \eta_B \\ y_E(g) &= h_{SE} \cdot P_S(g) \cdot x_S + \eta_E \end{aligned} \tag{3.2}$$

Pour 101 intervalles de temps discret g ($g = 0$ à 1), on ajuste la puissance de la source comme suit : $P_S(g) = m(g) \cdot P_{TOT}$ où $m(g) = m(g-1) - 0{,}01$ et $m(g_0) = 1$, c'est à dire qu'à la dernière allocation de puissance, la puissance allouée à la source Alice est nulle. On évalue à chaque instant discret g le taux d'erreur au niveau de Bob et Eve en comparant les signaux reçus $y_B(g)$ et $y_E(g)$ avec le signal $x_S(g)$ tel expliqué à la section 2.4.5. Les résultats de l'évaluation du taux d'erreur pour $\alpha = 2$ et pour $\alpha = 3{,}5$ sont illustrés aux figures 3.4a et 3.4b.

On voit que les résultats diffèrent beaucoup pour les deux valeurs de α. Dans l'espace libre où $\alpha = 2$ le seul paramètre qui affaiblit le signal émis par la source est la distance. A la première allocation de puissance, le taux d'erreur au niveau de l'espion est très faible car l'espion est relativement proche



(a) $P_\eta = -70$ dBm. $P_{TOT} = -10$ dBm. Milieu de propagation : espace libre où $\alpha = 2$.



(b) $P_\eta = -70$ dBm. $P_{TOT} = -10$ dBm. Milieu de propagation : urbain où $\alpha = 3{,}5$.

FIGURE 3.4 – *Taux d'erreur au niveau de Bob et Eve. Absence du relais brouilleur.*

de la source, le canal *Source-Espion* est alors fiable, contrairement au taux d'erreur au niveau du récepteur légitime qui vaut $P_{e_B} = 5{,}5 \cdot 10^{-2}$ car la distance **Source-Récepteur** est plus grande que la distance **Source-Espion** ce qui fait que le signal de cette source se dégrade davantage avant qu'il soit reçu par le récepteur légitime. Quand on commence à diminuer la puissance allouée à la source, la portée du signal émis par cette source perd de sa fiabilité davantage et cela va affecter en premier lieu le récepteur légitime qui est loin de la source. Ainsi, on voit dans la figure 3.4a que le taux d'erreur de ce récepteur croit rapidement pour atteindre $P_{e_B} = 5 \cdot 10^{-1}$ à la cent et unième allocation de puissance ($g = 101$), alors que le taux d'erreur au niveau de l'espion croit d'une façon moins rapide que celui du récepteur légitime car l'espion est plus proche de la source que le récepteur légitime l'est : le canal *Source-Espion* demeure fiable jusqu'à la trentième allocation de puissance ($g = 30$). Après, le taux d'erreur de l'espion commence à augmenter car la puissance d'émission de la source devient de plus en plus faible, il atteint $P_{e_E} \approx 5 \cdot 10^{-1}$ à la dernière allocation de puissance ($g = 101$).

On conclut que cette configuration du réseau où le milieu de propagation est l'espace libre est favorable pour l'espion plus que pour le récepteur légitime.

À la figure 3.4b on montre les résultats de la même simulation pour $\alpha = 3{,}5$ qui représente le milieu de propagation urbain où le taux d'atténuation du signal est plus important. Cela est causé par les multiples obstacles qui affaiblissent le signal de la source en plus de l'affaiblissement due à la propagation

de ce même signal. Au temps discret initial g_0, le taux d'erreur au niveau des deux récepteurs est déjà élevé : $P_{e_E} = 4{,}7 \cdot 10^{-1}$ et $P_{e_B} = 4{,}9 \cdot 10^{-1}$ car le taux d'affaiblissement α est élevé. La diminution de la puissance allouée à la source à chaque instant discret g ne fait que dégrader davantage le signal de la source. Ainsi, à la dernière allocation de puissance le taux d'erreur P_{e_B} au niveau du récepteur légitime est légèrement supérieur à $5 \cdot 10^{-1}$ et pour l'espion $P_{e_E} = 5 \cdot 10^{-1}$.

Cette configuration du réseau où le milieu de propagation est le milieu urbain est favorable quant à la perturbation de l'espion mais défavorable quant à la fiabilité de la liaison légitime.

Deuxième étape des simulations : on tient compte maintenant du signal brouilleur émit par le relais Charlie. À l'instant discret initial g_0, l'allocation de puissance est $P_S = 100\% \cdot P_{TOT}$ et $P_J = 0\% \cdot P_{TOT}$, c'est à dire que toute la puissance du système est allouée à la source Alice. A chaque instant discret g on évalue le taux d'erreur au niveau du récepteur Bob et de l'espion Eve et on réattribue la puissance du système de la source d'émission Alice vers le relais brouilleur Charlie. Cette réallocation de puissance se fait en fonction du temps discret g ($g \geq 1$) comme suit :

$$\begin{aligned} P_S(g) &= m(g) \cdot P_{TOT} \\ P_J(g) &= P_{TOT} - P_S(g) \\ m(g) &= m(g-1) - 0{,}01 \end{aligned} \tag{3.3}$$

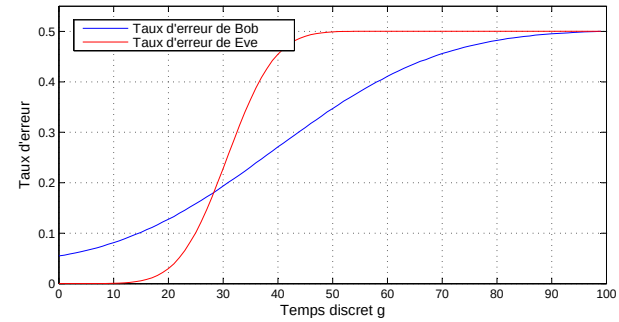
où $m(g_0) = 1$. Cela veut dire qu'à chaque instant discret g, on soustrait une quantité de puissance de la source et on l'ajoute au relais pour faire de nouveau les évaluations des taux d'erreurs au niveau de Bob et Eve. Au total, on considère 101 instants discrets g. Au niveau de ces deux récepteurs, le bruit blanc gaussien s'additionne à la séquence transmise par les terminaux émetteurs au moment de sa réception par les dits récepteurs. Les deux séquences reçues y_B et y_E sont de la forme :

$$\begin{aligned} y_B(g) &= h_{SB} \cdot P_S(g) \cdot x_S + h_{JB} \cdot P_J(g) \cdot x_J + \eta_B \\ y_E(g) &= h_{SE} \cdot P_S(g) \cdot x_S + h_{JE} \cdot P_J(g) \cdot x_J + \eta_E \end{aligned} \tag{3.4}$$

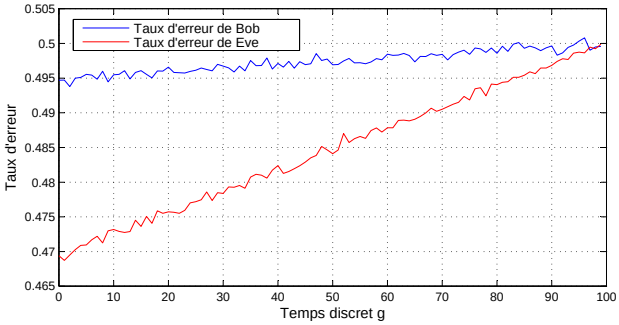
En considérant les positions des différents terminaux indiquées à la figure 3.2, l'évaluation des différents taux d'erreurs au niveau de Bob et Eve pour chaque temps discret g donne les résultats indiqués aux figures 3.5a et 3.5b.

À l'instant discret initial g_0, la totalité de la puissance P_{TOT} est allouée à la source Alice pour l'émission du signal d'information. En l'absence du signal brouilleur ($P_J = 0$), ce dernier est alors reçu sans erreur par Eve et avec un taux d'erreur relativement faible par Bob : le canal *Alice-Eve* est fiable car le signal émis par Alice arrive à Eve sans que l'affaiblissement du signal nuit à la qualité du signal. Cette situation favorable pour Eve est relativement défavorable pour Bob qui a un taux d'erreur de $P_{e_B} = 5{,}5 \cdot 10^{-2}$. Cette situation favorable pour l'espion va persister pour les 11 premières allocations de puissance ($g = 0$ à $g = 10$) où le signal de brouillage reste faible pour qu'il soit perturbateur.

À la figure 3.5b, les variations des taux d'erreurs P_{e_B} et P_{e_E} ont la même allure sauf que dans ce cas, le milieu de propagation (milieu urbain) engendre d'importants affaiblissements au signal de



(a) $P_\eta = -70$ dBm. $P_{TOT} = -10$ dBm. $d_{SJ} = 5$ m. Milieu de propagation : espace libre où $\alpha = 2$.



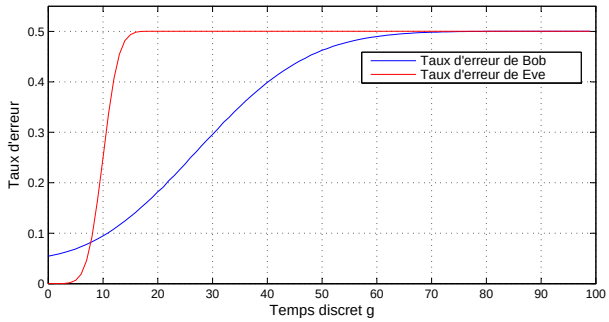
(b) $P_\eta = -70$ dBm. $P_{TOT} = -10$ dBm. $d_{SJ} = 5$ m. Milieu de propagation : urbain où $\alpha = 3{,}5$.

FIGURE 3.5 – *Taux d'erreur au niveau de Bob et Eve sous l'influence du signal brouilleur.*

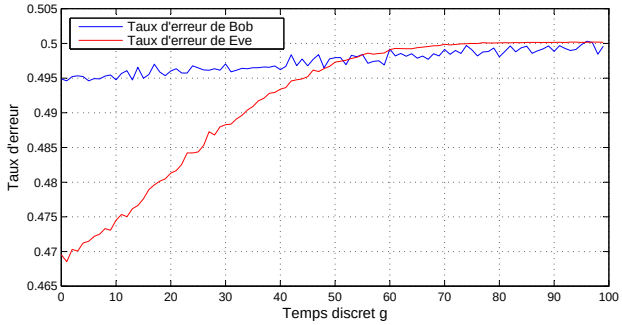
la source Alice avant qu'il soit reçu par Bob et Eve. Dès l'allocation de puissance initiale, le taux d'erreur au niveau de Bob et Eve est très élevé avec $P_{e_B} = 4{,}9 \cdot 10^{-1}$ et $P_{e_E} = 4{,}7 \cdot 10^{-1}$. À chaque nouvelle allocation de puissance, ces taux d'erreurs continuent d'augmenter car la puissance allouée au brouilleur devient suffisante pour que le signal de brouillage devient perturbateur : le taux d'erreur de l'espion commence à augmenter très rapidement pour atteindre $P_{e_E} = 0{,}5$ après la $90^{\text{ème}}$ allocation de puissance, alors que pour Bob le taux d'erreur atteint $P_{e_B} = 0{,}5$ à la $50^{\text{ème}}$ allocation de puissance. Cela est dû au fait que la distance **Charlie-Bob** est plus grande que la distance **Charlie-Eve** au même temps que la distance **Alice-Eve** est plus petite que la distance **Alice-Bob**, ce qui fait que l'espion est soumis à l'effet de brouillage plus que Bob mais il profite d'une réception fiable avec Alice plus que Bob.

Troisième étape des simulations : on déplace le relais brouilleur à la nouvelle coordonnée $d_{SJ} = 10$ m soit 10 m de la source Alice et on refait les mêmes évaluations des taux d'erreurs pour 101 temps discret g en commençant par l'allocation initiale $P_S(g_0) = 100\% \cdot P_{TOT}$ et $P_J(g_0) = 0\% \cdot P_{TOT}$. Les figures 3.6a et 3.6b montrent les résultats obtenus de l'a simulation.

À la figure 3.6a, puisque le relais est plus proche de Bob et de Eve, la situation favorable pour l'espion ne va persister que pour les 5 premières allocations de puissance ($g = 0$ à $g = 4$) après quoi son taux d'erreur croit très rapidement pour atteindre $P_{e_E} = 0{,}5$ à la $16^{\text{ème}}$ allocation de puissance seulement et y



(a) $P_\eta = -70$ dBm. $P_{TOT} = -10$ dBm. $d_{SJ} = 10$ m. Milieu de propagation : espace libre où $\alpha = 2$.



(b) $P_\eta = -70$ dBm. $P_{TOT} = -10$ dBm. $d_{SJ} = 10$ m. Milieu de propagation : urbain où $\alpha = 3{,}5$.

FIGURE 3.6 – *Taux d'erreur au niveau de Bob et Eve sous l'influence du signal brouilleur.*

reste pour les allocations de puissance restantes. Pour le récepteur légitime, toutes les allocations sont défavorables pour lui assurer une liaison fiable avec la source Alice. À chaque quantité de puissance ajoutée au relais, l'effet perturbateur de ce dernier est nettement supérieur à celui pour la première position du relais $d_{SJ} = 5$ m. Le taux d'erreur de Bob atteint lui aussi $P_{e_B} = 0{,}5$ après la $70^{\text{ème}}$ allocation de puissance. Cela est dû au fait qu'en mettant le relais proche des récepteurs, l'effet perturbateur devient important même pour de petites quantités de puissance allouées au relais.

À la figure 3.6b, quelle que soit l'allocation de puissance appliquée, le récepteur Bob demeure toujours très perturbé à cause des fortes atténuations que le signal de Alice subi et son taux d'erreur varie entre $4{,}9 \cdot 10^{-1}$ et $5 \cdot 10^{-1}$. L'espion qui est plus proche de la source voit son taux d'erreur varier entre $4{,}7 \cdot 10^{-1}$ et $5 \cdot 10^{-1}$.

Ces simulations montrent clairement l'effet positif apporté par le brouillage coopératif utilisant du bruit gaussien pour l'augmentation de la confusion de l'espion. Cet effet rend l'utilisation du concept de brouillage coopératif prometteuse. On peut étendre la notion de brouillage coopératif à des systèmes à $(M+1)$ émetteurs, un récepteur et un espion. M relais émetteurs contribuent alors à l'augmentation de la capacité secrète de la liaison légitime entre la source et le récepteur légitime comme le montre la figure 3.7.

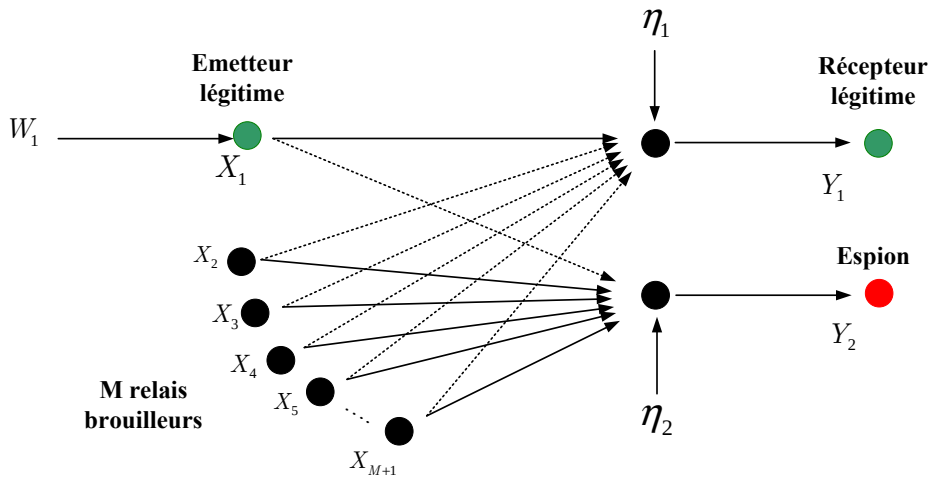


FIGURE 3.7 – *Principe du brouillage coopératif pour un canal sous écoute à M relais qui contribuent à l'augmentation de la capacité secrète de la source [13].*

3.4 Application du brouillage coopératif pour la sécurité des réseaux sans fil

3.4.1 Simulation d'un réseau multi-utilisateurs avec relais brouilleur avec disposition linéaire des terminaux : cas d'un espion mobile

3.4.1.1 Description du réseau de communication simulé

Dans ce scénario, on considère le réseau sans fil simple illustré à la figure 3.8. Les trois terminaux légitimes Alice, Charlie et Bob se positionnent d'une façon linéaire aux coordonnées respectives 0 m (l'origine de l'axe), 25 m et 50 m. Par contre, l'espion Eve est libre de se déplacer entre l'émetteur et le récepteur sur la même ligne droite [5].

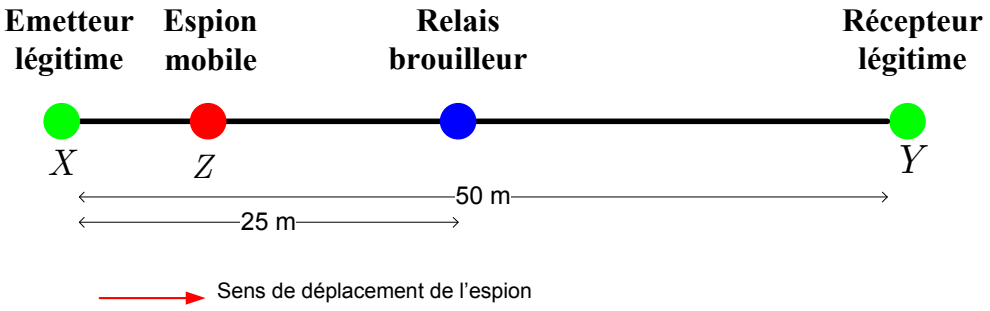


FIGURE 3.8 – *Réseau sans fil simple soumis à une contrainte de puissance P_{TOT}, constitué de l'émetteur Alice, du récepteur Bob, du relais brouilleur Charlie et de l'espion mobile Eve.*

3.4.1.2 Déroulement des simulations et résultats obtenus

L'émetteur Alice génère un signal aléatoire binaire de longueur $n = 20\,000$ bits, de puissance $P_S = -10$ dBm et modulé en BPSK. Au même instant, le relais Charlie émet un signal aléatoire binaire de même longueur $n = 20\,000$ bits à la puissance $P_J = -10$ dBm. Le réseau est soumis à du bruit blanc gaussien de puissance $P_\eta = -70$ dBm. On considère que le milieu de propagation est l'espace libre où $\alpha = 2$. Au niveau de Bob et de Eve, les signaux reçus s'écrivent alors de la forme suivante [19] :

$$\begin{aligned} y_B(g) &= h_{SB} \cdot P_S \cdot x_S(g) + h_{JB} \cdot P_J \cdot x_J(g) + \eta_B \\ y_E(g) &= h_{SE} \cdot P_S \cdot x_S(g) + h_{JE} \cdot P_J \cdot x_J(g) + \eta_E \end{aligned} \tag{3.5}$$

où h est le gain de chaque canal, y est le signal reçu par le récepteur, η est le bruit blanc gaussien reçu par chaque récepteur, P_J et P_S sont les puissances de brouillage et d'émission respectivement, où $P_J + P_S = P_{TOT}$.

À chaque position de Eve, entre 10 m et 90 m de l'origine, Alice et Charlie émettent deux signaux binaires avec les paramètres cités ci-dessus et on évalue au niveau de l'espion Eve le taux d'erreur P_{e_E}. Cette évaluation du taux d'erreur se fait en comparant le signal original émit par la source avec le signal reçu par l'espion tel décrit à la section 2.4.5. Les résultats de la simulation sont illustrés à la figure 3.9.

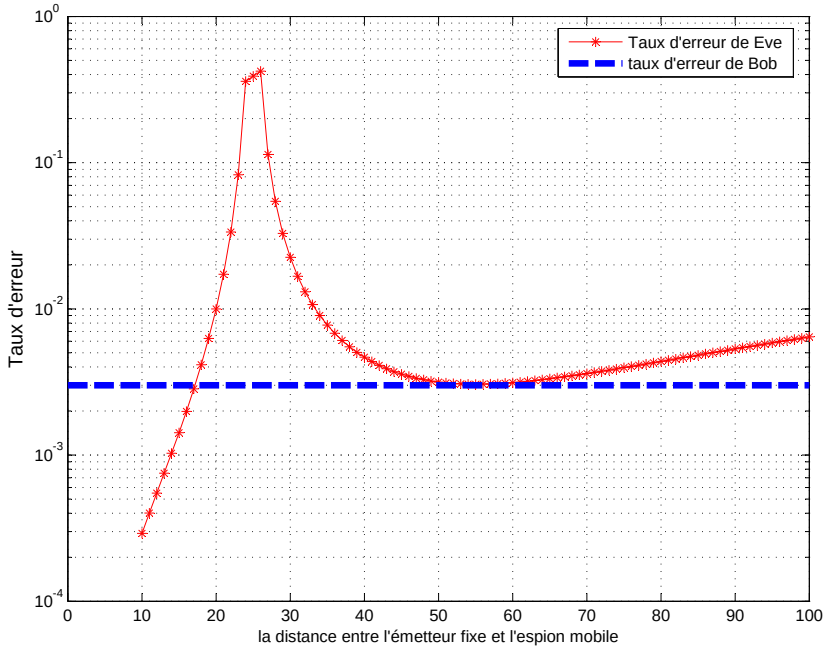


FIGURE 3.9 – *Variation du taux d'erreur P_{e_E} en fonction de la distance* ***Source-Espion*** *en mètres. $n = 20\,000$ bits, $P_S = -10$ dBm, $P_J = -10$ dBm, $P_\eta = -70$ dBm. $\alpha = 2$. $P_{e_B} = 3 \cdot 10^{-3}$.*

3.4.1.3 Interprétation des résultats

On note que le réseau sans fil est soumis à une contrainte de puissance totale $P_{TOT} = P_S + P_J$ où P_S est la puissance d'émission de la source et P_J est la puissance de brouillage du relais. Quand l'espion est proche de la source le canal *Source-Espion* est fiable : le taux d'erreur au niveau de l'espion est $P_{e_E} = 3 \cdot 10^{-4}$, plus petit que le taux d'erreur au niveau de Bob qui vaut $P_{e_B} = 3 \cdot 10^{-3}$ car ce dernier est plus loin de la source que l'espion l'est. Au même instant, l'espion est loin du relais et donc l'effet de ce dernier est faible sur l'espion.

Quand l'espion s'éloigne de la source et s'approche du relais, l'effet de ce dernier devient de plus en plus important sur l'espion et même de petites quantités de puissances suffisent pour perturber l'espion. Le taux d'erreur au niveau de l'espion s'accroît davantage et atteint le maximum de $P_{e_E} = 4 \cdot 10^{-1}$ à 25 m de l'émetteur où l'espion est collé au relais. À cette position, l'effet du relais sur l'espion est le plus grand car la distance Relais-Espion est nulle. Le récepteur légitime Bob qui demeure à sa position a toujours un taux d'erreur fixe de $P_{e_B} = 3 \cdot 10^{-3}$ car la puissance de la source est fixe ainsi que les caractéristiques du canal légitime *Alice-Bob*. Après 25 m, le taux d'erreur de l'espion commence à diminuer de nouveau en s'éloignant du relais. Dans ce cas, le canal de l'espion *Source-Espion* commence à être davantage fiable au même temps que le canal *Relais-Espion* perd de sa fiabilité. Le taux d'erreur de l'espion atteint le minimum de $P_{e_E} = 3 \cdot 10^{-3}$ à 50 m (position de Bob) et c'est le même taux d'erreur que pour le récepteur légitime Bob (en appliquant un codage de canal, le récepteur Bob sera en mesure de détecter et de corriger les erreurs de sa réception). Au delà de 50 m qui est la position du récepteur légitime Bob l'espion s'éloigne davantage de la source Alice et la puissance du signal émis par cette source perd sa fiabilité à chaque déplacement de l'espion. Dans ce cas, le taux d'erreur de l'espion commence à augmenter peu à peu en fonction de la distance **Alice-Espion** et **Relais-Espion**.

On peut donc conclure que si on connaît la position de l'espion, comme le cas de cette stratégie étudiée, l'effet de brouillage coopératif peut améliorer d'une façon considérable la fiabilité de la communication légitime et la sécurité du réseau sans fil, à condition d'attribuer les puissances nécessaires à la source et au relais et de bien positionner le relais. Toutefois, la position de l'espion est généralement inconnue, comme on va l'étudier dans les stratégies de brouillages proposées aux sections suivantes. Dans ce cas, on cherche à augmenter la valeur du taux d'erreur moyen de l'espion sur toute la surface du réseau de communication.

3.4.2 Simulation d'un réseau d'utilisateurs à deux dimensions avec disposition aléatoire des terminaux : effet de la puissance d'émission

3.4.2.1 Réseau d'utilisateurs non soumis à l'effet de brouillage coopératif

On généralise ici le cas précédent du réseau linéaire simple en supposant un réseau d'utilisateurs à deux dimensions comme illustré à la figure 3.10. Ce réseau est composé de la source d'émission Alice positionnée au centre du réseau, du récepteur Bob placé aux coordonnées (15 m, 0 m) et de l'espion

mobile Eve qui peut se déplacer dans toute la surface du réseau.

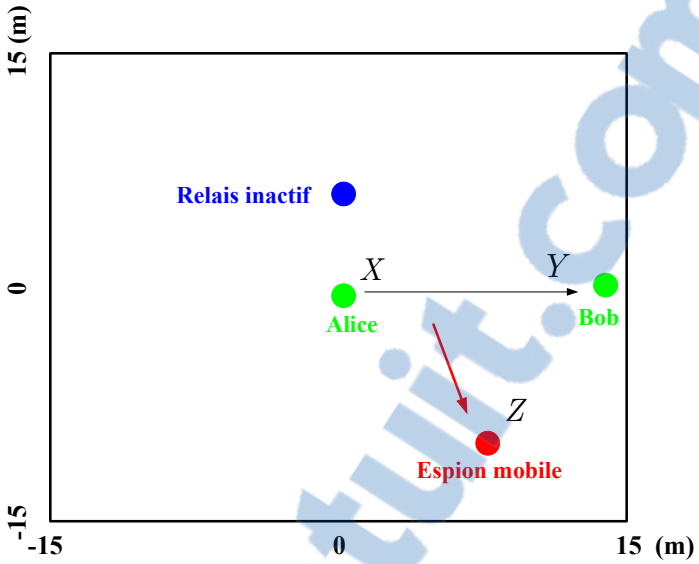


FIGURE 3.10 – *Réseau sans fil constitué de la source d'émission Alice* $(0\ m, 0\ m)$*, du récepteur Bob* $(15\ m, 0\ m)$ *et de l'espion mobile Eve pouvant se déplacer dans toutes les directions.*

La source Alice émet sur un canal gaussien, un signal aléatoire binaire de longueur $n = 100\,000$ bits à la puissance d'émission $P_S = 0$ dBm. L'espion peut se déplacer dans toute la surface du réseau de communication sans fil : il est donc capable de recevoir une copie du signal émis par la source. La simulation consiste à évaluer à chaque position possible de l'espion Eve, le taux d'erreur P_{e_E} au niveau de ce dernier ainsi que le taux d'erreur P_{e_B} au niveau du récepteur Bob. En considérant l'espace libre comme étant le milieu de propagation avec $\alpha = 2$, les résultats des simulations sont illustrés à la figure 3.11.

Cette figure montre l'allure de variation du taux d'erreur P_{e_E} au niveau de l'espion pour une puissance d'émission de Alice $P_S = 0$ dBm. Cette variation est une fonction croissante avec l'augmentation de la distance qui sépare Alice de Eve. Quand cette dernière est proche de Alice, le canal *Alice-Eve* est fiable et le signal que Eve reçoit n'est pas dégradé et son taux d'erreur est très faible. Quand Eve s'éloigne de Alice, la puissance du signal émis par Alice commence à diminuer en fonction de la distance **Alice-Eve**. Cette situation dégrade le signal émis par Alice et cause un nombre élevé de bits erronés ce qui engendre une augmentation progressive de P_{e_E} jusqu'à un taux d'erreur maximal $\approx 4{,}4 \cdot 10^{-1}$ à l'extrémité du réseau, où la distance d entre Alice et Eve est 21,21 m. Le taux d'erreur très faible de l'espion persiste jusqu'à une distance de 10 m autour de la source Alice après quoi ce taux d'erreur commence à augmenter très rapidement. Cette dégradation affecte aussi le récepteur Bob qui se trouve à 15 m de la source Alice où son taux d'erreur P_{e_B} vaut $2{,}6 \cdot 10^{-1}$.

Avec cette puissance d'émission, le réseau est sécurisée avec un taux d'erreur faible dans 65,44% de sa surface et avec un taux d'erreur moyen dans 31,12% et un taux d'erreur élevé dans 3,44% seulement

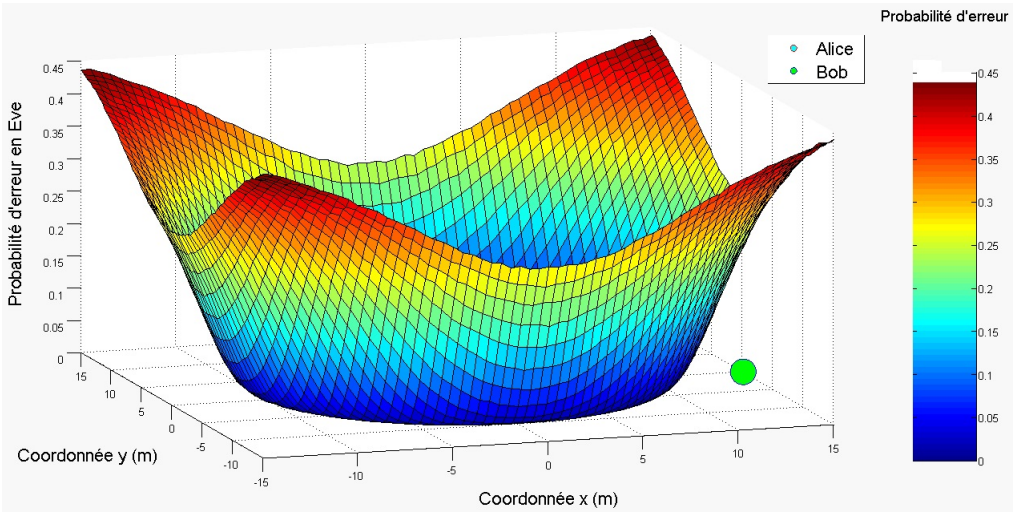


FIGURE 3.11 – *Variation du P_{e_E} en fonction de la position de l'espion Eve par rapport à l'émetteur Alice de coordonnées* $(0\ m, 0\ m)$, $P_S = 0\ dBm$, $P_\eta = -70\ dBm$, $\alpha = 2$, $P_{e_B} = 2{,}6 \cdot 10^{-1}$.

alors que le taux d'erreur moyen de l'espion sur toute la surface du réseau est $E[P_{e_E}] = 0{,}35$. On conclue que la puissance d'émission $P_S = 0$ dBm ne garantit pas une fiabilité de la liaison légitime entre Alice et Bob mais garantit une couverture sécuritaire acceptable.

Pour améliorer la fiabilité de la liaison légitime on doit augmenter la puissance d'émission de la source Alice. La nouvelle puissance est $P_S = 13$ dBm pour laquelle on refait la même simulation d'évaluation des taux d'erreur P_{e_E} et P_{e_B}. Les résultats sont illustrés à la figure 3.12.

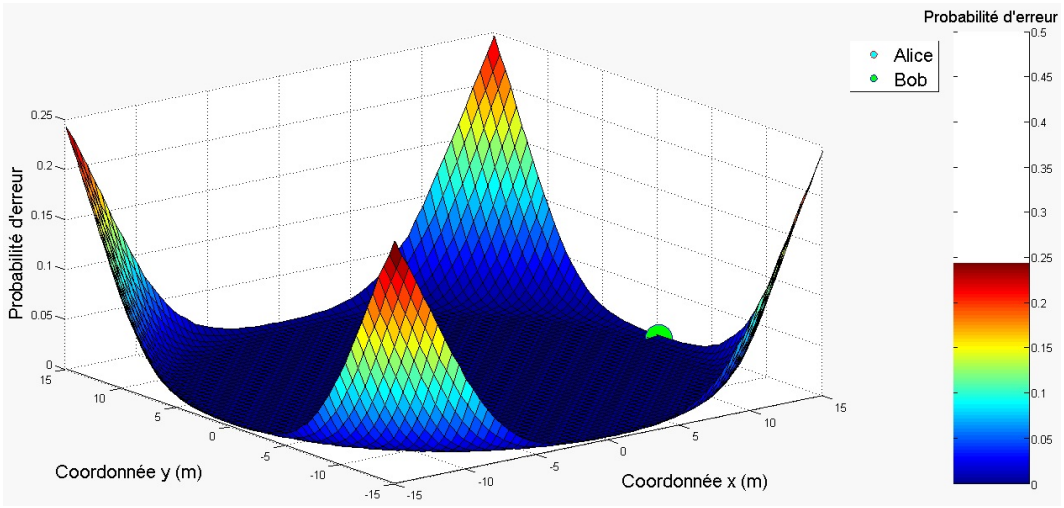


FIGURE 3.12 – *Variation de P_{e_E} en fonction de la distance de Eve par rapport à Alice de coordonnées* $(x = 0\ m, y = 0\ m)$, $P_S = 13\ dBm$, $P_\eta = -70\ dBm$, $P_{e_B} = 2{,}6 \cdot 10^{-3}$.

Avec la nouvelle puissance allouée à la source Alice, le taux d'erreur devient très faible presque partout dans le réseau sans fil et relativement moyen dans les régions les plus lointaines de la source

Alice où P_{e_E} atteint le maximum de $2{,}42 \cdot 10^{-1}$ à la distance $d = 21{,}21$ m de la source Alice. Cela est dû au fait que la puissance d'émission de la source Alice est maintenant plus élevée que le premier cas où $P_S = 0$ dBm seulement. L'influence de l'affaiblissement linéique du signal dû à la distance de coefficient $\alpha = 2$ n'est pas le même sur le signal de Alice pour les deux cas de puissance $P_S = 0$ dBm et $P_S = 10$ dBm même si le taux de diminution reste le même : lorsque $P_S = 0$ dBm, le taux d'erreur à l'extrémité du réseau à la distance $d = 21{,}21$ m vaut $\approx 4{,}4 \cdot 10^{-1}$. Ce taux d'erreur diminue jusqu'à la valeur $\approx 2{,}42 \cdot 10^{-1}$ lorsque $P_S = 13$ dBm. Le récepteur Bob qui se trouve à 15 m de la source a un taux d'erreur de $P_{e_B} = 2{,}6 \cdot 10^{-3}$ ce qui garantit une liaison fiable avec la source Alice.

Avec cette nouvelle puissance allouée à la source le réseau est sécurisée avec un taux d'erreur faible sur 99,33% de sa surface et avec un taux d'erreur moyen dans 0,67%. Le taux d'erreur moyen de l'espion sur toute la surface du réseau a chuté jusqu'à $E[P_{e_E}] = 0{,}01$. On conclut que la puissance d'émission $P_S = 13$ dBm garantit une fiabilité de la liaison légitime entre Alice et Bob mais la couverture sécuritaire est très vulnérable à l'écoute clandestine de l'espion. L'emploi d'un relais brouilleur est nécessaire pour augmenter le taux d'erreur moyen de l'espion car la diminution de la puissance d'émission va augmenter ce taux d'erreur moyen mais la fiabilité des communications légitimes sera perdue.

3.4.2.2 Réseau d'utilisateurs sous l'effet de brouillage :

Considérons maintenant le réseau sans fil de la figure 3.13. On veut évaluer le taux d'erreur P_{e_E} de Eve en fonction de sa distance de la source d'émission Alice sous l'effet du brouillage créé par le relais brouilleur ainsi que le taux d'erreur P_{e_B} au niveau du récepteur Bob. La source Alice émet un signal binaire aléatoire de longueur $n = 100\,000$ bits et modulé en BPSK à la puissance P_S au même temps que le relais Charlie émet un signal binaire de brouillage de même longueur à la puissance P_J. La puissance allouée au système est $P_{TOT} = 13$ dBm qui est la même que pour le cas précédent alors que la puissance du bruit blanc gaussien reçu par les récepteurs a une puissance de $P_\eta = -90$ dBm. La puissance P_{TOT} est dans ce cas partagée entre la source et le relais tel que $P_{TOT} = P_S + P_J$.

On refait les mêmes simulations décrites à la section 3.4.2.1 pour deux allocations de puissances différentes en tenant compte du signal brouilleur du relais pour évaluer le taux d'erreur P_{e_E} et P_{e_B} des signaux reçus (équation 3.5). On obtient les résultats illustrés à la figure 3.14.

Pour l'allocation de puissance égale entre la source et le relais dont les résultats sont illustrés à la figure 3.14a, le taux d'erreur de l'espion est élevé particulièrement autour du relais brouilleur où $P_{e_E} = 5 \cdot 10^{-1}$ et faible dans la zone proche de la source Alice et qui constitue la zone vulnérable aux actes d'espionnage de Eve. Le taux d'erreur d'erreur de l'espion augmente sous l'effet de deux facteurs :

1. Tout d'abord, si l'espion s'éloigne de la source Alice et du relais brouilleur, le taux d'erreur de l'espion augmente à cause de la dégradation du signal émis par Alice sous l'effet de l'affaiblissement.

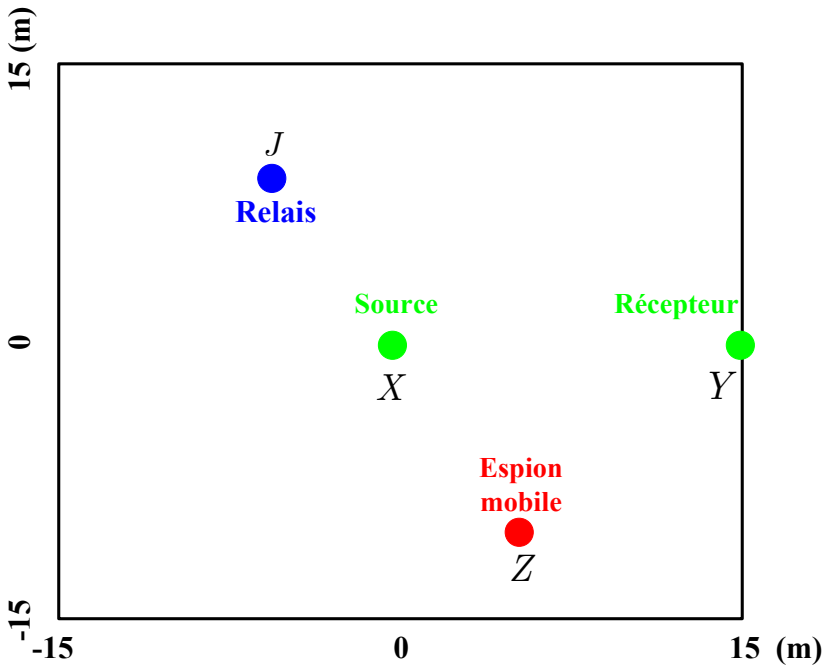


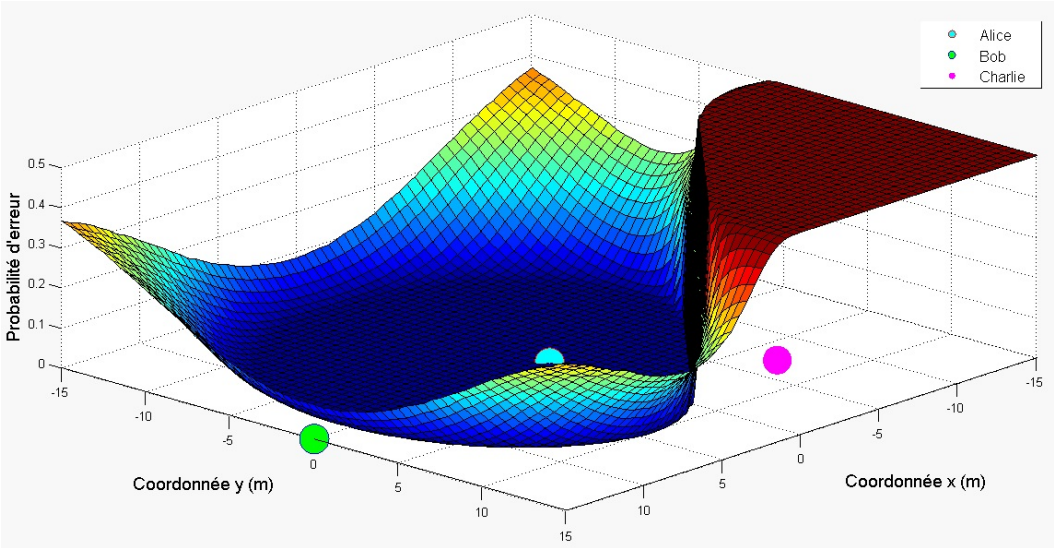
FIGURE 3.13 – *Réseau sans fil à deux dimensions, constitué de l'émetteur Alice* $(0\ m, 0\ m)$*, du récepteur Bob* $(15\ m, 0\ m)$*, du relais de brouillage Charlie* $(-9\ m, 9\ m)$ *et de l'espion mobile Eve.*

2. Le deuxième facteur est le bruit généré par le relais Charlie. Ce dernier a un effet significatif sur l'espion lorsque ce dernier est proche du relais, où son taux d'erreur atteint $P_{e_E} = 5 \cdot 10^{-1}$ tout autour du relais brouilleur. Cette région est considérée comme hautement sécurisée.

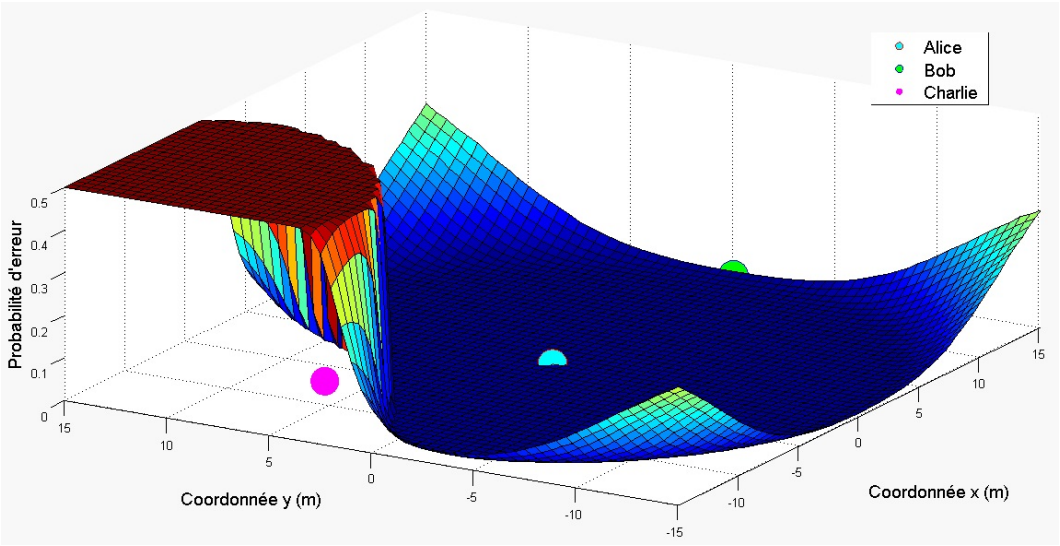
Avec cette allocation de puissance égale entre la source et le relais, le réseau est sécurisé avec un taux d'erreur faible sur 65,44% de sa surface et avec un taux d'erreur moyen sur 11,53% et avec un taux d'erreur élevé sur 23,03 %. On constate qu'avec l'utilisation du relais brouilleur, la zone a taux d'erreur élevé a largement augmenté alors qu'elle était nulle en l'absence du relais. Le taux d'erreur moyen de l'espion sur toute la surface du réseau a aussi augmenté à $E[P_{e_E}] = 0{,}165$.

On conclut que l'allocation de puissance égale entre la source et le relais garantit une couverture sécuritaire satisfaisante car la zone hautement sécurisée est assez grande ainsi que le taux d'erreur moyen sur toute la surface du réseau, mais la fiabilité de la liaison légitime entre Alice et Bob a diminué un peu car le taux d'erreur au niveau du récepteur légitime Bob est $P_{e_B} = 8{,}35 \cdot 10^{-2}$ ce qui rend la capacité de Bob à décoder le signal de Alice difficile.

Pour l'allocation de puissance favorisant la source Alice dont les résultats sont illustrés à la figure 3.14b, l'allure de variation du taux d'erreur de l'espion reste le même que pour une allocation de puissance égale sauf que le taux d'erreur moyen $E[P_{e_E}]$ de l'espion a passé de 0,165 à 0,097 car la portée du signal brouilleur a diminué laissant place à la domination du signal de forte puissance de la source Alice. Cela engendre une amélioration de la fiabilité de la liaison légitime où le taux d'erreur



(a) Allocation de puissance égale à 50%-50%. $P_{e_B} = 8{,}35 \cdot 10^{-2}$.



(b) Allocation de puissance favorisant la source à 80%-20%. $P_{e_B} = 8{,}7 \cdot 10^{-3}$.

FIGURE 3.14 – *Variation du P_{e_E} en fonction de la distance de Eve par rapport à Alice de coordonnées $(0\ m, 0\ m)$. $P_{TOT} = 13\ dBm$, $P_\eta = -90\ dBm$. $\alpha = 2$.*

de Bob a diminué à $P_{e_B} = 8{,}7 \cdot 10^{-3}$ mais la zone vulnérable où le taux d'erreur est faible a augmenté à 81,91% contre 65,44% seulement pour une allocation de puissance égale. La zone moyennement sécurisée a passé à 2,28% contre 11,53% précédemment et la zone fortement sécurisée a passé à 15,80% contre 23,03% précédemment.

3.5 Conclusion

Dans ce chapitre, on a pu montrer que l'on peut sécuriser une communication entre deux entités communicantes légitimes dans un réseau sans fil ouvert en présence d'un ou de plusieurs espions sans avoir recours à une clé privée de chiffrement partagée entre eux, mais en exploitant les caractéristiques physiques des canaux. Cela est possible par l'application du concept de brouillage coopératif qui assure un débit secret garantissant une communication sécurisée comme présenté à la section 3.2.

À la section 3.3, on a analysé les résultats de la simulation du concept de brouillage coopératif pour la sécurité d'un réseau sans fil via une stratégie simple où on a pu démontrer que l'efficacité de ce concept dépend de plusieurs paramètres principalement la position du relais brouilleur dans le réseau sans fil par rapport à l'espion et au récepteur légitime. La connaissance des statistiques du réseau à savoir principalement l'état du canal principal et du canal de l'espion est un point clé pour assurer l'efficacité de ce concept.

À la section 3.4, on a étudié plusieurs situations de brouillage coopératifs pour évaluer les paramètres de réseau qui affectent l'efficacité du brouillage coopératif en terme de fiabilité de liaison légitime entre communicants légitimes et en terme de confusion de l'espion. L'allocation de puissance entre la source d'émission et le relais brouilleur est un facteur très important pour pouvoir assurer une communication fiable entre l'émetteur et le récepteur. La quantité de puissance nécessaire à la source pour transmettre d'une façon fiable son signal d'information dépend de la distance entre l'émetteur et le récepteur. Puisque le réseau sans fil est soumis à une contrainte de puissance, une optimisation de la puissance allouée au relais de brouillage est nécessaire. Bien que l'augmentation de la puissance d'émission va favoriser aussi l'espion, l'utilisation d'un brouillage coopératif adéquat contribue à défavoriser l'espion. L'emplacement physique des relais joue aussi un rôle primordial dans l'efficacité et le rendement du brouillage coopératif. La détermination de cet emplacement du relais sera étudié dans le chapitre 6.

Chapitre 4

Brouillage coopératif dans les canaux à affaiblissement

4.1 Introduction

Dans ce chapitre, on s'intéresse au brouillage coopératif dans les réseaux sans fil à affaiblissement. À la section 4.2, on décrit le phénomène d'affaiblissement et on présente le modèle utilisé pour l'évaluer, ainsi que la contrainte de pertes de propagation et évanouissements liées aux réseaux sans fil à la section 4.3. À la section 4.4, on définit le cas particulier des canaux à affaiblissement de Rayleigh et à la section 4.5 la description du taux d'erreur caractérisant ce modèle de canal. À la section 4.6 on étudie une stratégie de brouillage coopératif pour la sécurité des réseaux sans fil avec des canaux gaussiens soumis à l'écoute dans un environnement à affaiblissement de Rayleigh.

4.2 Modèle de canal à trajets multiples variable dans le temps

Dans la pratique, le support des canaux sans fil se trouve dans des milieux où il y a divers obstacles. Pour cela, les canaux sans fil sont en général modélisés comme des canaux linéaires variables ayant une réponse impulsionnelle et une fonction de transfert variables dans le temps. Ces canaux sont en général non stationnaires, instables et présentent une complexité majeure en estimation du signal et en égalisation.

Dans un environnement à trajets multiples, quand l'émetteur transmet un signal, ce dernier se propage dans le support du canal de transmission, i.e. l'air, où il n'y a pas nécessairement une ligne de vue directe entre l'émetteur et le récepteur. Le récepteur reçoit alors une multitude de signaux complexes provenant de la réflexion du signal émis sur les obstacles rencontrés pendant son mouvement comme les immeubles [20].

En télévision analogique par exemple, la propagation par trajets multiples entraîne l'apparition d'une image fantôme qui est une copie atténuée de l'image principale. Pour les communications radio, la

longueur d'onde est très petite et en conséquence un tout petit déplacement de l'antenne entraîne des changements importants dans le signal. D'autre part, dans les communications radio numériques (tels que le système (GSM)) ce phénomène peut provoquer des erreurs multiples et affecter la qualité des communications. Les erreurs sont dues à l'interférence entre symboles (ISI) où des égaliseurs sont souvent utilisés pour corriger cette interférence [21] [22].

Le canal multivoie peut être modélisé par une réponse impulsionnelle qui comprend l'atténuation, le délai du signal et la modification de la phase sur toutes les versions du signal émis. La figure 4.1 montre la réponse impulsionnelle $h(t,\tau)$ d'un signal dans un canal à affaiblissement de Rayleigh.

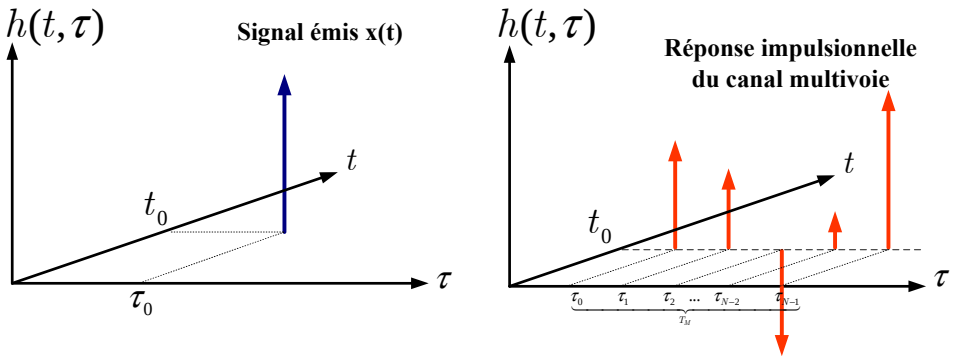


FIGURE 4.1 – *Réponse impulsionnelle d'un canal à trajets multiples.*

Les effets de la propagation multi-trajets sont contradictoires : interférences constructives ou destructives suivant la phase des versions des signaux reçus. Si le délai maximal τ_m est très inférieur à $\frac{1}{D}$, où D est la bande passante du canal [23], alors les composantes multivoie ne peuvent pas être distingués : on a alors affaire à une atténuation de bande étroite. Dans ce cas, l'enveloppe du signal reçu peut être modélisée par une loi dite de Rayleigh, en absence de chemin direct (LOS) entre l'émetteur et le récepteur. Autrement, s'il y a présence d'un chemin discret elle suit une loi dite de Rice. Si $\tau_m \gg \frac{1}{D}$, l'atténuation est dite de large bande. Le signal émis atteint le récepteur à travers de multiples chemins où le $i^{\text{ème}}$ chemin a une atténuation $\alpha_i(t)$ et un retard $\tau_i(t)$.

4.3 Contraintes liées aux réseaux sans fil : Pertes de propagation et évanouissements

Dans un environnement à évanouissement, le signal sans fil émis subit une grande dégradation à cause des effets de la propagation que ce soit pour une émission omnidirectionnelle ou pour une émission directive. La puissance du signal est atténuée lors de sa propagation sur de longues distances appelée pertes de puissance en fonction de la distance (path-loss). À la réception, on a plusieurs versions atténuées avec un retard pour chaque version, toutes affectées par du bruit. Dans un réseau cellulaire par exemple, on distingue un trajet principal et un trajet réfléchi qui peut interférer d'une manière constructive ou destructive avec ce dernier. Les évanouissements à petite échelle correspondent aux

fluctuations rapides en espace en temps et en fréquence du signal reçu qui sont causées par la dispersion du signal émis sur les objets rencontrés le long de son parcours. La diffraction génère des copies du signal original qui peuvent se combiner constructivement et augmenter ainsi le rapport signal-à-bruit (SNR) au récepteur ou de manière destructive en diminuant le (SNR) au récepteur.

4.4 Modèle statistique des canaux à affaiblissement de Rayleigh

Lorsque le signal émis sur un canal à affaiblissement subit des réflexions importantes, on applique le théorème centrale limite pour modéliser la réponse impulsionnelle du canal par un processus gaussien. Si ce processus est de moyenne nulle alors l'enveloppe de la réponse du canal suit une densité de probabilité de Rayleigh et la phase est uniformément distribuée sur l'intervalle $[0, 2\pi)$. Cela est dû au fait que la phase de chaque chemin peut changer par 2π radians lorsque le retard $\tau_i(t)$ change par $\frac{1}{f_c}$ où f_c est la fréquence porteuse du signal émis. Si f_c est grande, les petits mouvements relatifs dans le milieu peuvent causer des changements de 2π radians. Comme la distance entre l'émetteur et le récepteur est plus grande que la longueur d'onde de la fréquence porteuse, on peut supposer que la phase est répartie uniformément entre 0 et 2π radians et que les phases de chaque voie sont indépendantes. L'enveloppe est définie par le module de la réponse impulsionnelle du canal $|h(t,\tau)|$.

L'exigence qu'il y ait de nombreux diffuseurs présents signifie que l'évanouissement de Rayleigh peut être un modèle utile dans les milieux à forte densité comme les villes où il n'y a pas de ligne de vue directe entre l'émetteur et le récepteur. Ces objets vont atténuer, réfléchir, réfracter et diffracter le signal comme le montre la figure 4.2.

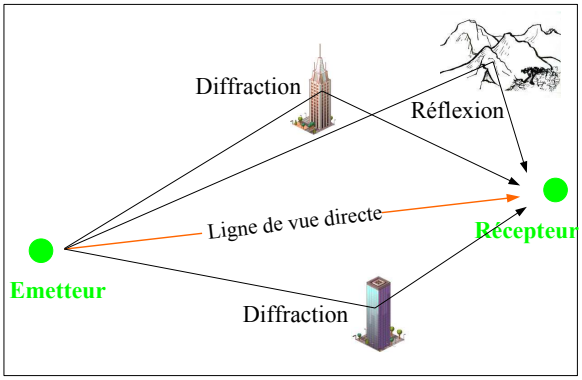


FIGURE 4.2 – *Effet de Rayleigh : les obstacles vont atténuer, réfléchir, réfracter et diffracter le signal émis.*

La figure 4.3 montre un exemple de la réponse du canal de transmission dans un environnement à affaiblissement de Rayleigh où il y a un grand nombre de réflecteurs tel que celui utilisé par les dispositifs sans fil (réseau cellulaire). Dans ce modèle, on suppose que l'amplitude varie de façon aléatoire selon une distribution de Rayleigh.

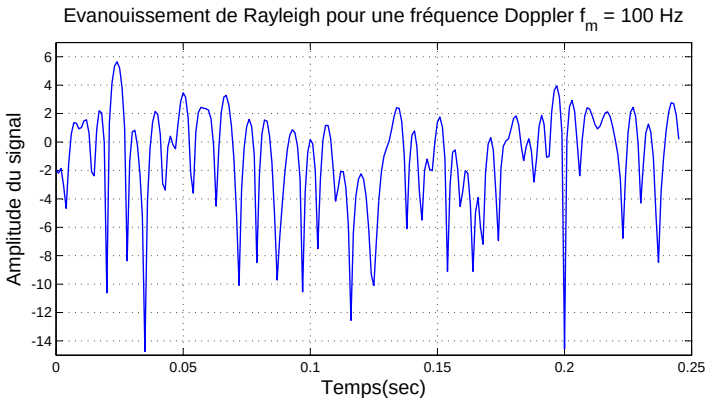


FIGURE 4.3 – *Exemple d'un signal radio suivant une distribution de Rayleigh.*

4.5 Paramètres caractéristiques du modèle de Rayleigh

4.5.1 Capacité secrète des canaux à affaiblissement

Wyner a défini la capacité secrète [3] comme étant la différence entre la capacité du canal légitime et celle du canal de l'espion (voir l'équation (2.14)). Dans [1], la capacité secrète du canal gaussien à entrée unique et sorties multiples SIMO soumis à l'écoute a été étudié. Ce canal peut être modélisé en un canal scalaire [1] en utilisant la théorie des communications [24] et peut être considéré comme un canal gaussien sous écoute [11] avec une seule entrée qui est la source d'émission et deux sorties : le récepteur légitime et l'espion.

La capacité secrète d'un canal gaussien soumis à l'écoute est [11] :

$$\begin{aligned} C_s &= C_m - C_e \\ C_m &= \tfrac{1}{2}\log\left(1+\tfrac{P}{\sigma_1^2}\right) \\ C_e &= \tfrac{1}{2}\log\left(1+\tfrac{P}{\sigma_1^2+\sigma_2^2}\right) \end{aligned} \tag{4.1}$$

où P est la puissance du canal. Les bruits appliqués à la sortie du canal légitime η_1 et du canal de l'espion η_2 sont indépendants et ayant des composantes indépendantes et identiquement distribuées $\mathcal{N}\left(0,\sigma_1^2\right)$ et $\mathcal{N}\left(0,\sigma_2^2\right)$ respectivement.

D'autre part, Parada et Blahut [1] déterminent la capacité secrète d'un système de diffusion dégradé (SIMO) par l'équation suivante :

$$C_s = \frac{1}{2}\log\left(\frac{1+\mathbf{h}^{\dagger}\sum_1^{-1}\mathbf{h}P_S}{1+(\mathbf{Hh})^{\dagger}\left(\mathbf{H}\sum_1\mathbf{H}^{\dagger}+\sum_2\right)^{-1}(\mathbf{Hh})P_S}\right) \tag{4.2}$$

où $\mathbf{h}\in\mathbb{C}^{m_r}$ et $\mathbf{H}\in\mathbb{C}^{m_r\times w_r}$ sont des paramètres de canal, m_r est le nombre d'antennes au récepteur, w_r est le nombre d'antennes à l'espion, P_S est la puissance de la source, $(.)^{\dagger}$ représente la transposé hermitienne, $\sum$ représente la matrice de covariance.

On peut écrire l'équation (4.2) sous la forme de Wyner $C_s = C_M - C_E$ avec :

$$\begin{aligned} C_m &= \tfrac{1}{2}\log\left(1+\mathbf{h}^{\dagger}\sum_1^{-1}\mathbf{h}\cdot P_S\right) \\ C_e &= \tfrac{1}{2}\log\left(1+(\mathbf{Hh})^{\dagger}\left(\mathbf{H}\sum_1\mathbf{H}^{\dagger}+\sum_2\right)^{-1}(\mathbf{Hh})\,P_S\right) \end{aligned} \tag{4.3}$$

Les équations présentés aux points 4.2 et 4.3 peuvent êtres appliquées pour le cas des canaux à affaiblissement. La capacité secrète est également donnée par l'équation (4.1), où l'effet d'affaiblissement est inclue en considérant que $\mathbf{h}(t)$ et $\mathbf{H}(t)$ sont des processus aléatoires en temps continu. De ce fait, la capacité secrète est aussi une valeur aléatoire et non pas une valeur déterministe.

4.5.2 Probabilité d'erreur

On peut aussi évaluer le taux du secret d'un canal soumis à l'écoute par l'évaluation des taux d'erreurs au niveau du récepteur légitime et au niveau de l'espion. Pour un canal de transmission soumis au bruit blanc gaussien avec modulation BPSK, l'expression du taux d'erreur avec détection cohérente à la réception est [25] :

$$P_e = \frac{1}{2}\mathrm{erfc}\left(\sqrt{\frac{E_b}{N_0}}\right) \tag{4.4}$$

où E_b est l'énergie par bit du signal émis, N_0 est la densité spectrale de puissance du bruit à la réception, $\mathrm{erfc}(z) = 1 - \mathrm{erf}(z)$ est la fonction d'erreur complémentaire avec :

$$\mathrm{erf}(z) = \frac{2}{\sqrt{\pi}}\int_0^z e^{-t^2}\,\mathrm{d}t. \tag{4.5}$$

Pour un canal de transmission à affaiblissement de Rayleigh, l'expression du taux d'erreur à la réception du signal émis modulé en BPSK avec un bruit gaussien $\eta(t)$ est donnée par [25] :

$$P_e = \frac{1}{2}\left(1 - \sqrt{\frac{E_b/N_0}{1+(E_b/N_0)}}\right) \tag{4.6}$$

La figure 4.4 montre les courbes théorique et simulée du taux d'erreur pour un canal de Rayleigh et un canal gaussien avec modulation BPSK.

4.6 Simulation des canaux sous écoute avec propagation multivoie : évanouissement de Rayleigh

4.6.1 Description du réseau de communication de la simulation

Dans cette section, on considère un cas plus proche de la réalité. En effet, comme mentionné dans les sections précédentes, le récepteur ne reçoit pas un seul signal, mais plutôt un signal multi-trajets

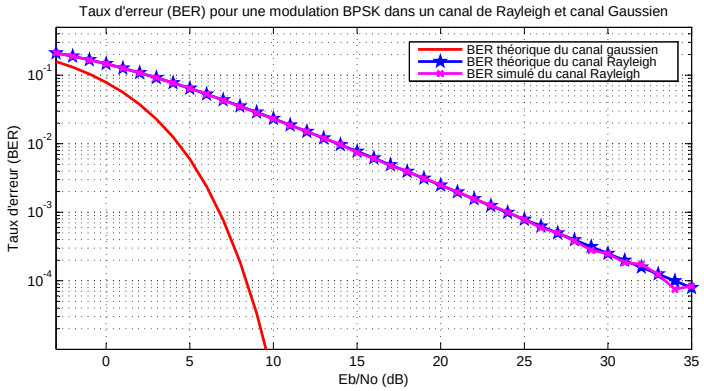


FIGURE 4.4 – *Courbes théorique et simulée du BER pour une modulation (BPSK) dans un canal à évanouissement de Rayleigh et un canal gaussien.*

constitué d'un ensemble de signaux de phase et d'amplitude différentes dus aux phénomènes de réflexion, de diffraction, et d'atténuation du signal émis. Considérons le réseau circulaire sans fil soumis à l'évanouissement de Rayleigh, illustré à la figure 4.5.

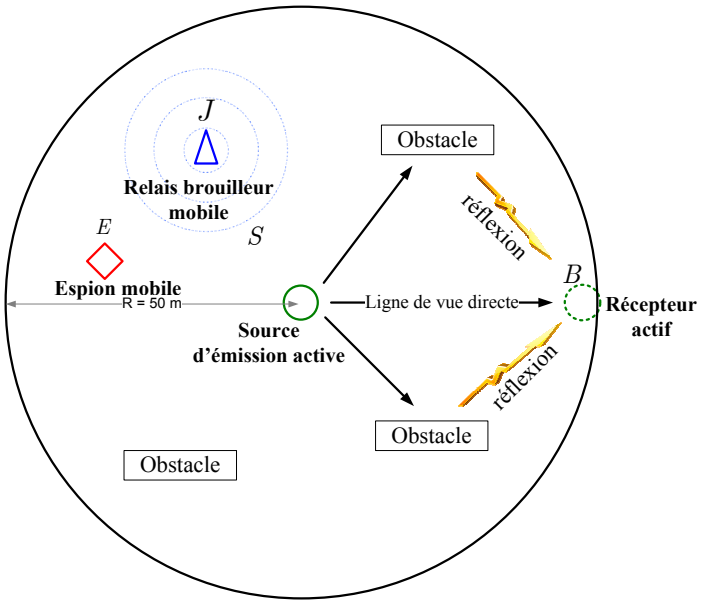


FIGURE 4.5 – *Réseau sans fil circulaire constitué d'une source d'émission centrale S, d'un récepteur B, d'un relais brouilleur J, d'un espion E sous l'effet d'évanouissement de Rayleigh.*

Ce réseau est composé d'une source Alice placée aux coordonnées $(0°, 0\text{ m})$, d'un récepteur Bob placé à l'extrémité du réseau aux coordonnées $(0°, 50\text{ m})$, d'un relais brouilleur placé aux coordonnées $(130°, 30\text{ m})$ et d'un espion de position fixe, aux coordonnées $(170°, 40\text{ m})$. La puissance du bruit blanc gaussien est $P_\eta = -80$ dBm et la puissance allouée au système est $P_{TOT} = 10$ dBm partagée

d'une façon équitable entre la source et le relais.

La source omnidirectionnelle émet un signal x_S de longueur $n = 20\,000$ bits à la puissance P_S dBm modulé en BPSK au même instant que le relais émet un signal brouilleur de même longueur à la puissance P_J dBm et modulé également en BPSK. Le signal x_S se propage dans le réseau et se reflète sur les obstacles qu'il rencontre. Cela mène à créer le phénomène de Rayleigh dans les quatre. On modélise l'affaiblissement de Rayleigh par la génération d'un signal pour chacun des quatre canaux du réseau : *source-récepteur*, *source-espion*, *relais-récepteur* et *relais-espion*. Ces signaux sont aléatoire de 20 000 échantillons espacés de 1 ms donnant une séquence totale de 100 s, comme illustré à la figure 4.6.

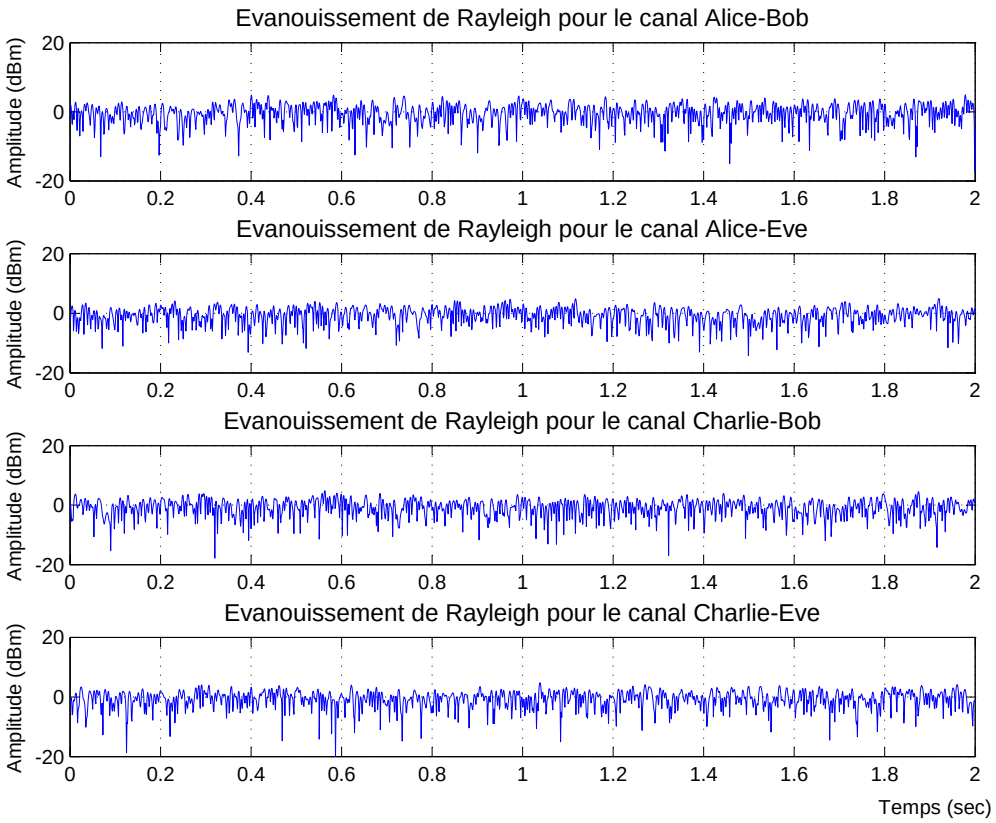
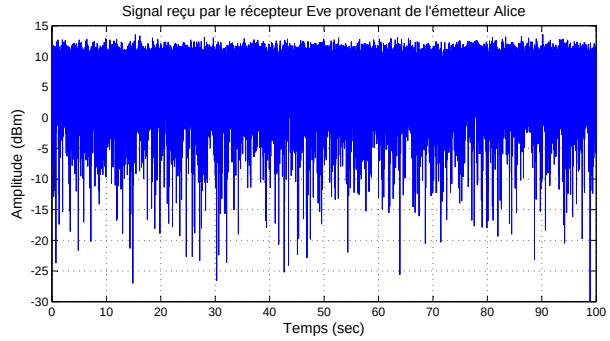


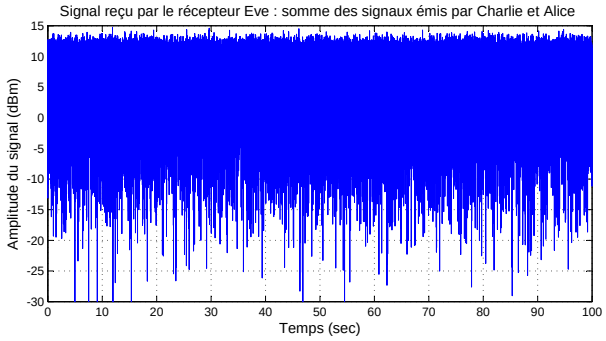
FIGURE 4.6 – *Une partie de l'allure des évanouissements de Rayleigh de* 100 *s dans les quatre canaux du réseau de communication sans fil.*

On multiplie le signal de la source avec le signal de Rayleigh du canal *Alice-Bob* généré au début pour simuler l'effet de propagation multivoie avec affaiblissement de Rayleigh. De même, on refait la même procédure de multiplication pour les trois autres canaux du réseau. Les deux signaux émis par Alice et Charlie soumis à l'effet d'affaiblissement de Rayleigh se propagent dans les canaux sans fil. Le récepteur légitime Bob et l'espion Eve reçoivent deux signaux avec affaiblissement et bruits additifs.

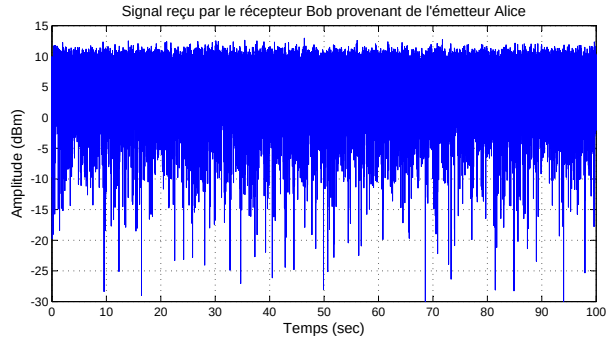
La figure 4.7a montre l'allure du signal reçu par l'espion Eve, alors que la figure 4.7b montre l'allure du signal reçu par le même espion, Eve, mais en lui ajoutant le signal reçu par le relais brouilleur. De même, la figure 4.7c montre l'allure du signal reçu par Bob provenant de l'émetteur Alice, alors que la figure 4.7d montre l'allure du signal reçu par le récepteur Bob, mais en lui ajoutant le signal reçu par le relais, Charlie.



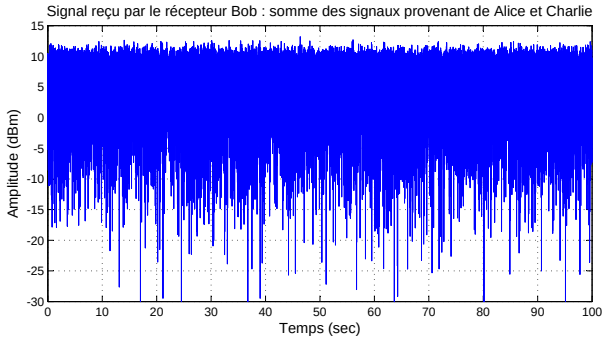
(a) Signal émis par Alice et reçu par Eve.



(b) Signal reçu par l'espion Eve : somme des signaux provenant des émetteurs Alice et Charlie.



(c) Signal émis par Alice et reçu par Bob.



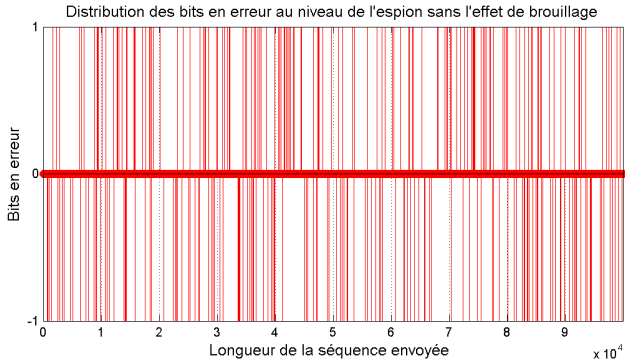
(d) Signal reçu par Bob : somme des signaux provenant des émetteurs Alice et Charlie.

FIGURE 4.7 – *Amplitude relative en dBm des signaux reçus par le récepteur légitime et l'espion.*

Considérons la variation du taux d'erreur au niveau du récepteur légitime Bob et de l'espion Eve, comme illustré à la figure 4.8. Ce taux d'erreur se calcul pour chaque récepteur en comparant la puissance de chaque bit a_i du signal reçu par ce récepteur avec la tension de même bit dans le signal original émis par la source Alice. Puisqu'on a deux niveaux de tension pour le cas de la modulation BPSK, alors si le signe de la tension du symbole a_i dans le signal reçu et le signal original émis par la source est le même, alors la transmission de ce bit a_i s'est faite sans erreur. Si le signe de la tension du a_i est inversé alors ce bit est reçu en erreur.

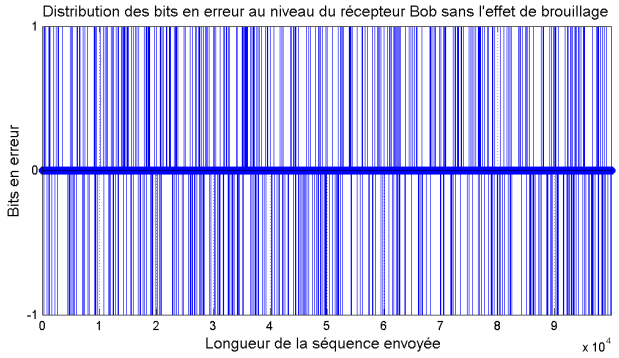
4.6.2 Interprétation des résultats

En analysant les séquences des bits en erreur sans l'effet du signal de brouillage émis par le relais Charlie, on voit qu'au niveau de l'espion Eve qui observe une version du signal du canal *Alice-Bob*,

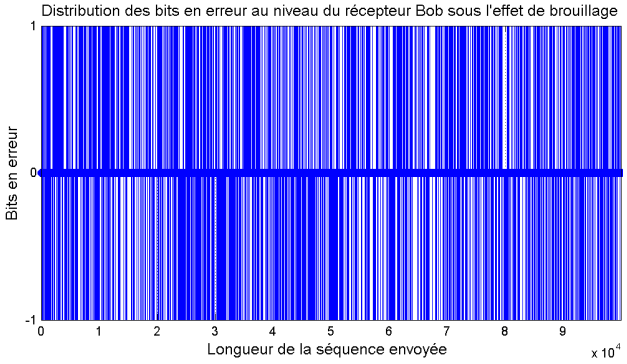


(a) Signal émis par Alice et reçu par Eve.

(b) Signal reçu par l'espion Eve : somme des signaux provenant des émetteurs Alice et Charlie.



(c) Signal émis par Alice et reçu par Bob.



(d) Signal reçu par Bob : somme des signaux provenant des émetteurs Alice et Charlie.

FIGURE 4.8 – *Illustration de la distribution temporelle des symboles en erreur observée aux récepteurs Bob et Eve, par rapport à la séquence originale envoyée de n = 20 000 bits.*

le taux d'erreur est $P_{e_E} = 3{,}2 \cdot 10^{-3}$. Au niveau du récepteur légitime Bob, le taux d'erreur est $P_{e_E} = 6{,}5 \cdot 10^{-3}$. Cela est prévisible car en l'absence du brouillage crée par le relais, les canaux *Alice-Eve* et *Alice-Bob* sont fiables et permettent aux deux récepteurs de bénéficier d'une communication avec un taux d'erreur faible. On constate que le taux d'erreur de l'espion est légèrement faible à celui du récepteur Bob car la source Alice est plus proche de l'espion que de ce récepteur. Le seul paramètre qui influe sur le signal reçu est la distance et la qualité du canal.

Sous l'influence du brouillage crée par le relais, les deux récepteurs sont perturbés et leur taux d'erreur augmente au même temps que leur fiabilité de communication diminue. Le taux d'erreur au niveau de l'espion augmente à $P_{e_E} = 1{,}5 \cdot 10^{-1}$ et on voit dans la figure 4.8b que la distribution temporelle des bits en erreur présente une bande rouge car le nombre de bits erronés est 15830 bits. La figure 4.8d montre la distribution temporelle des bits en erreur au niveau du récepteur Bob sous l'effet du brouillage, où son taux d'erreur a augmenté jusqu'à $P_{e_B} = 9{,}98 \cdot 10^{-3}$. Cela s'explique par le fait que par l'ajout du signal de brouillage généré par le relais Charlie les deux récepteurs Bob et Eve vont recevoir chacun en plus du signal de Alice, le signal généré par Charlie. Du fait que le relais est plus

proche de l'espion que du récepteur Bob, ceci cause une grande confusion pour l'espion Eve et ainsi son canal devient plus dégradé qu'avant : on voit clairement dans les résultats pour Eve un nombre très important de bits en erreur par rapport à la séquence envoyée par Alice. Un codage de canal adéquat peut corriger les erreurs de réception au niveau de Bob.

Si on déplace le relais encore plus proche de l'espion, ce dernier sera davantage perturbé et sa fiabilité de réception est alors perdue. Dans la réalité, la position de l'espion est inconnue, l'objectif est (comme mentionné au chapitre 3) de positionner le relais de tel sorte à augmenter la moyenne du taux d'erreur de l'espion sur toute la surface du réseau sans fil.

4.7 Conclusion

Dans ce chapitre, nous avons étudié l'effet de brouillage coopératif dans les réseaux sans fil situés dans les environnement à affaiblissement de Rayleigh. On a présenté à la section 4.2, le phénomène d'affaiblissement qui se crée lorsque le signal rencontre des obstacles sur son chemin de propagation. Ces obstacles modifient les caractéristiques physiques de ce signal. Ainsi, on a présenté à la section 4.5, les principaux paramètres caractérisant le modèle du canal de Rayleigh, en particulier le taux d'erreur, qui mesure le nombre de bits erronés reçus par rapport à la séquence d'origine envoyée par la source.

La capacité secrète des canaux à affaiblissement est présenté à la section 4.5.1. À la section 4.6, on a présenté les résultats de la simulation d'un réseau sans fil avec des canaux gaussiens soumis à l'écoute dans un environnement à affaiblissement de Rayleigh. Les résultats obtenus sont similaires à ceux obtenus pour des réseaux sans fil non soumis à l'environnement d'affaiblissement : le taux d'erreur au niveau de l'espion augmente ou diminue selon sa position par rapport à la position du relais brouilleur. L'application du concept de brouillage coopératif pour la sécurisation des communications entre deux entités communicantes légitimes dans un réseau sans fil ouvert en présence d'un ou de plusieurs espions doit obéir à certaines conditions pour que le brouillage favorise les récepteurs légitimes tout en augmentant le taux d'erreur de ou des espions dont leurs positions est généralement inconnue. On constate que l'utilisation d'un seul relais brouilleur dans un réseau de communication sans fil ne donne pas beaucoup de choix quant à la confusion de l'espion : on doit donc chercher le meilleur emplacement de ce relais brouilleur selon la puissance allouée ainsi que celle allouée à la source pour pouvoir trouver le meilleur emplacement de ce relais pour garantir le maximum de confusion à l'espion. Puisque le réseau sans fil est soumis à une contrainte de puissance, une optimisation de la puissance allouée au relais de brouillage est nécessaire pour garantir cette confusion.

Chapitre 5

Brouillage coopératif dans les réseaux multi-relais brouilleurs

5.1 Introduction

Dans ce chapitre, on considère des réseaux de télécommunications à $N_J > 1$ relais brouilleurs en considérant des réseaux sans fil de surface plus grande que celles précédemment considérer. L'implémentation de ces relais doit se faire d'une façon à conserver une bonne qualité de la liaison légitime tout en maximisant la surface de la région brouillée et avec l'allocation de puissance adéquate.

À la section 5.2, on explique l'effet de l'allocation de puissance sur les performances du brouillage coopératif. Cette puissance dépensée doit être mise en évidence : la réduction de la puissance est devenue un besoin crucial dans les télécommunications actuelles, tant au niveau des terminaux que des réseaux. Il est alors nécessaire de développer des outils pour évaluer et quantifier la consommation de puissance dans un réseau sans fil donné. D'ailleurs, les relais sont déjà eux-mêmes une solution pour réduire la consommation de puissance dans les terminaux mobiles car non seulement ils augmentent la portée des communications (et augmenter ainsi le nombre d'utilisateurs potentiels), mais aussi en se positionnant à proximité des utilisateurs, la puissance de transmission du réseau et des utilisateurs est réduite (augmentation de l'autonomie des utilisateurs et économie sur la facture d'énergie pour les fournisseurs de service réseau [13] [21]).

À la section 5.3, on évalue la fiabilité des liaisons légitimes entre deux communicants fixes alors qu'un espion mobile observe des versions des séquences envoyées par la source d'émission. L'allocation de puissance entre cette source et le relais brouilleur demeure statique pendant que ce dernier change de position par rapport à la position des deux terminaux légitimes afin évaluer l'influence du signal brouilleur sur la fiabilité de réception et évaluer aussi le taux d'erreur moyen de l'espion sur toute la surface du réseau.

À la section 5.4, on augmente le nombre de relais brouilleurs à 2 et à 8 à la section 5.5. Dans ces

cas, il y a deux allocations de puissance à évaluer : l'allocation entre la puissance d'émission et la puissance de brouillage ainsi que la redistribution de la puissance de brouillage entre les relais brouilleurs eux-mêmes. Pour cela, plusieurs stratégies d'allocation de puissance sont étudiés pour des positions connues des relais brouilleurs afin d'en tirer les avantages et les inconvénients.

5.2 Contrainte de consommation de puissance

Considérons la figure 5.1 dans laquelle on définie un réseau sans fil sous écoute constitué de N_S émetteurs, de N_B récepteurs, de N_J relais et de N_E espions.

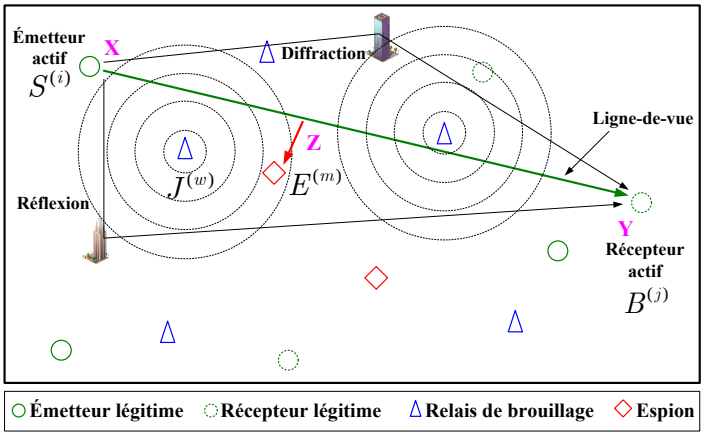


FIGURE 5.1 – *Disposition (aléatoire) des différents terminaux dans un réseau sans fil soumis à l'écoute clandestine de l'espion.*

Ce réseau de communication est soumis à une contrainte de puissance totale P_{TOT} tel que :

$$P_{TOT} = P_S + \sum_{i=1}^{N_J} P_J^{(i)} \tag{5.1}$$

où P_S est la puissance allouée à la source d'émission, $P_J^{(i)}$ est la puissance allouée au $i^{\text{ème}}$ relais brouilleur et P_{TOT} est la puissance totale allouée au réseau de communication.

Lors de la conception du réseau sans fil, les relais doivent être positionnés de telle façon à couvrir toute la surface du réseau. À un temps discret donné g, un émetteur $S^{(i)}$ établit une communication avec un récepteur $B^{(j)}$ via un canal sous écoute où un ou plusieurs espions $(E^{(1)}, \cdots, E^{(N_E)})$ observent une version des données échangées. Selon la distance qui sépare l'émetteur du récepteur, un ou plusieurs relais brouilleurs peuvent s'impliquer pour brouiller les signaux. Pour les simulations présentées dans ce chapitre on adopte une disposition aléatoire des différents terminaux comme illustré à la figure 5.2.

On s'intéresse à la question suivante : *comment peut-on choisir l'allocation de puissance adéquate qui permet de conserver la fiabilité de la liaison légitime en assurant la plus grande couverture sécuritaire ?*

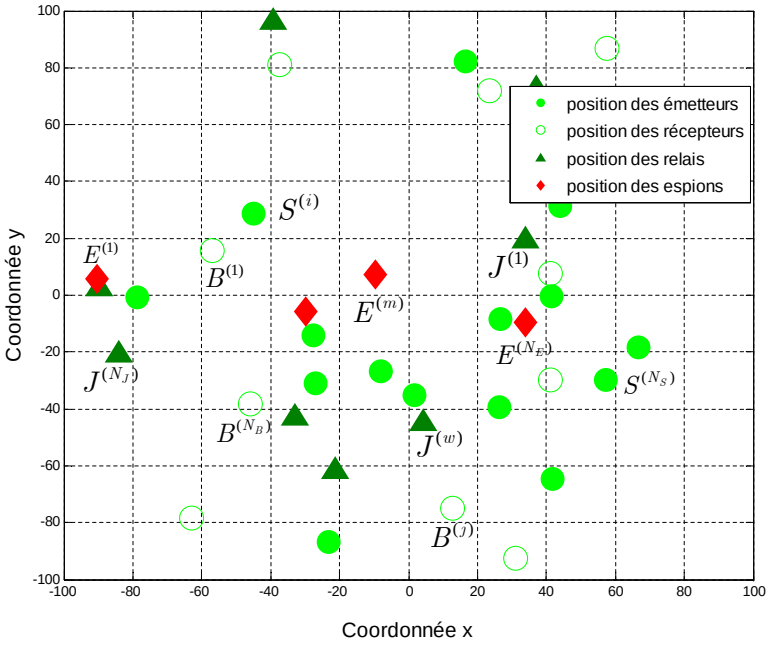


FIGURE 5.2 – *Exemple de disposition aléatoire des terminaux dans un réseau sans fil soumis à l'écoute.* $N_S = 10$ *émetteurs,* $N_B = 10$ *récepteurs,* $N_J = 7$ *relais et* $N_E = 4$ *espions.*

Parmi les solutions envisageables, on procède à une allocation adaptative de la puissance P_J en attribuant un nombre adéquat de relais brouilleurs qui réalisent le maximum de confusion au niveau de l'espion comme illustré à la figure 5.3.

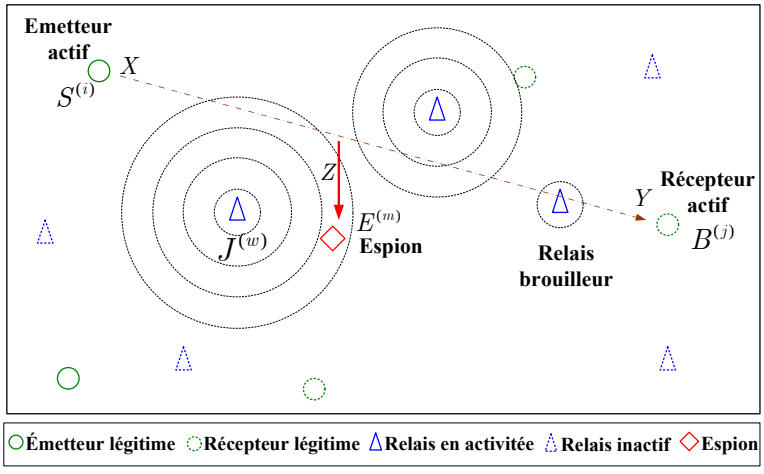


FIGURE 5.3 – *Disposition des terminaux. Ici, uniquement les relais se trouvant dans la zone où le signal de la source est fiable : les autres relais demeurent en veille.*

L'allocation adaptative de puissance peut se faire en ne choisissant que les relais qui se trouvent dans

la zone où le signal de la source $S^{(i)}$ est fiable : les autres relais demeurent en veille. Chaque relais impliqué dans le brouillage se voit alloué une puissance $P_{J^{(w)}}$, $w = \{1,...,N_J\}$ selon sa distance par rapport à l'emplacement physique du canal entre l'émetteur $S^{(i)}$ et le récepteur $B^{(j)}$. Ceci aura une meilleure répercussion sur le bilan de puissance. Supposons par exemple que pour l'établissement de la communication entre la source d'émission $S^{(i)}$ et le récepteur $B^{(j)}$ trois relais brouilleurs soient nécessaires pour sécuriser la communication établie. Puisque le système est soumis à une contrainte de puissance alors la puissance totale pour l'envoi des données est : $P_{TOT} = P_{S^{(i)}} + P_J$, où $P_{S^{(i)}}$ est la puissance allouée à la source d'émission $S^{(i)}$ et P_J est la puissance totale de brouillage qui s'écrit sous la forme :

$$P_J = P_{J^{(1)}} + P_{J^{(2)}} + P_{J^{(3)}} \tag{5.2}$$

Il ne sert à rien d'activer un relais brouilleur éloigné de la région de portée du signal de la source d'émission. De plus, si on a une meilleure connaissance de l'état du canal on peut allouer de la puissance entre ces trois relais brouilleurs de telle sorte que chaque relais $J^{(w)}$ a une quantité de puissance $P_{J^{(w)}}$ qui est une fonction de la puissance du signal x_S de la source $S^{(i)}$ à l'emplacement physique de ce relais :

$$P_{J^{(w)}} = f(d(J^{(w)},S^{(i)})) \tag{5.3}$$

où $d(J^{(w)},S^{(i)})$ est la distance entre le relais brouilleur $J^{(w)}$ et la source $S^{(i)}$. Plus la source est loin du relais et moins on alloue de la puissance à ce relais car la puissance du signal x_S diminue sous l'effet de l'affaiblissement de propagation.

5.3 Simulation d'un réseau sans fil sous écoute avec un seul relais brouilleur : effet de l'allocation de puissance

Dans cette section, on simule un réseau sans fil mono-relais pour deux allocations de puissance : une allocation favorisant la source d'émission et une allocation équitable où la puissance P_{TOT} est partagée également entre la source d'émission et le relais brouilleur.

5.3.1 Description du réseau de communication simulé

Considérons le réseau sans fil circulaire de rayon $r = 100$ m soumis à l'écoute illustré à la figure 5.4, constitué d'une source d'émission fixe S, d'un récepteur fixe B, d'un relais brouilleur J de position aléatoire et d'un espion E qui peut se déplacer dans toute la surface du réseau.

La source qui a une diffusion omnidirectionnelle se positionne au centre du réseau circulaire aux coordonnées $(0°, 0\text{ m})$ alors que le récepteur Bob se positionne à l'extrémité du réseau aux coordonnées $(0°, 100\text{ m})$. Le relais brouilleur dont sa coordonnée radiale est $\rho_J = 50$ m se positionne dans quatre coordonnées angulaires différentes avec un écart de 90° à chaque déplacement. La puissance totale allouée au système : P_{TOT} = 100 mW (20 dBm) pour qu'elle corresponde aux dimensions du réseau sans fil typique.

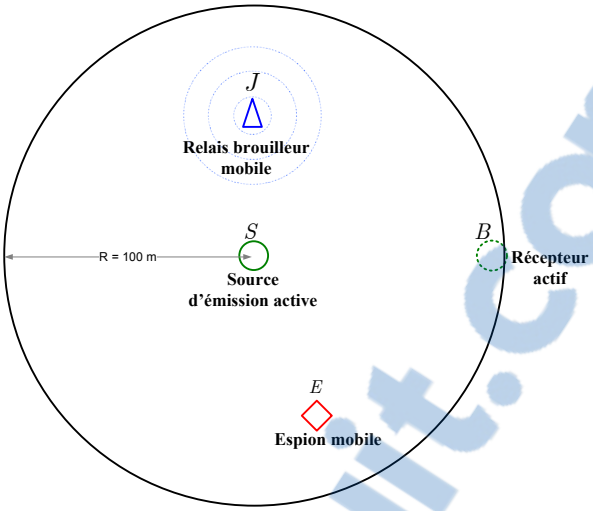


FIGURE 5.4 – *Réseau sans fil circulaire de rayon $r = 100$ m soumis à l'écoute constitué d'un émetteur, d'un récepteur, d'un relais brouilleur et d'un espion mobile.*

5.3.2 Description des simulations

On veut déterminer l'influence de la position du relais brouilleur sur le taux d'erreur au niveau du récepteur Bob et de l'espion pour le cas d'une allocation de puissance statique entre la source d'émission et le relais brouilleur. La source d'émission émet à la puissance P_S dBm un signal binaire aléatoire de longueur $n = 100\,000$ bits modulé en BPSK. Le relais brouilleur émet au même moment à la puissance P_J dBm un signal binaire brouilleur de même longueur modulé lui aussi en BPSK. Tous les canaux du réseau sont soumis à du bruit blanc gaussien de puissance $P_\eta = -80$ dBm [5]. Le bruit blanc gaussien s'ajoute aux signaux reçus par Bob et par l'espion causant ainsi des erreurs de réception. Le signal reçu est de la forme :

$$y_B = h_{SB} \cdot P_S \cdot x_S + h_{JB} \cdot P_J \cdot x_J + \eta_B \tag{5.4}$$

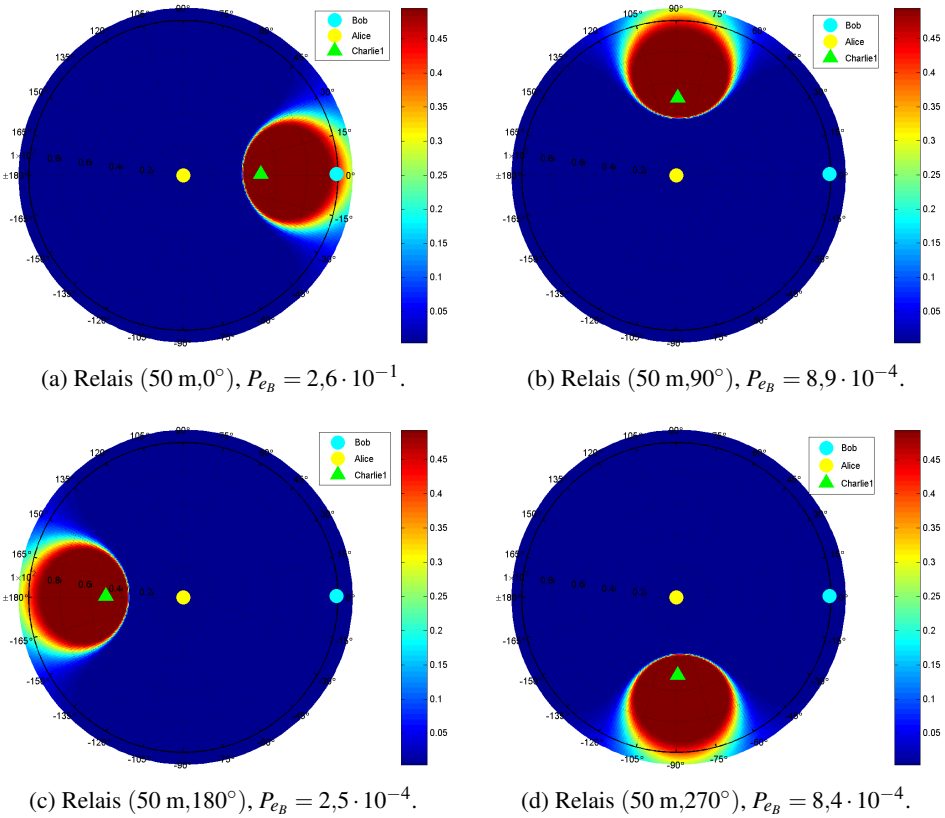
$$y_E = h_{SE} \cdot P_S \cdot x_S + h_{JE} \cdot P_J \cdot x_J + \eta_E \tag{5.5}$$

où h désigne le gain de chaque canal de communication : $h_{AB} = \sqrt{(x_B - x_A)^2 + (y_B - y_A)^2}^{(-\alpha)}$. α désigne le coefficient de l'affaiblissement de propagation auxquels les canaux sont soumis : pour l'espace libre α vaut 2. y est le signal reçu, η est le bruit blanc gaussien, P_J et P_S sont les puissances de brouillage et d'émission avec $P_J + P_S = P_{TOT}$.

La simulation consiste à observer pour chacune des quatre positions du relais brouilleur les séquences reçues par le récepteur Bob et par l'espion mobile et évaluer les taux d'erreurs pour le récepteur légitime, P_{e_B}, et pour l'espion, P_{e_E}. L'évaluation des taux d'erreur se fait comme expliqué à la section 2.4.5. Pour chaque position du relais, il y a une seule valeur de P_{e_B} à évaluer. En ce qui concerne l'espion, on calcule en plus du taux d'erreur P_{e_E} pour chaque position de l'espion, l'espérance de de touts les taux d'erreurs obtenus pour l'espion $E[P_{e_E}]$ pour l'ensemble des positions que peut prendre cet espion dans le réseau sans fil.

5.3.3 Allocation de puissance : $P_S = 0{,}8 \cdot P_{TOT}$, $P_J = 0{,}2 \cdot P_{TOT}$

Pour l'allocation de puissance suivante ($P_S = 0{,}8 \cdot P_{TOT}$, $P_J = 0{,}2 \cdot P_{TOT}$), l'évaluation des taux d'erreurs P_{e_B} et P_{e_E} donne les résultats illustrés à la figure 5.5.



(a) Relais $(50\text{ m},0^\circ)$, $P_{e_B} = 2{,}6 \cdot 10^{-1}$.

(b) Relais $(50\text{ m},90^\circ)$, $P_{e_B} = 8{,}9 \cdot 10^{-4}$.

(c) Relais $(50\text{ m},180^\circ)$, $P_{e_B} = 2{,}5 \cdot 10^{-4}$.

(d) Relais $(50\text{ m},270^\circ)$, $P_{e_B} = 8{,}4 \cdot 10^{-4}$.

FIGURE 5.5 – *Effet de brouillage coopératif dans un réseau sans fil soumis à l'écoute composé de l'émetteur Alice* $(0\text{ m},0^\circ)$, *du récepteur Bob* $(100\text{ m},0^\circ)$, *du brouilleur mobile Charlie et de l'espion mobile Eve.* $P_{TOT} = 20$ *dBm*, $P_S = 0{,}8 \cdot P_{TOT}$, $P_J = 0{,}2 \cdot P_{TOT}$, $P_\eta = -80$ *dBm.*

La figure 5.5 montre les valeurs des taux d'erreur P_{e_E} pour l'espion et P_{e_B} pour le récepteur légitime pour chaque emplacement du relais brouilleur dans le réseau soumis à l'écoute. On constate que le taux d'erreur au récepteur légitime varie selon la position du relais brouilleur. En considérant qu'une communication entre la source d'émission et le récepteur Bob est fiable si $P_{e_B} \leq 10^{-3}$, on peut grouper les valeurs de P_{e_B} en deux catégories :

1. **Région où le taux d'erreur du récepteur légitime est favorable,** $P_{e_B} \leq 10^{-3}$: Lorsque le relais se trouve aux coordonnées angulaires $\pm 90^\circ$ et 180°, la distance entre ce relais et le récepteur légitime est considérée suffisamment grande pour que la puissance attribuée au relais lui permette d'être perturbateur. La valeur maximale du taux d'erreur P_{e_B} est $8{,}9 \cdot 10^{-4}$. Cette situation très favorable pour assurer une liaison légitime fiable est considérée comme défavorable quant à la perturbation de l'espion. Avec cette allocation de puissance l'espion bénéficie d'une

réception fiable ou avec un taux d'erreur faible ($P_{e_E} \leq 2 \cdot 10^{-1}$) dans 88,89% de la surface du réseau alors que seulement 2,49% de la surface du réseau est sécurisée avec un taux d'erreur moyen ($2 \cdot 10^{-1} < P_{e_E} \leq 4 \cdot 10^{-1}$) et avec un taux d'erreur élevé dans 8,61% ($P_{e_E} > 4 \cdot 10^{-1}$). L'espérance du taux d'erreur de l'espion sur l'ensemble de la surface du réseau est seulement $E[P_{e_E}] = 0{,}0493$.

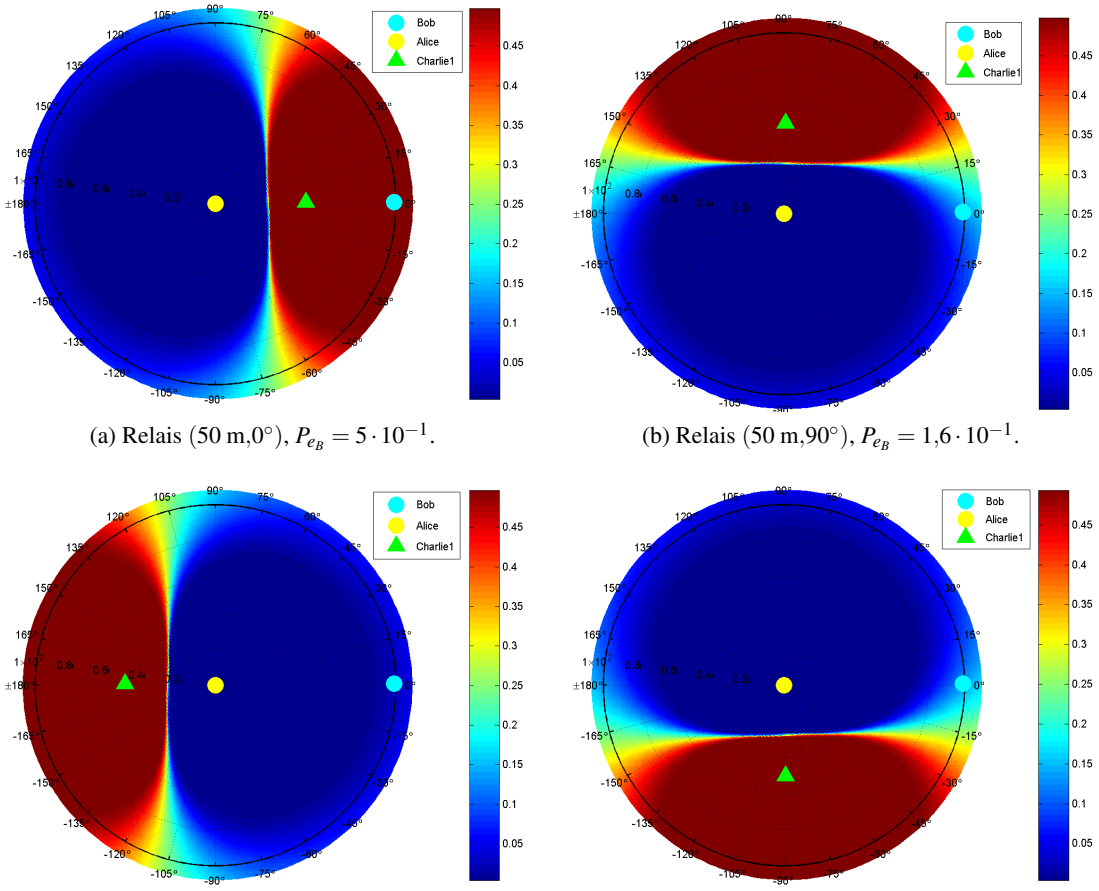
2. **Région où le taux d'erreur au récepteur est non fiable, soit $P_{e_B} > 10^{-3}$** : Cela est dû au fait que le relais se trouve entre la source Alice et le récepteur Bob et son signal brouilleur est très perturbateur pour ce récepteur malgré qu'il soit de faible puissance car la distance entre eux est petite. Cela laisse le taux d'erreur P_{e_B} augmenter jusqu'à $P_{e_B} = 2{,}6 \cdot 10^{-1}$. La fiabilité de la liaison légitime est perdue car le récepteur trouve le décodage du signal reçu par Alice très difficile, voir impossible. Pour l'espion, les mêmes statistiques de sécurité sont obtenues vu que la coordonnée radiale du relais reste la même à $\rho = 50$ m ainsi que l'allocation de puissance, ce qui laisse à l'espion une grande région où son taux d'erreur soit très faible.

5.3.4 Allocation de puissance : $P_S = 0{,}5 \cdot P_{TOT}$, $P_J = 0{,}5 \cdot P_{TOT}$

Après avoir favorisé la source d'émission quant à termes d'allocation de puissance, on modifie cette allocation de puissance à un partage égal entre la source et le relais : $P_S = P_J = \frac{P_{TOT}}{2}$. La source d'émission émet à la nouvelle puissance P_S un signal binaire aléatoire de longueur $n = 100\,000$ bits modulé en BPSK. Le relais brouilleur émet à la nouvelle puissance P_J un signal de brouillage binaire et aléatoire de même longueur et modulé également en BPSK également. Pour chaque position du relais dans le réseau on évalue le taux d'erreur au niveau du récepteur Bob et de l'espion. La figure 5.6 montre les résultats obtenus pour P_{e_B} et P_{e_E}.

L'analyse des résultats obtenus avec cette deuxième allocation de puissance nous montre que toutes les positions possibles du relais engendre des taux d'erreurs inacceptables pour le récepteur Bob pour assurer une liaison légitime fiable. Lorsque le relais se trouve à la coordonnée $(50\text{ m}, 0^\circ)$ le taux d'erreur $P_{e_B} = 5 \cdot 10^{-1}$ car le relais est non seulement proche du récepteur Bob mais en plus la puissance du signal brouilleur émis par ce relais est maintenant plus importante au même temps que le signal de la source est moins puissant que celui dans l'allocation de puissance précédente. Même lorsque le relais est très loin de ce récepteur à la coordonnée $(50\text{ m}, 180^\circ)$ P_{e_B} reste grand et ne permet pas une liaison fiable avec la source car $P_{e_B} = 5 \cdot 10^{-2} \geq 10^{-3}$. La puissance du signal émis par la source ne lui permet pas d'atteindre Bob avec fiabilité à cause de l'affaiblissement de propagation de coefficient $\alpha = 2$ auxquels les canaux gaussiens du réseau sont soumis. Pour les deux autres positions du relais qui sont $(50\text{ m}, \pm 90^\circ)$ le taux d'erreur $P_{e_B} = 1{,}6 \cdot 10^{-1}$ et est considéré également comme inacceptable.

Pour l'espion, la surface dans laquelle sa capacité à recevoir avec fiabilité ou avec un taux d'erreur faible s'est largement réduite à cause de la dominance du signal brouilleur sur une grande partie du réseau. La surface faiblement sécurisée est passé de 88,89% à seulement 50% laissant place à l'augmentation de la zone moyennement sécurisée qui est passé à 12,43% au lieu de 2,49% et à la zone hautement sécurisée qui est passé à 37,57% au lieu de 8,61%. Cette zone hautement sécurisée



(a) Relais $(50\text{ m},0°)$, $P_{e_B} = 5 \cdot 10^{-1}$.

(b) Relais $(50\text{ m},90°)$, $P_{e_B} = 1{,}6 \cdot 10^{-1}$.

(c) Relais $(50\text{ m},180°)$, $P_{e_B} = 5 \cdot 10^{-2}$.

(d) Relais $(50\text{ m},270°)$, $P_{e_B} = 1{,}6 \cdot 10^{-1}$.

FIGURE 5.6 – *Effet de brouillage dans un réseau circulaire composé d'un émetteur* $(0\text{ m},0°)$*, d'un récepteur* $(100\text{ m},0°)$*, d'un relais et d'un espion mobile Eve.* $P_{TOT} = 20$ *dBm,* $P_S = P_J = 0{,}5 \cdot P_{TOT}$*,* $P_\eta = -80$ *dBm.*

est localisée principalement autour du relais où le signal brouilleur est très fort. L'espérance du taux d'erreur de l'espion sur l'ensemble de la surface du réseau est passé à $E[P_{e_E}] = 0{,}2022$.

De cette simulation on conclut que dans un réseau sans fil soumis à l'écoute avec un seul relais de brouillage, deux paramètres sont à prendre en considération à savoir l'allocation de puissance entre la source d'émission et le relais brouilleur ainsi que l'emplacement de ce dernier. Puisqu'un seul relais de brouillage n'est pas suffisant pour sécuriser toute la surface du réseau sans fil, on doit le placer de telle façon à noyer la plus grande surface possible du réseau dans le brouillage sans nuire à la fiabilité du canal légitime en prenant en considération l'allocation de puissance appliquée.

Cette exigence impose la disponibilité d'une puissance nécessaire et suffisante pour le réseau complet pour que la communication légitime soit fiable et que le brouillage fonctionne efficacement. Dans les deux allocations de puissance simulées on constate que pour chaque allocation il y a des limites contradictoires.

5.4 Simulation d'un réseau sans fil sous écoute avec deux relais brouilleurs

Après avoir simulé le comportement d'un réseau sans fil soumis à l'écoute comportant un seul relais brouilleur où on a constaté des limites d'utilisation en terme de brouillage de l'espion et de fiabilité des liaisons légitimes, on opte maintenant pour un réseau sans fil à $N_J = 2$ relais brouilleurs. En appliquant les mêmes paramètres utilisés pour la simulation avec relais brouilleur unique, on analyse les résultats obtenus quant à la sécurité et à la fiabilité de la liaison légitime avec deux relais brouilleurs.

5.4.1 Description du réseau de communication à deux relais brouilleurs

Considérons le réseau de communication sans fil circulaire illustré à la figure 5.7.

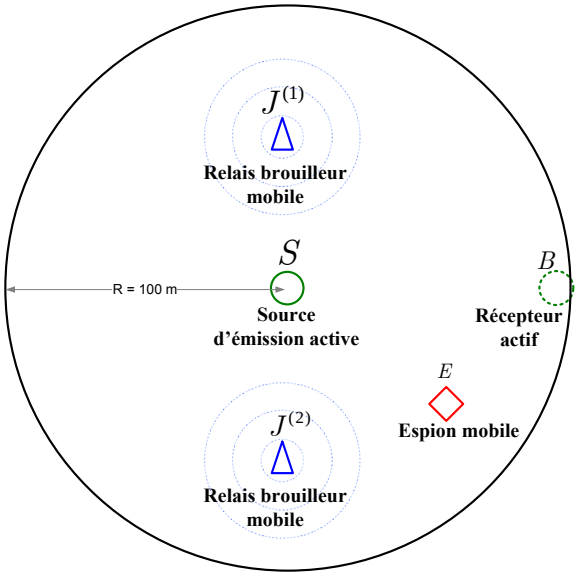


FIGURE 5.7 – *Réseau de communication sans fil soumis à l'écoute avec $N_J = 2$ relais brouilleurs.*

Ce réseau est constitué de la source d'émission Alice placée au centre aux coordonnées $(0\text{ m},0^\circ)$, du récepteur légitime Bob placée à l'extrémité du réseau aux coordonnées $(100\text{ m},0^\circ)$, de l'espion mobile Eve libre de se déplacer dans toute la surface du réseau de communication et de $N_J = 2$ relais brouilleurs. On alloue à ce réseau une puissance P_{TOT} tel que $P_{TOT} = P_S + \sum_{l=1}^{N_J=2} P_{J^{(l)}}$ partagée entre la source d'émission pour la transmission au récepteur Bob et les 2 relais brouilleurs. Plusieurs facteurs peuvent être mis en jeux pour créer différents scénarios de brouillage :

– la procédure d'allocation de puissance entre les terminaux émetteurs (source d'émission, relais brouilleurs) : allocation équitable entre la source et les relais, allocation favorisant la source d'émission, allocation favorisant les relais, allocation équitable entre les relais, etc...

– le nombre N_J de relais brouilleurs et leur position (Dans ce cas $N_J = 2$),

– la position de l'émetteur et du récepteur.

Le réseau comprend deux canaux entre la source d'émission et le récepteur légitime et l'espion ainsi que 4 canaux entre les différents relais et les récepteurs. Chaque canal du réseau de communication est soumis à du bruit blanc gaussien η de puissance P_η et a un gain h_{ij} qui dépend de la distance du canal qui est soumis à un affaiblissement de propagation de coefficient $\alpha = 2$. Comme pour le cas d'un réseau à relais brouilleur unique, on considère deux allocations de puissance pour que la source et les relais brouilleurs $J^{(1)}$ et $J^{(2)}$ puissent émettre des signaux binaires aléatoires de longueur $n = 100\,000$ bits modulés en BPSK aux puissances respectives P_S, $P_{J^{(1)}}$ et $P_{J^{(2)}}$. La même puissance $P_{TOT} = 20$ dBm est attribuée au réseau sans fil. La puissance du bruit blanc gaussien reçu par Bob et Eve a une puissance $P_\eta = -80$ dBm. Les trois signaux se propagent dans le canal de transmission et les signaux reçus sont :

$$y_B = h_{SB} \cdot P_S \cdot x_S + \sum_{i=1}^{2} h_{J^{(i)}B} \cdot P_J \cdot x_{J^{(i)}} + \eta_B \tag{5.6}$$

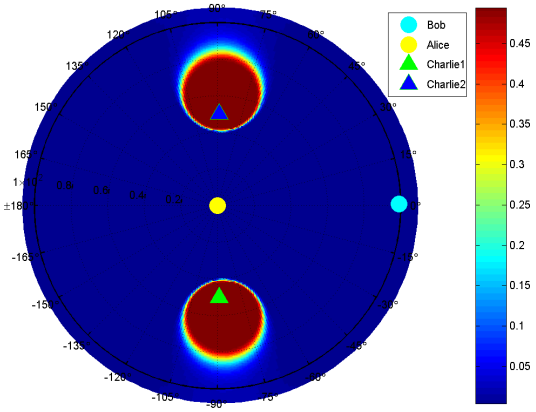
$$y_E = h_{SE} \cdot P_S \cdot x_S + \sum_{i=1}^{2} h_{J^{(i)}E} \cdot P_J \cdot x_{J^{(i)}} + \eta_E \tag{5.7}$$

On souhaite évaluer l'effet de la variation de la coordonnée angulaire des deux relais et de l'allocation de puissance sur les taux d'erreurs P_{e_E} et P_{e_B}.

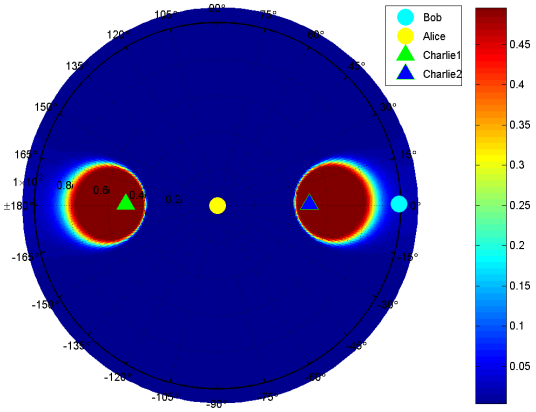
5.4.2 Allocation de puissance favorisant la source : $P_S = 0{,}8 \cdot P_{TOT}$, $P_J = 0{,}2 \cdot P_{TOT}$

Dans ce cas, la grande partie de la puissance P_{TOT} est attribuée à la source pour émettre son signal x_S. Le reste de la puissance est partagée également entre les relais $J^{(1)}$ et $J^{(2)}$. Les résultats de l'évaluation des taux d'erreurs sont illustrés à la figure 5.8.

La figure 5.8a montre la variation du taux d'erreur pour l'espion où les relais se trouvent aux coordonnées $(50\text{ m}, \pm 90°)$. Cette allocation est largement favorable quant à la fiabilité de la liaison légitime puisque le taux d'erreur au niveau de Bob est $P_{e_B} = 4{,}2 \cdot 10^{-4}$. Pour l'espion, le taux d'erreur est faible dans une large partie du réseau car le signal de la source est trop fort par rapport à ceux des deux relais brouilleurs. Les statistiques de sécurité montrent que 92,49% de la surface du réseau est couverte avec un taux d'erreur faible pour l'espion. Avec la même allocation de puissance cette surface de faible sécurité était de 88,89% avec un seul relais. Cette augmentation est dû au fait que la même quantité de puissance $(0{,}2 \cdot P_{TOT})$ est maintenant divisée entre les deux relais, donc la puissance du signal brouilleur est maintenant plus faible par rapport à la configuration à relais unique ce qui provoque la diminution des maximas du taux d'erreur P_{e_E}. Cela fait basculer une partie de la zone précédemment hautement sécurisée à la zone moyennement sécurisée qui vaut maintenant 1,15% de la surface totale. De même, une partie de la zone moyennement sécurisée bascule vers la zone faiblement sécurisée. Au même temps, la zone où le taux d'erreur P_{e_E} est nulle diminue à cause de la présence du deuxième



(a) Relais $(50\text{ m}, \pm 90°)$, $P_{e_B} = 4{,}2 \cdot 10^{-4}$.



(b) Relais $(50\text{ m}, 0°)$ et $(50\text{ m}, 180°)$, $P_{e_B} = 1{,}97 \cdot 10^{-2}$.

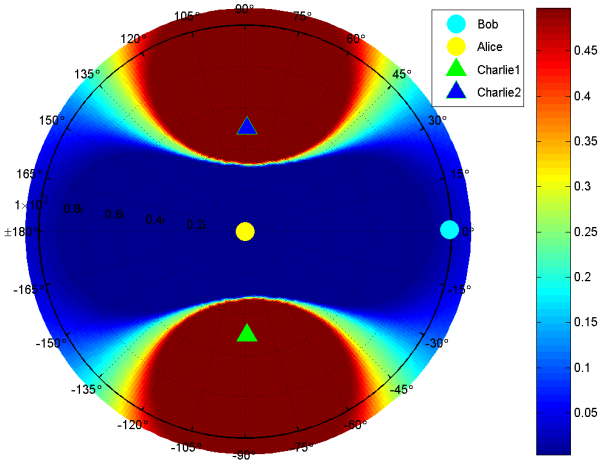
FIGURE 5.8 – *Variation du P_{e_E} sous l'effet du brouillage coopératif. $N_J = 2$, $P_{TOT} = 20$ dBm, $P_S = 0{,}8 \cdot P_{TOT}$, $P_{J(1)} = P_{J(2)} = 0{,}1 \cdot P_{TOT}$, $P_\eta = -80$ dBm.*

relais. L'espérance du taux d'erreur de l'espion sur l'ensemble de la surface du réseau est maintenant $E[P_{e_E}] = 0{,}0366$.

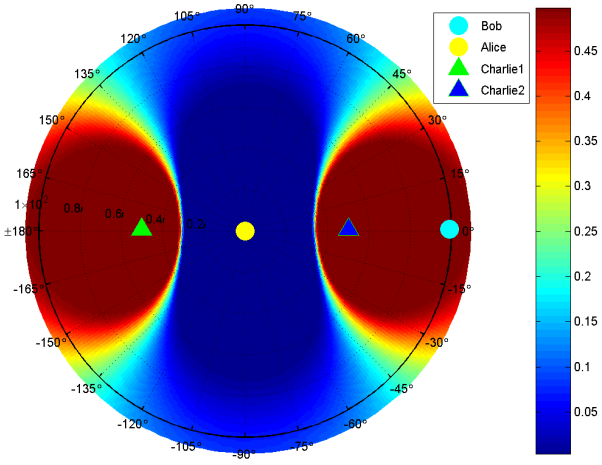
La figure 5.8b montre les résultats de la même simulation pour les nouvelles coordonnées polaires des deux relais $(50\text{ m}, 0°)$ et $(50\text{ m}, 180°)$. Cette nouvelle disposition des relais créent une perturbation moyenne pour le récepteur qui voit son taux d'erreur augmenter à $P_{e_B} = 1{,}97 \cdot 10^{-2}$ car le relais de coordonnée $(50\text{ m}, 0°)$ est proche du récepteur Bob et le peu de puissance allouée à ce relais va faire perdre la fiabilité de la liaison légitime entre Alice et Bob. Pour l'espion, les mêmes statistiques de sécurité sont obtenues car la coordonnée radiale des deux relais n'a pas changé. Le changement de la coordonnée angulaire du relais n'affecte pas les statistiques de sécurité.

5.4.3 Allocation de puissance égale : $P_S = 0{,}5 \cdot P_{TOT}$, $P_J = 0{,}5 \cdot P_{TOT}$

Dans ce cas, la puissance allouée au système est partagée d'une façon égale entre l'émission et le brouillage. La puissance de brouillage P_J est partagée également entre les relais $J^{(1)}$ et $J^{(2)}$. Les simulations d'évaluation des taux d'erreurs P_{e_B} et P_{e_E} nous donne les résultats affichés à la figure 5.9.



(a) Relais $(50\text{ m}, \pm 90°)$, $P_{e_B} = 4 \cdot 10^{-2}$.



(b) Relais $(50\text{ m}, 0°)$ et $(50\text{ m}, 180°)$, $P_{e_B} = 4{,}9 \cdot 10^{-1}$.

FIGURE 5.9 – *Variation du taux d'erreur de l'espion sous l'effet du brouillage coopératif.* $N_J = 2$, $P_{TOT} = 20$ *dBm*, $P_S = 0{,}5 \cdot P_{TOT}$, $P_{J^{(1)}} = P_{J^{(2)}} = 0{,}25 \cdot P_{TOT}$. $P_\eta = -80$ *dBm.*

La figure 5.9a montre le taux d'erreur pour l'espion lorsque la droite reliant les deux relais est perpendiculaire à la ligne droite reliant la source et le récepteur Bob. Dans ce cas, les relais sont relativement loin de ce récepteur mais puisque la puissance allouée à chaque relais est plus grande par rapport à celle de la première allocation de puissance favorisant la source, le taux d'erreur au niveau de ce récepteur augmente à $P_{e_B} = 4 \cdot 10^{-2}$ qui est considéré comme inacceptable car la fiabilité de la liaison

avec la source est perdue et le récepteur trouve le décodage du signal de la source très difficile, voir impossible. Au même moment, la puissance allouée à la source a diminué.

Pour l'espion, sa capacité à recevoir le signal de Alice avec fiabilité a largement diminué dans une grande partie du réseau à cause de ce basculement de la puissance de la source vers les deux relais brouilleurs. Ainsi, dans 39,54% de la surface du réseau seulement le taux d'erreur de l'espion est faible et cette zone constitue la zone vulnérable aux actes d'écoute illégal de l'espion. Avec les mêmes paramètres de simulation cette zone vulnérable constituait 92,49% de la surface du réseau dans le cas de l'allocation de puissance favorisant la source tel étudié à la sous section 5.4.2. La diminution de la zone vulnérable engendre l'augmentation de la zone sécurisée par un taux d'erreur moyen qui constitue 21,15% de la surface du réseau et de la zone hautement sécurisée qui constitue 39,30% de la surface du réseau. L'espérance du taux d'erreur pour l'espion sur l'ensemble de la surface du réseau a augmenté considérablement à $E\left[P_{e_E}\right] = 0{,}2218$.

La figure 5.9b montre le taux d'erreur pour l'espion lorsque les deux relais sont alignés avec la source et le récepteur légitime dont l'un des relais se positionne entre ces deux terminaux communicants. Dans ce cas, le relais est tellement proche du récepteur Bob que ce dernier est complètement perturbé et son taux d'erreur est $P_{e_B} = 4{,}9 \cdot 10^{-1}$. Cela est dû à l'augmentation de la puissance du signal brouilleur au même moment que la puissance du signal de la source a diminué en plus de l'affaiblissement du signal de ce dernier sous l'effet de l'affaiblissement de propagation. Pour l'espion, les mêmes statistiques de sécurité sont obtenus car la position radiale des deux relais n'a pas changée.

5.4.4 Discussion sur les configurations à deux relais

Dans la section 5.4, on a simulé le comportement d'un réseau de communication sans fil avec deux relais brouilleurs. Cette simulation comportait l'effet de la variation de l'allocation de puissance entre la source d'émission ainsi que la position des deux relais brouilleurs. Chaque stratégie avait des avantages et des inconvénients. Néanmoins, le niveau de sécurité du réseau est plus élevé qu'avec des stratégies à relais unique.

5.5 Simulation d'un réseau à 8 relais brouilleurs

Dans la section 5.4 on a montré les limites du concept de brouillage coopératif dans les réseaux à deux relais brouilleurs quant à la fiabilité et de sécurité. Dans cette section, on simule le comportement des réseaux sans fil soumis à l'écoute avec $N_J = 8$ relais brouilleurs. De même, on considère deux allocations de puissance : -1- une allocation égale entre l'émission de la source et le brouillage où la puissance dédiée au brouillage est partagée également entre les 8 relais. -2- une allocation égale entre l'émission de la source et le brouillage où chaque relais lui est allouée une puissance qui dépend de sa distance du récepteur légitime.

5.5.1 Partage égale de la puissance de brouillage

Dans cette stratégie de brouillage coopératif la puissance $P_{TOT} = 20$ dBm est partagée également entre l'émission et le brouillage : $P_S = P_J = P_{TOT}/2$. La puissance de brouillage P_J est elle même partagée équitablement entre les relais : $J^{(i)} = P_J/8$ avec $i = 1, ..., 8$. La source demeure à sa position centrale $(0\text{ m}, 0°)$ et le récepteur Bob à l'extrémité du réseau $(100\text{ m}, 0°)$. Les huit relais sont placés autour de la source Alice avec un angle $\theta = 45°$ entre chaque deux relais tel que indiqué à la figure 5.10. touts ces relais ont la même coordonnée radiale $\rho = 50$ m et créent chacun un signal de brouillage indépendant binaire de longueur $n = 100\,000$ bits et qui interfère les terminaux se trouvant dans son champ de portée.

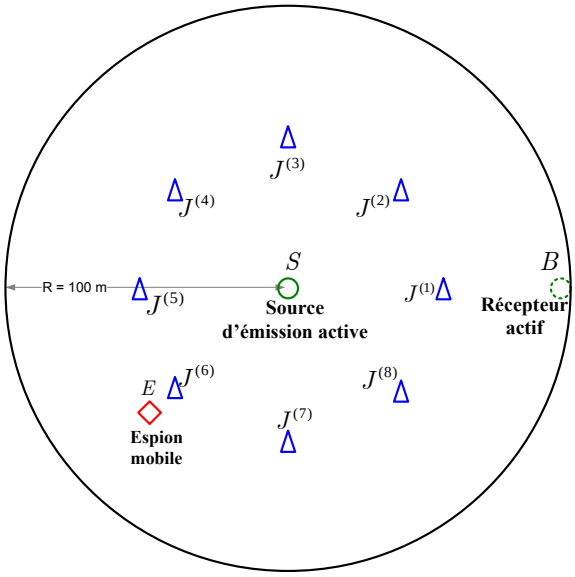


FIGURE 5.10 – *Réseau sans fil de télécommunication constitué d'un émetteur, d'un récepteur, d'un espion mobile et de* 8 *relais brouilleurs. Les relais forment un cercle autour de l'émetteur.*

Au niveau du récepteur légitime et de l'espion, les signaux reçus s'écrivent comme suit :

$$\begin{aligned} y_B &= h_{SB} \cdot P_S \cdot x_S + \sum_{i=1}^{8} \left(h_{J^{(i)}B} \cdot P_{J^{(i)}} \cdot x_{J^{(i)}}\right) + \eta_B \\ y_E &= h_{SE} \cdot P_S \cdot x_S + \sum_{i=1}^{8} \left(h_{J^{(i)}E} \cdot P_{J^{(i)}} \cdot x_{J^{(i)}}\right) + \eta_E \end{aligned} \tag{5.8}$$

On répète la même simulation d'évaluation des taux d'erreur P_{e_B} et P_{e_E} en utilisant les mêmes paramètres des sections précédentes et avec la nouvelle allocation de puissance. Les résultats des simulations sont affichés à la figure 5.11.

Les relais brouilleurs forment un cercle qui entoure la source d'émission et qui crée un obstacle entre ce dernier et le récepteur Bob. Dans la figure, on constate une ceinture comprise entre l'abscisse 40 m et l'abscisse ≈ 70 m dans laquelle on a huit maximas du taux d'erreur aux positions des relais

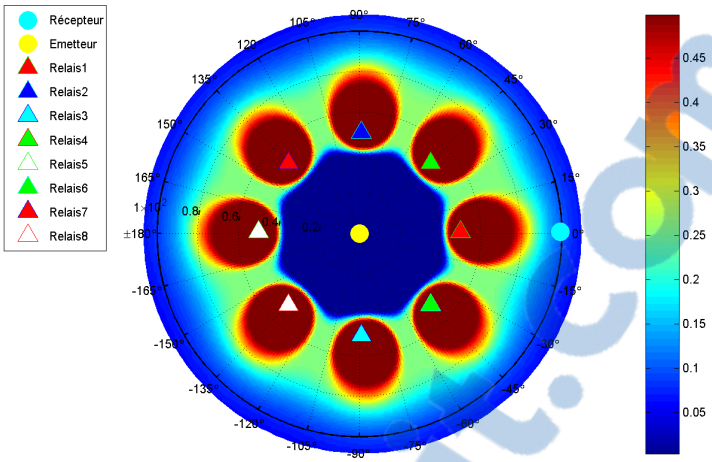


FIGURE 5.11 – *Variation du P_{e_E} en fonction des signaux de brouillage. N_J = 8, P_{TOT} = 20 dBm, $P_\eta = -80$ dBm, $P_S = P_J = 0{,}5 \cdot P_{TOT}$, $P_{e_B} = 6{,}5 \cdot 10^{-2}$.*

avec $P_{e_E} = 5 \cdot 10^{-1}$. On précise que le diamètre de ces zones de maximas dépend principalement de la puissance de brouillage attribuée à chaque relais et de l'affaiblissement de propagation auxquels les canaux sont soumis de coefficient α. Avec une puissance de brouillage valant 6% de la puissance totale P_{TOT} le diamètre des maximas est de $\rho \approx 30$ m. Si l'espion se trouve dans ces régions de maximas il est fortement brouillé. En dehors des zones de maximum le taux d'erreur diminue mais reste élevé. Le taux d'erreur dans la zone comprise entre la source d'émission et $\rho = 40$ m est très faible, voir nulle, car le signal de la source est plus fort que le signal de brouillage ce qui fait que les terminaux qui s'y trouvent bénéficient d'une meilleure réception et forme ainsi la région vulnérable aux actes d'espionnage. Dans la région où $\rho > 70$ m, le taux d'erreur commence à diminuer car les signaux brouilleurs commence à s'affaiblir sous l'influence de l'affaiblissement de propagation de coefficient $\alpha = 2$ pour atteindre $P_{e_E} = 6{,}5 \cdot 10^{-2}$ et ne reste pratiquement que le signal de la source Alice qui a une puissance beaucoup plus grande soit 50% de la puissance P_{TOT} contre 6% seulement pour chaque relais brouilleur. Ce signal de la source sous l'effet de l'affaiblissement de propagation perd lui aussi de la puissance.

En ce qui concerne le récepteur légitime, ce dernier se trouve dans une région à moyenne intensité de brouillage où le relais le plus proche se situe à 50 m de ce récepteur. Cette distance va affaiblir le signal de brouillage avant son arrivée et permet au récepteur de bénéficier d'une communication avec la source avec un taux d'erreur relativement faible $P_{e_B} = 6{,}5 \cdot 10^{-2}$. Ce taux ne permet pas d'assurer une communication fiable avec la source.

Avec cette allocation de puissance, on obtient les statistiques de sécurité suivantes : 25,55% de la surface du réseau est fortement sécurisée, 24,04% de la surface du réseau est moyennement sécurisée et 50,41% est faiblement sécurisée et cette région constitue la région la plus vulnérable quant à termes de sécurité. L'espérance du taux d'erreur pour l'espion sur l'ensemble de la surface du réseau a augmenté

considérablement à $E\left[P_{e_E}\right] = 0{,}1728$.

Vu la non fiabilité de la liaison légitime, on doit chercher une autre allocation de puissance pour rétablir cette fiabilité en admettant qu'une communication légitime fiable a un taux d'erreur $P_e \leq 1 \cdot 10^{-3}$.

5.5.2 Partage variable de la puissance de brouillage

Après avoir procédé à un partage égale de la puissance P_J entre les relais brouilleurs où $P_{J(i)} = P_J/N_J$, on s'intéresse ici à une allocation variable de puissance où on alloue à chaque relais une quantité de puissance en fonction de la distance entre ce relais et le récepteur légitime comme illustré à la figure 5.12.

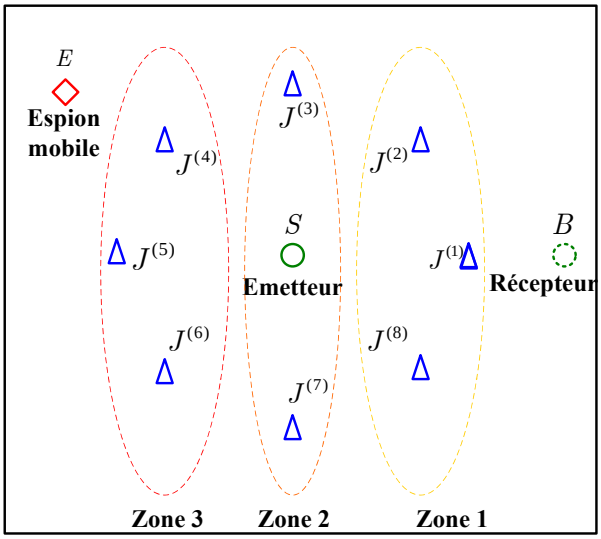


FIGURE 5.12 – *Réseau sans fil constitué d'un émetteur, d'un récepteur, d'un espion mobile et de N_J = 8 relais brouilleurs.*

On regroupe les relais en trois zones comme illustré à la figure 5.12 où on alloue au relais de chaque zone un niveau de puissance spécifique comme suit :

- relais de la zone 1 : $P_{J(i)} = 5\% \cdot P_J$, $i = 1,2,8$.
- relais de la zone 2 : $P_{J(i)} = 11\% \cdot P_J$, $i = 3,7$.
- relais de la zone 3 : $P_{J(i)} = 21\% \cdot P_J$, $i = 4,5,6$.

où $P_J = P_S = P_{TOT}/2$ et $N_J = 8$. Ce nouveau partage de la puissance P_J veut dire que plus le relais est loin du récepteur Bob et plus on alloue davantage de puissance à ce relais. Cela dans le souhait d'améliorer la fiabilité de la liaison entre la source et ce récepteur sans nuire au taux d'erreur moyen de l'espion sur toute la surface du réseau. En procédant à l'exécution de la même simulation d'évaluation des taux d'erreurs P_{e_B} et P_{e_E} avec les nouvelles attributions de puissance on obtient ainsi les résultats illustrés à la figure 5.13.

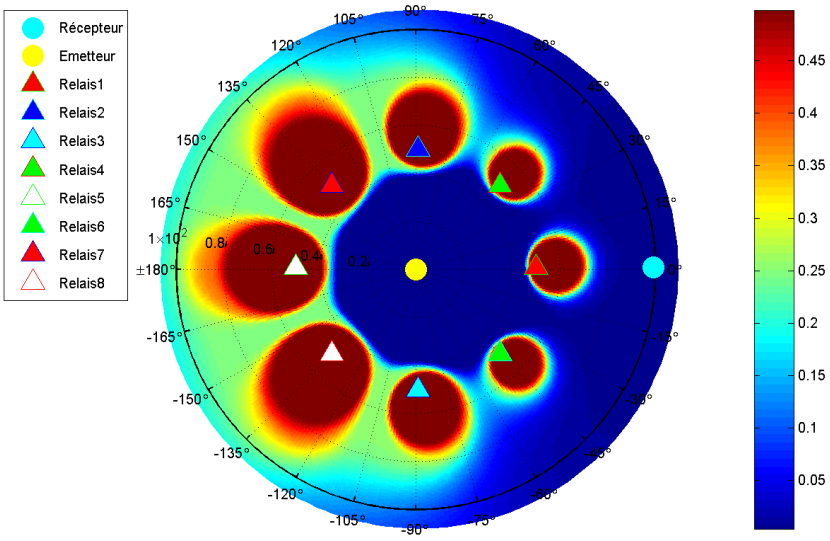


FIGURE 5.13 – *Variation du taux d'erreur de l'espion en fonction des signaux de brouillage.* $N_J = 8$, $P_{TOT} = 20$ *dBm*, $P_S = P_J = 0{,}5 \cdot P_{TOT}$, $P_{e_B} = 1{,}3 \cdot 10^{-3}$.

Les résultats obtenus nous montrent clairement que la distribution de puissance sur les relais brouilleurs a un effet direct sur le taux d'erreur au niveau du récepteur légitime. Les relais du groupe 1 ont une faible puissance d'émission ce qui laisse la région les entourant faiblement sécurisée. Malgré cette situation non souhaitable quant à la sécurité du réseau mais cela permet au récepteur Bob de bénéficier d'une communication fiable avec la source Alice avec un taux d'erreur $P_{e_B} = 1{,}3 \cdot 10^{-3}$ où la puissance du signal x_S demeure la même que celle de la stratégie précédente.

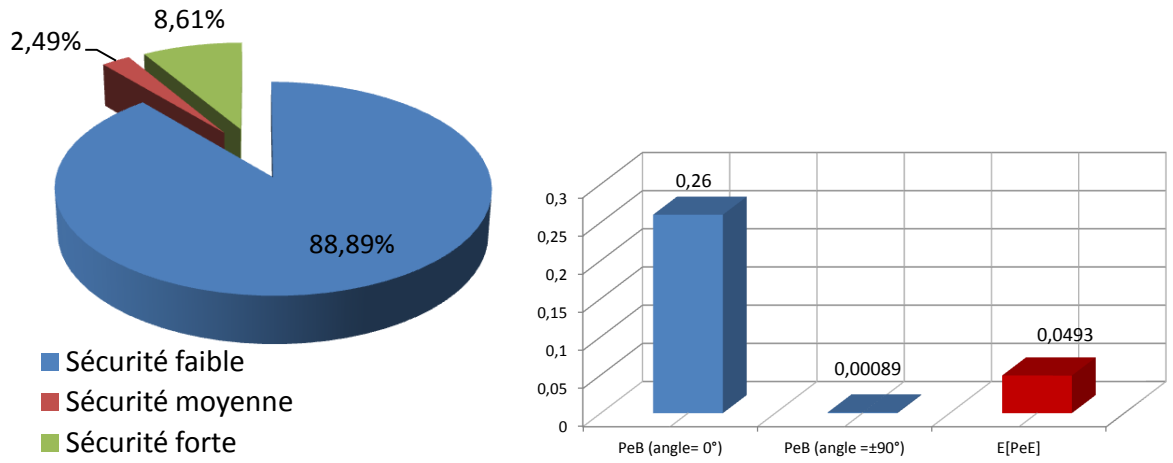
Les statistiques de sécurité quant aux perturbations au niveau de l'espion ont changées avec le changement de l'allocation de puissance : 44,85% de la surface du réseau est faiblement sécurisée et se situe principalement entre les relais à faible puissance d'émission et le récepteur Bob. Avec un partage égal de la puissance de brouillage entre les 8 relais cette zone couvrirait 29,42% seulement de la surface du réseau. La zone sécurisée par un taux d'erreur moyen constitue 29,57% du réseau enregistrant une diminution par rapport à celle obtenue avec un partage équitable de la puissance de brouillage entre les relais. La zone fortement sécurisée a diminué à 25,58%. L'espérance du taux d'erreur pour l'espion sur l'ensemble de la surface du réseau a augmenté considérablement à $E[P_{e_E}] = 0{,}1658$.

5.6 Discussion sur les résultats de fiabilité et sécurité obtenus avec 1, 2 et 8 relais

Dans ce qui suit, on fait une discussion de l'ensemble des résultats obtenus concernant la sécurité du réseau et la fiabilité des liaisons légitimes.

La figure 5.14 montre les statistiques de couverture sécuritaire et de fiabilité de la liaison légitime

entre Alice et Bob pour une configuration mono relais avec allocation de puissance favorisant la source Alice. Une grande partie du réseau est non sécuritaire à cause de la faible intensité du signal brouilleur et la dominance du signal émis par Alice, ce qui permet une fiabilité de réception lorsque le relais est loin de Bob. Cette fiabilité est perdue lorsque le relais se met entre Alice et Bob malgré la faible puissance de brouillage.



(a) Sécurité du réseau. $N_J = 1$.

(b) Fiabilité de liaison légitime. $N_J = 1$.

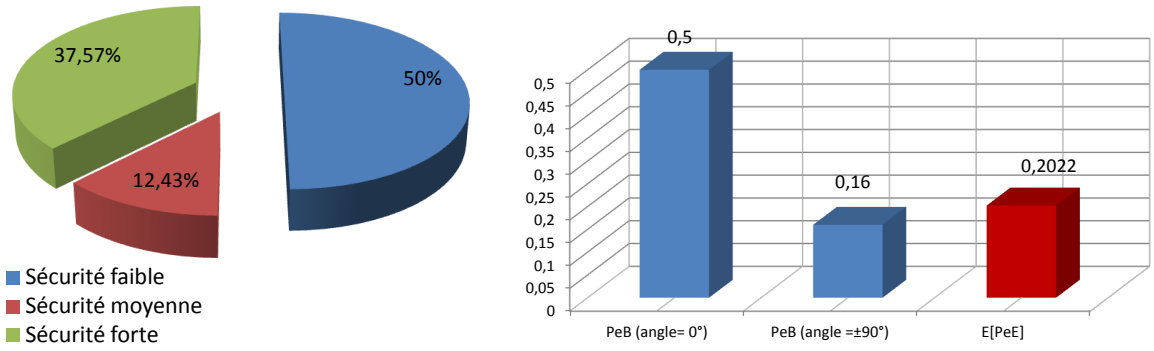
FIGURE 5.14 – *Statistiques de sécurité et de fiabilité pour un réseau à $N_J = 1$ relais brouilleur. $P_S = 0{,}8 \cdot P_{TOT}$ dBm. $P_J = 0{,}2 \cdot P_{TOT}$ dBm.*

Cette fiabilité est totalement perdue quelle que soit la position du relais lorsqu'on a une allocation de puissance équitable entre la source et le relais comme illustré à la figure 5.15 car le brouillage est maintenant plus important et permet malgré cette perte de fiabilité d'améliorer considérablement la couverture sécuritaire du réseau en basculant des régions du réseau de la zone faiblement sécurisée aux zones moyennement et fortement sécurisée. Ainsi, l'espérance du taux d'erreur de l'espion sur toute la surface du réseau $E[P_{e_E}]$ passe de 0,0493 à 0,2022.

A la figure 5.16, avec la même allocation de puissance favorisant la source, soit $P_S = 0{,}8 \cdot P_{TOT}$ dBm et $P_J = 0{,}2 \cdot P_{TOT}$ dBm, le taux sécuritaire a baissé car lorsqu'on a deux relais brouilleurs la puissance de brouillage est divisé par deux ce qui rend l'influence du signal brouilleur très limitée et engendre l'augmentation de la zone faiblement sécurisée jusqu'à 92,49% de la surface du réseau. Cela permet au même temps d'améliorer relativement la fiabilité de la liaison légitime lorsque le relais est positionné entre la source Alice et le récepteur Bob.

Malgré que la fiabilité de la liaison légitime est perdue pour une allocation de puissance équitable entre l'émission et le brouillage quelle que soit la position des deux relais, mais la présence de ce deuxième relais à permis d'élargir la zone moyennement et fortement sécurisée comme on peut le voir à la figure 5.17

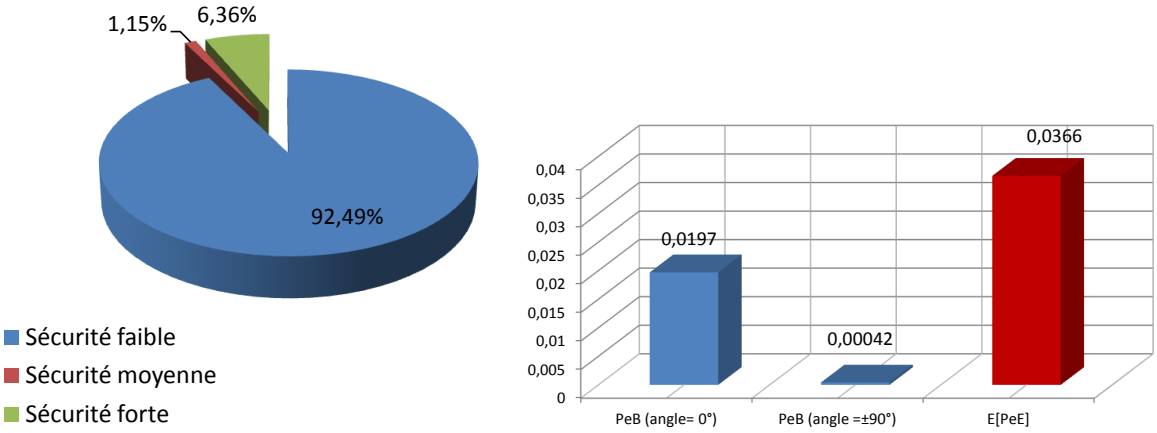
Avec une configuration réseau à 8 relais avec répartition équitable de la puissance de brouillage sur



(a) Sécurité du réseau. $N_J = 1$.

(b) Fiabilité de liaison légitime. $N_J = 1$.

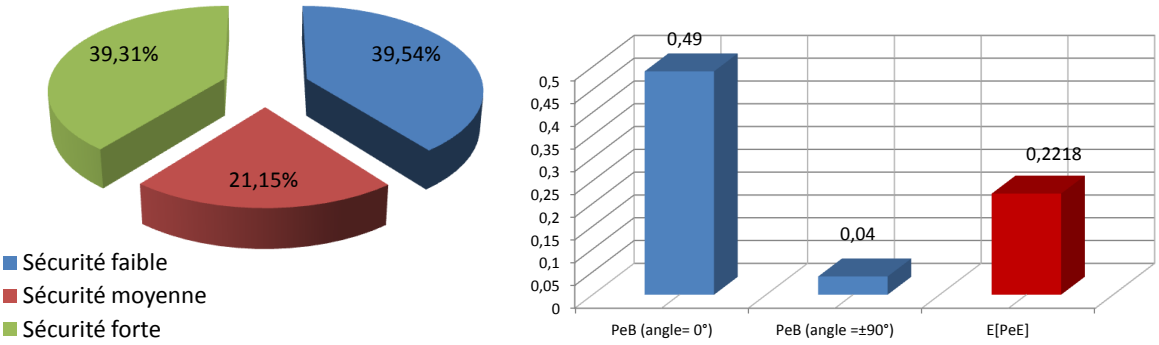
FIGURE 5.15 – *Statistiques de sécurité et de fiabilité pour un réseau à $N_J = 1$ relais brouilleur. $P_S = 0{,}5 \cdot P_{TOT}$ dBm. $P_J = 0{,}5 \cdot P_{TOT}$ dBm.*



(a) Sécurité du réseau. $N_J = 2$.

(b) Fiabilité de liaison légitime. $N_J = 2$.

FIGURE 5.16 – *Statistiques de sécurité et de fiabilité pour un réseau à $N_J = 2$ relais brouilleur. $P_S = 0{,}8 \cdot P_{TOT}$ dBm. $P_J = 0{,}2 \cdot P_{TOT}$ dBm.*

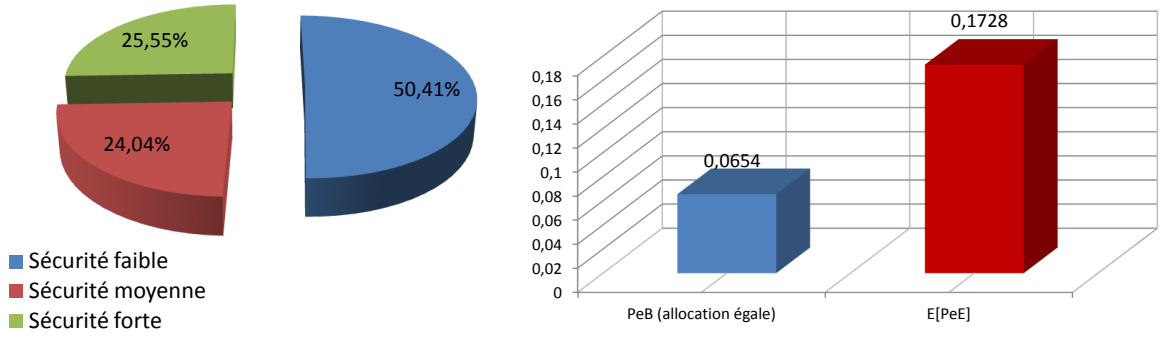


(a) Sécurité du réseau. $N_J = 2$.

(b) Fiabilité de liaison légitime. $N_J = 2$.

FIGURE 5.17 – *Statistiques de sécurité et de fiabilité pour un réseau à $N_J = 2$ relais brouilleur. $P_S = 0{,}5 \cdot P_{TOT}$ dBm. $P_J = 0{,}5 \cdot P_{TOT}$ dBm.*

ces relais, on a pu conserver les mêmes statistiques de sécurité tout en baissant le taux d'erreur P_{e_B} au niveau du récepteur Bob de $0{,}16(\alpha = \pm 90°)$ et $0{,}5(\alpha = 0°)$ jusqu'à $6{,}5 \cdot 10^{-2}$ même si ce nouveau taux d'erreur est non fiable aussi. Voir figure 5.18.

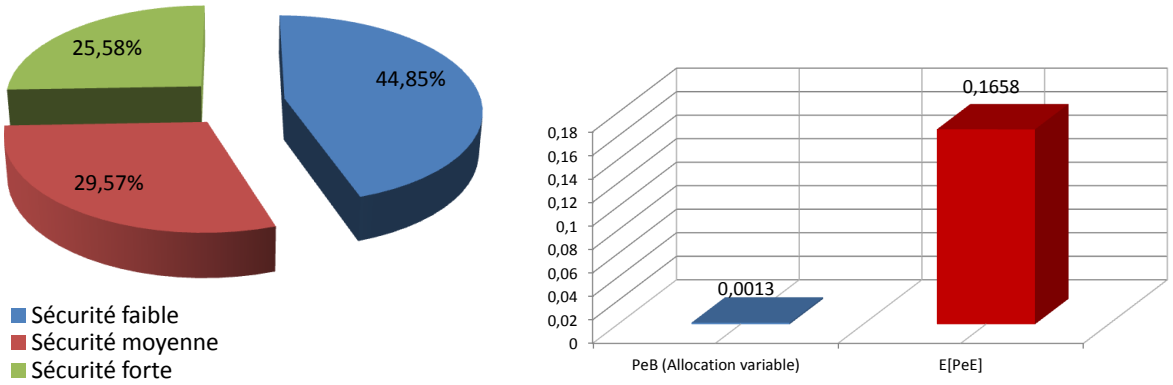


(a) Sécurité du réseau. $N_J = 8$.

(b) Fiabilité de liaison légitime. $N_J = 8$.

FIGURE 5.18 – *Statistiques de sécurité et de fiabilité pour un réseau à $N_J = 8$ relais brouilleur. $P_S = 0{,}5 \cdot P_{TOT}$ dBm. $J^{(i)} = P_J/8$ dBm avec $i = 1,\ldots,8$ dBm.*

Avec une allocation variable entre les 8 relais où on attribue de la puissance à chaque relais selon sa distance du récepteur Bob, la fiabilité de la liaison légitime est nettement améliorée en conservant un taux de couverture sécuritaire acceptable en diminuant la zone faiblement sécurisée, comme illustré à la figure 5.19.



(a) Sécurité du réseau. $N_J = 8$.

(b) Fiabilité de liaison légitime. $N_J = 8$.

FIGURE 5.19 – *Statistiques de sécurité et de fiabilité pour un réseau à $N_J = 8$ relais brouilleur. $P_S = 0{,}5 \cdot P_{TOT}$ dBm. $P_{J^{(i)}} = 5\% \cdot P_J$ $(i = 1{,}2{,}8)$. $P_{J^{(j)}} = 11\% \cdot P_J$ $(j = 3{,}7)$. $P_{J^{(m)}} = 21\% \cdot P_J$ $(m = 4{,}5{,}6)$.*

5.7 Conclusion

Dans ce chapitre, nous avons étudié l'effet de brouillage coopératif entre les utilisateurs légitimes dans un réseau sans fil multirelais soumis à l'écoute. On a présenté à la section 5.2 la contrainte de partage de puissance entre l'émission et le brouillage et son influence sur les performances du brouillage

coopératif. Nous avons présenté une analyse des résultats de simulation de stratégies de brouillage coopératif avec un seul relais brouilleur pour les réseaux sans fil avec canaux gaussiens à la section 5.3 où on a montré que l'efficacité de ce brouillage est en lien direct avec l'allocation de puissance. Deux critères de communication qui varient inversement doivent êtres gérés qui sont la fiabilité de la liaison légitime entre la source et le récepteur ainsi que le taux d'erreur moyen de l'espion sur l'ensemble de la surface du réseau de communication. Par la mesure du taux d'erreur au niveau du récepteur légitime et au niveau des espions sous l'effet de brouillage généré par un seul relais, on a montré que peu importe l'allocation de puissance utilisée, un seul relais ne peut pas couvrir toute la surface du réseau, en particulier si le réseau est de dimensions importantes.

Ce partage de puissance devient plus compliqué dans le cas de stratégies de brouillage coopératif à $N_J = 2$ relais, comme étudié à la section 5.4. Dans ce cas, deux allocations doivent être prises en considération : le partage de puissance entre l'émission et le brouillage et le partage de la puissance de brouillage entre les deux relais brouilleurs. Les stratégies à deux relais brouilleurs permettent plus de flexibilité et d'efficacité que les stratégies à relais unique, car la surface d'influence de chaque relais est réduite. Ainsi, de petites quantités de puissance suffisent à chaque relais pour brouiller les espions présents dans son champs d'influence. Cette nouvelle configuration de terminaux donne plus de sécurité au réseau tout en assurant une communication fiable avec l'utilisateur légitime si chaque relais a la puissance nécessaire pour brouiller les terminaux à proximité sans que le signal de brouillage puisse atteindre le récepteur légitime. Cette contrainte constitue une limitation de sécurité puisque cela engendre des zones non sécurisées.

En raison de la limitation de l'effet de brouillage avec une architecture à deux relais brouilleurs, on a opté à la section 5.5 pour un réseau à $N_J = 8$ relais brouilleurs. Cette configuration a nettement amélioré le taux de couverture sécuritaire du réseau. Le taux de couverture sécuritaire augmente ou diminue selon qu'on attribue plus ou moins de puissance aux relais brouilleurs. Cette dernière configuration garantit à la fois une communication légitime fiable et un taux de brouillage plus élevé pour les utilisateurs non légitimes, qu'avec 2 relais seulement. Néanmoins, il reste encore des zones non sécurisées : celles-ci ne peuvent être supprimées totalement, du moins dans la zone où se trouve le récepteur légitime, car brouiller cette zone va perturber aussi le récepteur légitime et affecter sa fiabilité. Donc, une stratégie d'optimisation de la fiabilité de liaison pour le récepteur légitime et du taux d'erreur moyen de l'espion doit être mis en place. Cela constitue le sujet du chapitre 6.

L'affaiblissement de propagation a un double effet : l'affaiblissement du signal émis par la source va amplifier l'effet de brouillage sur l'espion, car le signal de la source se dégrade davantage pendant son parcours. Cela est considéré comme un avantage en terme de sécurité du réseau. Par contre, cet affaiblissement va perturber la fiabilité de la liaison légitime, surtout si l'allocation de puissance appliquée ne fournit pas assez de puissance à la source pour que son signal soit reçu par le récepteur avec fiabilité, sous l'effet de cet affaiblissement.

Chapitre 6

Renforcement de la sécurité à la couche physique

6.1 Introduction

Lors la conception de mesures de sécurité au niveau de la couche physique dans les réseaux sans fil, l'idée de base est à la fois d'assurer la probabilité d'erreur de décodage la plus faible pour le récepteur légitime et d'obtenir la probabilité d'erreur la plus élevée possible pour l'espion. Ce dernier étant de position aléatoire dans le réseau sans fil, l'objectif est alors d'augmenter au maximum l'espérance de la probabilité d'erreur de cet espion sur toute la surface du réseau sans fil.

Dans ce chapitre, on évalue le concept du brouillage coopératif pour la sécurité du signal émis par une source omnidirectionnelle placée au centre d'un réseau sans fil de forme circulaire, vers un récepteur légitime. Cette évaluation se base sur deux paramètres : la recherche du meilleur emplacement des N_J relais et la recherche de la meilleure allocation de puissances qui partage la puissance totale P_{TOT} entre la source et ces relais pour également avoir les meilleures résultats possibles quant à la fiabilité de la liaison légitime et de couverture sécuritaire. Ces paramètres sont liés directement à la performance du brouillage coopératif.

Le chapitre est organisé comme suit : à la section 6.2, on explique brièvement comment le développement des travaux de recherche sur le canal sous écoute a mené à la mise en place du concept de brouillage coopératif pour le renforcement et l'amélioration de la sécurité à la couche physique des réseaux sans fil soumis à l'écoute clandestine.

À la section 6.3, on valide le principe des résultats des travaux présentés par Dong et al. dans [5]. A la section 6.4, étant donné la présence de 3 relais brouilleur, on propose un algorithme automatisé qui améliore le brouillage coopératif en quatre étapes : -1- le meilleur emplacement du premier relais $J^{(1)}$, -2- la recherche de l'allocation de puissance entre la source et le relais donnant les meilleurs résultats de fiabilité et de sécurité, -3- le meilleur emplacement des relais $J^{(2)}$ et $J^{(3)}$ pour l'amélioration des

résultats obtenus avec un seul relais et -4- la recherche de l'allocation de puissance qui garantissent le maximum de la surface du réseau noyée dans le brouillage tout en gardant une fiabilité de la liaison légitime, en supposant que la puissance de brouillage est partagée équitablement entre ces 3 relais.

6.2 Brouillage coopératif pour la sécurité à la couche physique

Le développement de l'exploitation du principe du canal sous écoute, proposé initialement par Wyner [3] mène à la naissance du concept de brouillage coopératif pour la sécurité des communications dans les réseaux multi-utilisateurs sur la base de la couche physique par l'exploitation des caractéristiques physiques du canal sans fil.

Alors que la source transmet son message à sa destination, un ou plusieurs relais brouilleurs émettent des signaux brouilleurs afin de plonger la plus grande surface possible du réseau sans fil dans la confusion, sans toute fois nuire à la fiabilité de la liaison légitime. Ce concept s'inscrit dans la coopération entre les utilisateurs légitimes [15].

Pour améliorer les débits de communications sécurisées, ce relais (dont les conditions de canal ne lui permet pas une communication sécurisée) va soit augmenter la puissance de son signal et ainsi le rapport signal à bruit (SNR) au récepteur légitime, soit diminuer le (SNR) de l'espion. Cela se fait par l'ajout d'un signal de brouillage généré par ce même relais [26]. Si l'espion est affecté par du bruit et de l'interférence (brouillage) plus que le récepteur légitime, alors ce brouillage va avoir un effet plus néfaste sur cet espion que sur le récepteur légitime, ce qui peut entraîner une augmentation du débit de communication sécurisé.

Cependant, cette approche exige implicitement la connaissance de l'état de tous les canaux existants (CSI), pour que le brouillage n'ait pas un effet négatif sur le récepteur légitime du réseau. Dans la pratique, cette connaissance est obtenue par un mécanisme de coopération entre les relais, d'où le nom de brouillage coopératif.

On rappelle que l'efficacité du brouillage coopératif repose entre autres sur le positionnement des N_J relais brouilleurs sur la surface du réseau sans fil de sorte que les canaux de brouillage *Relais-Espion* soient meilleurs que les canaux *Relais-Récepteur* au maximum, au même temps que le canal *Source-Récepteur* soit fiable. Dans ce cas, le relais brouilleur peut contribuer à renforcer la capacité secrète entre la source et le récepteur en cessant d'envoyer de l'information utile au récepteur et en envoyant du bruit gaussien indépendant à ce récepteur et à l'espion simultanément. Étant donné que le canal *Relais-Espion* est meilleur, cela augmente davantage la quantité d'interférence vers l'espion que vers le récepteur : le relais contribue ainsi à l'augmentation de la capacité secrète de la liaison légitime entre la source et le récepteur légitime.

Dans [15], afin que l'espion ne soit pas en mesure de décoder les messages qu'il observe de la communication légitime, on propose deux scénarios pour ajouter du bruit généré artificiellement afin de sécuriser les communications à la couche physique de telle sorte que la réception ne soit pas dégradée ;

soit par l'utilisation d'une source multi-antennes, soit par l'utilisation de plusieurs relais brouilleurs mono-antenne. Dans les deux scénarios, on maintient un niveau de capacité secrète déterminé qui permet une communication sécurisée entre les interlocuteurs légitimes.

6.3 Application du concept de brouillage coopératif pour la sécurité des réseaux sans fil

On rappelle que selon les résultats obtenus à la section 3.4.1 pour le brouillage coopératif appliqué à un réseau avec disposition linéaire des terminaux, l'efficacité du brouillage coopératif dépend en grande partie de la puissance attribuée à la source d'information et au relais, ainsi que la position de ce dernier vis-à-vis la position du récepteur légitime et de l'espion. Ce dernier étant de position aléatoire, l'objectif est non pas d'augmenter son taux d'erreur mais plutôt d'augmenter la valeur moyenne de son taux d'erreur sur toute la surface du réseau de communication.

Dans le modèle étudié dans [5], le relais a une position statique, ce qui n'est pas nécessairement la position qui donne des résultats les plus favorables quant à la fiabilité de la liaison légitime et le brouillage de l'espion quelle que soit la position de ce dernier.

Considérant deux facteurs qui évoluent inversement : le positionnement du relais et la détermination de l'allocation de puissance devient très difficile à établir, car pour garantir une communication fiable entre source et récepteur légitime où $P_{e_B} \leq P_{e_{seuil}}$, il faut donner de la puissance suffisante à la source. Cette attribution de puissance peut nuire à l'efficacité du relais brouilleur et le taux d'erreur moyen de l'espion risque de diminuer. Inversement, si on favorise le relais quant à l'allocation de puissance on augmente alors la probabilité d'erreur moyenne $E[P_{e_E}]$ de l'espion mais cela risque de faire perdre la fiabilité de la communication légitime et le taux d'erreur P_{e_B} au récepteur devient grand.

6.4 Amélioration du brouillage coopératif

Dans ce qui suit, on veut améliorer les résultats obtenus au chapitre 5 quant à la fiabilité de la liaison légitime et la perturbation de l'espion.

Dans la surface circulaire de rayon $r = 100$ m illustrée à la figure 6.1, la source souhaite établir une communication fiable et sécurisée avec le récepteur qui se trouve à l'extrémité du réseau aux coordonnées polaires $(0°, 100\,\text{m})$, quant à la source, elle se positionne au centre de la surface aux coordonnées $(0°, 0\,\text{m})$. On veut que le taux d'erreur P_{e_B} au niveau de ce récepteur soit au maximum égal à 10^{-3} tout au long de la période de communication au même moment que l'espérance du taux d'erreur de l'espion sur toute la surface du réseau soit le plus grand possible.

Pour cela, on divise notre simulation en quatre étapes comme suit :

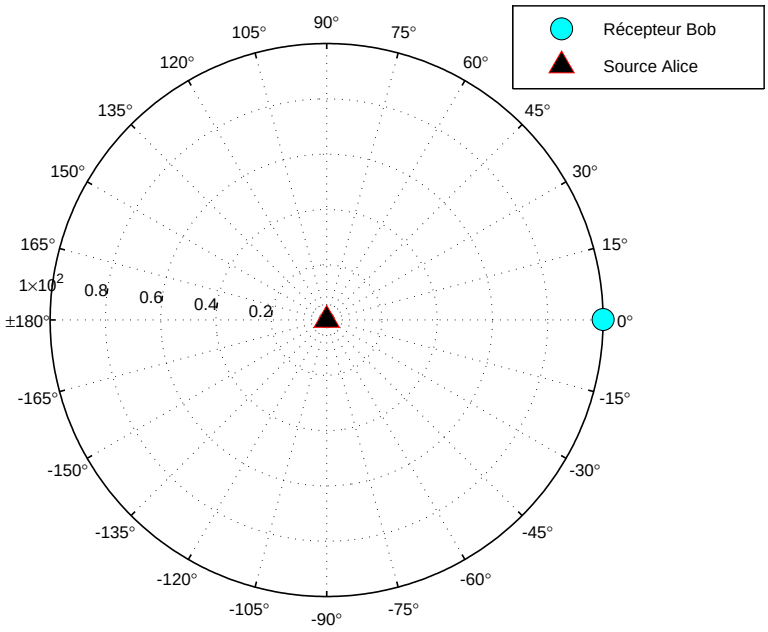


FIGURE 6.1 – *Disposition des terminaux légitimes dans la surface circulaire de rayon $r = 100$ m.*

6.4.1 Étape 1 : Positionnement idéal du relais brouilleur

A la figure 6.2, on schématise les principales opérations de cette étape pour le positionnement idéal du relais de coordonnées polaires $\left(\theta^J, \rho^J\right)$.

Le but de cette première partie de la simulation est de positionner le relais Charlie dans la surface circulaire pour deux objectifs clés : avoir une communication fiable entre la source d'information Alice et le récepteur légitime Bob en garantissant que le taux d'erreur de ce dernier soit au plus égal à la valeur seuil 10^{-3} et que l'espérance des taux d'erreurs de l'espion sur toute la surface du réseau soit le plus grand possible.

Le principe de la simulation est d'évaluer à chaque position possible du relais sur la surface du réseau les taux d'erreur P_{e_B} et P_{e_E} pour 11 allocations de puissance différentes entre la source Alice et Charlie.

Le réseau de la figure 6.1 est soumis à une contrainte de puissance $P_{\text{TOT}} = 20$ dBm avec $P_{\text{TOT}} = P_S + P_J$. A la réception, un bruit blanc gaussien de puissance P_η = -80 dBm s'ajoute aux signaux reçus par Bob et Eve ce qui cause des erreurs dans le décodage de ces signaux reçus [5]. Ces signaux s'écrivent comme indiqué dans les équations (6.1) et (6.2) :

$$y_B = h_{SB} \cdot P_S \cdot x_S + h_{JB} \cdot P_J \cdot x_J + \eta_B \tag{6.1}$$

$$y_E = h_{SE} \cdot P_S \cdot x_S + h_{JE} \cdot P_J \cdot x_J + \eta_E \tag{6.2}$$

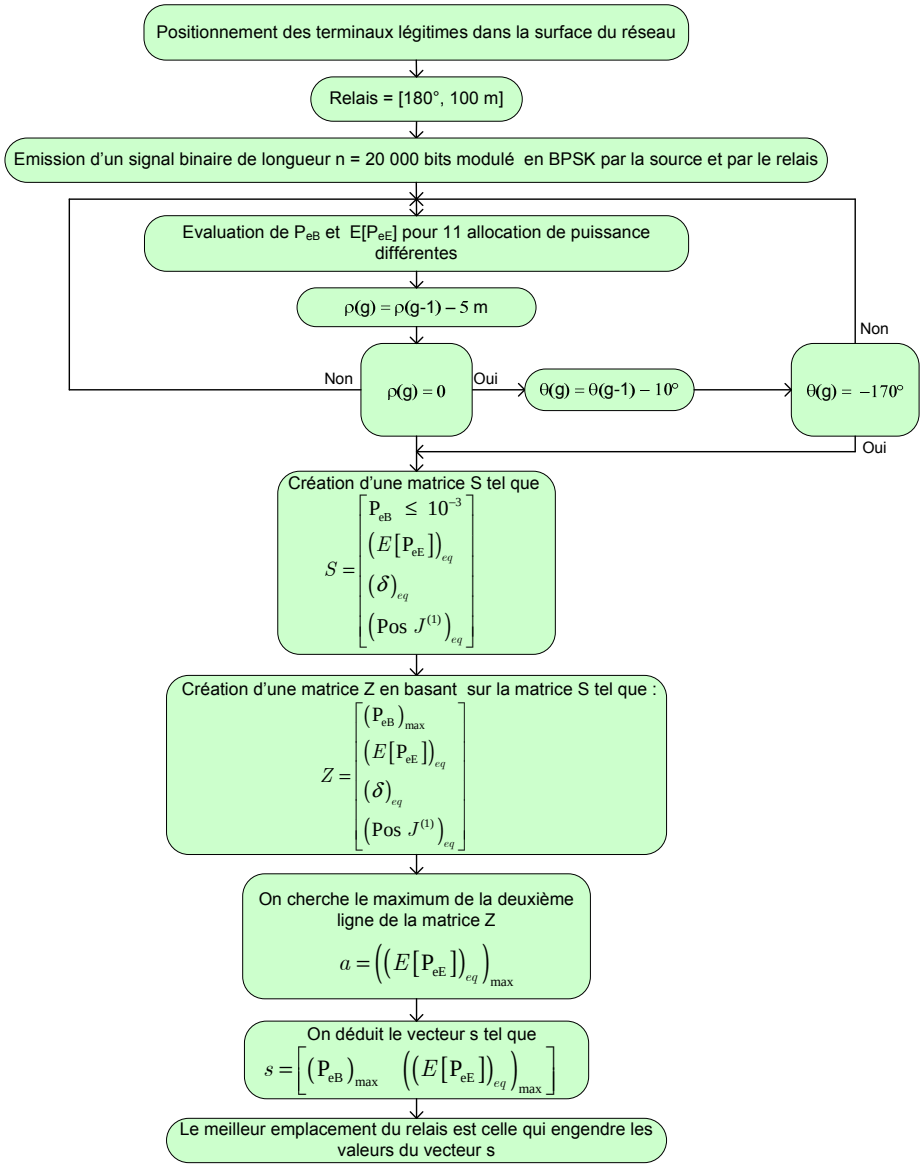


FIGURE 6.2 – *Algorithme de la recherche du meilleur emplacement du relais brouilleurs.*

6.4.1.1 Déplacement du relais brouilleur

La figure 6.3 illustre la procédure de déplacement du relais brouilleur dans la surface circulaire. La position initiale du relais est $(180°, 100\,\text{m})$. Le relais parcourt toute la surface du réseau par la variation de sa coordonnée angulaire d'un angle $\phi = 10°$ et de sa coordonnée radiale d'une distance $\rho = 5$ m. Au total, le relais se positionne dans 756 positions différentes qui couvrent toute la surface du réseau. A chacune de ces positions, la source omnidirectionnelle Alice émet à la puissance P_S un signal binaire x_S de longueur $n = 20\,000$ bits modulé en BPSK au même moment que Charlie émet à la puissance $P_J^{(1)}$ un signal brouilleur x_J de même longueur et modulé également en BPSK et on

évalue les taux d'erreurs P_{e_B} et $E\left[P_{e_E}\right]$ pour 11 allocations de puissance différentes tel que expliqué au point 2.4.5.

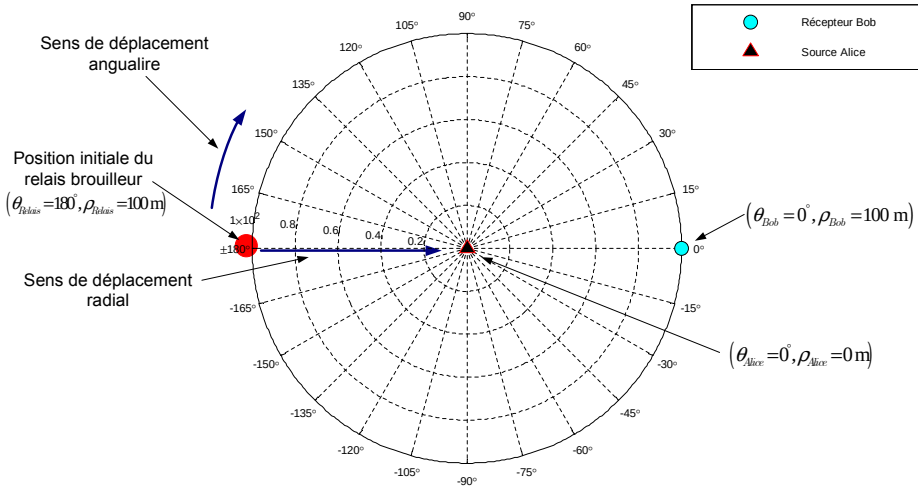


FIGURE 6.3 – *Procédure de déplacement du relais brouilleur dans la surface circulaire.*

6.4.1.2 Évaluation des taux d'erreurs aux récepteurs

On écrit l'allocation de puissance entre la source et le relais comme suit : $P_J = \delta \cdot P_{\text{TOT}}$ et $P_S = (1-\delta) \cdot P_{\text{TOT}}$, où δ est un nombre réel qui varie de 0 à 1 avec un pas de 0,1. Chaque allocation de puissance s'écrit en fonction du temps discret g comme suit :

$$P_J(g) = \delta(g) \cdot P_{\text{TOT}} \tag{6.3}$$

$$P_S(g) = (1-\delta(g)) \cdot P_{\text{TOT}} \tag{6.4}$$

où $\delta \in [0,\, 1]$ est le coefficient de partage de la puissance totale P_{TOT} entre la source et le relais. Au total, on obtient 11 allocations de puissance différentes.

Les équations indiquées dans (6.1) et (6.2) s'écrivent alors comme suit :

$$y_B(g) = h_{SB} \cdot (1-\delta(g)) \cdot P_{\text{TOT}} \cdot x_S + h_{JB} \cdot \delta(g) \cdot P_{\text{TOT}} \cdot x_J + \eta_B \tag{6.5}$$

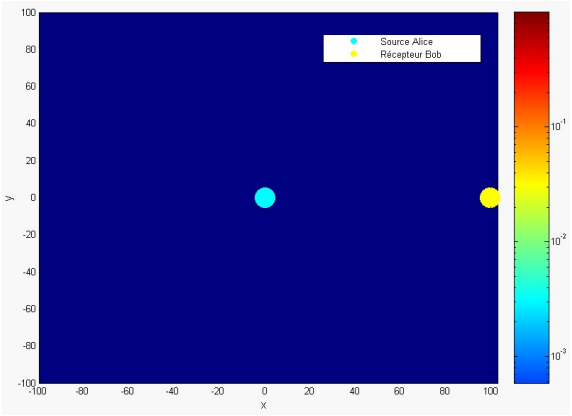
$$y_E(g) = h_{SE} \cdot (1-\delta(g)) \cdot P_{\text{TOT}} \cdot x_S + h_{JE} \cdot \delta(g) \cdot P_{\text{TOT}} \cdot x_J + \eta_E \tag{6.6}$$

Pour chacune des 756 positions possibles du relais on évalue à chaque position les taux d'erreur P_{e_B} et $\mathrm{E}[P_{e_E}]$ pour chaque allocation de puissance. Les résultats obtenus montrent que la valeur des taux d'erreurs P_{e_B} et $\mathrm{E}[P_{e_E}]$ dépends particulièrement :

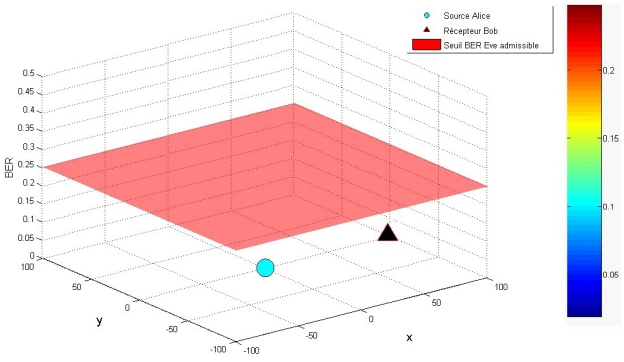
- de l'allocation de puissance entre la source et le relais,
- de l'emplacement du relais dans la surface du réseau.

Dans ce qui suit, on présente quelques résultats de l'évaluation des taux d'erreurs P_{e_B} et $\mathrm{E}[P_{e_E}]$ lorsque le relais parcours toute la surface circulaire.

À la figure 6.4, on montre les résultats de l'évaluation des taux d'erreur P_{e_B} et $\mathrm{E}[P_{e_E}]$ pour $\delta = 0$ c'est à dire $P_S = 1 \cdot P_{\mathrm{TOT}}$ et $P_J = 0 \cdot P_{\mathrm{TOT}}$. Toute la puissance est allouée à la source. Dans ce cas, quelle que soit la position du relais dans le réseau, la liaison légitime est très fiable à cause de la forte puissance du signal x_S et l'absence du signal brouilleur x_J. Le bruit blanc gaussien reste sans effet visible sur la qualité du signal de la source. La même situation est observée pour l'espérance du taux d'erreur de l'espion qui est très faible quelle que soit la position du relais, comme illustré à la 6.4b.



(a) P_{e_B} en fonction de la position du relais.

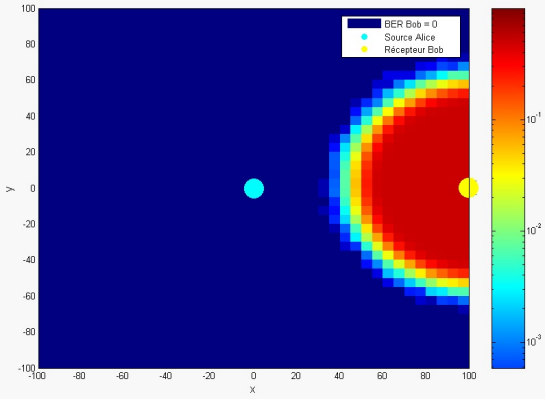


(b) $E(P_{e_E})$ en fonction de la position du relais.

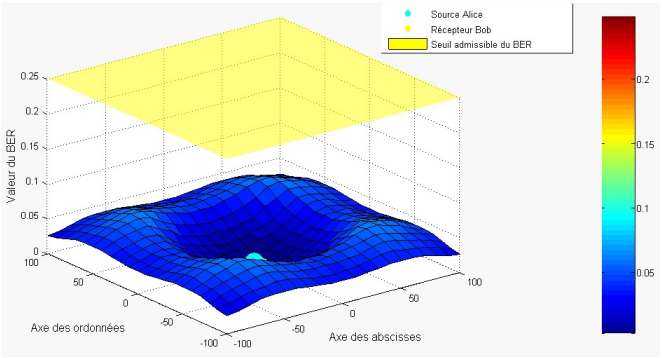
FIGURE 6.4 – *Évaluation de P_{e_B} au récepteur Bob de coordonnées $(0°, 100\ m)$ et $E[P_{e_E}]$ de l'espion pour chaque position possible du relais dans le réseau. $\delta = 0$: $P_S = P_{TOT}$, $P_J = 0$.*

À la figure 6.5, on montre le résultats de l'évaluation des taux d'erreur P_{e_B} et $E[P_{e_E}]$ pour $\delta = 0{,}2$, soit $P_S = 0{,}8 \cdot P_{\mathrm{TOT}}$ et $P_J = 0{,}2 \cdot P_{\mathrm{TOT}}$. Dans ce cas, le signal brouilleur n'est plus négligeable et on voit dans la figure que lorsque le relais se place au voisinage du récepteur Bob, ce dernier est perturbé et son taux d'erreur P_{e_B} n'est pas nul. Lorsque le relais se positionne loin de ce récepteur alors la liaison légitime redevienne de nouveau fiable.

Pour l'espion, lorsqu'on place le relais très proche de la source Alice, par exemple à une position ayant la coordonnée radiale $(10\ \mathrm{m})$, l'espérance du taux d'erreur $E[P_{e_E}]$ est très faible car ce relais se trouve dans une région où le signal de la source est fort et plus dominant que le signal brouilleur, ce qui laisse la réception de l'espion fiable. Lorsque le relais se place aux positions ayant la coordonnée radiale $(\approx 50\ \mathrm{m})$, ce relais est relativement loin de la source au même temps que la puissance du signal de la source a diminué sous l'effet de l'atténuation par propagation de coefficient $\alpha = 2$. $E[P_{e_E}]$ atteint alors sa plus grande valeur $\approx 5{,}8 \cdot 10^{-2}$. Si le relais se trouve aux régions éloignées de la source aux extrémités du réseau, la zone de couverture de ce relais baisse car la puissance du signal brouilleur n'est pas suffisante pour couvrir toute la surface du réseau, en particulier les régions opposées à la position de ce relais.



(a) P_{e_B} en fonction de la position du relais dans le réseau.

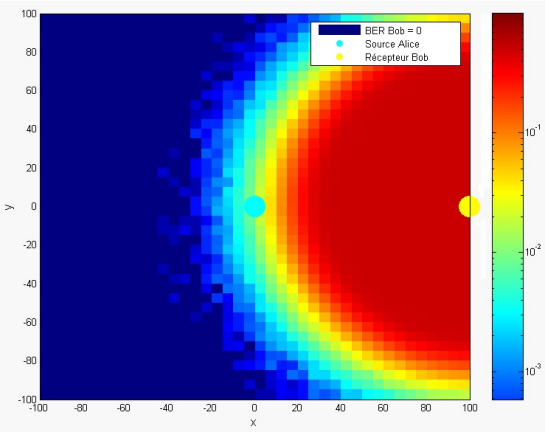


(b) $E(P_{e_E})$ en fonction de la position du relais dans le réseau.

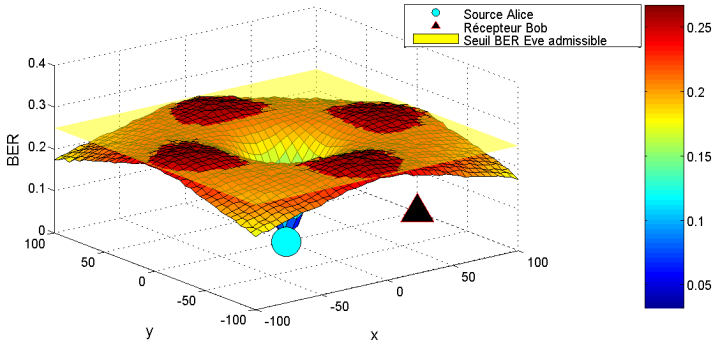
FIGURE 6.5 – *Évaluation de P_{e_B} au récepteur Bob de coordonnées $(0°,100\ m)$ et $E[P_{e_E}]$ de l'espion pour chaque position possible du relais dans le réseau. $\delta = 0{,}2$: $P_S = 0{,}8 \cdot P_{TOT}$, $P_J = 0{,}2 \cdot P_{TOT}$.*

Pour l'allocation de puissance où $\delta = 0{,}4$, soit $P_S = 0{,}6 \cdot P_{\text{TOT}}$ et $P_J = 0{,}4 \cdot P_{\text{TOT}}$, l'évaluation des taux d'erreur P_{e_B} et $E[P_{e_E}]$ sont illustrés à la figure 6.6. Le signal brouilleur a une puissance considérable par rapport à la puissance du signal de la source. Dans ce cas, même si on place le relais relativement loin du récepteur Bob, ce dernier est perturbé car au même moment que le signal x_J est devenu plus fort, le signal x_S est devenue faible. Cette situation engendre l'augmentation du nombre de positions du relais pour lesquelles le taux d'erreur P_{e_B} est élevé, comme illustré à la figure 6.6a.

Pour l'espion, l'allure de variation de $E[P_{e_E}]$ est la même que celle décrite dans la figure 6.5b, sauf que maintenant, le maximum atteint par ce taux d'erreur pour les positions intermédiaires du relais est 0,26 puisque la puissance allouée au relais a augmenté alors qu'au même moment la puissance de la source a diminué.



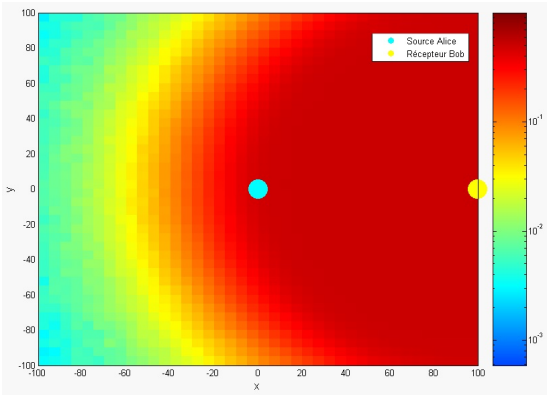
(a) P_{e_B} en fonction de la position du relais.



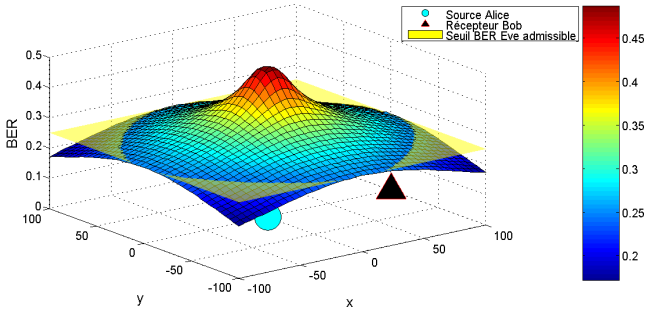
(b) $E(P_{e_E})$ en fonction de la position du relais.

FIGURE 6.6 – *Évaluation de P_{e_B} au récepteur Bob de coordonnées $(0°,100\ m)$ et $E[P_{e_E}]$ de l'espion pour chaque position possible du relais dans le réseau. $\delta = 0{,}4$: $P_S = 0{,}6 \cdot P_{TOT}$, $P_J = 0{,}4 \cdot P_{TOT}$.*

En continuant à augmenter le coefficient δ, davantage de puissance est allouée au relais et les taux d'erreurs P_{e_B} et E$[P_{e_E}]$ augmentent également, tel indiqué aux figures 6.7 et 6.8.

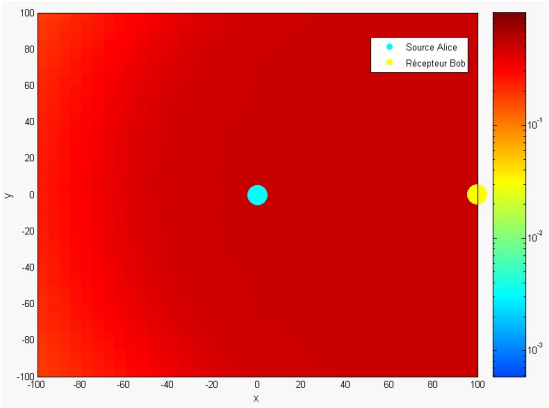


(a) P_{e_B} en fonction de la position du relais.

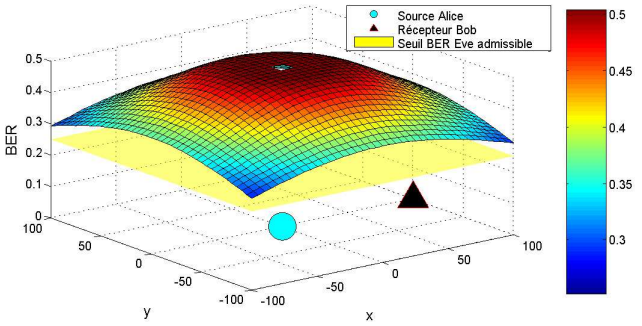


(b) $E(P_{e_E})$ en fonction de la position du relais.

FIGURE 6.7 – *Évaluation de P_{e_B} au récepteur Bob de coordonnées $(0°,100\ m)$ et E$[P_{e_E}]$ de l'espion pour chaque position possible du relais dans le réseau. δ = 0,6 : $P_S = 0{,}4 \cdot P_{TOT}$, $P_J = 0{,}6 \cdot P_{TOT}$.*



(a) P_{e_B} en fonction de la position du relais.



(b) $E(P_{e_E})$ en fonction de la position du relais.

FIGURE 6.8 – *Évaluation de P_{e_B} au récepteur Bob de coordonnées $(0°,100\ m)$ et E$[P_{e_E}]$ de l'espion pour chaque position possible du relais dans le réseau. δ = 0,8 : $P_S = 0{,}2 \cdot P_{TOT}$, $P_J = 0{,}8 \cdot P_{TOT}$.*

Ces évaluations des taux d'erreurs nous permettent d'extraire les positions du relais et les allocations de puissance qui offrent des valeurs du taux d'erreur de $P_{e_B} \leq 10^{-3}$ et de $E[P_{e_E}] \geq 2{,}5 \cdot 10^{-1}$.

Pour chacune des 756 positions possibles du relais dans la surface circulaires, on compte sous forme de pourcentage le nombre d'allocations de puissance pour lesquelles le taux d'erreur P_{e_B} est acceptable ainsi que les allocations de puissance pour lesquelles l'espérance du taux d'erreur $E[P_{e_E}]$ est acceptable. Ces pourcentages sont utilisés pour l'étape suivante.

6.4.1.3 Tableau synthèse des pourcentages des BER favorables des récepteurs

Comme cité précédemment, la coordonnée angulaire du relais varie de 180° jusqu'à $-170°$ avec un pas de variation de $-10°$ alors que la coordonnée radiale varie de 100 m à 0 m avec un pas de variation de 5 m, ce qui nous donne 756 positions possibles pour le relais dans la surface circulaire. Pour chacune de ces 756 positions, on compte sous forme de pourcentage le nombre des allocations de puissance qui satisfait aux conditions $P_{e_B} \leq 10^{-3}$ et de $E[P_{e_E}] \geq 2{,}5 \cdot 10^{-1}$.

On obtient donc une matrice **S** de 36 lignes et 21 colonnes correspondant au nombre de positions angulaires et de positions radiales que le relais peut prendre. On cherche ensuite dans cette matrice la plus grande valeur du pourcentage favorable du taux d'erreur P_{e_B}, on la note $(P_{e_B})_{max}$.

Éventuellement, d'autres éléments de la matrice **S** peuvent être égales à la valeur P_{e_B}, on la note $(P_{e_B})_{max}$, c'est pour cela qu'on cherche dans la matrice **S** s'il existe d'autres valeurs de P_{e_B} qui sont égales à $(P_{e_B})_{max}$ et on les sauvegarde dans la matrice **Z**. Cette dernière est constituée de deux lignes comme suit :

- Première ligne : contient toutes les valeurs du pourcentage favorable du P_{e_B} qui sont égales à $(P_{e_B})_{max}$.
- Deuxième ligne : contient le pourcentage favorable du taux d'erreur moyen de Eve $(Taux_E)$ correspondant à chaque valeur $(P_{e_B})_{max}$ qui est obtenus avec la même position du relais et la même allocation de puissance.

Évidemment, il y a une correspondance entre chaque valeur de la matrice **Z** et le couple "Position du relais-Allocation de puissance". Le but de la matrice **Z** est d'extraire la position du relais qui engendre les meilleurs résultats quant à la fiabilité de la liaison légitime et le taux de couverture sécuritaire.

Dans la simulation, les éléments de la matrice **Z** de dimensions $(2, 71)$ sont affichés dans le tableau 6.1.

Pour comprendre l'utilité des éléments de la matrice **Z** illustrés dans le tableau 6.1, on explique le cas du premier élément qui est le couple "81,81% - 9,09% ". Ce couple veut que pour la première position du relais qui est $(180°, 100\,\text{m})$, lorsqu'on applique 11 allocations de puissances différentes, alors 81,81% de ces allocations de puissances donnent des taux d'erreur P_{e_B} fiable au récepteur Bob et 9,09% de ces mêmes allocations donnent des taux d'erreurs moyens $E[P_{e_E}] \geq 2{,}5 \cdot 10^{-1}$.

Dans la deuxième ligne de la matrice **Z** on cherche la plus grande valeur de $E[P_{e_E}]$:

$$a = max\,[E[P_{e_E}]]\,. \tag{6.7}$$

Après la détermination des valeurs du vecteur $\mathbf{s} = [a \quad (P_{e_B})_{max}]$, on fait le lien avec la table des positions du relais pour localiser la position de ce dernier qui a engendré les éléments du vecteur **s**.

1 81,81% 9,09%	2 81,81% 9,09%	3 81,81% 18,18%	4 81,81% 18,18%	5 81,81% 18,18%	6 81,81% 18,18%	7 81,81% 18,18%	8 81,81% 9,09%	9 81,81% 9,09%
10 81,81% 18,18%	11 81,81% 18,18%	12 81,81% 18,18%	13 81,81% 18,18%	14 81,81% 9,09%	15 81,81% 9,09%	16 81,81% 18,18%	17 81,81% 18,18%	18 81,81% 18,18%
19 81,81% 18,18%	20 81,81% 9,09%	21 81,81% 9,09%	22 81,81% 18,18%	23 81,81% 18,18%	24 81,81% 18,18%	25 81,81% 18,18%	26 81,81% 9,09%	27 81,81% 9,09%
28 81,81% 18,18%	29 81,81% 18,18%	30 81,81% 18,18	31 81,81% 9,09%	32 81,81% 9,09%	33 81,81% 18,18%	34 81,81% 18,18%	35 81,81% 9,09%	36 81,81% 9,09%
37 81,81% 18,18%	38 81,81% 9,09%	39 81,81% 9,09%	40 81,81% 9,09%	41 81,81% 9,09%	42 81,81% 9,09%	43 81,81% 9,09%	44 81,81% 18,18	45 81,81% 9,09%
46 81,81% 9,09%	47 81,81% 18,18	48 81,81% 18,18%	49 81,81% 9,09%	50 81,81% 9,09%	51 81,81% 18,18%	52 81,81% 18,18%	53 81,81% 18,18	54 81,81% 9,09%
55 81,81% 9,09%	56 81,81% 18,18%	57 81,81% 18,18%	58 81,81% 18,18%	59 81,81% 18,18%	60 81,81% 9,09%	61 81,81% 9,09%	62 81,81% 18,18%	63 81,81% 18,18%
64 81,81% 18,18%	65 81,81% 18,18%	66 81,81% 9,09%	67 81,81% 9,09%	68 81,81% 18,18%	69 81,81% 18,18%	70 81,81% 18,18%	71 81,81% 18,18%	

TABLE 6.1 – *Éléments de la matrice* $\mathbf{Z}$*. La première ligne contient les valeurs maximums des pourcentages favorables de* P_{e_B}*.*

6.4.1.4 Déduction de la position idéale du relais brouilleur

Le vecteur **s** permet à l'algorithme de déduire la position du relais brouilleur qui offrent les résultats quant à la fiabilité et la sécurité du réseau lorsqu'on évalue les taux d'erreur P_{e_B} et $E[P_{e_E}]$ pour toutes les allocations de puissance possibles. La figure 6.9 illustre la position idéale du relais brouilleur.

Le relais se positionne aux coordonnées polaire $[180°, 90\text{ m}]$ lui permettant de brouiller la plus grande surface du réseau en garantissant une communication fiable entre la source Alice et le récepteur Bob.

6.4.2 Étape 2 : détermination de l'allocation de puissance adéquate

Dans la première étape de la simulation on a déterminé la position du relais qui offre les meilleurs résultats quant à la fiabilité de la liaison légitime et au taux de couverture sécuritaire.

Maintenant, on suppose le réseau circulaire avec la même disposition des terminaux légitimes étudié dans le chapitre 5 avec un relais Charlie $J^{(1)}$ placé aux coordonnées $[180°, 90\text{ m}]$. On veut déterminer l'allocation de puissance qui nous garantie le maximum de l'espérance du taux d'erreur $E[P_{e_E}]$.

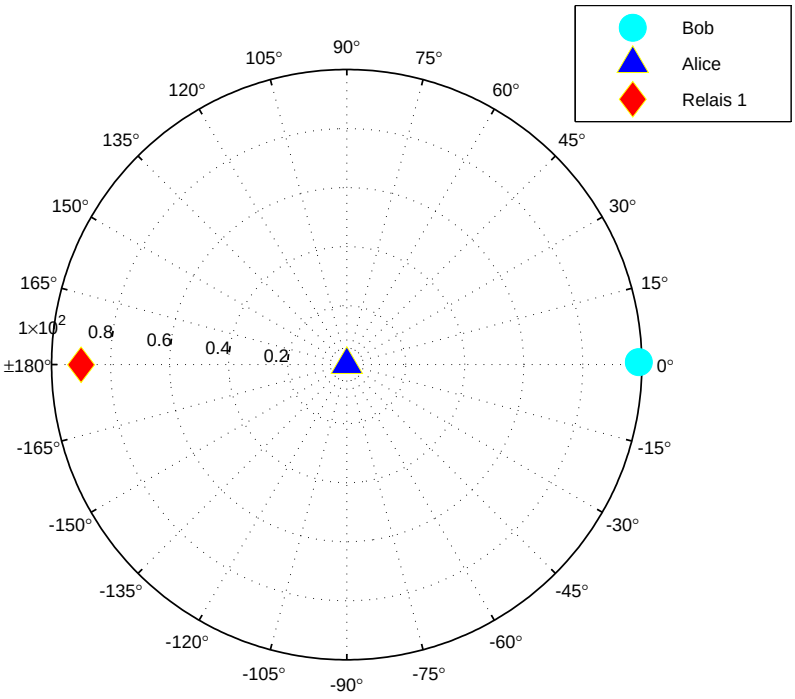


FIGURE 6.9 – *Position du relais brouilleur qui engendre les meilleurs résultats de fiabilité de liaison légitime et de taux de sécurité du réseau.*

Pour cela, la source omnidirectionnelle Alice émet à la puissance $P_S(g)$ variable dans le temps un signal binaire aléatoire de longueur $n = 50\,000$ bits modulé en BPSK au même instant que le relais émet à la puissance variable dans le temps $P_J(g)$ un signal binaire de brouillage modulé en BPSK également. L'objectif est d'évaluer pour chaque allocation de puissance les taux d'erreurs P_{e_B} et $E[P_{e_E}]$ où le pas de variation du coefficient de partage de puissance δ est $5 \cdot 10^{-3}$. Les signaux reçus au niveau de Bob et de Eve s'écrivent dans le temps comme suit :

$$y_B(g) = h_{SB} \cdot (1 - \delta(g)) \cdot P_{\text{TOT}} \cdot x_S + h_{JB} \cdot \delta(g) \cdot P_{\text{TOT}} \cdot x_J + \eta_B \tag{6.8}$$

$$y_E(g) = h_{SE} \cdot (1 - \delta(g)) \cdot P_{\text{TOT}} \cdot x_S + h_{JE} \cdot \delta(g) \cdot P_{\text{TOT}} \cdot x_J + \eta_E \tag{6.9}$$

Les évaluations des taux d'erreurs sont illustrés à la figure 6.10 pour 201 allocations de puissances différentes allant de celles favorisant la source à celles favorisant le relais.

On constate que pour les petites valeurs du coefficient δ, une grande partie de la puissance P_{TOT} est allouée à la source ce qui garantit une fiabilité de communication entre Alice et Bob. Même l'espion profite d'une réception fiable. Plus on augmente δ et plus le signal brouilleur devient perturbateur pour Bob et Eve jusqu'à ce que P_{e_B} dépasse le seuil autorisé pour ce dernier et la fiabilité est alors perdue. Donc la valeur adéquate de δ est le point d'intersection de la courbe de variation de P_{e_B} avec

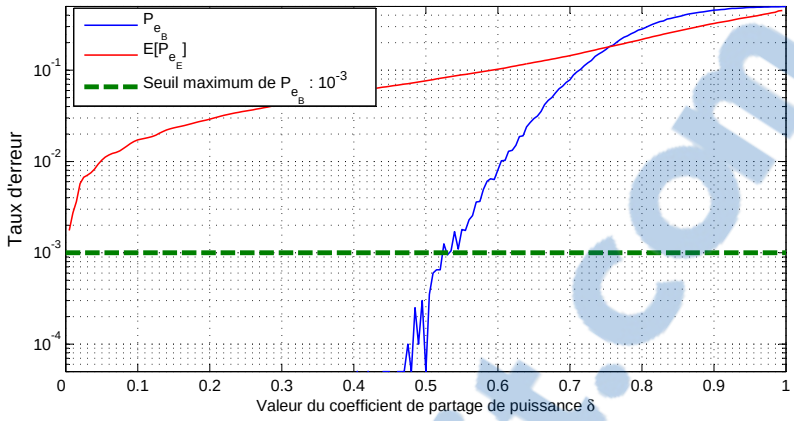


FIGURE 6.10 – *Évaluation des taux d'erreurs P_{e_B} et $E[P_{e_E}]$ en fonction de l'allocation de puissance entre la source et le relais.*

la droite du seuil 10^{-3}. La valeur adéquate de δ retournée par l'algorithme est $\delta = 0{,}53$ avec laquelle on obtient la plus grande valeur de $E[P_{e_E}]$ tout en garantissant la fiabilité de la liaison légitime.

L'évaluation du taux d'erreur de l'espion ainsi que les statistiques de sécurité obtenus avec $\delta = 0{,}53$ et la position idéale du relais sont présentés dans ce qui suit

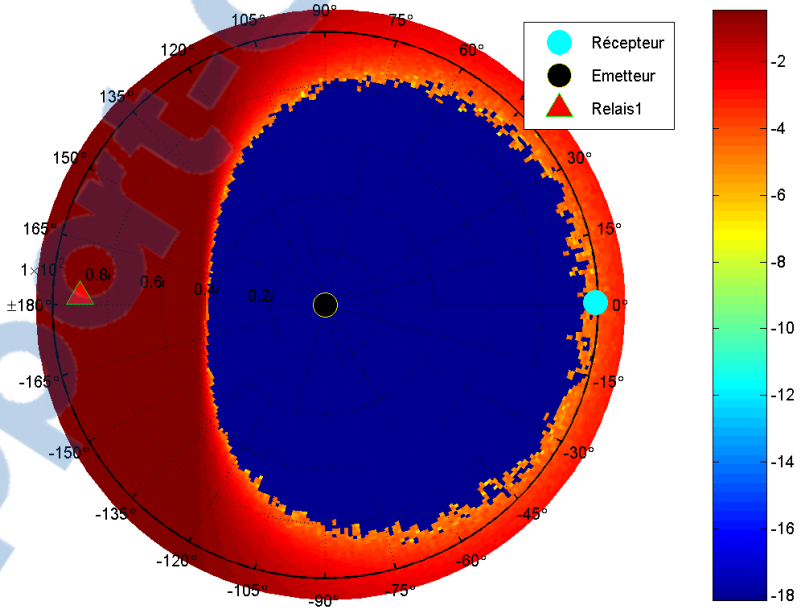


FIGURE 6.11 – *Variation de P_{e_E} en fonction de la position de l'espion dans la surface circulaire. $P_{e_B} = 8{,}5 \cdot 10^{-4}$.*

On constate que la puissance allouée au relais brouilleur lui permet de brouiller de façon considérable le réseau sans fil en particulier la région proche de lui où le taux d'erreur est de $\approx 0{,}5$. Plus on

s'éloigne du relais et plus le signal brouilleur perd de sa puissance sous l'effet de l'affaiblissement de propagation de coefficient $\alpha = 2$ dont les canaux du réseau sont soumis.

Au même instant, le signal de la source commence à augmenter mais le taux d'erreur demeure élevé avec une moyenne de 0,4 dans cette zone qui est considérée comme sécurisée car le taux d'erreur reste assez grand pour l'espion. La troisième zone est celle dans laquelle le taux d'erreur peut descendre jusqu'à 0,3. Cette zone est considérée comme la zone de transition entre la zone sécurisée et la zone moins sécurisée qui présente des éventuelles fuites d'informations vers l'espion. La quatrième zone est considérée comme le début de la zone non sécurisée ou faiblement sécurisée dans laquelle le taux d'erreur descend jusqu'à 0,1. Cela est non acceptable pour que le réseau soit sécurisée. Dans cette zone, le signal de brouillage devient davantage faible contrairement au signal de la source qui devient plus fort chaque fois qu'on se rapproche de cette source. La dernière zone est celle comprise entre la source et le récepteur légitime. Dans cette zone, la puissance du signal émis par la source est tellement fort que le signal de brouillage de faible puissance devient négligeable et a peu d'influence sur les terminaux présents dans cette zone et le taux d'erreur devient très faible, voir nulle. Cette zone couvre aussi l'emplacement du récepteur légitime et permet à ce dernier de bénéficier d'une communication fiable avec le taux d'erreur $P_{e_B} = 8{,}5 \cdot 10^{-4}$. Ce récepteur légitime se trouve à l'extrémité de la zone de fiabilité de communication, après quoi, le taux d'erreur augmente et dépasse la valeur seuil autorisée du taux d'erreur pour Bob.

Avec cette allocation de puissance, on obtient les statistiques de sécurité suivantes : 29,38% de la surface du réseau est fortement sécurisée, 2,1% de la surface du réseau est moyennement sécurisée et 68,52% est faiblement sécurisée et cette région constitue la région la plus vulnérable quant à termes de sécurité. L'espérance du taux d'erreur pour l'espion sur l'ensemble de la surface du réseau vaut $E[P_{e_E}] = 0{,}1486$.

Avec un pas de variation du coefficient de partage de puissance δ de l'ordre de 10^{-3} on a obtenu le taux d'erreur $P_{e_B} = 8{,}5 \cdot 10^{-4}$ donc très légèrement inférieur à la valeur seuil admissible. Cela veut dire qu'une quantité de puissance ε non nécessaire à la source lui est attribuée. On peut basculer cette quantité de puissance ε de la source vers le relais en respectant la contrainte de fiabilité et à condition que le récepteur légitime ne change pas de coordonnées.

La différence dans les statistiques de sécurité ne sont pas visibles, mais cela permet d'augmenter davantage la zone noyée dans le brouillage. La figure 6.12 montre la variation du taux d'erreur de l'espion en fonction de l'allocation de puissance ajustée.

L'allure du graphe est semblable à celui de la figure 6.11, mais le taux d'erreur au récepteur est passé de $P_{e_B} = 8{,}5 \cdot 10^{-4}$ à $P_{e_B} = 1{,}00 \cdot 10^{-3}$. Cela a permis une très légère attribution de puissance supplémentaire au relais. Il peut arriver que l'allocation de puissance ne peut être ajustable si le taux d'erreur du récepteur avant ajustement atteint déjà sa valeur seuil, soit 10^{-3}.

Quant aux statistiques de sécurité, la zone fortement sécurisée est passé de 29,38% à 29,41% en-

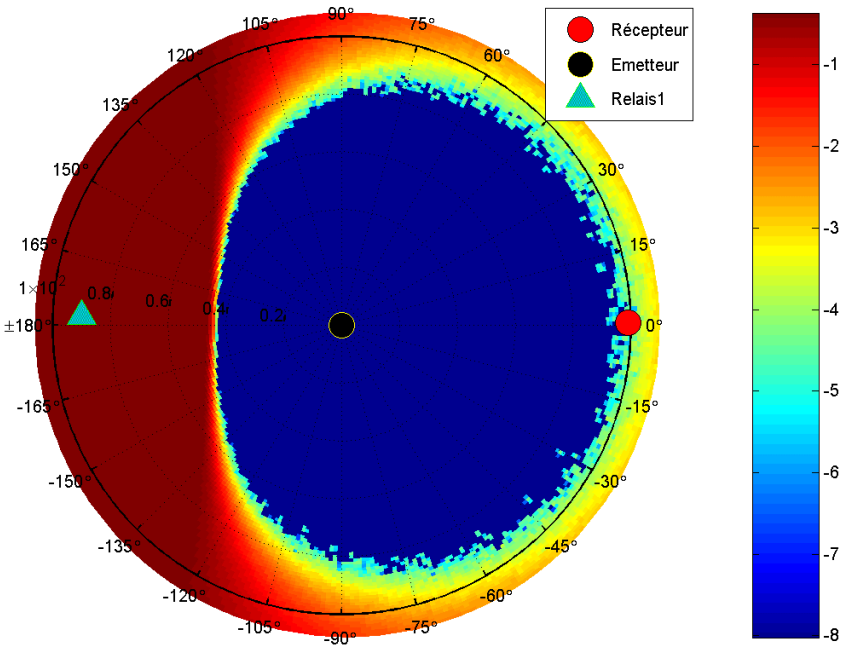


FIGURE 6.12 – *Variation de P_{e_E} en fonction de la position de l'espion dans la surface circulaire.* $P_{e_B} = 1{,}00 \cdot 10^{-3}$.

gendrant une baisse de la zone moyennement sécurisée de 2,1% à 2,08% et de la zone faiblement sécurisée de 68,52% à 68,51% alors que l'espérance du taux d'erreur pour l'espion sur l'ensemble de la surface du réseau vaut $E[P_{e_E}] = 0{,}1490$.

6.4.2.1 Statistiques de sécurité et de partage de puissance

La figure 6.13 montre les statistiques obtenues avant et après l'ajustement de l'allocation de puissance. A la fin du processus, l'algorithme attribue les puissances entre la source et le relais, ainsi que les statistiques de fiabilité et de sécurité, comme suit : 47,995% est allouée à la source Alice, lui permettant d'assurer une communication fiable avec le récepteur Bob qui se trouve à 100 m d'elle. 52,005% de la puissance est allouée au relais lui permettant de brouiller la surface du réseau où :

1. 29,41% de la surface du réseau est sécurisée par un taux d'erreur très élevé, d'au moins $2{,}5 \cdot 10^{-1}$,
2. 2,08% de la surface est sécurisée par un taux d'erreur d'intensité moyenne, compris entre $1{,}5 \cdot 10^{-1}$ et $2{,}5 \cdot 10^{-1}$
3. 68,51% de la surface est sécurisée par un taux faible, inférieur à $1{,}5 \cdot 10^{-1}$

On peut conclure que les pourcentages 29,41%, 2,08%, 68,51%, de surface de réseau, représentent respectivement, la zone fortement sécurisée, la zone moyennement sécurisée et la zone non sécurisée ou faiblement sécurisée.

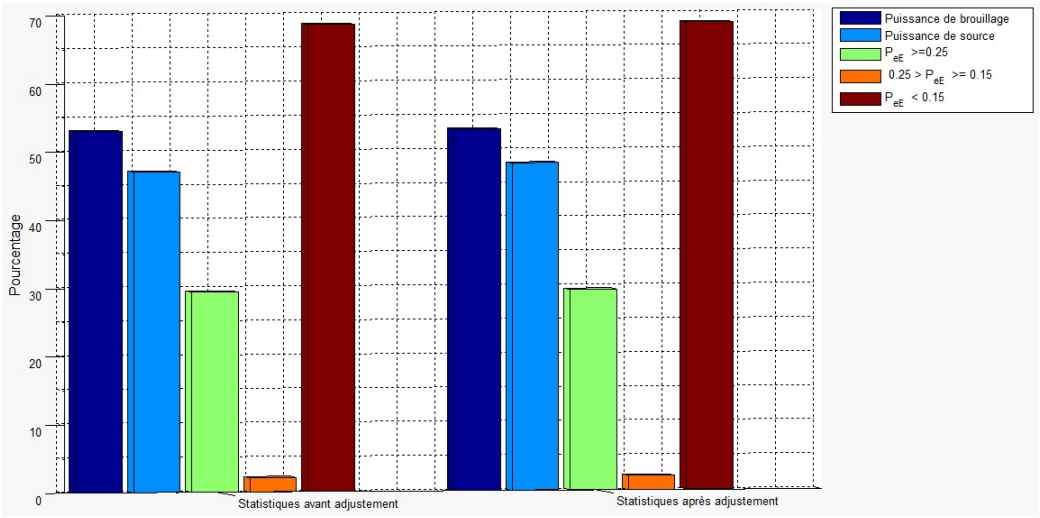


FIGURE 6.13 – *Statistiques de sécurité et de partage de puissance avant et après l'ajustement de l'allocation de puissance entre la source et le relais.*

6.4.3 Étape 3 : Amélioration du brouillage par l'ajout de relais

Après avoir évalué le brouillage coopératif pour la sécurité d'une surface circulaire avec un seul relais, on considère maintenant le réseau illustré à la figure 6.14.

L'objectif maintenant est d'améliorer les résultats de fiabilité et de sécurité obtenus avec un relais unique où $E[P_{e_E}] = 0{,}1490$ seulement. Pour cela, on ajoute deux relais supplémentaires $J^{(2)}$ et $J^{(3)}$ à ce réseau et on cherche à les placer dans la surface du réseau de tel sorte à avoir la plus grande surface possible du réseau noyée dans le brouillage et obtenir des statistiques de sécurité meilleurs que celle obtenus avec un seul relais. L'algorithme présenté à la figure 6.15 résume les principales étapes pour arriver à cet objectif.

Dans ce cas, on a trois signaux de brouillage, $x_J^{(1)}$, $x_J^{(2)}$, $x_J^{(3)}$, générés respectivement par les relais omnidirectionnelles $J^{(1)}$, $J^{(2)}$ et $J^{(3)}$ en plus du signal x_S généré par la source omnidirectionnelle.

La même puissance P_{TOT} = 20 dBm est allouée au système pour pouvoir comparer les résultats obtenus précédemment. Le bruit reçu par le récepteur et l'espion a une puissance P_η = -80 dBm [5].

La simulation consiste à émettre par la source un signal binaire x_S de longueur n = 20 000 bits à la puissance P_S au même instant que chaque relais émet un signal brouilleur binaire de même longueur à la puissance $P_J^{(i)}, i = 1,2,3$ pour brouiller l'espion. Les signaux reçus au récepteur légitime et à l'espion sont :

$$\begin{aligned} y_B &= h_{SB} \cdot P_S \cdot x_S + \sum_{i=1}^{3} \left(h_{J^{(i)}B} \cdot P_{J^{(i)}} \cdot x_{J^{(i)}} \right) + \eta_B \\ y_E &= h_{SE} \cdot P_S \cdot x_S + \sum_{i=1}^{3} \left(h_{J^{(i)}E} \cdot P_{J^{(i)}} \cdot x_{J^{(i)}} \right) + \eta_E \end{aligned} \tag{6.10}$$

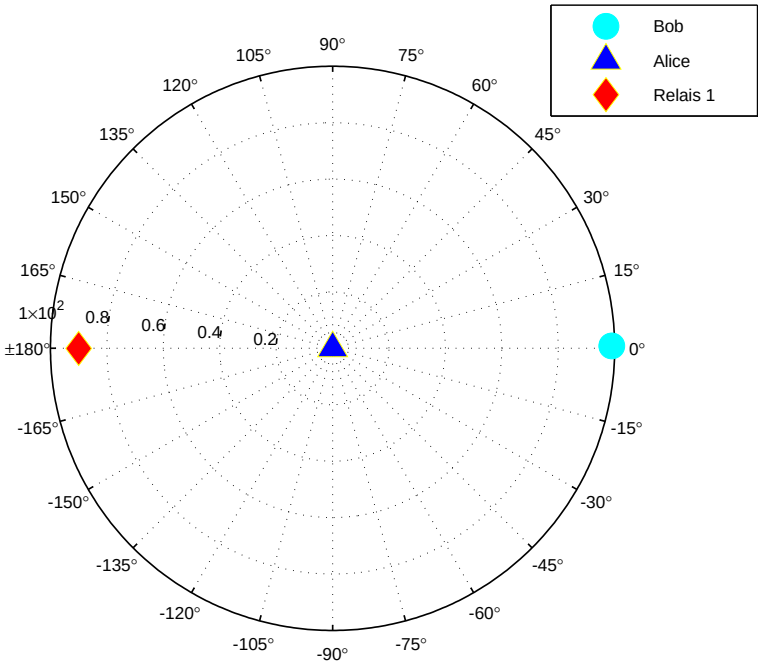


FIGURE 6.14 – *Réseau circulaire composé de la source Alice, du récepteur Bob et du relais brouilleur Charlie. $r = 100$ m.*

A la réception, on évalue le taux d'erreur en comparant les signaux y_B et y_E avec le signal x_S tel que expliqué au point 2.4.5 lorsque les relais $J^{(2)}$ et $J^{(3)}$ parcours toute la surface du réseau circulaire. La procédure de déplacement de ces deux relais est expliquée dans ce qui suit.

6.4.3.1 Déplacement des relais $J^{(2)}$ et $J^{(3)}$

À la figure 6.16, on montre la procédure de déplacement des relais $J^{(2)}$ et $J^{(3)}$. Au début, ces relais se positionnent aux coordonnées polaires $(180°,100\text{ m})$. A partir de ce point les deux relais se déplacent par le changement de leur coordonnée radiale avec un pas de déplacement de $d = 5$ m jusqu'à ce qu'ils arrivent au point central du réseau de coordonnées $(180°,0\text{ m})$.

Après cela, Les relais reviennent à la coordonnée radiale $\rho = 100$ m et on décrémente la coordonnée angulaire du relais $J^{(2)}$ de $10°$ et on incrémente celle du relais $J^{(3)}$ de $10°$. On déplace ensuite les relais radialement comme avant sans changer leur angle jusqu'à ce qu'ils arrivent au point central de nouveau.

On continue de déplacer les deux relais radialement avec changement de leur coordonnée angulaire d'une façon opposée jusqu'à ce que les relais arrivent aux coordonnées $(0°,0\text{ m})$. Les deux relais se sont positionnées chacun dans 209 emplacements différents permettant de couvrir l'ensemble de la surface circulaire.

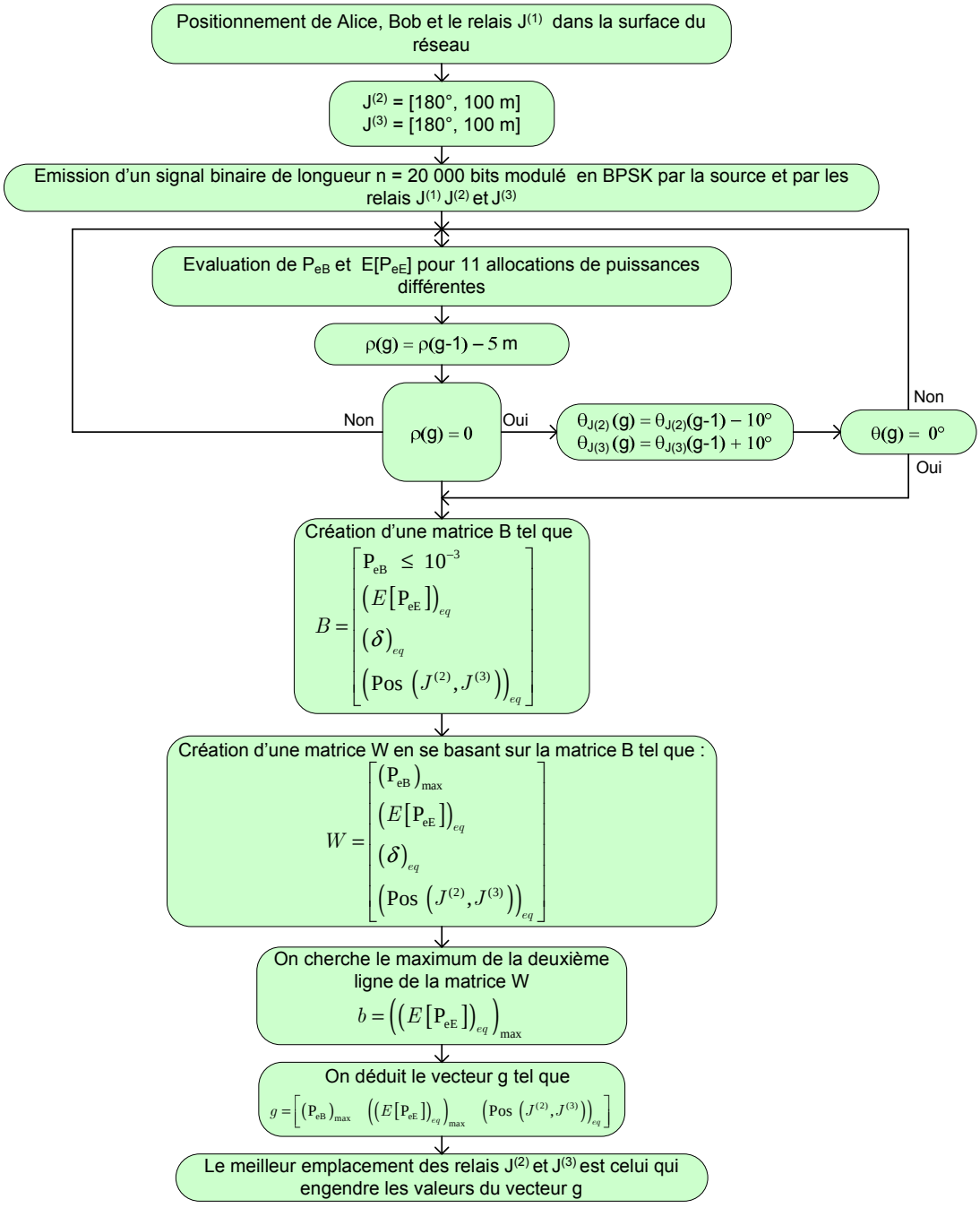


FIGURE 6.15 – *Algorithme de recherche du meilleur emplacement des relais $J^{(2)}$ et $J^{(3)}$.*

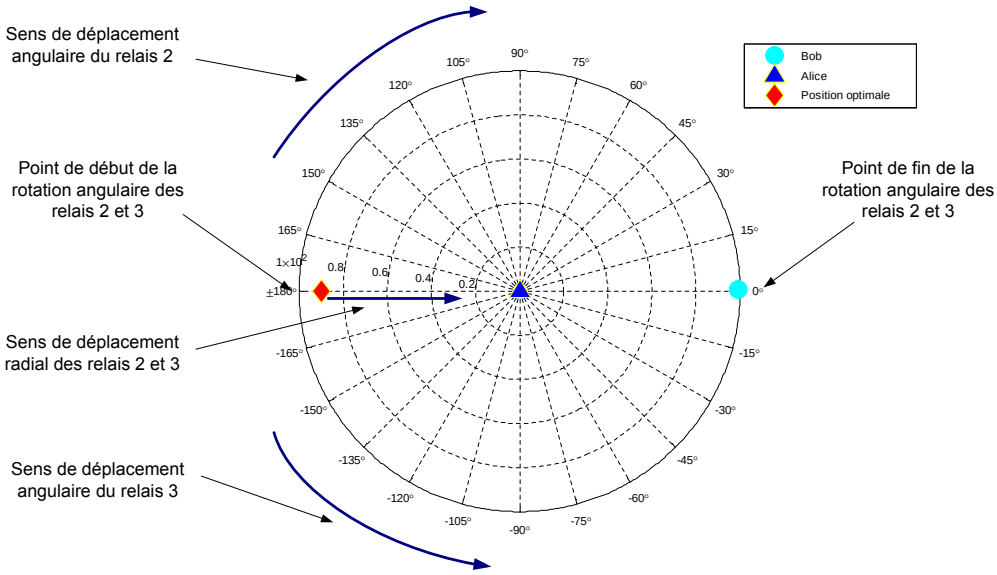


FIGURE 6.16 – *Procédure de déplacement des relais $J^{(2)}$ et $J^{(3)}$ dans le réseau circulaire.*

6.4.3.2 Évaluation du taux d'erreur des récepteurs

Pour chacune des 209 emplacements des relais, on exécute la simulation citée au point 6.4.3 pour 11 allocations de puissance différentes comme expliqué au point 6.4.1.2. Chaque allocation de puissance est telle que :

$$P_S(g) = ((1-\delta(g)) \cdot P_{TOT} \tag{6.11}$$

$$P_J(g)^{(i)} = (\delta(g) \cdot P_{TOT})/3 \tag{6.12}$$

où $\delta(g)$ est le coefficient de partage de puissance au temps discret g avec $g \in [0, 11]$ et $\delta \in [0, 1]$

En considérant (6.11) et (6.12), les équations dans (6.10) s'écrivent alors comme suit :

$$\begin{aligned} y_B &= h_{SB} \cdot ((1-\delta(g)) \cdot P_{TOT}) \cdot x_S + \sum_{i=1}^{3} (h_{J^{(i)}B} \cdot ((\delta(g) \cdot P_{TOT})/3) \cdot x_{J^{(i)}}) + \eta_B \\ y_E &= h_{SE} \cdot ((1-\delta(g)) \cdot P_{TOT}) \cdot x_S + \sum_{i=1}^{3} (h_{J^{(i)}E} \cdot ((\delta(g) \cdot P_{TOT})/3) \cdot x_{J^{(i)}}) + \eta_E \end{aligned} \tag{6.13}$$

Au total, $209 \cdot 11 = 2299$ évaluations différentes des taux d'erreur P_{e_B} et $E[P_{e_E}]$ simultanément couvrant toute la surface du réseau. Les résultats de ces évaluations sont illustrés aux figures 6.17 et 6.18.

On constate dans 6.17 que la variation du P_{e_B} dépend de la position des relais brouilleurs $J^{(2)}$ et $J^{(3)}$ et de l'allocation de puissance appliquée. On peut regrouper les résultats en deux sous groupes :

- Les taux d'erreurs admissibles : pour lesquels $P_{e_B} \leq 10^{-3}$ et constituent une minorité par rapport à l'ensemble des BER calculés.
- Les taux d'erreurs non admissibles : pour lesquels $P_{e_B} > 10^{-3}$ et constituent une majorité par rapport à l'ensemble des BER calculés.

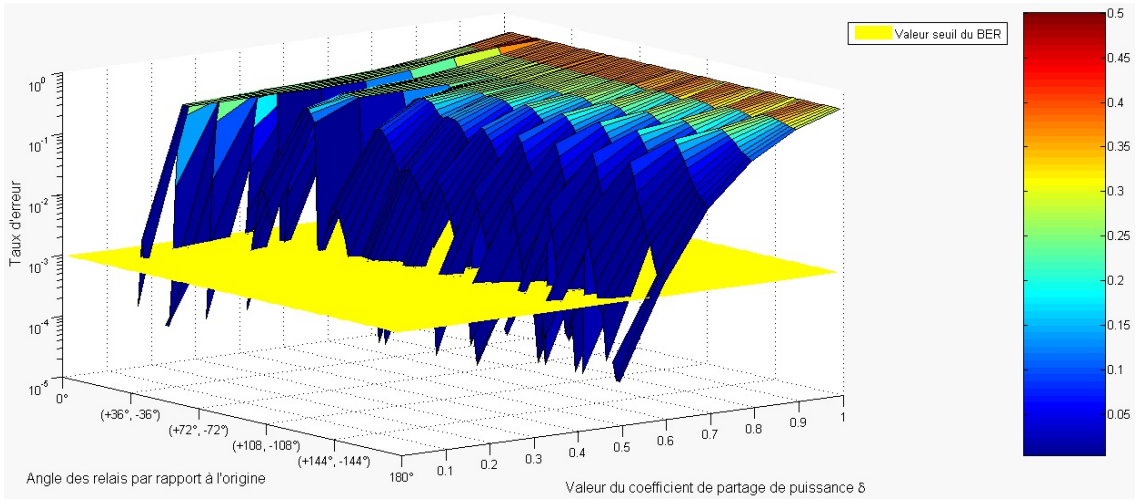


FIGURE 6.17 – *Variation du taux d'erreur P_{e_B} au récepteur en fonction de la position des trois relais et de l'allocation de puissance.*

Selon la procédure de déplacement des relais $J^{(2)}$ et $J^{(3)}$ expliquée dans 6.16, ces relais se rapprochent davantage du récepteur à chaque incrémentation de leur position. Lorsque l'angle entre les relais $J^{(2)}$ et $J^{(3)}$ et l'origine est supérieur à 72°, ces derniers sont relativement loin du récepteur et donc de la première allocation de puissance ($P_S = 100\%P_{TOT}$) jusqu'à la septième allocation ($P_S = 30\%P_{TOT}$) on a P_{e_B} très petit. A la huitième allocation la valeur de P_{e_B} dépend de la position des relais. Ainsi, si ces derniers sont éloignés de Bob alors P_{e_B} est très faible. S'ils sont proche de Bob alors P_{e_B} est grand et n'est plus acceptable. À partir de la neuvième allocation P_{e_B} commence à augmenter quelle que soit la coordonnée radiale des relais $J^{(2)}$ et $J^{(3)}$ car la puissance d'émission de la source est faible par rapport à la puissance des signaux de brouillage même si les relais sont éloignés du récepteur. Ainsi, P_{e_B} dépasse beaucoup la valeur seuil jusqu'à atteindre la valeur 0,5 à la dernière allocation qui favorise le brouillage sur l'émission.

Lorsque l'angle entre les relais $J^{(2)}$ et $J^{(3)}$ et l'origine est inférieur à 72° on constate que les taux d'erreurs P_{e_B} admissibles commencent à diminuer graduellement même si des allocations de puissance favorisant la source sont appliquées.

Lorsque l'angle entre les relais $J^{(2)}$ et $J^{(3)}$ et l'origine est inférieur à 36° le taux d'erreur P_{e_B} devient non admissible après la troisième allocation malgré que cette dernière attribue à la source 80% de la puissance du système.

À la figure 6.18, on évalue le taux d'erreur moyen de l'espion $\mathrm{E}[P_{e_E}]$ sur toute la surface du réseau en fonction de la position des relais $J^{(2)}$ et $J^{(3)}$ et en fonction de l'allocation de puissance entre l'émission et le brouillage.

On constate que le taux d'erreur moyen $E[P_{e_E}]$ dépend de la position des relais et de l'allocation de puissance. A chaque incrémentation de l'allocation de puissance la puissance dédiée au brouillage

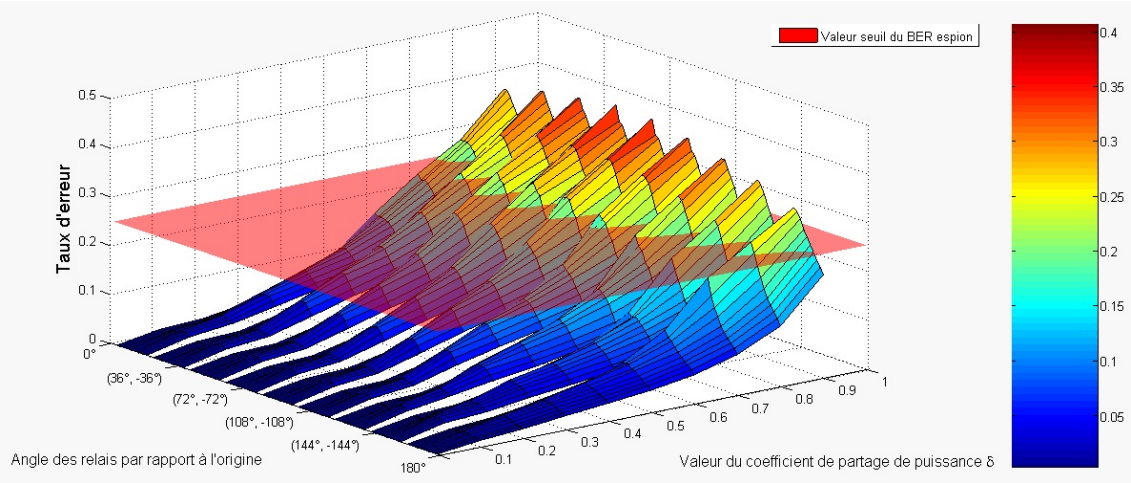


FIGURE 6.18 – *Variation du $E[P_{e_E}]$ en fonction de la position des relais et de l'allocation de puissance.*

augmente et engendre l'augmentation du taux d'erreur moyen de l'espion. On constate aussi que pour une coordonnée radiale donnée pour les relais $J^{(2)}$ et $J^{(3)}$, le taux d'erreur moyen de l'espion reste le même indépendamment de la coordonnée angulaire de ces relais. En combinant les résultats illustrés aux figures 6.17 et 6.18, on peut trouver les positions des relais $J^{(2)}$ et $J^{(3)}$ qui offrent les meilleures résultats quant à termes de fiabilité et de sécurité.

6.4.3.3 Sélection des P_e favorables des récepteurs

En se basant sur les résultats de l'évaluation de P_{e_B} et $E[P_{e_E}]$ de la phase précédente, on crée une matrice **B** de trois lignes comme suit :

- La première ligne contient toutes les valeurs $P_{e_B} \leq 10^{-3}$.
- La deuxième ligne contient les $E[P_{e_E}]$ obtenus conjointement avec chaque valeur de $P_{e_B} \leq 10^{-3}$.
- La troisième ligne contient la position des relais $J^{(2)}$ et $J^{(3)}$ correspondante aux valeurs de chaque couple $(P_{e_B},\ E[P_{e_E}])$ de la première et la deuxième ligne de la matrice **B**.

Dans la simulation, la matrice **B** est de dimensions (3,94), soit 94 valeurs du P_{e_B} qui sont admissibles mais chacune de ces 94 valeurs a une valeur de $E[P_{e_E}]$ différente.

On cherche dans la matrice **B** la première plus grande valeur de P_{e_B} et on la note $(P_{e_B})_{max}$. Après quoi, on cherche dans la matrice **B** s'il y a d'autres valeurs de P_{e_B} qui sont égales à cette valeur $(P_{e_B})_{max}$. On crée une matrice **W** de trois lignes comme suit :

- première ligne : toutes les valeurs $(P_{e_B})_{max}$ trouvés dans la matrice **B**.
- deuxième ligne : $\mathrm{E}[P_{e_E}]$ obtenue conjointement avec chaque valeur $(P_{e_B})_{max}$.
- troisième ligne : la position des relais $J^{(2)}$ et $J^{(3)}$ correspondante à chaque couple de valeurs $((P_{e_B})_{max}, \mathrm{E}[P_{e_E}])$.

La matrice **W** nous garantit que P_{e_B} est la plus grande valeur admissible. Cela nous permet d'économiser sur la puissance à fournir à la source et basculer la plus grande quantité de puissance possible aux relais brouilleurs. Dans la deuxième ligne de **W** on cherche la plus grande valeur de $\mathrm{E}[P_{e_E}]$ et on la note $(\mathrm{E}[P_{e_E}])_{max}$.

On obtient finalement un vecteur **g** comme suit :

$$\mathbf{g} = [(P_{e_B})_{max},\ \ (\mathrm{E}[P_{e_E}])_{max},\ \ POS_{eq}]\,. \tag{6.14}$$

où POS_{eq} est la position des relais $J^{(2)}$ et $J^{(3)}$ qui garantit le maximum de $(P_{e_B})_{max}$ et $(\mathrm{E}[P_{e_E}])_{max}$. Dans la simulation le vecteur **g** est comme suit :

Désignation	$(P_{e_B})_{max}$	$(\mathrm{E}[P_{e_E}])_{max}$	POS_{eq}
Valeur	$8{,}5 \cdot 10^{-4}$	$1{,}875 \cdot 10^{-1}$	$(\pm 90°, 50\mathrm{m})$

TABLE 6.2 – Valeurs des éléments du vecteur **g**.

6.4.3.4 Déduction du meilleur emplacement des relais $J^{(2)}$ et $J^{(3)}$

Le vecteur **g** permet à l'algorithme de déduire la meilleure position des relais brouilleurs qui engendrent les meilleurs résultats quant à termes de fiabilité de la liaison légitime et du taux de couverture sécuritaire comme illustré à la figure 6.19.

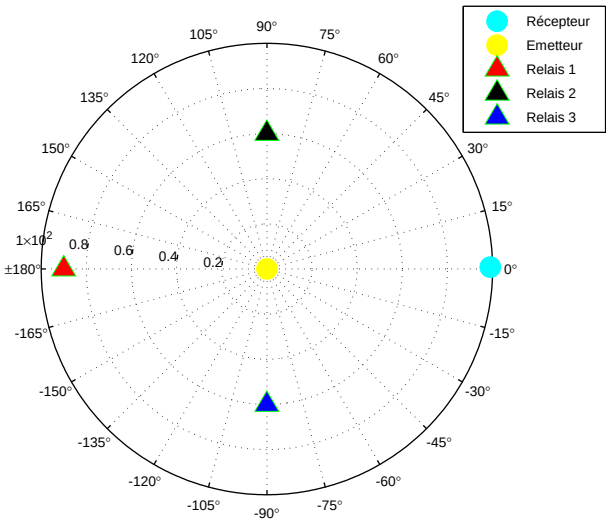


FIGURE 6.19 – *Emplacement des relais brouilleurs qui engendre les meilleures valeurs du* $E(P_{e_E})$ *et* P_{e_B}.

Les relais se positionnent aux coordonnées polaires $[\pm 90°, 50\,\mathrm{m}]$. Ces positions permet à l'ensemble des relais de brouiller de la meilleure façon.

6.4.4 Étape 4 : recherche de l'allocation de puissance qui maximise le brouillage coopératif

Dans l'étape précédente on a pu déterminer le meilleur emplacement des relais $J^{(2)}$ et $J^{(3)}$ qui engendrent le maximum de l'espérance du taux d'erreur $E[P_{e_E}]$ de l'espion tout en garantissant une fiabilité de la liaison légitime.

Maintenant, on suppose le réseau circulaire avec la même disposition des terminaux légitimes illustré dans la figure 6.19. On veut déterminer l'allocation de puissance qui garantie le maximum de l'espérance du taux d'erreur $E[P_{e_E}]$ en garantissant la fiabilité de la liaison entre la source et Bob.

Pour cela, la source omnidirectionnelle Alice émet à la puissance $P_S(g)$ variable dans le temps un signal binaire aléatoire de longueur $n = 50\,000$ bits modulé en BPSK au même instant que chaque relais émet à la puissance variable dans le temps $P_J^{(i)}(g)$ un signal binaire de brouillage de même longueur et modulé en BPSK également.

L'objectif est d'évaluer pour chaque allocation de puissance les taux d'erreurs P_{e_B} et $E[P_{e_E}]$ où le pas de variation du coefficient de partage de puissance δ est $5 \cdot 10^{-3}$. Les signaux reçus au niveau de Bob et de Eve s'écrivent comme suit :

$$\begin{aligned} y_B &= h_{SB} \cdot ((1-\delta(g)) \cdot P_{TOT}) \cdot x_S + \sum_{i=1}^{3} (h_{J^{(i)}B} \cdot ((\delta(g) \cdot P_{TOT})/3) \cdot x_{J^{(i)}}) + \eta_B \\ y_E &= h_{SE} \cdot ((1-\delta(g)) \cdot P_{TOT}) \cdot x_S + \sum_{i=1}^{3} (h_{J^{(i)}E} \cdot ((\delta(g) \cdot P_{TOT})/3) \cdot x_{J^{(i)}}) + \eta_E \end{aligned} \tag{6.15}$$

Au total, 201 évaluations des taux d'erreurs P_{e_B} et $E[P_{e_E}]$ correspondantes aux nombres d'allocations de puissances.De même que pour le cas d'un réseau à relais brouilleur unique, on constate que pour les petites valeurs du coefficient δ, une grande partie de la puissance P_{TOT} est allouée à la source ce qui garantie une fiabilité entre Alice et Bob. Avec l'augmentation du coefficient δ la réception de Bob commence à être perturbé à cause de l'influence du signal brouilleur au même instant que le signal de la source s'affaiblit. Le taux d'erreur P_{e_B} dépasse le seuil autorisé lorsque $\delta = 46{,}5$ où la fiabilité est alors perdue. Avec cette allocation de puissance, on évalue le taux d'erreur au niveau de l'espion sur toute la surface du réseau ainsi que le taux d'erreur au niveau du récepteur légitime. Les résultats sont illustrés à la figure 6.20.

Avec l'ajout de deux relais supplémentaires une plus grande surface du réseau est brouillée où chaque relais brouille la région proche de lui où le taux d'erreur est de $\approx 0{,}5$. Plus on s'éloigne des trois relais et plus le signal brouilleur perd de sa puissance sous l'effet de l'affaiblissement par propagation de coefficient $\alpha = 2$ dont les canaux du réseau sont soumis. Au même temps, la puissance allouée à la source lui permet d'acheminer son signal x_S au récepteur Bob avec fiabilité où le taux d'erreur $P_{e_B} = 1{,}00 \cdot 10^{-3}$. La zone non fiable a largement diminuée ce qui améliore le taux de couverture sécuritaire.

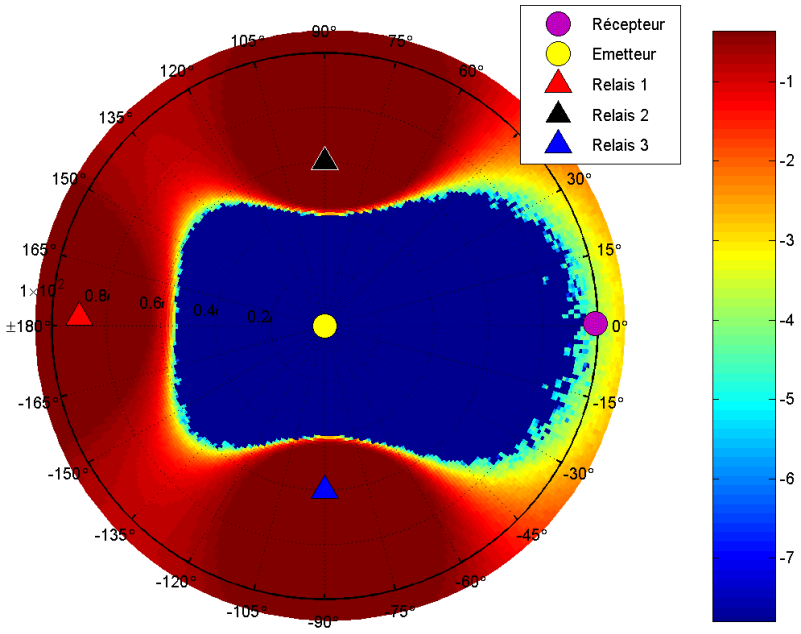


FIGURE 6.20 – *Variation de P_{e_E} en fonction de la position de l'espion dans la surface circulaire.* $P_{e_B} = 1{,}00 \cdot 10^{-3}$.

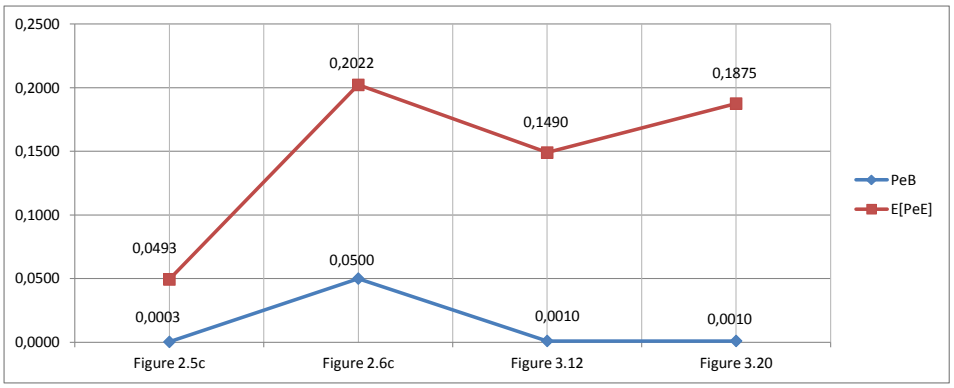
Avec cette nouvelle disposition à 3 relais, on obtient les statistiques de sécurité suivantes : 34,91% de la surface du réseau est fortement sécurisée, 17,59% de la surface du réseau est moyennement sécurisée et 47,50% est faiblement sécurisée et cette région constitue la région la plus vulnérable quant à termes de sécurité. L'espérance du taux d'erreur pour l'espion sur l'ensemble de la surface du réseau a pour sa part augmenté à $E[P_{e_E}] = 0{,}1875$. On remarque que le taux d'erreur au niveau de Bob est déjà à valeur maximale donc on peut pas faire un ajustement supplémentaire de l'allocation de puissance.

6.4.5 Achèvement de l'algorithme et statistiques de sécurité et de partage de puissance

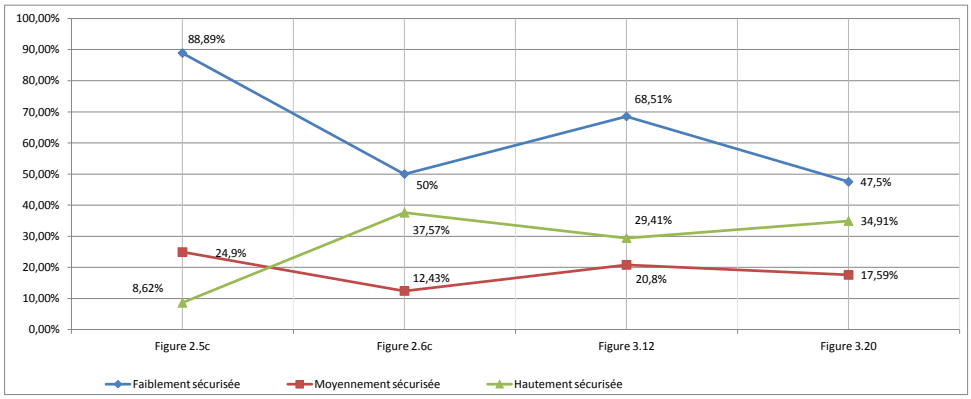
La figure 6.21 montre une comparaison des statistiques de sécurité et de fiabilité obtenus avec les configurations de réseau étudiés dans 5.5c, 5.6c, 6.12 et 6.20. Cette figure illustre les différents résultats obtenus quant à termes de fiabilité et de sécurité du réseau. Les résultats diffèrent selon le nombre et la disposition des relais ainsi que l'allocation de puissance appliquée.

Pour la figure 5.5c où l'allocation de puissance manuelle favorise la source, la réception au niveau de Bob est excellente mais 88,89% de la surface du réseau est vulnérable aux actes d'espionnage à cause de la puissance élevé du signal x_S de la source par rapport à la faiblesse du signal brouilleur. Le taux d'erreur au niveau de Bob est $P_{e_B} = 2{,}5 \cdot 10^{-4}$.

Pour la figure 5.6c le partage manuel équitable de la puissance P_{TOT} a engendrer l'amélioration de la



(a) Statistiques de fiabilité pour chaque configuration



(b) Statistiques de couverture sécuritaire pour chaque configuration.

FIGURE 6.21 – *Comparaison des statistiques de fiabilité des liaisons légitimes et de couvertures sécuritaire pour les configurations de réseau étudiés dans 5.5c, 5.6c, 6.12 et 6.20. Alice* $(0\ m, 0°)$, *Bob* $(100\ m, 0°)$. $P_{TOT} = 20\ dBm$, $P_{\eta} = -80\ dBm$.

couverture sécuritaire et l'augmentation brusque de l'espérance du taux d'erreur de l'espion $E[P_{e_E}]$ de 0,0493 à 0,2022 mais la fiabilité de la liaison légitime entre la source et le récepteur légitime est perdue car $P_{e_E} = 5 \cdot 10^{-2}$. Donc on a améliorer la couverture sécuritaire sans conserver la fiabilité.

Pour la figure 6.12 le partage de la puissance P_{TOT} entre la source et le relais unique $J^{(1)}$ s'est fait d'une façon automatique c'est à dire qu'on a attribué à la source exactement la puissance nécessaire et suffisante pour garantir une liaison fiable avec Bob et le reste de la puissance est attribué au relais pour brouiller le maximum du réseau. Ainsi, l'espérance du taux d'erreur $E[P_{e_E}]$ n'a diminué qu'à 0,1490.

Enfin, pour la figure 6.20 où le réseau dispose de 3 relais $J^{(1)}$ et $J^{(2)}$ et $J^{(3)}$, le partage de la puissance P_{TOT} s'est également fait d'une façon automatique. Dans ce cas, au même moment que la liaison légitime est maintenue fiable, les statistiques de sécurité se sont améliorés où la zone vulnérable à l'espionnage à passé de 68,51% à seulement 47,5% et l'augmentation de la région hautement sécurisée de 29,41% à 34,91%

6.5 Conclusion

Dans ce chapitre on a proposé une méthode d'amélioration du brouillage coopératif en se basant sur les résultats des travaux présentés par Dong et al. dans [5] et les analyses des configurations de réseaux étudiés dans les chapitres précédents.

À cet effet, on a rappelé à la section 6.2 les principaux travaux qui ont menés à la mise en place du concept de brouillage coopératif pour le renforcement et l'amélioration de la sécurité à la couche physique des réseaux sans fil soumis à l'écoute clandestine. À la section 6.3, on a expliqué les résultats des travaux présentés par Dong et al. [5] où on a conclu que l'efficacité du brouillage coopératif est en lien direct avec l'emplacement des N_J relais brouilleur par rapport à l'espion et au récepteur légitime ainsi que l'allocation de puissance entre l'émission et le brouillage.

À la section 6.4, on a analysé les résultats obtenus de l'exécution de l'algorithme automatisé qui cherche le meilleur emplacement du relais unique pour améliorer le brouillage coopératif pour la sécurité d'une surface circulaire composée d'une source, d'un récepteur légitime, d'un relais brouilleur $J^{(1)}$ et d'un espion mobile qui peut se déplacer sur toute la surface du réseau. La fuite d'informations non désirée est due au fait que la région où se trouve le récepteur légitime ne doit pas être brouillée et constitue ainsi une vulnérabilité quant à terme de sécurité. Cet algorithme cherche aussi la meilleure allocation de puissance qui maximise le brouillage coopératif. À la sous-section 6.4.3, on a analysé les résultats obtenus de l'exécution de l'algorithme qui cherche le meilleur emplacement de 2 relais dans un réseau circulaire à relais unique. Dans ce cas, les résultats obtenus avec cette nouvelle configuration du réseau en termes de brouillage du réseau sont nettement supérieurs à ceux obtenus avec un relais unique en conservant la fiabilité de la liaison légitime.

Si P_{e_B} est inférieur à la valeur seuil, il est possible de ré-allouer l'excès de puissance de la source vers les relais pour maximiser les statistiques de sécurité sans nuire à la fiabilité de la liaison légitime.

Chapitre 7

Conclusion

7.1 Rappel du contexte

Dans ce mémoire de maîtrise, nous avons étudié des stratégies de brouillage coopératif pour garantir un taux de sécurité acceptable dans les réseaux sans fil, tout en assurant une liaison fiable entre la source et le récepteur légitime. Ce concept de brouillage coopératif repose sur la collaboration entre les utilisateurs légitimes du réseau pour brouiller au maximum, le ou les espions présents dans le réseau, en exploitant les propriétés physiques des canaux de communications. Alors que la source transmet le signal d'information, un ou plusieurs relais émettent un signal de brouillage de telle sorte qu'il confonde les espions présents dans le réseau sans dégrader la liaison avec le récepteur légitime. La connaissance des statistiques du réseau, à savoir principalement l'état du canal principal et du canal de l'espion, est un point clé pour assurer l'applicabilité et l'efficacité de ce concept.

7.2 Synthèse du mémoire

Au chapitre 2, on a rappelé les principales notions de base, sur lesquelles est fondé le concept de brouillage coopératif, en particulier le modèle de canal sous écoute de Shannon ainsi que le modèle de Wyner, et comment une communication est sécurisée dans un canal bruité, soumis à l'écoute. Au chapitre 3, on a démontré qu'en ayant recours au brouillage coopératif, on peut sécuriser une communication entre deux entités communicantes légitimes dans un réseau sans fil ouvert en présence d'un ou plusieurs espions, sans avoir recours nécessairement à une clé privée de chiffrement partagée entre eux, et garantir ainsi un débit secret garantissant une communication sécurisée, sous certaines conditions. Au chapitre 4, on a étudié l'effet de brouillage coopératif dans les réseaux sans fil situés dans les environnement à affaiblissement. Le récepteur reçoit une multitude de signaux de fréquences et de déphasages différents. Les résultats obtenus sont similaires à ceux obtenus pour des réseaux sans fil non soumis à l'environnement d'affaiblissement : le taux d'erreur au niveau des récepteurs augmente ou diminue selon leur position par rapport à la position du relais brouilleur et de la source d'émission. Au chapitre 5, on a proposé des stratégies de brouillage coopératif pour la sécurité et la fiabilité des

réseaux sans fil soumis à l'écoute, afin de montrer la limite de chaque stratégie proposée, peu importe l'allocation de puissance utilisée. Dans ce cadre, un seul relais ne pouvant couvrir toute la surface du réseau, nous avons alors étudié le brouillage dans le même type de réseau mais avec deux relais. On a montré que cette nouvelle configuration donne plus de sécurité au réseau tout en assurant une communication fiable avec l'utilisateur légitime si chaque relais a la puissance nécessaire pour brouiller les terminaux à proximité sans que le signal de brouillage puisse atteindre le récepteur légitime. Cette contrainte constitue une limitation de sécurité puisque cela engendre des zones non sécurisées. En raison de la limitation de l'effet de brouillage avec une architecture à deux relais brouilleurs, on a étudié par la suite des réseaux à plusieurs relais brouilleurs. Cette configuration a nettement amélioré le taux de couverture sécuritaire du réseau. Le taux de couverture sécuritaire augmente ou diminue selon l'allocation qu'on attribue plus ou moins de puissance aux relais brouilleurs. Néanmoins, il reste toujours des zones non sécurisées, quelle que soit la stratégie de brouillage coopératif utilisée. L'objectif principal du brouillage coopératif est que cette zone non sécurisée soit la plus faible possible. Cet objectif a été étudié dans le chapitre 6. En se basant sur les limites constatées dans les stratégies de brouillage coopératif analysées au chapitre précédent, on a discuté des résultats d'un algorithme permettant le positionnement N_J relais brouilleurs disponibles dans le réseau sans fil, et de l'allocation de puissance, pour l'obtention des meilleurs résultats en terme de fiabilité de liaison entre émetteur et récepteur légitimes, tout en limitant la fuite d'information vers des terminaux espions.

7.3 Contribution du mémoire

Le travail de recherche présente une contribution en sécurité de la couche physique, basé sur le brouillage coopératif, pour la sécurité des canaux gaussiens soumis à l'écoute, d'un seul espion.

7.3.1 Validations des travaux antérieurs

Notre travail repose sur la validation du principe des résultats du modèle proposé dans [5], qui présente un réseau linéaire avec une configuration à un seul relais brouilleur. Dans le chapitre 3, on a vérifié expérimentalement les deux principaux facteurs qui influent directement sur l'efficacité du brouillage coopératif, soit l'emplacement du relais brouilleur par rapport au récepteur légitime et à l'espion, ainsi que la stratégie de partage de la puissance allouée au système entre la source d'émission et le relais brouilleur. Plus le relais est près d'un terminal et plus ce dernier est perturbé par le signal brouilleur plus ou moins important selon la puissance allouée au relais et celle allouée à la source d'émission.

7.3.2 Proposition d'un algorithme d'optimisation

Au chapitre 6, nous avons proposé un algorithme automatisé, qui permet de rechercher le meilleur emplacement des relais brouilleurs et le partage de la puissance allouée au système, entre les différents terminaux émetteurs. Cet algorithme prend en considération, entre autres, les dimensions du réseau, la puissance allouée au système, la position de la source d'émission et du récepteur légitimes, et le nombre de relais brouilleurs, N_J. On souhaite avoir une liaison fiable entre la source d'émission et le

récepteur légitime, dont le taux d'erreur doit être au plus égal à une valeur seuil, P_{e_B}. L'algorithme est appliqué à deux configurations ; un réseau sans fil à un seul relais brouilleurs et à 3 relais brouilleurs. Il place ces relais de telle sorte que le canal légitime entre l'émetteur et le récepteur ne soit pas perturbé par le signal de brouillage. Au même instant, puisque la position de l'espion est généralement inconnue et aléatoire, l'algorithme d'optimisation garantit un taux d'erreur moyen de l'espion le plus élevé possible.

7.4 Suggestions de travaux futurs

Le travail présenté dans ce mémoire constitue un scénario simple, qui peut être la base de plusieurs travaux futurs. Les possibilités de son développement sont résumés principalement dans les points cités ci-dessous :

7.4.1 Ajout de codage de canal

Les canaux simulés dans les différentes stratégies sont des canaux gaussiens soumis à l'écoute. Malgré que l'algorithme d'optimisation garantit que le taux d'erreur du récepteur légitime ne dépasse pas la valeur seuil autorisée, l'absence d'un codage de canal rend l'opération de correction des erreurs au niveau de la réception difficile. L'application d'un codage de canal adéquat (exemple : codage LDPC) permet la détection et la correction des erreurs de transmission.

7.4.2 Collaboration entre les espions

Les stratégies de brouillage coopératif présentés dans le mémoire, prennent en considération la présence d'un espion unique dans la surface du réseau sans fil. On peut étendre cet algorithme pour considérer des réseaux sans fil comportant plus d'un espion, soit N_E espions. La collusion entre les espions peut être étudiée. En effet, les espions peuvent coopérer entre eux pour contourner les différents niveaux et couches de sécurité du réseau sans fil en question.

7.4.3 Collaboration entre les relais brouilleurs

Les relais brouilleurs diffusent des signaux brouilleurs d'une façon omni-directionnelle. L'utilisation de relais brouilleurs multi-antennes et la collaboration entre ces relais permettrait à chaque relais d'orienter la direction d'émission de son signal de brouillage, en prenant en compte la partie couverte par les relais voisins.

Annexe A

Description des programmes Matlab

Dans cette annexe, on fait une description des programmes Matlab développés pour ce mémoire et utilisés pour obtenir les différents résultats présentés dans ledit mémoire.

A.1 Simulation du principe de brouillage coopératif

Le programme *"PrincipeDuBrouillage.m"* est utilisé à la section 3.3 pour simuler le principe du brouillage coopératif dans le réseau sans fil linéaire soumis à l'écoute avec des canaux gaussiens, décrit à la figure 3.2 et montrer la différence fondamentale entre le taux d'erreur au niveau des récepteurs avec et sans la présence du signal brouilleur.

A.2 Réseaux sans fil soumis à l'écoute avec et sans brouillage

A la section 3.4, trois programmes, *"BERVarEspionAvecRelais.m"*, *"BERVarEspionSansRelais.m"* et *"BrouillageForSecurCommunications.m"*, simulent la fiabilité de réception des terminaux légitime et espion dans un réseau sans fil dans le cas de la présence d'un relais brouilleur et le cas d'absence de ce dernier, pour pouvoir évaluer l'effet qu'apporte le signal brouilleur.

A.3 Modèle de Rayleigh pour le canal à affaiblissement

Cinq programmes sont développés comme suit : le programme *"ExempleSignalRayleigh.m"* réalise un signal binaire aléatoire selon le modèle de Rayleigh pour les canaux à affaiblissement, dont un exemple est présenté à la figure 4.3. Ce même programme est utilisé à la section 4.6 pour générer les différents signaux émis par la source et le relais, nécessaires pour simuler un réseau sans fil avec des canaux gaussien à affaiblissement de Rayleigh. Le programme *"BER TheoriqueSimuleCanalRayleighModulationBPSK.m"* permet de simuler le taux d'erreur dans les canaux gaussien et de Rayleigh, dont un exemple de simulation est présenté à la figure 4.4. La probabilité d'erreur est définie au point 4.5.2, comme étant l'un des paramètres caractéristiques du modèle de Rayleigh.

A.4 Simulation des canaux sous écoute avec propagation multivoie

À la section 4.6, le programme développé *"BErVarEspionAvecRelaisRayleigh.m"* permet d'observer l'allure des signaux émis par la source et le relais et les signaux reçus par le récepteur légitime et l'espion sous l'effet du signal de brouillage tel que montré aux figures 4.6 et 4.7, ainsi que la distribution des bits en erreur au niveau des mêmes récepteurs tel que montrée à la figure 4.8. Les mêmes observations sont faites pour le cas d'absence du signal brouilleur.

A.5 Simulation du brouillage coopératif : effet de l'allocation de puissance

Au chapitre 5, quatre programmes ont été développés, *"BErEspionMultiRelais.m"*, *"BErEspionMultiRelais2.m"*, *"VarBErEspionEnergieVar.m"* et *"VarBErEspionEnergieVar V2.m"*, pour évaluer l'effet de l'allocation de puissance sur le rendement du brouillage coopératif pour une allocation de puissance équitable entre l'émission et le brouillage et une allocation de puissance favorisant l'émission. Pour chaque allocation de puissance, le relais prend plusieurs position.

A.6 Simulation du brouillage coopératif : effet du nombre de relais brouilleurs

À la section 5.4, un programme a été développé, *"NetworkDeuxRelais.m"* pour évaluer l'efficacité du brouillage coopératif pour différentes stratégies d'allocation de puissance et de positions des terminaux, incluant deux relais brouilleurs. Deux autres programmes *"NetworkHuitRelais.m"* et *"NetworkHuitRelais V3.m"* permettent à la section 5.5 de faire la même évaluation pour le cas de réseau sans fil incluant 8 relais brouilleurs.

A.7 Amélioration du brouillage coopératif

Au chapitre 6, le programme développé *"Optimisation emplacement allocation.m"* permet l'amélioration des résultats obtenus en termes de fiabilité de la liaison légitime et de couverture sécuritaire pour un réseau sans fil avec canaux gaussiens soumis à l'écoute clandestine des chapitres précédents. L'algorithme permet de positionner les 3 relais brouilleurs présents dans le réseau, ainsi que la recherche de la meilleure allocation de puissance entre la source d'émission et ces 3 relais, de telle façon à avoir une communication fiable entre cette source et le récepteur légitime, en même instant que la moyenne du taux d'erreur de l'espion sur l'ensemble de la surface du réseau soit le plus grand possible.

Annexe B

Statistiques sur les taux d'erreur au niveau des récepteurs sous l'effet d'un relais brouilleur unique

B.1 Statistiques sur les taux d'erreur au niveau du récepteur légitime

Pour chacune des 756 positions possibles du relais $J^{(1)}$, soit (21 positions radiales) $\times$ (36 positions angulaires), on fait varier le coefficient d'allocation de puissance δ entre la source et le relais, de la valeur 0 à la valeur 1, avec un pas de variation de 0,1 et on évalue à chaque variation d'allocation le taux d'erreur P_{e_B} au niveau du récepteur légitime.

Pour ces 756 positions possibles, on compte le nombre d'allocations de puissance, soit m, qui donnent un taux d'erreur favorable pour le récepteur, $P_{e_B} \leq 10^{-3}$. Le nombre restant des allocations, soit i, sont considérés alors comme défavorables pour lesquels $P_{e_B} > 10^{-3}$.

On peut déduire ainsi pour chaque position possible du relais, le pourcentage des allocations qui donnent des taux d'erreurs favorables pour le récepteur légitime, par rapport à l'ensemble des taux d'erreurs calculés pour la même position du relais, soit $(m)/(m+i)$.

Les résultats numériques des pourcentages des taux d'erreur favorables au récepteur légitime sont rapportés au tableau suivant :

B.2 Statistiques sur les taux d'erreur moyen au niveau de l'espion

De même, pour les différentes positions possibles du relais $J^{(1)}$, on fait varier le coefficient d'allocation de puissance δ et on évalue à chaque variation d'allocation non pas le taux d'erreur au niveau de l'espion, mais plutôt le taux d'erreur moyen de ce dernier, $\mathrm{E}[P_{e_E}]$. On calcule le pourcentage des taux d'erreur favorables en terme de confusion de l'espion, soit $\mathrm{E}[P_{e_E}] \geq 2{,}5 \cdot 10^{-1}$, de la même manière

rayon ρ (m) / Angle θ (°)	100	95	90	85	80	⋯	40	35	30	25	20	15	10	5	0
180°	81	81	81	81	81	⋯	72	63	63	63	63	54	54	54	45
170°	81	81	81	81	81	⋯	72	63	63	63	63	54	54	54	45
160°	81	81	81	81	81	⋯	72	63	63	63	63	54	54	54	45
150°	81	81	81	81	81	⋯	72	63	63	63	63	54	54	54	45
140°	81	81	81	81	81	⋯	63	63	63	63	63	54	54	54	45
130°	81	81	81	81	72	⋯	63	63	63	63	54	54	54	54	45
120°	81	81	81	72	72	⋯	63	63	63	63	54	54	54	54	45
110°	81	81	72	72	72	⋯	63	63	63	54	54	54	54	54	45
100°	72	72	72	72	72	⋯	63	63	54	54	54	54	54	45	45
90°	72	72	72	72	72	⋯	54	54	54	54	54	54	45	45	45
80°	72	72	72	72	72	⋯	54	54	54	54	45	45	45	45	45
70°	72	72	72	63	63	⋯	54	45	45	45	45	45	45	45	45
60°	72	63	63	63	63	⋯	45	45	45	45	45	45	45	45	45
50°	63	63	63	54	54	⋯	36	36	36	36	36	45	45	45	45
40°	63	54	54	54	54	⋯	36	36	36	36	36	36	45	45	45
30°	54	54	54	45	45	⋯	27	27	27	27	36	36	45	45	45
20°	54	45	45	45	36	⋯	18	18	27	27	36	36	45	45	45
10°	45	45	45	36	36	⋯	9	18	18	27	27	36	36	45	45
0°	45	45	36	36	27	⋯	9	18	18	27	27	36	36	45	45
−10°	45	45	45	36	36	⋯	9	18	18	27	27	36	36	45	45
−20°	54	45	45	45	36	⋯	18	18	27	27	36	36	45	45	45
−30°	54	54	54	45	45	⋯	27	27	27	27	36	36	45	45	45
−40°	63	54	54	54	54	⋯	36	36	36	36	36	36	45	45	45
−50°	63	63	63	54	54	⋯	36	36	36	36	36	45	45	45	45
−60°	72	63	63	63	63	⋯	45	45	45	45	45	45	45	45	45
−70°	72	72	72	63	63	⋯	54	45	45	45	45	45	45	45	45
−80°	72	72	72	72	72	⋯	54	54	54	54	45	45	45	45	45
−90°	72	72	72	72	72	⋯	54	54	54	54	54	54	45	45	45
−100°	72	72	72	72	72	⋯	63	63	54	54	54	54	54	45	45
−110°	81	81	72	72	72	⋯	63	63	63	54	54	54	54	54	45
−120°	81	81	81	72	72	⋯	63	63	63	63	54	54	54	54	45
−130°	81	81	81	81	72	⋯	63	63	63	63	54	54	54	54	45
−140°	81	81	81	81	81	⋯	63	63	63	63	63	54	54	54	45
−150°	81	81	81	81	81	⋯	72	63	63	63	63	54	54	54	45
−160°	81	81	81	81	81	⋯	72	63	63	63	63	54	54	54	45
−170°	81	81	81	81	81	⋯	72	63	63	63	63	54	54	54	45

TABLE B.1 – *Pourcentage des taux d'erreur favorables de P_{e_B} en fonction de la position du relais et de l'allocation de puissance.*

qu'on a fait pour le récepteur légitime. Les taux d'erreur moyens défavorables sont alors ceux qui vérifient $\mathrm{E}[P_{e_E}] < 2{,}5 \cdot 10^{-1}$.

Les résultats numériques de l'évaluation du pourcentage du taux d'erreur moyen favorable à l'espion sont rapportés au tableau suivant, dans lequel on constate que pour une valeur donnée du rayon ρ du relais, le pourcentage du taux d'erreur moyen favorable au niveau de l'espion demeure fixe quelle que soit la coordonnée angulaire θ du relais :

rayon ρ (m) / Angle θ (°)	100	95	90	85	80	⋯	40	35	30	25	20	15	10	5	0
180°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
170°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
160°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
150°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
140°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
130°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
120°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
110°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
100°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
90°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
80°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
70°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
60°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
50°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
40°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
30°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
20°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
10°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
0°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−10°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−20°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−30°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−40°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−50°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−60°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−70°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−80°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−90°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−100°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−110°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−120°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−130°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−140°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−150°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−160°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0
−170°	9	9	18	18	18	⋯	27	27	27	36	36	36	36	36	0

TABLE B.2 – *Pourcentage des taux d'erreur favorables de $E[P_{e_E}]$ en fonction de la position du relais et de l'allocation de puissance.*

Annexe C

Relation entre l'indice de positionnement des relais et leurs coordonnées

```
%%%%Relation entre l'indice de positionnement des relais $J^(2)$ et $J^(3)$
et leurs coordonnées polaires et cartésiennes%%%%
RayonRelaisDeux      = abs(RayonMax-RayonMin)
     - (mod(TABLEAU4(1,4),(abs((RayonMax-RayonMin)/ResolutionRayonRelais)+1))-1)
                     * abs(ResolutionRayonRelais);
AngleRelaisDeux      = AngleRelaisUnRadian
                     + ResolutionAngleRelaisRadian
     * floor(TABLEAU4(1,4)/(abs((RayonMax-RayonMin)/ResolutionRayonRelais)+1));
RelaisDeuxPolaire    = [AngleRelaisDeux RayonRelaisDeux];
RelaisDeuxCartesien  = [RayonRelaisDeux
                     * cos(AngleRelaisDeux) RayonRelaisDeux*sin(AngleRelaisDeux)];

RayonRelaisTrois     = RayonRelaisDeux;
AngleRelaisTrois     = -AngleRelaisDeux;
RelaisTroisPolaire   = [AngleRelaisTrois RayonRelaisTrois];
RelaisTroisCartesien = [RayonRelaisTrois
                     * cos(AngleRelaisTrois) RayonRelaisTrois*sin(AngleRelaisTrois)];

AllocationFinale=(TABLEAU4(1,3)*abs(ResolutionEnergie))-abs(ResolutionEnergie);
```

Cet algorithme convertit chaque indice de position des relais $J^{(2)}$ et $J^{(3)}$ en coordonnées polaires et cartésiennes, permettant de déterminer leur position sur la surface du réseau sans fil.

Annexe D

Évaluation du taux d'erreur au niveau des récepteurs pour un réseau à 3 relais brouilleurs

D.1 Résultats numériques de l'évaluations du taux d'erreur au niveau du récepteur légitime

Pour chaque position des relais $J^{(2)}$ et $J^{(3)}$ sur la surface circulaire du réseau, on évalue le taux d'erreur P_{e_B} du récepteur légitime, en fonction du coefficient de partage de puissance δ entre la source et les relais brouilleurs. Le relais $J^{(1)}$ demeure à sa position optimale, déjà déterminée dans la première partie de l'exécution de l'algorithme d'optimisation. Chaque position de ces deux relais est codée par un entier, tel expliqué à la section **??**. La variation de ce taux d'erreur est représentée graphiquement à la figure 6.17.

Une partie des résultats numériques obtenus de l'évaluation sont rapportés dans le tableau suivant :

indice position	Valeur du coefficient de partage de puissance entre source et brouillage δ										
	0	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
1	0	0	0	0	0	0	0,0001	0,0031	0,0441	0,2079	0,5017
2	0	0	0	0	0	0	0,0001	0,0031	0,0441	0,2079	0,5017
3	0	0	0	0	0	0	0,0002	0,0043	0,0434	0,2158	0,4976
4	0	0	0	0	0	0	0,0001	0,0042	0,0497	0,2189	0,5039
5	0	0	0	0	0	0	0	0,0044	0,0501	0,2258	0,4981
6	0	0	0	0	0	0	0,0001	0,0056	0,0563	0,2286	0,5045
7	0	0	0	0	0	0	0,0002	0,0063	0,0566	0,2420	0,5009
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
12	0	0	0	0	0	0	0,0004	0,0134	0,1001	0,2812	0,5010
13	0	0	0	0	0	0	0,0006	0,0187	0,1157	0,2914	0,5010
14	0	0	0	0	0	0	0,0010	0,0240	0,1308	0,3056	0,5009
15	0	0	0	0	0	0	0,0016	0,0297	0,1508	0,3137	0,4945
16	0	0	0	0	0	0,0001	0,0031	0,0437	0,1756	0,3220	0,5036
17	0	0	0	0	0	0,0001	0,0058	0,0590	0,1966	0,3314	0,4961
18	0	0	0	0	0	0,0003	0,0084	0,0907	0,2213	0,3371	0,4991
19	0	0	0	0	0	0,0002	0,0184	0,1233	0,2441	0,3365	0,4975
20	0	0	0	0	0	0,0013	0,0323	0,1683	0,2597	0,3413	0,4970
21	0	0	0	0	0,0001	0,0040	0,0693	0,2119	0,2656	0,3393	0,4988
22	0	0	0	0	0,0001	0,0108	0,1285	0,2429	0,2686	0,3397	0,4998
23	0	0	0	0	0	0	0,0001	0,0026	0,0445	0,2107	0,4998
24	0	0	0	0	0	0	0,0002	0,0038	0,0457	0,2175	0,5004
25	0	0	0	0	0	0	0,0001	0,0039	0,0483	0,2192	0,5029
26	0	0	0	0	0	0	0,0001	0,0040	0,0512	0,2236	0,4978
27	0	0	0	0	0	0	0,0001	0,0050	0,0554	0,2306	0,5018
28	0	0	0	0	0	0	0,0003	0,0060	0,0588	0,2354	0,4959
29	0	0	0	0	0	0	0,0004	0,0066	0,0631	0,2378	0,4987
30	0	0	0	0	0	0	0,0003	0,0088	0,0725	0,2491	0,4999
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮9
197	0	0,0001	0,2541	0,2545	0,2545	0,2545	0,2545	0,2555	0,2701	0,3441	0,5014
198	0	0,2511	0,2545	0,2545	0,2545	0,2545	0,2550	0,2647	0,3201	0,4298	0,5010
199	0	0,5031	0,5031	0,5031	0,5031	0,5031	0,5031	0,5031	0,5031	0,5031	0,5031
200	0	0,2545	0,2545	0,2576	0,4317	0,5029	0,5031	0,5031	0,5031	0,5031	0,5031
201	0	0,2508	0,2545	0,2545	0,2545	0,2545	0,2546	0,2582	0,2928	0,3895	0,5019
202	0	0	0,2542	0,2545	0,2545	0,2545	0,2545	0,2553	0,2686	0,3411	0,5025
203	0	0	0,0180	0,2541	0,2545	0,2545	0,2545	0,2551	0,2688	0,3351	0,5003
204	0	0	0	0,0987	0,2542	0,2545	0,2545	0,2553	0,2657	0,3390	0,4980
205	0	0	0	0,0035	0,1786	0,2544	0,2545	0,2551	0,2678	0,3379	0,4994
206	0	0	0	0,0001	0,0343	0,2276	0,2544	0,2551	0,2656	0,3337	0,5022
207	0	0	0	0	0,0032	0,1214	0,2478	0,2551	0,2676	0,3386	0,4988
208	0	0	0	0	0,0008	0,0380	0,2018	0,2536	0,2678	0,3389	0,4997
209	0	0	0	0	0,0001	0,0116	0,1260	0,2412	0,2677	0,3390	0,4998

TABLE D.1 – Valeurs numériques de l'évaluation du P_{e_B} en fonction de la position des trois relais et de l'allocation de puissance.

D.2 Résultats numériques de l'évaluations du taux d'erreur moyen au niveau de l'espion

De même, pour chaque position des relais $J^{(2)}$ et $J^{(3)}$ sur la surface circulaire du réseau, on évalue le taux d'erreur moyen $\mathrm{E}[P_{e_E}]$ au niveau de l'espion, cela en fonction du coefficient de partage de puissance δ entre la source et les relais brouilleurs. Le relais $J^{(1)}$ demeure à sa position optimale déjà déterminée dans la première partie de l'exécution de l'algorithme d'optimisation. Chaque position de ces deux relais est codée par un entier, tel expliqué à la section **??**. La variation de ce taux d'erreur est représentée graphiquement à la figure 6.18.

Une partie des résultats numériques obtenus de l'évaluation sont rapportés dans le tableau suivant :

ind. pos.	Valeur du coefficient de partage de puissance entre source et brouillage δ								
	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9
1	0.0053	0.0114	0.0189	0.0295	0.0449	0.0676	0.1020	0.1552	0.2423
2	0.0060	0.0127	0.0208	0.0320	0.0478	0.0709	0.1058	0.1593	0.2467
3	0.0065	0.0137	0.0222	0.0340	0.0502	0.0739	0.1093	0.1633	0.2508
4	0.0074	0.0149	0.0234	0.0355	0.0524	0.0768	0.1129	0.1677	0.2555
5	0.0081	0.0160	0.0248	0.0370	0.0542	0.0792	0.1161	0.1717	0.2600
6	0.0088	0.0173	0.0265	0.0391	0.0566	0.0820	0.1196	0.1762	0.2649
7	0.0091	0.0183	0.0284	0.0414	0.0596	0.0855	0.1235	0.1806	0.2695
8	0.0092	0.0192	0.0305	0.0441	0.0631	0.0897	0.1283	0.1856	0.2745
9	0.0093	0.0194	0.0316	0.0463	0.0661	0.0937	0.1333	0.1912	0.2799
10	0.0090	0.0196	0.0323	0.0483	0.0690	0.0982	0.1391	0.1976	0.2858
11	0.0083	0.0199	0.0328	0.0494	0.0720	0.1021	0.1447	0.2048	0.2922
12	0.0077	0.0199	0.0327	0.0503	0.0736	0.1065	0.1509	0.2125	0.2994
13	0.0073	0.0191	0.0328	0.0508	0.0756	0.1100	0.1578	0.2215	0.3066
14	0.0068	0.0178	0.0330	0.0515	0.0773	0.1136	0.1636	0.2312	0.3161
15	0.0064	0.0166	0.0315	0.0518	0.0787	0.1167	0.1712	0.2404	0.3244
16	0.0059	0.0156	0.0300	0.0509	0.0802	0.1218	0.1776	0.2514	0.3315
17	0.0056	0.0141	0.0269	0.0499	0.0810	0.1254	0.1881	0.2615	0.3361
18	0.0052	0.0129	0.0234	0.0467	0.0818	0.1319	0.1990	0.2718	0.3429
19	0.0052	0.0123	0.0215	0.0406	0.0792	0.1371	0.2159	0.2852	0.3461
20	0.0052	0.0117	0.0196	0.0362	0.0722	0.1460	0.2385	0.2938	0.3486
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
23	0.0093	0.0162	0.0241	0.0347	0.0495	0.0713	0.1049	0.1574	0.2449
24	0.0104	0.0182	0.0269	0.0380	0.0532	0.0753	0.1088	0.1612	0.2487
25	0.0110	0.0199	0.0292	0.0409	0.0568	0.0793	0.1132	0.1659	0.2530
26	0.0116	0.0210	0.0310	0.0435	0.0599	0.0835	0.1183	0.1712	0.2576
27	0.0120	0.0224	0.0329	0.0459	0.0630	0.0873	0.1231	0.1768	0.2627
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
28	0.0120	0.0241	0.0350	0.0487	0.0669	0.0922	0.1289	0.1834	0.2685
29	0.0117	0.0250	0.0368	0.0516	0.0708	0.0975	0.1352	0.1905	0.2753
30	0.0113	0.0252	0.0385	0.0539	0.0743	0.1023	0.1413	0.1978	0.2828
31	0.0107	0.0251	0.0398	0.0563	0.0777	0.1073	0.1480	0.2057	0.2908
32	0.0101	0.0249	0.0401	0.0579	0.0811	0.1117	0.1545	0.2142	0.2996
33	0.0096	0.0243	0.0396	0.0589	0.0837	0.1167	0.1612	0.2230	0.3081
34	0.0085	0.0226	0.0391	0.0581	0.0862	0.1213	0.1688	0.2325	0.3167
35	0.0077	0.0211	0.0382	0.0579	0.0863	0.1258	0.1760	0.2430	0.3275
36	0.0066	0.0189	0.0357	0.0575	0.0871	0.1278	0.1842	0.2538	0.3365
37	0.0065	0.0176	0.0336	0.0554	0.0875	0.1314	0.1908	0.2649	0.3454
38	0.0056	0.0151	0.0300	0.0529	0.0860	0.1327	0.1996	0.2767	0.3502
39	0.0055	0.0143	0.0254	0.0493	0.0854	0.1364	0.2067	0.2853	0.3600
40	0.0055	0.0133	0.0231	0.0417	0.0808	0.1404	0.2206	0.2920	0.3612
41	0.0055	0.0130	0.0212	0.0373	0.0735	0.1478	0.2410	0.2973	0.3567
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
45	0.0131	0.0228	0.0329	0.0451	0.0614	0.0842	0.1179	0.1689	0.2525
46	0.0139	0.0253	0.0363	0.0493	0.0664	0.0902	0.1243	0.1753	0.2581
47	0.0139	0.0274	0.0396	0.0535	0.0715	0.0959	0.1308	0.1822	0.2644
48	0.0136	0.0289	0.0422	0.0573	0.0761	0.1013	0.1370	0.1894	0.2711
189	0.0078	0.0175	0.0284	0.0433	0.0637	0.0913	0.1296	0.1834	0.2637
190	0.0090	0.0190	0.0305	0.0460	0.0667	0.0948	0.1335	0.1872	0.2668
191	0.0098	0.0202	0.0321	0.0483	0.0697	0.0984	0.1374	0.1911	0.2701
192	0.0102	0.0212	0.0336	0.0503	0.0723	0.1016	0.1411	0.1951	0.2732
193	0.0103	0.0221	0.0350	0.0521	0.0746	0.1046	0.1449	0.1991	0.2767
194	0.0100	0.0229	0.0363	0.0539	0.0770	0.1076	0.1486	0.2031	0.2802
195	0.0097	0.0234	0.0375	0.0558	0.0794	0.1106	0.1523	0.2073	0.2840
196	0.0093	0.0233	0.0385	0.0576	0.0817	0.1139	0.1563	0.2116	0.2880
197	0.0089	0.0226	0.0388	0.0592	0.0844	0.1169	0.1601	0.2159	0.2917
198	0.0084	0.0217	0.0389	0.0607	0.0866	0.1204	0.1643	0.2204	0.2966
199	0.0079	0.0209	0.0384	0.0611	0.0893	0.1237	0.1684	0.2256	0.3016
200	0.0075	0.0198	0.0369	0.0614	0.0908	0.1276	0.1728	0.2301	0.3064
201	0.0072	0.0183	0.0355	0.0610	0.0928	0.1306	0.1780	0.2352	0.3112
202	0.0067	0.0170	0.0339	0.0602	0.0940	0.1347	0.1820	0.2410	0.3182
203	0.0064	0.0161	0.0309	0.0585	0.0945	0.1376	0.1887	0.2459	0.3251
204	0.0058	0.0153	0.0287	0.0551	0.0947	0.1423	0.1937	0.2532	0.3308
205	0.0055	0.0139	0.0257	0.0513	0.0934	0.1448	0.2020	0.2605	0.3350
206	0.0052	0.0127	0.0228	0.0459	0.0912	0.1499	0.2093	0.2695	0.3412
207	0.0052	0.0123	0.0211	0.0399	0.0840	0.1526	0.2213	0.2836	0.3451
208	0.0052	0.0117	0.0194	0.0360	0.0725	0.1572	0.2387	0.2934	0.3482

TABLE D.2 – Valeurs numériques de l'évaluation du $\mathrm{E}[P_{e_E}]$ en fonction de la position des trois relais et de l'allocation de puissance.

Bibliographie

[1] P. Parada et R. Blahut, "Secrecy Capacity of SIMO and Slow Fading Channels," *IEEE Transactions On Information Theory*, pp. 2152–2155, 2005.

[2] C. E. Shannon, "A Mathematical Theory of Communication," *Bell System Technical Journal*, vol. 27, pp. 379–423, 623–656, juillet 1948.

[3] A. D. Wyner, "The Wire-Tap Channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, octobre 1975.

[4] I. Csiszàr et J. Korner, "Broadcast Channels with Confidential Messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[5] L. Dong, Z. Han, A. P. Petropulu et H. V. Poor, "Cooperative Jamming for Wireless Physical Layer Security," *IEEE/SP 15th Workshop on Statistical Signal Processing*, pp. 417–420, 2009.

[6] I. Csiszàr et P. C. Shields, *Information Theory and Statistics : A Tutorial. Foundations and Trends in Communications and Information Theory*, vol. 1. Now Publishers, Hanover, Massachussetts, 2004.

[7] M. Bloch et J. Barros, *Physical Layer Security - From Information Theory to Security Engineering*. Cambridge University Press, 2011.

[8] G. Battail, *Théorie de l'Information, Application aux Techniques de Communication*. Masson, Paris, 1997.

[9] R. L. Rivest, A. Shamir et L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communication of the ACM*, vol. 21, février 1978.

[10] M. Majri, *Cryptographie*. Notes de cours, Université Laval, Québec, 2013.

[11] S. K. Leung-Yan-Cheong et M. E. Hellman, "The Gaussian Wire-Tap Channel," *IEEE Transactions on Information Theory*, vol. IT-24, pp. 451–456, juillet 1978.

[12] A. E. Gamal et K. Young-Han, *Network Information Theory*. Cambridge University Press, 2011.

[13] R. Bassily, E. Ekrem, H. Xiang, E. Tekin, J. Xie, M. R. Bloch, S. Ulukus et A. Yener, "Cooperative Security at the Physical Layer," *IEEE Signal Processing Magazine*, septembre 2013.

[14] L. Dong, Z. Han, A. Petropulu et H. V. Poor, “Secure Wireless Communications via Cooperation,” *46th Annual Allerton Conf. Commun., Control, and Computing*, septembre 2008.

[15] R. Negi et S. Goel, “Secret Communication Using Artificial Noise,” *IEEE Transactions on Vehicular Technology*, vol. 3, pp. 1906–1910, septembre 2005.

[16] E. Tekin et A. Yener, “The General Gaussian Multiple Access and Two-Way Wire-Tap Channels : Achievable Rates and Cooperative Jamming,” *IEEE Transactions on Information Theory*, vol. 54, p. 2735–2751, juin 2008.

[17] E. Tekin et A. Yener, “The Multiple Access Wire-Tap Channel : Wireless Secrecy and Cooperative Jamming,” *Information Theory and Applications Workshop*, janvier 2007.

[18] E. Tekin et A. Yener, “Achievable Rates for the General Gaussian Multiple Access Wire-Tap Channel with Collective Secrecy,” *44th Annual Allerton Conference on Communication, Control, and Computing*, décembre 2006.

[19] M. Dehghan, D. L. Goeckel, M. Ghaderi et Z. Ding, “Energy Efficiency of Cooperative Jamming Strategies in Secure Wireless Networks,” *IEEE Transactions on Wireless Communications*, vol. 11, pp. 3025–3029, septembre 2012.

[20] M. K. Islam et R. Liu, “Polar Coding for Fading Channel,” *Information Science and Technology*, pp. 1096–1098, mars 2013.

[21] T. David et P. Viswanath, *Fundamentals of Wireless Communications*. Cambridge University Press, 2005.

[22] V. Orlić et M. Lutovac, “A Solution for Efficient Reduction of Intersymbol Interference in Digital Microwave Radio,” *Telecommunication in Modern Satellite, Cable, and Broadcasting Services, IEEE*, pp. 463–466, octobre 2009.

[23] Peter Monsen, “Fading Channel Communications : Adaptive processing can reduce the effects of fading on beyond-the-horizon digital radio link,” *IEEE Communications Magazine*, pp. 16–25, 1980.

[24] J. M. Wozencraft et I. M. Jacobs, “Principles of Communication Engineering,” *John Wiley & Sons, Inc*, vol. New York, London, Sydney, 1965.

[25] M. Divya, “Bit Error Rate Performance of BPSK Modulation and OFDM-BPSK with Rayleigh Multipath Channel,” *International Journal of Engineering and Advanced Technology (IJEAT)*, vol. 2, avril 2013.

[26] L. Dong, Z. Han, A. Petropulu et H. V. Poor, “Improving Wireless Physical Layer Security via Cooperating Relays,” *IEEE Transactions on Signal Processing*, vol. 58, mars 2010.