**ID Sidney :**

* Y a t-il un avantage à ne pas updater l’AN au même rythme que les symboles ? (e.g., plus lent ?)
* Si l’incertitude sur H est connue, peut-on modifier les statistiques de l’AN pour atténuer les effets négatifs engendrés par l’incertitude de H ? Est-ce qu’une analyse des indices de Sobol du système de PLS nous donnerait qqch ? (chaque sous-porteuse est une RV et Q-N AN aussi)
* Pour étudier plus à fond notre PLS, il faudrait déterminer le best estimateur possible pour Eve (si elle sait par exemple qu’Alice envoie un signal avec de l’AN) => demander conseil à François
* **Multiuser**: multiple Bob, and the FD TR OFDM PLS scheme helps in getting orthogonal data at Bobs while ensuring SR elsewhere. En fonction de l’état de l’art, à voir mais on pourrait faire un papier qui combine le multiplexage spatial en utilisant du symbol-level precoding avec de l’AN. Egalement, sans AN, si on adresse plusieurs utilisateurs avec plusieurs data, chaque data étant vue comme du bruit ailleurs, a t’on besoin de rajouter de l’AN ? Peut-être cela dépend du nombre d’utilisateurs, du channel, etc. => très intéressant à étudier je pense.

Mais même sans bruit, ça peut être intéressant. Si avec un BOR de N on peut adresser N utilisateurs avec les mêmes ressources, alors c’est mieux que de simplement diviser la bande en N pour N utilisateurs puisqu’avec notre schéma, on a un gain de diversité fréquentiel en plus (finalement un peu comme en CDMA ?) ? => j’imagine que ça doit déjà exister…

* Study of true worst-case scenarios: how are the performance when we launch an optimization at Eve’s for her estimation?
* 2nd paper: proof that under which channel features, one achieves a positive SR. Knowing the frequency diversity within Bob’s channel, can we derive the SR if we assume Eve having a super flat frequency response (or oppositely, a super diversity channel?). Also, we should show how immune we are to a MIMO eavesdropper.
* ID premier papier journal : bien présenter le gain du TR en time domain, puis décrire l’analogie fréquentiel et sa possible implémentation en OFDM. Ensuite, dire que ce gain produit un SR mais que sans connaître le canal d’Eve, il est impossible à connaître (et qu’en fonction du canal, le gain peut être tellement faible que le SR peut être très faible). D’où l’idée de rajouter de l’AN (en gros, prendre du temps sur la première partie pour expliquer le TR). Expliquer avec des phrases le fctnt de la spreading matrix (du pt de vu temp et freq, et dire d ou vient le gain). Regarder l’hypothèse forte où Eve connaît le canal de Bob.
* L’AN ne peut pas être deviné car il s’agit en fait d’une clé de crypto aussi longue que la data itself (merci Shanon). Peut-être essayer d’expliquer cela dans la communauté Computer Science Crypto pour mieux vendre le PLS. Une clé super longue dont Bob n’a pas besoin !!!)
* Dans notre schéma, l’utilisation de ressources supplémentaires pourrait être tolérée si elle ne sert qu’à échanger une clé de crypto. D’ailleurs, ces ressources supplémentaires pourraient être la même (un seul AN) pour plusieurs utilisateurs => scénario à creuser. A VOIR, PAS SUR
* Il existe une bound Information theory pour le scénario de Sidney sans AN (p8 du livre de Trappe). Cette bound considère connaître le canal d’Eve, mais devrait être dérivable (au moins numériquement) dans le cas où on ne connaît pas Eve. (est-ce que les articles OFDM PLS sans AN en wireless communication ont utilisé certaines de ces bounds pour comparaison ?)
* Peut-on trouver un estimateur optimal pour Eve ? (meilleur qu’une démodulation classique ?)
* On peut avoir un positive secrecy rate avec de l’OFDM classique sans AN : il suffit de faire un precoding avec optimal power allocation pour Bob et du coup, le canal de Bob est meilleur que celui d’Eve. Le problème, c’est qu’Alice ne peut pas connaître le SR sur lequel coder dans ce cas. L’ajout d’AN doit permettre d’assurer un certain rate quoiqu’il en soit !
* Si on envoie I et Q sur différentes antennes séparées, on n’est peut-être même pas obligé de communiquer sur le SR. On peut peut-être même éviter le secrecy coding (juste faire un pre-coding, mais c’est tout). Du coup, scénario à imaginer très vite !!
* Tracer la capacité du canal classique pour qu’on voit à quel point on perd en data rate with respect to non-secure communication => this ratio could also be an interesting key parameter to optimize !
* Étendre le schéma à du 1 vers N (broadcast). Optimiser l’AN pour que la data (ou les data, avec du symbol precoding pour faire du SDMA) soit intelligible aux N utilisateurs, mais qu’il y ait toujours bien du bruit partout ailleurs)
* Utiliser les résultats analytiques qui existent pour prendre en compte la corrélation spatiale des canaux, et donc la corrélation entre He et Hb (pour un nombre de taps donné) et ainsi plotter des map de BER en fonction des différentes distributions d’AoA qui donnent des résultats analytiques sur la corrélation.
* ID papier journal : après la dérivation de alpha\_opt, bien expliquer avec des phrases de quels termes/features il dépend et insister sur ce que cela implique pratiquement (non connaissance du SR à Alice si on ne connaît pas la puissance de He est un problème…). Tous les termes intermédiaire K, T, etc. devraient comporter le subscript E ou B, pour que le lecteur voit directement la dépendance de chaque terme. 3 paramètres à étudier : noise, diversity, channel power : take one of these parameters being constant between Eve and Bob and study what happens when the 2 others vary with a given ratio bw Eve and Bob => so 3 situations. Check then when all 3 vary when Eve has always the best values => worst case scenario.
* Faire 2 scénarios : A) trouver un scénario où on peut assurer une limite inférieure de SR mais qui est garanti => sécurité optimale. B) trouver un scénario où on ajoute la sécurité qu’on peut sans être gourmand en énergie (là, si on fait des choses dans le côté MU, on aura besoin de personnes faisant du codage.)
* Trouver le worst case scenario pr le SR. Quel est le parametre qui fait changer le SR le plus rapidement: la diff de puissance entre He et Hb ou la diff de correlation ?
* S’associer à des gens qui font du BF MU (Francesco Guidi ?) dans le contexte de la 5G pour calculer le SR apporté par le fait qu’il y ait plusieurs utilisateurs et que d’une certaine manière, cela apporte de la sécurité intrinsèque au schéma (par contre dans ce cas, de quelle sécurité parle-t-on ? car pas de codage spécifique au débit du SR pour assurer une secrecy parfaite, mais simplement un brouillage des autres utilisateurs sur l’utilisateur de base… Comment qualifier cela ? On rajouterait ou pas de l’AN en fonction de qu’achieve déjà le BF MU classique (si il y a beaucoup d’utilisateurs, peut-être pas la peine, si peu, alors oui).
* En fonction de ce que donne les dérivations en cours avec He et Hb qui ont des puissances différentes, essayer ensuite de se fixer un scénario comme suit. On calcul et on trace la CDF correspondant à la probabilité d’atteindre une perfect secrecy en utilisant un rate donné. Les statistiques seraient obtenues à partir de vrais canaux. L’idée serait ensuite de trouver une corrélation entre les statistiques du canal de Bob et le rate auquel on assure une perfect secrecy. Du genre, si le canal de Bob affiche une corrélation fréquentielle inférieure à XX, alors on peut communiquer secrètement à un rate de XXbit/s. Essayer de faire ça dans le contexte de la 5G où pour sécuriser la communication, on utilise BOR blocs ressources supplémentaires (en fréquence).
* Si le canal fréquentiel présente de la corrélation, on pourrait jouer sur les emplacements des 1 et des -1 de la spreading matrix. Peut-être aussi en fonction de la puissance dans chaque sous-porteuse et aussi en fonction du ratio de puissance entre le signal et l’AN
* Si notre schéma peut toujours donner un positive secrecy rate pour Bob à la seule condition que Hb soit plus décorrélé que He, possible de faire une antenne pour Bob avec plein de scatterers autour de lui pour assurer une faible corrélation fréquentielle => calcul de la position des scatterers intéressant à faire (dans la voiture par exemple, on a assez d’espace pour mettre des scatterers. Mais Eve pourrait en avoir beaucoup aussi. Mais il suffit peut-être que les corrélations soient égales)
* Essayer de décliner la technique pour plusieurs scénarios : dans l’IoT, la connaissance du canal de Bob doit être limité. D’ailleurs, l’OFDM est peut-être un peu groumant pour un node. Pour le VLC, canal ultra riche en MP, donc cool pour nous. Mais l’OFDM doit être différent car pas d’IQ ? quel schéma pour l’IR-UWB du standard BAN ? etc. Reprendre les applications de la review et voir quels collègues travaillent là-dessus pour leur proposer la PLS.
* Quid de la sécurité dans le champ proche de l’antenne ? tester les canaux avec les équations de champ d’un dipôle ou autre. Peut-on utiliser la « diversité » du champ proche d’une antenne pour ajouter de la sécurité sur des communications champ proche très faible fréquence ? Peut-être que grâce à toutes les composantes de champ (en r2, r3, etc.), les canaux entre deux récepteurs en champ proche sont décorrélés même si environnement LOS ? (et si l’antenne n’est pas à symétrie de révolution, ce qui doit souvent être le cas en champ proche, non ?)
* pas de sens d’assurer un SINR a bob puis de mettre l’énergie restante dans l’AN: seul un code achieve perfect secrecy (optimiser le sr reste le mieux). Car dans cette approche, on considère de ne pas utiliser un code pour garantir le SR. Garantir un SINR à Bob n’est pas directement lié aux performances (taux de modulation, etc.) de la communication que l’on va pouvoir atteindre sur Bob car cela dépend du canal d’Eve, et le code pour communiquer avec Bob sera établi en fonction du SR
* si Eve est capable d’estimer l’AN, quelles sont ses perf ? (1/ elle connait le canal de bob, 2/ elle connait l’AN ;une séquence aléatoire ne l’est jamais totalement (dixit computer science), 3/ si elle connait les deux, c’est mort non ? Comment Eve peut estimer son propre canal avec une séquence aléatoire ? Peut-être en utilisant juste les preamble et du learning?
* Voir la robustesse de notre schéma : mauvaise estimation du canal influe comment sur la liaison et la sécurité ?
* Le canal de Bob peut être connu par Eve (car Bob doit le donner à Alice si Alice ne fait pas l’estimation du canal elle-même)
* Trouver une procédure pour analyser si un schéma est robustesse d’un point de vue sécurité ou non (par exemple, comparer en calculant la corrélation les symboles reçus au niveau de l’eavesdropper et les vrai symboles (ou les symboles reçus au niveau de Bob)
* Analyse de l’influence du canal sur la PLS : Simuler des canaux outdoor urbains avec François, et comparer des méthodes de PLS dans différents scénarios (faire des map spatiales de SR et BER dans des cas où Eve est normal user ou vraiment eavesdropper puissante !). Étudier 3 cas : canal statique, canal statique où seul Bob se déplace, et canal dynamique où Bob se déplace). Regarder instantaneous SR et ergodic SR.
* Possibilite de faire une covert communication avec notre scheme. Le bruit doit etre orthogonal a bob mais doit etre une data intelligible a eve (ie, la covert data). Contraintes supp ds le calcul de w
* **Investigate « signature antennas » :** the radiation pattern is quite chaotic and precoding is done in such a way that only the recombination of all multipath convolved with this pattern cancel the AN (or just investigate the benefit of using such a chaotic antenna of Bob, and not at Eve, to see if it decreases the frequency correlation of the channel and thus improve the PLS. Perform ray-tracing simulations and measurements to check that).
* **Rajouter le ratio de puissance entre He et Hb pour justifier de refaire tous les calculs dans le papier journal. Observer ensuite l’alpha opt et voir s’il dépend ou non de ce ratio (le SR sûrement mais le alpha opt ?) Pareil si on suppose que Bc est différente entre He et Hb ?? Y a t’il un SR minimum garantie ? Est-ce que le nouveau schéma IQ peut garantir un minimum de SR ?**
* **New scheme :** une fois que l’on connaît le canal, on envoie I et Q sur des sub-carriers de manière séparée. Après despreading, on retrouve des symboles complexes bons chez Bob, mais chez Eve, après despresding, la quadrature IQ n’est pas respectée (faire attention : le gain sur I et Q sera à égaliser différemment pour qu’il soit identique sur I et Q. Un BOR de 2 ne donnera pas vraiment de gain dû au TR, perte de SNR, mais pas de perte pour l’AN. A étudier. (faire aussi I et Q sur plusieurs antennes avec précodage, plus de dimensions…). Ici, on perd le gain dû au TR (pas de débit par rapport à Globecom), sauf si BOR>=4 (mais quand même gain TR 2 fois plus faible par rapport à Globecom), mais dans un canal flat où le gain TR est assez faible, là on gagne à pas mettre d’AN. Du coup, compromis à faire en fonction de l’état de canal.
* Comment assurer un certain SR ? Le problème est si on considère Eve noiseless, si son canal est beaucoup plus fort que celui de Bob, il n’est peut-être pas toujours possible d’obtenir un SR positif… (AN n’est peut-être pas suffisant) En fait, il semblerait que si car l’effet du AN sur Eve est en HE^2 alors que l’effet du signal est en HE.HB\*. => étudier le cas limite : abs(HB) négligeable devant abs(HE) (cad le cas ou Eve est collée à la station de base et Bob en est loin).
* Refaire la dérivation du SINR et du SR quand Eve a des capabilities de higspeed processing et où donc elle peut égaliser sous-porteuse par sous-porteuse avant le despreading.
* **Calcul de W= > creuser des optima en fonction des contraintes/critères (si Eve connaît le canal de Bob, si corrélation non constante sur la bande de fréquence, variance non constante sur la bande/allocation de puissance en fonction des sous-porteuses. Il existe des algo pour optimiser la capacité de la com. Faire pareil pour le SR…). Épuiser le scénario « on ne connaît pas Eve »**
* Regarder les standards 5G utilisant OFDM ou similaires et regarder combien de sous-porteuses on peut utiliser. Dans la technique TR, on n’est pas obligé de prendre des sous-porteuses adjacentes. Si on en a 20 à choisir parmi 500, on peut maximiser l’espacement pour faire en sorte que les sous-porteuses redondantes soient le plus décorrélées possible. On pourrait même imaginer utiliser plusieurs sous-bandes (e.g., @ 900MHz et @ 2.6GHz) si le standard le permet
* **Etudier la faisabilité de la PLS : si Eve a no noise, à partir de quel niveau de noise a bob, aucun SR n’est possible ? Mettre une variable Ke ou Kb qui représente la puissance du canal.**
* **Calcul des SINR en fonction de la corrélation fréquentielle du canal possible ?**
* Calculer le SR et alpha optimal en fonction du canal qui est connu à Alice (Prendre en compte les corrélations entre random variable pr être plus précis, en considérant plusiurs types de canaux)
* Multicast
* Miso: 1/ juste pr faire du gain BF en plus 2/ pr ajouter du an sur les multiples antennes. Le AN devient une matrice (antennes x U), et dont l energy peut etre mise plus sur les antennes ou plus sur U, ou un compromis
* Analyse de canaux corrélés (montrer notamment l’impact des différentes stratégies de la matrice AN)
* Multi-utilisateurs : chaque utilisateur peut agir comme du bruit pour les autres. Donc considérer (ou évaluer) qu’un certain taux de secrecy est déjà assuré de base dans ce cas de MU-BF : calculer le SR en fonction du nombre d’utilisateur adressé. Sachant cela, déterminer quelle est la meilleure technique à utiliser pour atteindre le SR voulu (rajouter s’il le faut de l’AN).
* Donner une métrique simple pour ajuster les secrecy requirements vis-à-vis des attentes des couches supérieurs.
* On risque d’avoir du mal à faire accepter l’idée du PLS car on manque peut-être d’un backgorund théorique comme en crypto (voir ce qu’ils ont eux).
* En fonction des statistiques du canal, dire à priori si la communication peut être secure ou pas

**NEW IDEA OCT-NOV 2020 :**

* Tracer la SR sur une map obtenu par ray tracing. Et là on pourrait montrer des résultats du genre, xx% des emplacements, le SR est au-dessus de YY (donc pas ergodic, point spatial par point spatiale sans variation temporelle du canal).
* Dérivation modèle MIMO hybrid AN sans aucune correl pour voir si c’est possible d’assurer du SR ou non.