Analysis of Anti-Eavesdropping Performance of Spatially Selective Modulation in an Indoor Environment

Hitoto YONAWA,* Hisato IWAI,* and Shinsuke IBI*

(Received March 10, 2023)

As a physical layer security technique, we have proposed spatially selective modulation (SSM) which consists of multiple transmitting antennas and a single receiving antenna. In the method, the modulated signal is decomposed into multiple phase-modulated signals having constant amplitude, and the signals are transmitted from each of the transmitting antennas. Properly controlling the phase of the transmitted signals allows only at the location of the legitimate receiver to receive the desired modulated signal. The previous study on SSM has used a statistical channel model assuming Rayleigh fading for the quantitative analysis of the performance. In this paper, the propagation characteristics in an indoor environment are calculated by the ray-tracing by which the performance of SSM for spatial geometry and the distribution of the transmitter and the receiver can be evaluated. Based on the characteristics obtained from the analysis, the secret transmission performance was evaluated, and the effectiveness of SSM was verified in the assumed environment.

Key words: physical layer security, secure information transmission, radio wave propagation, ray-tracing, indoor environment

キーワード：物理層セキュリティ，秘密情報伝送，電波伝搬，レイトレーシング，室内環境

室内環境における空間選択性変調方式の盗聴耐性に関する分析

與縄 洋斗，岩井 誠人，衣斐 信介

1. はじめに

近年，無線技術の急速な普及に伴い盗聴対策技術の重要性が高まっている．無線通信における盗聴対策は，共通鍵暗号方式や公開鍵暗号方式といった，計算量的安全性に基づく暗号技術が一般的である[1,2]．これらの暗号方式では，伝送する情報に対してある種の鍵を導入することで通信の機密性を確保しているが，暗号化された情報は第三者も受信可能であるため解読される危険性がある．また，暗号・復号化のための演算処理が大きいため，計算能力の低い移動通信機器に適用する際に問題となる場合がある．

そこで，最近では物理層における情報理論的安全性に基づく無線セキュリティ技術が注目されている[3]．この技術の代表的なものとして，電波伝搬特性を活用した秘密鍵共有方式[4]や秘密情報伝送方式[5]が挙げられる．これらの電波を用いた方式では，電波伝搬特性の可逆性や場所依存性を活用することで無線通信の機密性を確保しており，第三者が正規送受信局間の電波伝搬特性を推定することが困難であることを安全性の根拠としている．

* Faculty of Science and Engineering, Department of Electronics, Doshisha University, Kyotanabe, Kyoto, 610-0321, Japan
Telephone: +81-774-65-6267, Fax: +81-774-65-6801, E-mail: iwai@mail.doshihsa.ac.jp

秘密情報伝送に関する方式の一つに，所定の方向に存在する正規受信局においてのみ，所望の変調信号を形成する指向性変調(Directional Modulation)が提案されている[6,7]．この方式では，複数の送信アンテナによる送信位相を適切に制御することで，方向的に機密性を持つ伝送を行うことが可能となる．しかし指向性変調では見通し内環境を対象としているため，陸上移動通信のような見通し外，マルチパス伝搬環境では適用することが難しい．

そこで，指向性変調と近い構成を有し，マルチパス環境にも適用可能な秘密情報伝送方式として，所定位置にある正規受信局においてのみ所望の変調信号が形成される空間選択性変調方式(SSM: Spatially Selective Modulation)が提案されている[8]．過去のSSMの性能評価[8-10]では，それぞれのチャネルが独立なレイリー分布に基づく統計的なチャネルモデルを用いて評価されている．SSMに限らず，物理層セキュリティを確立するための技術方式では，統計モデルを用いた理論評価を主体とするものが多く，正規受信局や盗聴局の位置関係等，現実的な環境モデルを設定した評価はあまり行われていない[11]．

そこで本論文では，実環境を想定した環境モデルにおいて，決定論的手法であるレイトレーシングにより伝搬特性を求め，SSMの秘密伝送性能を評価する．これにより，送受信位置や環境構造といった個々の環境下における盗聴耐性の空間分布等を評価することが可能となる．本論文では，具体的な環境モデルとして，什器の無い室内空間を想定して評価を行い，文献[8-10]で示されるようなSSMの秘密伝送性能を定量的に分析し，想定環境下における有効性を検討する．また，空間的評価により得られるSSMの盗聴耐性に関する分析を行うことで，想定する室内環境下において，秘密伝送性能が劣化するような地点の解析をするとともに，盗聴耐性を改善することができる方法についても検討を行う．

2. 空間選択性変調方式(SSM)

2.1 SSMの概要

空間選択性変調方式(SSM)は，所望の受信局位置に対して選択的な秘密情報伝送を実現する方式である．

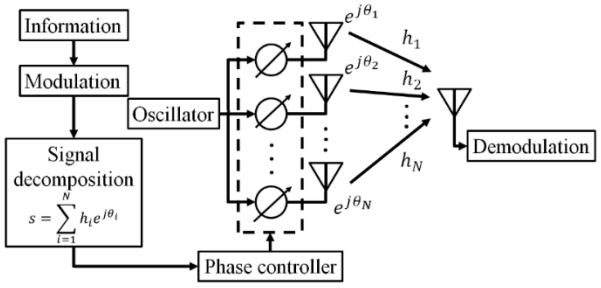


Fig. 1. Configuration of SSM.

伝送システムは複数(N とする)の送信アンテナと単一の受信アンテナで構成される．この方式の構成例をFig. 1に示す[8]．なお本論文では，送信局が情報送信の対象とする所望の受信局を正規受信局，それ以外の第三者の受信局を盗聴局と記述する．また，正規送受信局，盗聴局を含む全伝搬路はマルチパス環境であるとする．

上記のシステムにおいて，各送信アンテナから送信される信号は定振幅の位相変調信号であり，ある受信位置に対して，各送信・受信アンテナ間の伝搬チャネルの振幅・位相変動を受けた信号が空間的に合成され，一つの受信シンボルが形成される．SSMでは送信局-正規受信局間の伝搬チャネル係数に基づく信号分解を送信側で取り入れることで，正規受信局で所望の変調シンボルが再形成されるように送信信号の位相を制御する．一方盗聴局では，マルチパス環境における電波伝搬特性の場所依存性により，正規受信局とは異なる伝搬チャネル係数を有するため，所望の変調シンボルは再形成されない．これを具体的に示すと，まず情報信号を変調した変調シンボル s は，i 番目の送信アンテナと正規受信局アンテナ間のチャネル係数h_i $(i = 1, 2, \cdots N)$に基づき，次式を満たすように N 個の位相変調信号 $\exp(j\theta_i)$に分解される．

$$s = \sum_{i=1}^{N} h_i e^{j\theta_i} \tag{1}$$

各アンテナから送信される $\exp(j\theta_i)$が，チャネル係数h_iを経て空間上でベクトル合成され，正規受信局で変調信号 s が生成されるよう送信位相θ_iが決定される[8]．この送信位相の具体的な決定法は，2.3 節に記している．それに対して盗聴局では，正規受信局とは異なるチャネル係数$h_{e,i}$を有することから，変調シンボ

ル s が正しく形成されない.

SSM では，このようにして受信位置に対して選択的な秘密情報伝送が実現される.

2.2 信号分解の実現条件と変調余裕度

2.2.1 信号分解の実現条件

SSM では，指向性変調と同様に定振幅信号を取り扱うため，所望の変調シンボル s を複数の位相変調信号に分解するには，正規局間のチャネル係数がある条件を満たさなければならない. まず, 正規局間のチャネル係数を以下の条件を満たすように並べ替える. このような並び替えを行っても, 以下の説明の一般性は失われない.

$$|h_1| \geq |h_2| \geq \cdots \geq |h_N| \tag{2}$$

この条件下において, 次の条件を満たす場合に, 信号分解が可能となる.

$$\sum_{i=1}^{N} |h_i| \geq |s_{\max}| \tag{3}$$

$$|h_1| - \sum_{i=2}^{N} |h_i| \leq |s_{\min}| \tag{4}$$

なお，$s_{\max}$は所望の変調シンボルの最大振幅点，$s_{\min}$は最小振幅点をそれぞれ表す.

これらの条件は，SSM の送信信号が定振幅であることに起因する. 信号分解は, 各送信アンテナからの受信信号のベクトル和により変調シンボル s を表現することと等価であるため，ベクトル和で表現可能な範囲は各チャネル係数の大きさに依存する．その最大範囲は，各受信信号$h_i \exp(j\theta_i)$が全て同相となる場合であり，信号分解により所望の変調シンボルを表現するには，この最大範囲が変調シンボルの最大値$|s_{\max}|$以上である必要があることから，式(3)が信号分解の一つの条件となる．同様に，式(4)はベクトル和で表現可能な最小範囲に関する条件を表している. 16 QAM を例としてこれらの条件を図示すると Fig. 2 のように表すことができる. つまり, 図中の灰色の円環領域内に全ての変調信号点が存在する場合に限り，信号分解が可能となる.

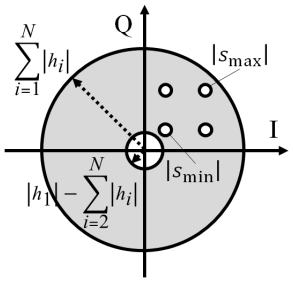


Fig. 2. Area where signal decomposition is possible.

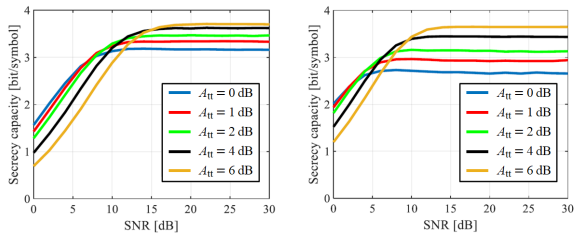
本論文では, 信号分解が可能となる, つまり正規受信局におけるチャネル係数が式(3)，式(4)の条件を満たす割合を実現率，信号分解ができない割合を非実現率と定義する．これらは SSM の伝送性能を評価する際の指標となり，送信アンテナ数を増加させると非実現率が低下することが確認されている [10].

2.2.2 変調余裕度

式(3)の等号が成立する場合，すなわち変調シンボルの最大値$|s_{\max}|$を信号分解する場合には，位相θ_iの組み合わせは全て同相となり，一意に決定されることとなる．一方，式(3)の右辺を左辺より小さく設定すると，θ_iの組み合わせは一意ではなくなり，組み合わせの選択に自由度が生まれる. その結果, 同一シンボルに対してもθ_iを変化させることが可能となり，例えば，盗聴局の受信信号を 1 シンボル毎等で時間的に変化させることが可能となる．これにより守秘性を高めることができるが，その一方で，$|s_{\max}|$を小さく設定することは，信号分解の実現率や雑音に対する伝送品質を低下させることになる．このような$\sum_{i=1}^{N}|h_i|$に対する$|s_{\max}|$の余裕度を表すパラメータを変調余裕度A_{tt}と定義し，次式で表す.

$$A_{\mathrm{tt}} = \frac{1}{|s_{\max}|} \sum_{i=1}^{N} |h_i| \tag{5}$$

変調余裕度に関する評価の一例として，従来の評価モデルである，レイリーフェージングに基づく統計チャネルモデルにて，秘密保持容量 *SC* (Secrecy capacity)に対する変調余裕度の特性を Fig. 3 に示す. 図の横軸は信号対雑音比 SNR(Signal to Noise Ratio)を表しており，この評価では，アンテナ 1 本当たりの



(a) N=4　　(b) N=8

Fig. 3. Characteristics of secrecy capacity for A_{tt}.

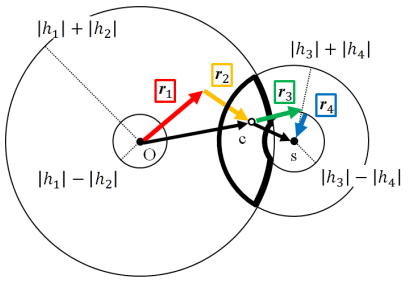


Fig. 4. Concept of signal decomposition (N=4).

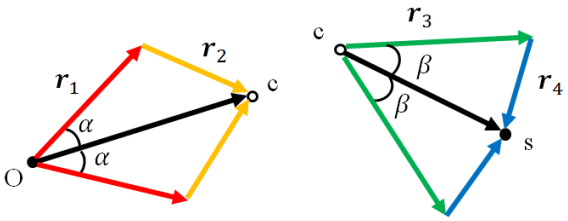


Fig. 5. Signal decomposition of vector $\overrightarrow{\mathrm{Oc}}$ and vector $\overrightarrow{\mathrm{cs}}$.

平均送信電力対受信機雑音電力比と定義している．また，受信局における伝搬チャネル係数は平均電力が 1 となるように規格化されている．なお，秘密保持容量とは，第三者(盗聴局)に情報を漏らさずに通信を行うことができる通信路容量を意味する．本論文では，2 値のデータを取り扱う 2 元対称通信路を仮定して秘密保持容量を求める．正規受信局のビット誤り率を p，盗聴局におけるビット誤り率を p_e とすると，秘密保持容量 SC は次式で表される [9]．

$$SC = H_b(p_e) - H_b(p) \tag{6}$$

なお，$H_b(p)$はエントロピー関数であり，次式で与えられる [12]．

$$H_b(p) = -p\log_2 p - (1-p)\log_2(1-p) \tag{7}$$

Figure 3 から，SNR の大きさに応じて，適切な変調余裕度A_{tt}の値が異なるので，対象環境に応じて適宜設定を行う必要があることがわかる．また，送信アンテナ数を増加させると，より低い SNR の領域でA_{tt}を高く設定することができる [9]．

2. 3 信号分解における送信位相の決定法

ここでは，信号分解における送信位相θ_iの決定法について示す．例として，送信アンテナ数 N=4 の場合における信号分解の概念図をフェーザ表示で Fig. 4 に示す．

まず，長さが各チャネル係数の絶対値$|h_i|$と等しい 4 本のベクトル $\boldsymbol{r}_i$ $(i = 1, 2, \cdots 4)$を考える．なお，各チャネル係数h_iは式(1)の条件を満たしているものとする．信号分解は原点 O から変調シンボル点 s に至るベクトルをこの 4 本のベクトル$\boldsymbol{r}_1$，$\boldsymbol{r}_2$，$\boldsymbol{r}_3$，$\boldsymbol{r}_4$の和で表現することと等価であり，伝送システムにおいてベクトル$\boldsymbol{r}_i$は各送信アンテナからの受信信号を意味する．この状態を実現するために，信号分解の実現条件に基づき「原点 O を中心とする，半径$|h_1|+|h_2|$の円と半径$|h_1|-|h_2|$の円で囲まれた円環領域」と「変調シンボル点 s を中心とする，半径$|h_3|+|h_4|$の円と半径$|h_3|-|h_4|$の円で囲まれた円環領域」が重なる領域(図の太枠で囲まれた領域)からランダムに 1 点を選択し，その点を c とする．これらの円環領域は，それぞれベクトル$\boldsymbol{r}_1$，$\boldsymbol{r}_2$，及び$\boldsymbol{r}_3$，$\boldsymbol{r}_4$の 2 本のベクトルの合成で表すことができる領域を意味するため，それらの円環領域が重なる部分に存在する点を選択することで，原点 O から変調シンボル点 s までのベクトルを，4 本のベクトル$\boldsymbol{r}_1$，$\boldsymbol{r}_2$，$\boldsymbol{r}_3$，$\boldsymbol{r}_4$で表現することができる．

N=4 の場合では，Fig. 5 に示すようにベクトル$\overrightarrow{\mathrm{Oc}}$を 2 本のベクトル$\boldsymbol{r}_1$，$\boldsymbol{r}_2$を用いて表現すればよく，2 通りの分解方法が存在する．ここで，角度αは余弦定理から求められ，次式で表される．

$$\alpha = \cos^{-1}\left(\frac{\left|\overrightarrow{\mathrm{Oc}}\right|^2 + |h_1|^2 - |h_2|^2}{2\left|\overrightarrow{\mathrm{Oc}}\right||h_1|}\right) \tag{8}$$

これを利用することで，2 本のベクトル$\boldsymbol{r}_1$，$\boldsymbol{r}_2$の偏角φ_1，φ_2が求まる．なお，式(8)に示す角度αの符号は，信号分解の選択性を増加させるため，変調シンボル毎にランダムに設定する．

$$\varphi_1 = \mathrm{Arg}\left(\overrightarrow{\mathrm{Oc}}\right) \pm \alpha \tag{9}$$

$$\varphi_2 = \mathrm{Arg}\left(\overrightarrow{\mathrm{Oc}} - \boldsymbol{r}_1\right) \tag{10}$$

同様にして，点 c から変調シンボル点 s に至るベクトル$\overrightarrow{\mathrm{cs}}$も 2 本のベクトル$\boldsymbol{r}_3$，$\boldsymbol{r}_4$を用いて表現することで，各ベクトルの偏角$\varphi_3$，$\varphi_4$が求められる．

$$\beta = \cos^{-1}\left(\frac{|\overrightarrow{\mathrm{cs}}|^2 + |h_3|^2 - |h_4|^2}{2|\overrightarrow{\mathrm{cs}}||h_3|}\right) \tag{11}$$

$$\varphi_3 = \mathrm{Arg}\left(\overrightarrow{\mathrm{cs}}\right) \pm \beta \tag{12}$$

$$\varphi_4 = \mathrm{Arg}\left(\overrightarrow{\mathrm{cs}} - \boldsymbol{r}_3\right) \tag{13}$$

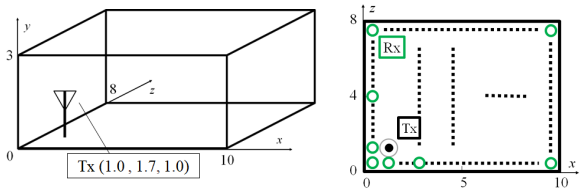
最終的に，各送信アンテナから送信される位相変調信号の位相θ_iは，ベクトル$\boldsymbol{r}_i$の偏角φ_iから各チャネル係数の偏角 Arg(h_i)を減算することで求められる．

3 章および 4 章における評価では，送信アンテナ数 N として 8 の場合も行っている．N=8 の場合の送信位相決定法は，基本的に N=4 の場合と同様である．8 個の正規局間のチャネル係数を式(2)に沿って並べ替えた後，Fig. 4 と同様に h_1～h_4のグループで合成可能な円環領域(半径が$\sum_{i=1}^{4}|h_i|$以下，$|h_1| - \sum_{i=2}^{4}|h_i|$以上の円環領域)と h_5～h_8のグループで合成可能な円環領域(半径が$\sum_{i=5}^{8}|h_i|$以下，$|h_5| - \sum_{i=6}^{8}|h_i|$以上の円環領域)が重なる領域からランダムに中間点 c’を決定する．そのあと，原点 O から c’へのベクトル$\overrightarrow{\mathrm{Oc'}}$，及び，c’から変調シンボル点 s までのベクトル$\overrightarrow{\mathrm{c's'}}$をそれぞれ 4 個のチャネルの合成で表す方法は，$N$=4 の場合の位相決定方法と同じである．

3. レイトレーシングによる SSM の特性評価

3.1 解析環境

Figure 6 に示す 10 m×3 m×8 m の室内空間においてレイトレーシング解析[13]を行った．同図(a)は三次元斜視図，(b)は x-z 平面図で表現しており，什器の無い全面コンクリートの簡易な環境を想定している．このレイトレーシング解析には，比較的計算が簡易かつ，厳密に受信点に到達するレイを探索可能なイメージング法を採用する．



(a) Elevational view. (Unit: m) (b) Plan view of x-z.

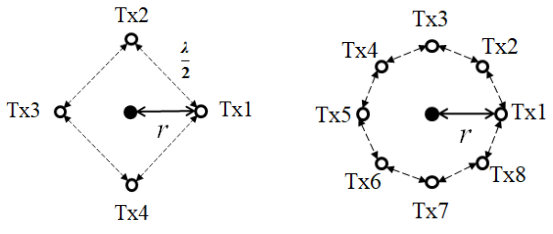
Fig. 6. Analysis environment for ray-tracing.

Table 1. Analysis parameters.

Measurement frequency	2.4 GHz
Modulation system	16 QAM, 64 QAM, 256 QAM
Number of transmitting antennas	4, 8
Number of receiving antennas	1
Room size	10.0 m × 3.0 m × 8.0 m
Coordinate of transmitting antenna	(x, y, z) = (1.0 m, 1.7 m, 1.0 m)
Coordinate of receiving antenna	Equally placed on grid points (0.05 m)
Antenna arrangement	Circular
	Radius: 0.0221 m, 0.0442 m, 0.0884 m
Maximum number of reflections in ray-tracing	4
Material constant of wall (concrete)	Relative permittivity: 6.76
	Conductivity: 0.0023 S/m

解析では，送信局を固定位置(1.0, 1.7, 1.0) m，受信局を y=1.7 m の室内平面内の 5 cm 間隔格子点上に配置し，各受信点での伝搬特性をレイトレーシングにより計算する．得られた伝搬特性を用いて計算機上で SSM を構築し，室内環境における SSM の秘密伝送性能を評価する．SSM の盗聴耐性に関する評価は，盗聴局のビット誤り率(BER: Bit Error Rate)を主な指標とする．

正規受信局，及び盗聴局は上記の伝搬特性を計算した受信点の中から選択するが，基本的には一つの計算フローにおいて，正規受信局を一点に固定配置し，それ以外の受信点は全て盗聴局であるとして評価を行う．また，各正規受信局地点において，信号分



(a) S_4 (b) S_8

Fig. 7. Arrangement of transmitting antenna element.

解が実現できない場合は，その地点での送信は行わないものとする．解析に使用した諸元を Table 1 に示す．送信アンテナ数は 4，及び 8 と設定しており，その素子配置は Fig. 7 に示すように円形アレー配置とし，それぞれ S_4，S_8 と呼ぶこととする．また，その配置半径は．隣接アンテナ素子との間隔が想定する周波数 2.4 GHz において半波長($\lambda/2$)となる値として，$r = \lambda/(2\sqrt{2}) = 0.0442$ m とする．変調方式は，特に記述がない場合は 16 QAM とする．なお信号対雑音比 SNR については，受信局の各位置で，信号電力(S)と雑音電力(N)の比(S/N)とする．実環境では，送信機からの距離の増加に伴って SNR は低下するが，この SNR の設定は全ての受信地点で SNR が一定であるという想定である．

また，伝送シミュレーションにおいて，各受信点に対する送信シンボル数は 100 とし，伝搬チャネルは送信側で既知であるとする．そのため，正規受信局から送信局に対して，伝搬チャネルの推定を目的としたパイロット信号は導入しない．ただし正規受信局では，伝搬チャネル係数に基づく振幅補償を行うため，送信局から正規受信局に対してパイロット信号の送信を行い，正規受信局でも伝搬チャネル係数の推定が正しく行われているものと仮定する．盗聴局では，送信局から正規受信局に対するパイロット信号を得ることができるものとし，そのパイロット信号を用いて受信信号の位相補償を行う．

3.2 伝送特性の評価

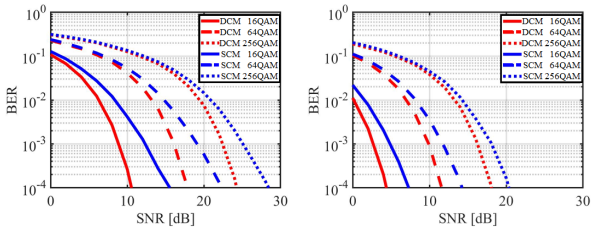
3.2.1 SNR に対する諸特性

正規受信局における SNR に対する BER 特性を Fig. 8 に，盗聴局における BER 特性を Fig. 9 に，それぞれ示す．正規受信局は，$(x, y, z) = (8.5, 1.7, 3.5)$ m の位置に固定配置している．一方盗聴局は，y=1.7 m 平面上の複数地点が評価対象であり，その位置ごとに結果が異なることから，この複数点に対する累積分布(CDF: Cumulative Distribution Function)を用いて結果を示している．

Figure 8 から，送信アンテナ数の増加により正規受信局の BER 特性が改善されることが確認できる．これは，アンテナ数の増加による送信ダイバーシチの効果が要因である[9]．また，レイトレーシングによる決定論的チャネルモデル(Deterministic Channel Model: DCM)と統計チャネルモデル(Statistical Channel Model: SCM)を比較すると，同一の SNR に対して DCM の方が低い BER 特性となっているが，これは今回想定した環境が厳密なレイリーフェージングモデルではなく，直接波の存在する環境であることに起因すると考えられる．

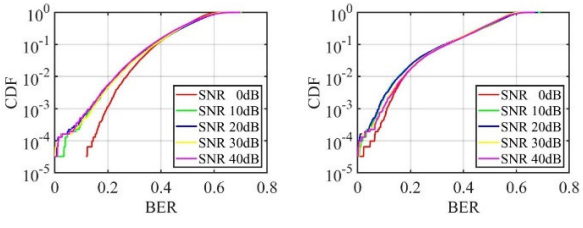
Figure 9 では，送信アンテナ数 N が 4，8 それぞれの場合において，盗聴局における SNR に対する BER の変化は小さい．今回の SNR の変化範囲では，盗聴局 BER への影響は，雑音電力の大きさによらず，SSM による盗聴局 BER を劣化させる働きが大きいため，SNR の変化による大きな影響は見られなかったと考えられる．ただし，N=4 の SNR が 0 dB の BER 特性は他の場合よりも大きい．この場合は，低 SNR 環境であり，その結果として盗聴局 BER が増加することを示しているが，同じ SNR でも N=8 の場合にはこの特性は現れていない．これは，盗聴局においても正規受信局と同様に，アンテナ数の増加が送信ダイバーシチ効果を拡大させており，低い SNR を補っているものと考えられる．

以上の結果より，SSM の盗聴耐性評価において雑音の影響は小さいと考えられる．つまり，SSM では



(a) N=4　(b) N=8

Fig. 8. Characteristics of BER at legitimate receiver.



(a) N=4　(b) N=8

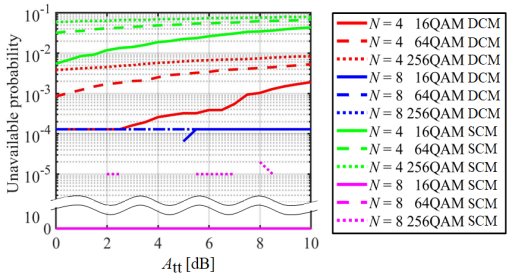
Fig. 9. Characteristics of BER at eavesdropper. (16 QAM)

雑音の大小に関わらず通信の機密性が確保されているといえる. 盗聴評価においては, 盗聴局にとって有利な設定を取り扱うことから，上記の結果を踏まえて，次節以降においては雑音の無い環境を想定した評価を行う.

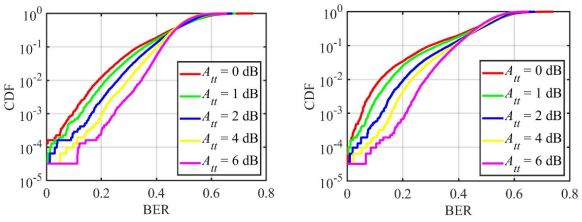
3. 2. 2　変調余裕度に関する諸特性

Figure 10 に，変調余裕度A_{tt}変化時の非実現率特性を示す．なお，同図の DCM は，正規受信局位置をy=1.7 m の平面内で 5 cm 間隔毎に変化させ，各地点においてレイトレーシングで計算した伝搬特性に基づき信号分解の実現可否を判定している．同図から，変調余裕度，及び多値数の増加により非実現率が増加することが確認できる．多値数が増加すると$s_{\min}$の振幅が小さくなり，式(4)で示される条件式を満たす確率が低下するためである．また，文献 [10]で示されるように，送信アンテナ数の増加によって非実現率が改善されることがわかる.

また DCM と SCM を比較すると，N=4 における DCM の非実現率が減少しているが，これは文献 [9]に示されるように, DCM では直接波の存在する環境下で解析を行っているためである．なお，DCM では，正規受信局が送信アンテナの極めて近傍に位置する場合があり，その地点では信号強度の偏りが大きくなり，実現不可となっていた．DCM，特に N=8 の場合に，非実現率が SCM より大きく，一定の値を有しているのはこれが原因である.



次に, 変調余裕度に対する盗聴局の BER 特性を Fig. 11 に示す．なお，正規受信局は 3.2.1 節と同様の位置に配置している. 同図から, 余裕度の増加により盗聴局 BER が低い値，例えば 0.2 以下となる割合が減少することが確認できる．これは，2.2.2 節で示したように，余裕度を増加させることで同一の変調シンボルに対しても送信位相の組み合わせを変化させることができることに起因する. これにより, 例えばある変調シンボルに対して偶発的に復調可能な伝搬チャネル係数を有する盗聴局においても，送信位相の組み合わせの多様性が増加することで，他の変調シンボルの復調が困難となる.



(a) N=4　　(b) N=8

Fig. 11. Characteristics of BER at eavesdropper for A_{tt}.

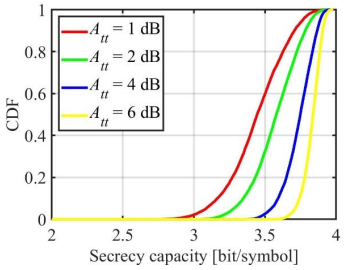


Fig. 12. Characteristics of secrecy capacity for A_{tt}.

変調余裕度は，上述のように実現率や正規受信局 BER 等の伝送特性, 及び盗聴局の BER 特性にも影響を与えるパラメータであり，変調余裕度に対する SSM の性能を評価するには, 2.2.2 節で示した秘密保持容量を評価指標に用いることで，伝送性能と機密性の双方を総合的に評価することが可能である．この秘密保持容量は, ある正規受信局位置に対して, 盗聴局位置毎に計算される．これを定量的に評価する目的で，正規受信局を室内 0.1 m 間隔毎に配置し，それぞれの正規受信局地点における盗聴局全地点平均の秘密保持容量を，各正規受信局における秘密保持容量の計算値とする. この計算フローにおいて, 変調余裕度を変化させ，各正規受信局における秘密保持容量値を計算した場合の CDF 特性を Fig. 12 に示す.

同図から, 変調余裕度の増加により, 想定環境内において秘密保持容量が大きい値となる割合が増加することがわかる．これは，Fig. 10 に示した変調余裕

度の増大に伴う非実現率の増加と比べて，Fig. 11 に示した盗聴局BERに及ぼす機密性の改善効果の方が，SSM の性能に与える影響が大きいことを意味する．また，Fig. 3 にも示したように，SNR が十分大きい場合には同様の特性が見られていることから，雑音の無い環境を想定した今回の結果でもこのような特性が得られたと考えられる．

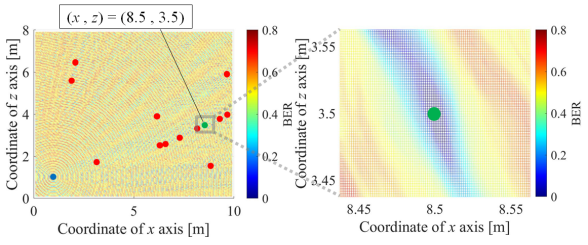
3. 3　SSM の空間分布に関する評価

3. 3. 1　盗聴局 BER の空間分布

盗聴局 BER の空間分布を Fig. 13 に示す．送信局は図の青点，正規受信局は緑点で示す位置に固定配置している．また，送信アンテナ数は 4 である．同図(a)は室内全体での空間分布，(b)は正規受信局近傍を拡大した分布を表している [14,15]．

(b)に示す正規受信局近傍では，マルチパスフェージング伝搬路の空間相関の観点からチャネルの相関が強く，盗聴局のBERが減少しているが，その範囲の正規受信局からの距離は半波長程度と小さく，その距離からの盗聴は現実的ではない．一方，(a)に示す正規受信局近傍以外では，空間全体にわたって盗聴局BERが0.4~0.6であり，十分な盗聴耐性が示されている．その一方で，同図に赤点で示す位置に盗聴局BERが0.1以下となる地点(以下，BER低下地点とする)が局所的に点在している．このようなBER低下地点では盗聴の危険性が高いため，詳細な分析を行う必要がある．

本論文では，盗聴耐性を定量的に評価することを目的として，BER 低下地点数の割合を BER 低下場所率(BDLP: BER decrease location probability)と定義する．BDLP は，想定環境内における受信点の総数に対する BER 低下地点の総数の比で与えられる．



(a) Whole space.　(b) Vicinity of legitimate receiver.

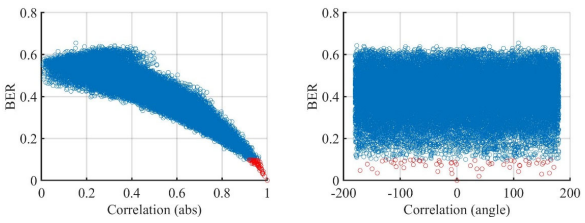
Fig. 13. Spatial distribution of BER at eavesdropper.

3. 3. 2　盗聴局 BER 低下地点の分析

3.3.1節で示した盗聴局BER低下地点について，分析を行った結果を示す．まず，送信アンテナ数N=4において，正規受信局の4つのチャネルと，盗聴局の4チャネルをそれぞれ一系列とし，各盗聴局位置におけるこのチャネル系列間の相関係数(複素数)を計算した．求めた相関係数と，各盗聴局位置におけるBERの関係性をFig. 14に示す[15]．同図の(a)は相関係数の絶対値，(b)は位相と盗聴局BERとの関係を散布図で表現している．また同図において，盗聴局BER低下地点に該当する結果については赤点，それ以外は青点で示している．

Figure 14(a)より，盗聴局では，相関係数の絶対値が大きい，つまり，正規受信局のチャネル系列と盗聴局のチャネル系列の相関が高いほど，盗聴局BERが低下する傾向が確認できる．この結果から，正規受信局チャネルと相関の強いチャネルを有する盗聴局では情報の傍受が可能であると推測できる．

また同図(b)では，盗聴局BERが低下する場合のチャネル複素相関の位相は一様に分布していることが確認できる．本論文では，盗聴局の受信設定として受信信号の位相補償を前提としており，例えば正規受信局のチャネル全てに一定の位相変動が乗算されたチャネルを有する盗聴局においては，位相補償により情報の復調が可能となる．



(a) Absolute value.　(b) Phase.

Fig. 14. Distribution of correlation coefficient between channels at legitimate receiver and channels at eavesdropper.

4.　SSM の性能改善に関する検討

4. 1　送信アンテナ配置半径に関する特性

ここでは，Fig. 7に示した送信アンテナの素子配置における，配置半径rに関する特性評価について述べ

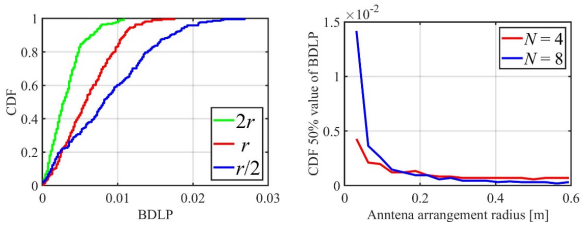
る．送信アンテナ素子の配置半径の変化により各送信アンテナ素子の位置が変化することになるため，各受信局のチャネル状況が変動し，SSMの機密性に影響を与えると推測される．そのため，まず配置半径とSSMの機密性を示す指標であるBER低下地点の割合(BDLP)との関係性を示し，SSMの機密性を向上できるような配置半径を明らかにする．

BDLPを定量的に評価するために，正規受信局位置を室内x-z平面全体にわたって変化させ，正規受信局位置毎にBDLPを計算し，環境内のCDF特性を求める．アンテナ配置半径を変化させることで，配置半径rに関するBDLPの特性を統計的に求める．

Figure 15(a)はアンテナ配置半径をr=0.0442 mを基準としてr/2, 及び2rに変化させた場合のBDLPのCDF特性を表す[14,15]．なお，送信アンテナ数Nは4である．同図から，アンテナ配置半径が大きくなるほど，想定環境下におけるBDLPが低い値となる確率，例えばBDLP<0.01となる確率が増加することが確認できる．

アンテナ配置半径とBDLPの関係性をより明確に示すために，Fig. 15(b)にアンテナ配置半径に対するBDLPのCDF50%値の特性を示す．同図から，送信アンテナ数Nが4，8のいずれの場合でも，アンテナ配置半径の増加に従いBDLPが減少することがわかる．つまり，アンテナ配置半径を増加させると，想定環境下におけるSSMの機密性が向上するといえる．

このアンテナ配置半径とBDLPの関係は，各送信アンテナと受信アンテナ間のチャネル相関に起因すると考えられる．送信アンテナの配置間隔が小さい場合，具体的には隣接アンテナ素子との間隔が半波長以下の場合，一般的にチャネルの空間相関特性により，各送信アンテナと単一の受信アンテナ間のチャネルの相関は強くなる[12]．その場合，想定環境内の全ての受信局において，各受信局が有するN個のチャネルは相関が強いものとなると推測される．これにより，環境内全域におけるチャネルの多様性が減少し，正規受信局と盗聴局のチャネルが近い値となり，環境内におけるBDLPが増加すると予測できる．



(a) CDF of BDLP. (N=4)　(b) CDF 50% value of BDLP.

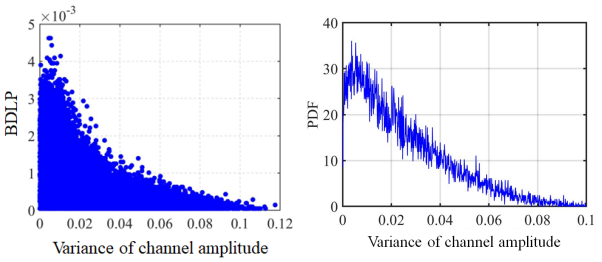
Fig. 15. Relation between BDLP and antenna arrangement radius.

4. 2　送信アンテナ選択方式

SSM の盗聴耐性を改善する方法として，Fig. 7(b)に示す 8 本の円形アレー送信アンテナ素子の内から，適切に 4 つのアンテナを選択して情報伝送を行うアンテナ選択方式を提案する．多数のアンテナから，少数のアンテナを適切に選択することで，送信電力等の伝送にかかるコストの抑制をはじめとして，Fig. 9 で見られたような，送信ダイバーシチによる盗聴局 BER 特性の改善効果を抑えることができる．なお，実際に伝送を行う場合を考慮して，送信アンテナの選択に使用可能な情報は正規受信局のチャネルのみとする．

正規受信局チャネルの振幅成分や位相成分に基づく情報と BDLP との間の関係について分析した．正規受信局におけるチャネルの振幅分散と BDLP との間に，Fig. 16(a)に示すような関係性が見られた．なお，送信アンテナ配置は S_4, 配置半径 r は標準値の 0.0442 m であり，同図の横軸の値であるチャネルの振幅の分散とは，次式で示される，全チャネル電力和の平方根による正規化チャネル振幅の分散 V である．

$$V=\frac{1}{4}\sum_{i=1}^{4}\left(\frac{|h_i|}{\sqrt{P_h}}-M_h\right)^2 \tag{14}$$



(a) Relation between variance V and BDLP.　(b) Distribution of variance V.

Fig. 16. Characteristics on variance V of channel amplitude.

上式において，P_hは受信局における 4 つのチャネルh_iの電力和，M_hは正規化振幅の平均値であり，それぞれ次式で計算される．

$$P_h = \sum_{i=1}^{4} |h_i|^2 \tag{15}$$

$$M_h = \frac{1}{4}\sum_{i=1}^{4} \frac{|h_i|}{\sqrt{P_h}} \tag{16}$$

Figure 16(a)から，正規受信局のチャネル振幅の分散値 V が大きくなるほど，想定環境下における BDLP が減少する傾向にあることが確認できる．これより，分散値 V が大きくなるように 8 本の送信アンテナから 4 本のアンテナを選択して情報伝送を行うことで，環境内の BDLP を低下させる，つまり，SSM の機密性を向上させることができると推測される．

なお，このように正規受信局のチャネル振幅の分散値 V と BDLP に関係性が見られる要因として，想定環境内における V の分布が関係していると考えられる．Fig. 16(b)は，正規受信局，盗聴局に関わらず，環境内の全ての受信局におけるチャネルの振幅分散 V に対する確率密度関数(PDF: Probability Density Function)を示している．同図より，V が大きくなるにつれて PDF が減少していることが確認できる．つまり，環境内において，V が大きい値を持つ受信点が少ないといえることから，正規受信局が V が大きいチャネルを有する場合には，盗聴局が正規受信局チャネルと同様に V が大きいチャネルを有する確率が相対的に減少し，結果的に BDLP が減少したと推測される．

上記の送信アンテナ選択法を用いて選択した素子配置を $S_{8C4,V}$ と表し，Fig. 7 に示した S_4，及び S_8 とともに，BDLP に関する CDF 特性を Fig. 17 に示す．同図から，想定環境内において，分散値 V を用いて送信アンテナを選択した方式 $S_{8C4,V}$ は，基準配置として設定した S_4，S_8 と比べて BDLP が低い値となることが確認できる．つまり，室内にわたって SSM の機密性を改善できているといえる．

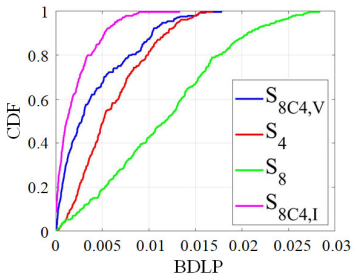


Fig. 17. BDLP for selection scheme of transmitting antenna.

一方で，同図に示す $S_{8C4,I}$ は，送信アンテナ素子 8 本のから 4 本を選択する組み合わせの内，BDLP が最小となる素子配置をカンニングにより選択した結果である．これと $S_{8C4,V}$ を比較すると，分散値 V による選択法にはまだ改善の余地があるといえる．

また，Fig. 17 では，S_4 と比べて S_8 は，環境内で BDLP が低い値となる割合が小さい結果となっていることが確認できる．本来であれば，送信アンテナの増加により受信局の有するチャネルの数が増加するため，チャネルの多様性が増すことになり，正規受信局と盗聴局のチャネルが偶発的に相関の高いものとなる確率が減少すると推測できる．言い換えると，送信アンテナ数の増加により BDLP が低下する割合が増えると考えられるが，この結果では，そのような傾向が見られていない．これは，アンテナ配置半径の大きさに起因するものであると考えられる．同図の結果では，アンテナ配置半径が S_4，S_8 共に標準値の 0.0442 m であり，アンテナ数が増加するほど隣接アンテナとの距離が近くなるため，送信アンテナ素子間のチャネル相関の上昇により，BDLP が増加したと考えられる．

5. 結論

本論文では，決定論的チャネルモデルであるレイトレーシング解析により，三次元室内環境における空間選択性変調方式(SSM)の伝送性能の評価，及び盗聴耐性向上に関する検討を行った．

伝送性能に関する評価では，従来の統計的チャネルモデルによる評価結果と同様に，今回の想定環境下においても正規受信局に対する選択的な秘密情報伝送の実現が確認された．

また，空間分布に関する評価では，室内全体にわたって盗聴局 BER が 0.4～0.6 と高い値を有することが確認された．一方，正規受信局近傍や正規受信局方向

において, 盗聴局BERが低下する地点も確認された.

上記の盗聴局 BER 低下地点の低減を目的として, 円形アレー送信アンテナの配置半径の変化や, 複数送信アンテナから適切にアンテナを選択するアンテナ選択方式を用いた場合における SSM の秘密伝送性能の評価を行ったところ, SSM の盗聴耐性が改善することが明らかとなった.

今回の研究では, 什器の無い見通し内環境環境での評価を行ったが, SSM の性質上, 見通し外の伝搬環境にも適用できるため, より実環境に近い解析モデルを用いて評価を行う必要がある.

本研究は, JSPS 科研費 JP21K040488 の助成を受けて行った. ここに記して謝意を表する.

参考文献

1) N. Sklavos and X. Zhang, *Wireless Security and Cryptography: Specifications and Implementations*, (CRC Press, Boca Raton, 2007).
2) 古原和邦, 今井秀樹, “線形符号の復号問題に基づいた強い意味で安全な公開鍵暗号方式”, 信学論(A), **J87-A**[7], 870-880 (2004).
3) 笹岡秀一, “電波伝搬特性に基づく物理層セキュリティ”, 信学技報, **115**[40], 13-18 (2015).
4) U. M. Maurer, “Secret Key Agreement by Public Discussion from Common Information”, *IEEE Trans. Inform. Theory*, **39**[3], 733-742 (1993).
5) H. Koorapaty, A. A. Hassan, and S. Chennakeshu, “Secure Information Transmission for Mobile Radio”, *IEEE Common. Lett.*, **4**[2], 52-55 (2000).
6) M. P. Daly and J. T. Bernhard, “Directional Modulation Technique for Phased Arrays”, *IEEE Trans. Antennas Propag.*, **57**[9], 2633-2640 (2009).
7) 栗山侑, 紀平一成, 大塚昌孝, 深沢徹, 米田尚史, “和差パターンを用いる指向性変調アレーアンテナの動的励振分布制御法”, 信学技報, **118**[504], 29-34 (2019).
8) 辻和輝, 笹岡秀一, 岩井誠人, “電波伝搬特性に基づく信号分解と空間ベクトル合成を用いた秘密情報伝送方式”, 信学論(B), **J100−B**[9], 782-794 (2017).
9) 福島大揮, 笹岡秀一, 岩井誠人, 衣斐信介, “送信アンテナ素子数の増加による空間選択性変調の性能改善”, 信学技報, **120**[179], 11-16 (2020).
10) D. Fukushima, H. Sasaoka, H. Iwai, and S. Ibi, “Evaluation of Performance Improvement of Space Selective Modulation by Increasing Number of Transmitting Antennas”, *IEICE Communication Express*, **9**[6], 207-212 (2020).
11) E. M. Vitucci, F. Mani, T. Mazloum, A. Sibille, and V. Degli Esposti, “Ray Tracing Simulations of Indoor Channel Spatial Correlation for Physical Layer Security”, *2015 9th European Conference on Antennas and Propagation* (*EuCAP*), Lisbon, Portugal, 1-5 (2015).
12) 三瓶政一, 前田忠彦, 岩井誠人, 市坪信一, 宮本伸一, 衣斐信介, 岡田実, ワイヤレス通信工学, (オーム社, 東京, 2014).
13) 今井哲朗, 電波伝搬解析のためのレイトレーシング法, (コロナ社, 東京, 2016).
14) H. Yonawa, H. Iwai, and S. Ibi, “Evaluation of Secret Transmission Performance of Spatially Selective Modulation”, *2022 International Symposium on Antennas and Propagation* (*ISAP*), Sydney, Australia, 183-184 (2022).
15) H. Yonawa, H. Iwai, and S. Ibi, “Analysis of Spatial Distribution of Secret Transmission Performance of SSM Using Ray-Tracing”, *IEICE Communication Express*, **X12-B**[6] (2023).