Vol.2015-DPS-163 No.20
Vol.2015-MBL-75 No.20
2015/5/29

無線伝送路情報を鍵として利用するセキュア通信方式の基礎研究

内藤 克浩[1,a)]　榊原 寛紀[2]　向井 洋介[2]　森 香津夫[2]　小林 英雄[2]

概要：無線信号は送信者の周辺に到達するため，所望の受信端末以外の盗聴端末も無線信号を受信可能である．そのため，無線信号の到達範囲内の盗聴者は，盗聴行為を発見されるリスクなしに，情報を容易に取得可能となる．現在の無線通信では，セキュリティ技術として，データリンク層・ネットワーク層などの上位プロトコルによる暗号技術を採用している．一方，暗号鍵の共有などを無線通信上で行うことは困難であることも知られており，物理層において所望の受信端末のみで復調が可能なセキュリティ技術の研究も近年行われている．本研究では，現実の通信環境はマルチパス通信環境のことが多く，無線伝送路特性は端末の場所により大きく異なる点に着目する．また，所望の受信端末への無線伝送路特性に合わせた信号を予め生成して送信するプレ等化技術を採用することにより，所望の受信端末のみが復調に成功するセキュア通信方式を提案する．数値例として，代表的なマルチパス通信環境において，所望の受信端末は正確に復調可能である一方，無線伝送路特性が異なる盗聴端末では，復調に失敗することをシミュレーションにより明らかにする．

キーワード：無線通信，物理層，セキュア通信，プレ等化技術，伝送路特性, IEEE 802.11a

1. はじめに

無線通信におけるブロードキャスト性は，セキュリティ技術と併用しない限り，安全ではないことが以前より指摘されている．そのため，無線信号が到達する範囲に存在する盗聴者は，発見されるリスクなく無線信号を傍受可能であり，伝送されている情報も確認可能である．無線通信では，データリンク層・ネットワーク層などの上位層において暗号化による対策が行われるのが一般的である．一方で，暗号化を採用するためには，暗号鍵を端末間で共有する手段が必要である．無線通信上で暗号鍵の共有を行うためには，暗号鍵を安全に配布，管理する枠組みが必要となるが，無線通信のブロードキャスト性により，実現は困難である．そこで，物理層の特性に着目することにより，物理層において所望の端末のみで復調が可能となるセキュリティ技術を実現する試みが進められている [1], [2].

物理層における基礎的なセキュリティ技術は，所望の受信端末が受信する信号品質と比べて，盗聴者が受信可能な信号品質を劣化させるものである．その結果として，盗聴者は無線信号を正確に復調することができず，情報の取得に失敗する．既存研究では，当初は送信用アンテナと受信用アンテナを各 1 本利用する SISO(Single-Input and Single-Output) システムを想定した方式が主流であり，送信アンテナを選択することにより，所望の受信端末における信号品質を改善し，その他の端末における受信品質を劣化させる方式も検討されている [3], [4]．近年では，複数の送受信アンテナを想定する MIMO(Multiple-Input and Multiple-Output) システムを前提とした方式が提案されている [5]．複数の送信アンテナを利用することにより，情報信号と人工雑音を同時に送信することが可能となり，安全性を改善している．なお，人工雑音を生成する際には，事前に特殊なコーディングを行うことにより，所望の受信端末は人工雑音を識別できる一方で，人口雑音を識別できない盗聴者は雑音の影響により復調処理を正常に行えない [7]．また，送信信号に指向性を持たせることにより，所望の受信端末における信号品質を改善する方法も提案されている [8], [9]．そして，近年ではセルラネットワークなどを想定した，より大規模な方式についての検討も始まりつつある．[10], [11] これらの方式では，物理層において新たな機能を追加する必要があるものが主流であり，既存の機器の設計を大幅に変更する必要がある．

[1] 愛知工業大学情報科学部
Faculty of Information Science, Aichi Institute of Technology, Toyota, Aichi 470-0392, Japan
[2] 三重大学大学院工学研究科電気電子工学専攻
Department of Electrical and Electronic Engineering, Mie University, Tsu, Mie 514-8507, Japan
[a)] naito@pluslab.org

本研究では，現実の通信環境は AWGN(Additive White Gaussian Noise) 環境のように安定した環境ではなく，多数のマルチパス波が存在するため，無線伝送路特性が場所により大きく異なることに着目する．無線伝送路特性は，場所が通信で利用する無線信号の半波長以上異なれば，一般的には独立して変化すると言われている．また，一般的な無線通信システムでは，このような無線伝送路特性の影響を受信側で取り除く等化処理を行うことにより，正しい復調処理を実現している．そのため，所望の受信端末のみが無線伝送路特性の影響を取り除くことが可能である一方，他端末は無線伝送路特性の影響を取り除けない方式が実現されれば，物理層による安全性を改善可能と考える．

本研究では，所望の受信端末との無線伝送路特性を予め推定することにより，送信端末から送信する信号を無線伝送路特性に合わせて送信するプレ等化技術を活用することにより，物理層におけるセキュア通信方式を提案する．無線伝送路特性を予め推定するためには，無線 LAN で規定される RTS/CTS(Request to Send/Clear to Send) などのデータパケットの送受信前に交換されるパケットを利用する．また，送信者は所望の受信端末において無線伝送路の影響を受けない信号が受信可能となるように，送信信号を推定した無線伝送路特性に応じて補正してから送信する．結果として，所望の受信端末では，無線伝送路の影響により，正確に復調可能な信号を受信できる．一方，盗聴者などは異なる無線伝送路の影響を受けることにより，復調可能な信号を受信できなくなる上，盗聴対象の端末間の無線伝送路特性が不明なため，等化処理も行うことができない．本研究では，IEEE 802.11a の仕様を想定したシミュレーションにより，代表的なマルチパス環境において，所望の受信端末は復調可能である一方で，盗聴者が復調誤りを起こすことを示す．

2. プレ等化技術を用いるセキュア通信方式

2.1 概要

本研究で提案する無線伝送路特性を鍵として利用するセキュア通信方式は，無線通信性能を特徴づける無線伝送路特性に着目したものである．一般に，端末間の無線伝送路特性は，同一周波数，同一時間では同一のものとなり，端末間の双方向通信は同一の無線伝送路特性の影響を受ける．一方，端末位置が通信周波数の半波長以上離れている場合，無線伝送路特性が全く異なるという独立性を持つ．そのため，受信端末とは異なる場所に存在する盗聴端末は，異なる無線伝送路特性の影響を受けた無線信号を受信することとなる．

図 1 に提案するプレ等化技術を用いるセキュア通信方式の概要を示す．本システムでは，無線 LAN 基地局などと通信する複数の端末を想定する．本図では，基地局である送信端末が受信端末と通信をしており，盗聴端末が送信端末と受信端末の通信内容の傍受を試みている．

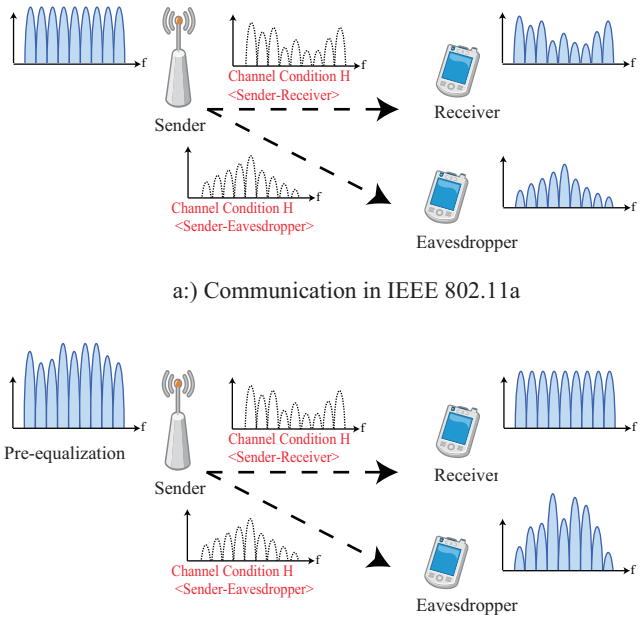

図 1 Overview of pre-equlization scheme for physical security.

図 1(a) で示される一般的な無線 LAN システムなどでは，送信端末は一般的な OFDM 信号を送信する．また，受信端末では，既知のパイロット信号を用いることにより無線伝送路特性の推定を行う．次に，受信端末により推定された無線伝送路特性を用いて受信信号を等化することにより，送信時とほぼ同様の信号を復元し，復調により情報を取得している．

図 1(b) で示される提案方式では，通信中の端末移動が少ない準静止環境を想定する．準静止環境では，送信端末と受信端末間の無線伝送路特性の時間変動は極めて少なくなるため，パケット転送の直前に無線伝送路の推定を行うことで，無線伝送路特性の推定値と実際のパケット転送時の無線伝送路特性はほぼ一致する．また，送信端末から受信端末宛の通信と受信端末から送信端末宛の通信では，同一周波数を利用している場合，無線伝送路特性は同一のものとなる．そこで，送信端末と受信端末間であらかじめ無線伝送路特性を推定することにより，送信端末は所望の受信端末までの無線伝送路特性を考慮した送信信号を送信する．このような処理をプレ等化処理と呼び，プレ等化処理された送信信号は，無線伝送路の影響を受けることにより，所望の受信端末のみで復調可能な信号となる．結果として，受信端末は正常に復調処理が可能となる一方，盗聴端末は異なる無線伝送路の影響を受ける上，プレ等化処理で利用した無線伝送路特性も不明なため，受信時に等化処理を行うこともできず，復調処理に失敗する．

2.2 システムモデル

図 2 に IEEE 802.11a のフレーム構造を示す．IEEE

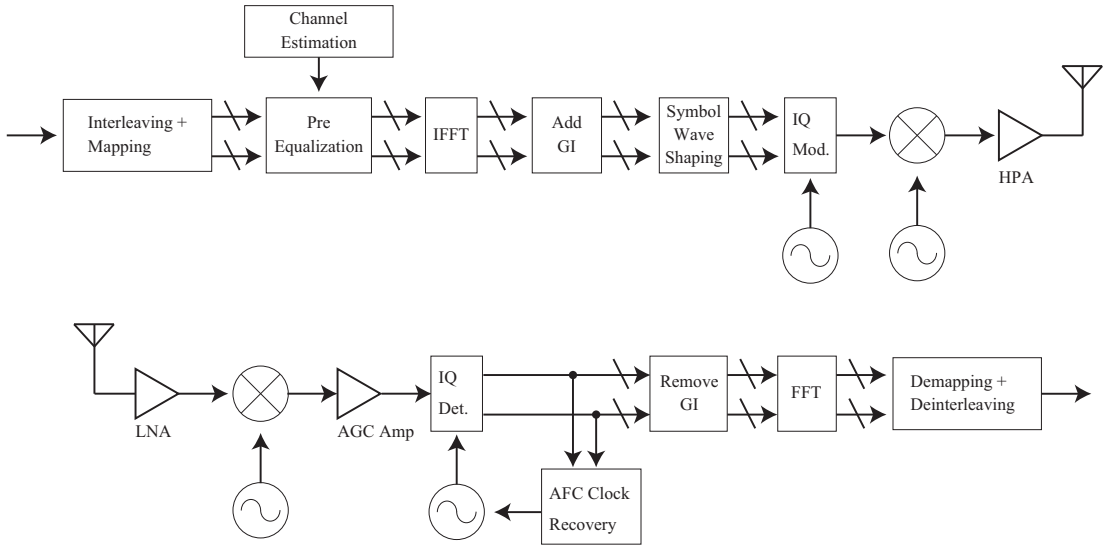

図 3 System model.

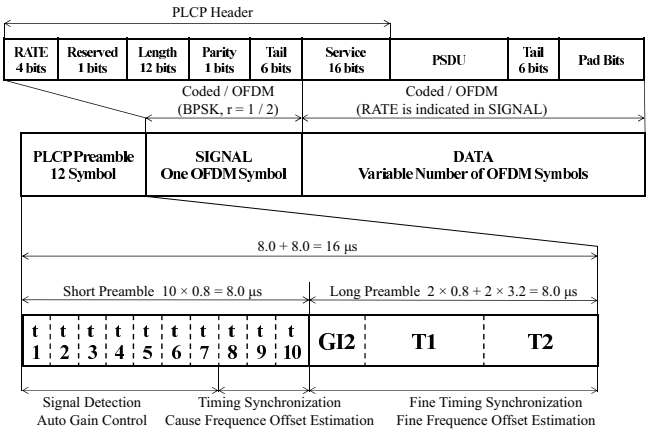

図 2 Frame structure.

802.11a のフレーム構造では，ショートプリアンブル，ロングプリアンブルに続き，OFDM シンボルが繰り返し送信される．また，プリアンブルの次の OFDM シンボルのみ制御情報が含まれており，その後の OFDM はペイロードデータが含まれている．提案方式のシステムにおいても，IEEE 802.11a と同一のフレーム構造を想定する．

図 3 に提案方式の通信モデルを示す．提案方式は IEEE 802.11a などの OFDM を利用する通信システムを想定する．OFDM を利用するシステムでは，送信データ系列を周波数方向にマッピングし，1 次変調を行う．また，データパケットの送信前に交換される制御パケットを利用して，伝送路特性を推定し，推定した伝送路特性を用いてプレ等化処理を行う．その後，IFFT(Inverse Fast Fourier Transform) を利用することにより，時間方向の信号を生成し，一般の OFDM システムと同様にガードインターバル (GI) を付加して送信を行う．

受信処理では，IEEE 802.11a と同様に，ショートプリアンブルを用いることで，AGC(Automatic Gain Control) の調整，信号検出，タイミング推定，周波数オフセット推定を行う．また，ロングプリアンブルを用いて，より正確なタイミング推定と周波数オフセット推定を行う．既存の IEEE 802.11a と異なる点は，既存方式では，ロングプリアンブルに含まれる既知のパイロットを利用して伝送路特性を推定し，推定した伝送路特性を利用して等化処理してから復調処理を行う．一方，提案方式の場合，送信時に伝送路特性に合わせてプレ等化処理を行っているため，受信時の等化処理は必要なく，直接復調処理を行う点である．なお，プレ等化処理をするのは，ペイロードデータを搬送するサブキャリア部だけであり，既知信号が含まれるパイロット用のサブキャリアにはプレ等化処理を行わない．また，上記のプリアンブルは標準のものを利用するため，ペイロード受信前に行われる信号検出，タイミング推定，周波数オフセット推定などの処理は同一である．

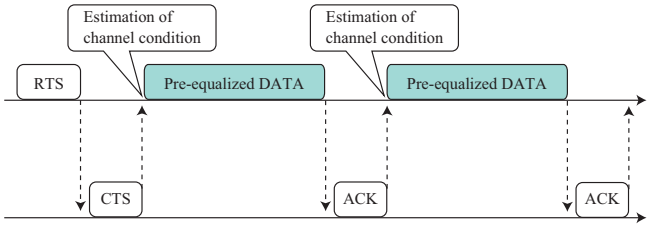

図 4 Communication signaling.

なお，受信端末と異なる位置に存在する盗聴端末には，プレ等化処理された信号が自らの無線伝送路を通して受信される．そのため，正確な復調処理を行うためには，プレ等化処理で利用した無線伝送路特性と，自らの無線伝送路特性が必要となる．しかし，プレ等化処理で利用した無線伝送路特性は知ることができないため，等化処理に失敗し，復調処理をしたとしても，多くのデータは誤りとなる．

2.3 通信シグナリング

提案方式では，プレ等化処理を行うために送信端末が無

線伝送路特性を予め知る必要がある．一般に無線伝送路特性は準静止環境においても，ゆっくりと時間的に変化しており，プレ等化処理を行う直前の無線伝送路特性の推定が必要である．図 4 は，RTS/CTS の機構を活用した無線伝送路特性を行う通信シグナリングである．提案方式の通信シグナリングでは，無線伝送路特性が不明な場合，RTS/CTS の通信を行うことにより，送信端末は CTS パケットを用いて無線伝送路を推定する．また，推定した無線伝送路特性を用いて，データパケットのデータサブキャリアのプレ等化処理を行う．なお，連続的にデータパケットを送信可能な場合は，データパケットの確認応答 (ACK) パケットを用いて，無線伝送路特性を改めて推定することにより，最新の無線伝送路特性を取得する．なお，RTS, CTS, ACK パケットは IEEE 802.11a に準拠したパケットを想定しており，データパケットのみプレ等化処理を行う．

2.4 プレ等化処理

提案方式では，データパケットは S 個のデータシンボルにより構成され，各データシンボルは M 個のサブキャリアから構成される．なお，FFT ポイント数を N，GI 長は N_g とする．また，送信端末は受信端末からの CTS パケットを利用して，送信端末と受信端末間の無線伝送路特性の推定を行う．ここで，CTS パケットに含まれるパイロット信号を $A_p(n)$ とし，送信端末と受信端末間の無線伝送路特性を $H(n)$ とした時，無線伝送路の影響を受けた周波数軸上の受信信号 $R(n)$ は，加法性白色ガウス雑音を $W(n)$ とすると，次式で与えられる．

$$R(n) = A_p(n) \cdot H(n) + W(n) \tag{1}$$

送信端末では，パイロット信号 $A_p(n)$ は既知であるため，次式を用いることにより，送信端末と受信端末間の推定された無線伝送路特性 $\hat{H}(n)$ を取得する．なお，n はサブキャリア番号を示す．

$$\begin{aligned}\hat{H}(n) =& \frac{R(n)}{A_p(n)} \\ =& \frac{A_p(n) \cdot H(n) + W(n)}{A_p(n)} \\ =& H(n) + \frac{W(n)}{A_p(n)}\end{aligned} \tag{2}$$

次に，s 番目シンボルにおける，サブキャリア番号 L_1 から L_2 までの M 個のサブキャリアの周波数軸送信データ $A(s,n)$ に対して，上記の無線伝送路特性 $\hat{H}(n)$ を用いて，下記の式に示すプレ等化処理を行う．

$$A_{peq}(s,n) = \frac{A(s,n)}{\hat{H}(n)} (0 \le s \le S-1) \tag{3}$$

プレ等化処理された周波数軸上の送信信号 $A_F(s,n)$ は，周波数軸信号の両端にエイリアス除去を目的として，ゼロパディングが挿入される．次に，次式で与えられる N ポイントの逆フーリエ変換処理により，時間軸信号 $a(s,k)$ に変換される．ここで，k はサンプル番号を示す．

$$\begin{aligned}a_{peq}(s,k) = \sum_{n=0}^{N-1} A_{peq}(s,n) \cdot e^{j\frac{2\pi nk}{N}} \\ (0 \le n \le N-1, 0 \le k \le N-1)\end{aligned} \tag{4}$$

時間軸上の信号に変換された信号は，シンボル間干渉によるチャネル間干渉を防ぐため，N_g サンプルを有する GIa_{gi} をデータシンボルの先頭に付加する．GI は次式で示される，時間軸信号の後方 N_g サンプルを複製した冗長信号であり，N_g は無線伝送路で発生すると想定される最大遅延時間以上のサンプル長に設定する必要がある．

$$a_{gi}(s,n_g) = a_{peq}(s, N-N_g+n_g)(0 \le n_g \le Ng-1) \tag{5}$$

準静止環境下における通信では，無線伝送路特性の時間変動は極めて少なく，一定とみなすことができることが知られている．このような条件における，GI を取り除いた受信信号は次式で与えられる．

$$r(s,k) = \begin{cases} \sum_{l=0}^{k} \rho_{peq}(s,k-l) + \\ \quad \sum_{l=k+1}^{L-1} \rho_l(s) \cdot a_{peq}(s, N+k-l) + w(s,k) \\ \quad (0 \le k \le L-1) \\ \sum_{l=0}^{L-1} \rho_l(s) \cdot a_{peq}(s, k=l) + w(s,k) \\ \quad (l \le k \le N-1) \end{cases} \tag{6}$$

ここで，$\rho_l(s)$ は s シンボルの l 番目の遅延波の時間軸伝送路インパルス応答であり，w は加法性白色ガウス雑音である．また，$(0 \le k \le N_g - 1)$ における受信信号の第二項目は GI を示す．なお，受信信号に対して N ポイントの FFT を用いることにより，周波数軸上の信号 $\hat{A}(s,n)$ に変換される．また，ゼロパディングを取り除き，復調を行うことにより，次式のように復調データが得られる．

$$\begin{aligned}\hat{A}(s,n) =& \sum_{k=0}^{N-1} r(s,k) \cdot e^{-j\frac{2\pi nk}{N}} \\ & A_{peq}(s,n) \cdot H(s,n) + W(s,n) \\ & \frac{A(s,n)}{\hat{H}(n)} \cdot H(s,n) + W(s,n) \\ & \approx A(s,n) + W(s,n)\end{aligned} \tag{7}$$

表 1 JTC Channel models

Model	Relative Delay (nsec) / Average Power (dB)							
Indoor residential A	0	50	100					
	0	-9.4	-18.9					
Indoor office A	0	50	100					
	0	-3.6	-7.2					
Indoor commercial A	0	50	100	150	200			
	0	-2.9	-5.8	-8.7	-11.6			
Outdoor urban low-rise areas	0	50	150	325	550	700		
Low antenna A	0	-1.6	-4.7	-10.1	-17.1	-21.7		
Outdoor residential areas	0	50	100	150	200	250	300	350
Low antenna A	0	-2.9	-5.8	-8.7	-11.6	-14.5	-17.4	-20.3

3. 数値例

提案方式の有効性を検討するため，Matlab による数値シミュレーションによる評価を実施した．無線システムとしては，IEEE 802.11a を想定し，図 2 に示す，IEEE 802.11a のフレーム構造を利用した．そのため，送信信号のフレームには，ブリアンブル部とペイロード部が含まれている．また，64 本のサブキャリアの内，48 本をデータ伝送に利用し，4 本はパイロット信号用に利用した．なお，12 本はゼロパディングが挿入されるため，利用していない．プレ等化処理はデータ伝送用のサブキャリアのみに適用し，受信側ではパイロット信号を利用した等化処理は行わない実装とした．チャネルモデルとしては，Joint Technical Committee (JTC) により提案されたアンテナ高が低い場合の室内及び屋外の伝送路モデルと一般的なマルチパス環境をモデル化した Rayleigh Fading 環境を用いた．利用した JTC チャネルモデルの詳細を表 1 に示す．表 1 では，各チャネルモデルで想定する各マルチパスの遅延量と減衰量が示されている．なお，利用したチャネルモデルでは，マルチパスの最大遅延量が GI 長より少ない環境である．また，シミュレーション諸元を表 2 に示す．

表 2 Simulation Parameters

Simulator	Matlab 2015b
Number of trials	10000
Communication device	IEEE802.11a
Number of symbols in a frame	10
Modulation scheme	QPSK
Number of FFT points	64
Number of data sub-carriers	48
Number of pilot subcarriers	4
Number of zero padding	12
Guard Interval	16 (0.8 [μs])
Bandwidth	20 [MHz]
Frequency	5.2 [GHz]
Channel model	JTC · Indoor residential A · Indoor office A · Indoor commercial A · Outdoor urban low-rise areas Low antenna A · Outdoor residential areas Low antenna A Rayleigh fading (Multi-path: 4)
Speed	1km/h

図 5 にプレ等化技術を利用せず，受信側で等化処理を行う場合のビット誤り率特性を提案方式の比較対象として示す．結果より，JTC モデルで想定される多くのチャネルモデルと Rayleigh Fading 環境は，近い特性を持つことが確認できる．これは，OFDM では GI 長内のマルチパスの影響を受けないため，チャネルモデルの差が大きな特性変化に結びつかなかったためと考えられる．なお，JTC Indoor residential A のみは，ビット誤り率特性が極めてよいことも確認できる．これは，JTC Indoor residential A では，想定するマルチパス数が少ない上，各マルチパスの減衰量が大きいため，直接波が特性を支配している．そのため，マルチパスの影響をあまり受けていないと考えられる．

図 6 にプレ等化技術を利用することで，受信側では等化処理を行わない，提案方式のビット誤り率特性を示す．本図の性能は所望の受信端末のビット誤り率を示すため，低いビット誤り率が要求される．結果より，図 5 と同様に，多くのチャネルモデルは類似した特性を持つことが確認される．また，JTC Indoor residential A のみは，ビット誤り率特性が極めてよいことも確認できる．さらに，図 5 と比較すると，若干特性が改善していることも確認できる．これは，予め伝送路状態に合わせて送信信号を生成しているため，受信時の等化処理で発生する雑音増幅の影響が少なくなったためと考えられる．

図 7 に提案方式の盗聴端末のビット誤り率特性を示す．

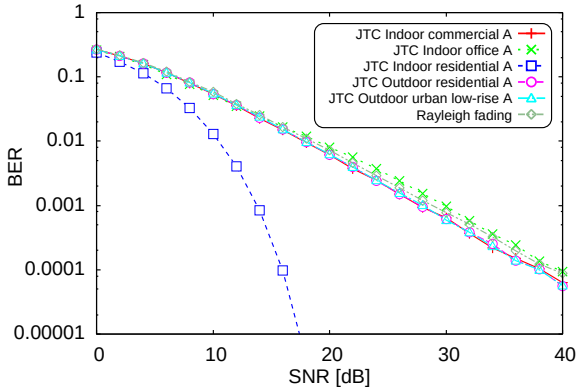

図 5 BER at an intended terminal(Conventional).

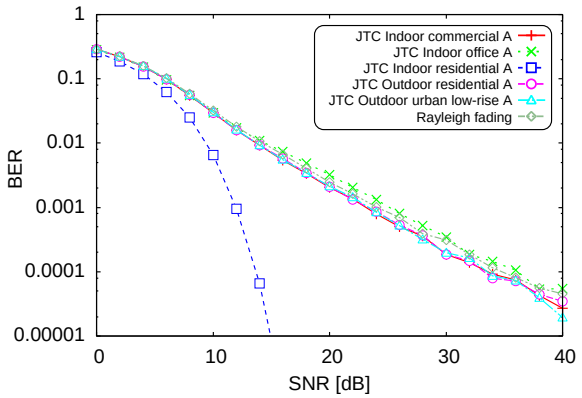

図 6 BER at an intended terminal(Proposed).

提案方式では，盗聴端末はプリアンブル部などを用いることにより，送信端末と盗聴端末間及び受信端末と盗聴端末間の伝送路特性の推定は可能である．しかし，送信端末と受信端末間の伝送路特性は，物理的に受信端末に近づかなければ推定が困難である．結果として，すべてのチャネルモデルにおいて，ビット誤り率がほぼ 0.5 となることが確認できる．つまり，盗聴端末が得られる情報量もほぼ 0 であることを示し，提案方式の有効性を確認できる．

4. まとめ

本研究では，実用上の伝送路特性はマルチパスの影響により，場所により特性が大きく異なることに着目した．また，送信端末と受信端末間の伝送路特性を予め考慮した送信信号を生成するプレ等化技術を用い，受信端末のみが正常に復調可能な，無線伝送路特性を鍵として利用するセキュア通信方式を提案した．提案方式では，盗聴端末が正常に復調をするためには，盗聴対象の端末に物理的に近ずく必要があり，盗聴行為をより困難にすることが可能である．また，数値例では端末間の通信は正常に行える一方で，盗聴端末は復調誤りにより情報をほとんど得られないことも確認した．

謝辞 本研究の一部は科研費 (26330103, 15H02697)，農林水産省 革新的技術創造促進事業 (異分野融合共同研究)，の助成を受けたものである．記して謝意を表する．

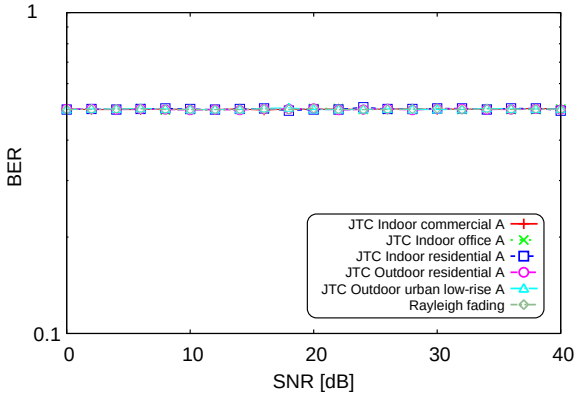

図 7 BER at eavesdroppers(Proposed).

参考文献

[1] A. D. Wyner, “The Wire-Tap Channel,” Bell System Technical Journal, Vol. 54, No. 8, pp. 1355–1387, October 1975.

[2] M. Bloch, J. Barros, M.R.D. Rodrigues, S.W. McLaughlin, “Wireless Information-Theoretic Security,” IEEE Transactions on Information Theory, Vol. 54 , No. 6, pp. 2515–2534, June 2008.

[3] P. Sudarshan, N.B. Mehta, A.F. Molisch, Jin Zhang, “Channel Statistics-Based RF Pre-Processing with Antenna Selection,” IEEE Transactions on Wireless Communications, Vol. 5, No. 12, pp. 3501–3511, December 2006.

[4] N. Yang, P.L. Yeoh, M. Elkashlan, R. Schober, I.B. Collings, “Transmit Antenna Selection for Security Enhancement in MIMO Wiretap Channels,” IEEE Transactions on Communications, Vol. 61, No.1, pp. 144–154, January 2013.

[5] A. Khisti, G. Wornell, W. Gregory, “Secure Transmission With Multiple Antennas I: The MISOME Wiretap Channel,” IEEE Transactions on Information Theory, Vol. 56, No. 7, pp. 3088–3104, July 2010.

[6] A. Khisti and G. Wornell, “Secure transmission with multiple antennas II: The MIMOME wiretap channel,” IEEE Transactions on Information Theory, Vol. 56, No. 11, pp. 5515–5532, November 2010.

[7] X. Zhouand, M. R. McKay, “Secure transmission with artificial noise over fading channels: Achievable rate and optimal power allocation,” IEEE Transactions on Vehicular Technology, Vol. 59, No. 8, pp. 3831–3842, July 2010.

[8] A. Mukherjee, A. L. Swindlehurst, “Robust Beamforming for Security in MIMO Wiretap Channels With Imperfect CSI,” IEEE Transactions on Signal Processing, Vol. 59, No. 1, pp. 351–361, September 2010.

[9] M. Pei, J. Wei, K.-K. Wong, and X. Wang, “Masked beamforming for multiuser MIMO wiretap channels with imperfect CSI,” IEEE Transactions on Wireless Communications, vol. 11, no. 2, pp. 544–549, February 2012.

[10] F. Rusek et al., “Scaling up MIMO: Opportunities and challenges with very large arrays,” IEEE Signal Processing Magazine, Vol. 30, No. 1, pp. 40–46, January 2013.

[11] Jun Zhu, R. Schober,V. K. Bhargava, “Secure Transmission in Multicell Massive MIMO Systems,” IEEE Transactions on Wireless Communications, Vol. 13, No. 9, pp. 4766–4781, July 2014.