Secret Key Agreement Scheme Based on BER Fluctuation in Radio Communication System

Takayasu KITANO*, Hisato IWAI* and Hideichi SASAOKA*

(Received July 13, 2009)

This paper proposes a private key agreement scheme using the fluctuations of BER (Bit Error Rate). In the proposed scheme, the received BER at both authorized users is used as the common information for key generation between them. BER is an appropriate indicator to characterize the wireless channel because it includes all factors to generate bit errors such as fluctuations of amplitude and phase, effect of delayed waves etc. In order to evaluate the performance of the proposed scheme, numerical simulations are carried out assuming the configurations and the parameters of wireless LAN system. The results of the simulations show that the proposed scheme successfully achieves the key agreement at SN ratio of 15dB when it is combined with data deletion and error correction schemes.

Key words ：information security, secret key agreement, pseudo BER, radio propagation

キーワード ： 情報セキュリティ，秘密鍵共有，擬似ビット誤り率，電波伝搬

陸上移動通信におけるビット誤り率変動に基づく秘密鍵共有方式

北野　隆康，岩井　誠人，笹岡　秀一

1. まえがき

無線通信の普及に伴い，盗聴対策などのセキュリティ対策が重要となっている．近年の盗聴対策として，情報を暗号化して伝送する暗号通信が一般的であり，送信者と受信者が共通の暗号鍵を用いる共通鍵（秘密鍵）暗号方式 [1, 2] がよく用いられている．共通鍵暗号方式は，送信者と受信者が共通の秘密鍵を用いて情報の暗号化と復号を行うため，計算量は少ないが，暗号通信を行う前に両者の間で秘密鍵を共有しておく必要がある．秘密鍵を共有するために鍵配送を行うことが多いが，無線通信ではその過程で秘密鍵が盗聴される危険性があり，安全な秘密鍵共有手法が重要となる．また，共有した秘密鍵は暗号通信を行うたびに使用するため，同じ秘密鍵を長期に渡って使用すると，暗号化情報のパターンから秘密鍵を解読される危険性もある．

そこで，電波伝搬の特徴を活用することで，鍵を配送することなく共有可能で，新たな秘密鍵の生成も容易な秘密鍵共有方式 [3-7] が提案されている．

一般に移動通信において電波伝搬の可逆性が成り立つこと，マルチパスフェージングの変動が場所に依存することから，送受信局が互いに信号の送受

* Department of Electronics, Doshisha University, Kyotanabe, Kyoto, 610-0321, Japan
Telephone: +81-774-65-6289, Fax: +81-774-65-6801, E-mail: eti1101@mail4.doshisha.ac.jp

信を行う場合，伝搬路特性は相関の高いものとなるが，場所が異なる他局での伝搬路特性は相関が低くなる [8, 9]．これより，正規の送信局と受信局でそれぞれ受信信号強度（RSSI: Received Signal Strength Indicator）などの伝搬路特性を測定すると，正規局間では互いに高相関となるが，盗聴局には低相関になる情報が得られる．そこで，得られた情報に閾値を設定し 2 値化処理を行うと，正規局でのみ共有可能な秘密鍵が生成できる．また，電波伝搬特性を活用して生成された秘密鍵は，再生成や共有が容易であるため，秘密鍵の使い捨ても可能である．

電波伝搬を活用した秘密鍵共有方式に関して，これまで，OFDM の周波数特性を用いた方式 [6]，可変指向性アンテナであるエスパアンテナ [10] を用いた方式 [7] などが提案され，広く検討されている．これらの研究は，鍵生成の共有情報として RSSI を用いて，その強度変動に基づいて秘密鍵を生成する方式である．秘密鍵生成のための共有情報として RSSI を用いると，直接波など支配的になる電波の経路が存在する環境において，生成した秘密鍵の盗聴耐性が低下することが報告されている [11, 12]．

そこで本論文では，秘密鍵生成のための共有情報として，従来より検討されている RSSI ではなく，ビット誤りを用いて秘密鍵を生成する方法を提案する．特に，受信局でのみ発生させることが可能で，ビット誤りとも関係のある擬似ビット誤りを用いて秘密鍵を生成する方式 [13]について検討する．

本論文では，まず電波伝搬特性を活用した秘密鍵共有方式について述べ，次に，擬似ビット誤り率を用いた秘密鍵の生成，および共有について検討する．そして，無線 LAN システムを想定したシミュレーションを行い，提案方式の有効性を示す．

2. 電波伝搬特性を活用した秘密鍵共有

2.1. 秘密鍵共有の原理

電波伝搬特性を活用した秘密鍵共有方式では，電波伝搬の特徴，つまり，電波伝搬の可逆性とマルチパスフェージングの場所・時間依存性を利用している． Fig. 1 に，電波伝搬特性を活用した秘密鍵共有方式の原理を示す．電波伝搬において，送受信局が

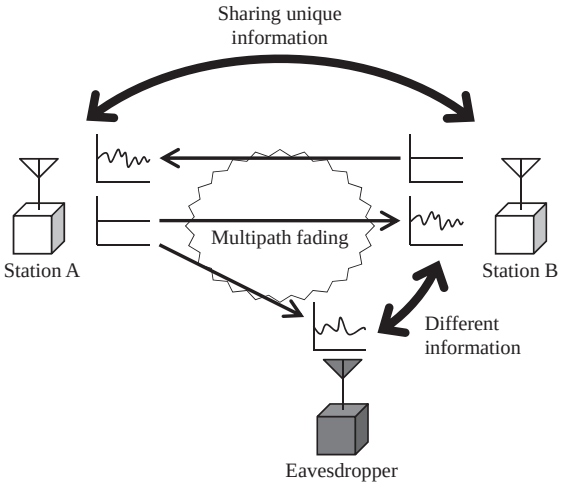


Fig. 1. Principle of secret key agreement scheme using channel characteristics.

同じ場所であれば，送信局と受信局が交代しても同じ経路を経て伝搬する（電波伝搬の可逆性）．これより，信号を A 局から B 局へ送信する場合と，その逆の B 局から A 局へ送信する場合で，伝搬路特性の相関が非常に高くなる．

一方，マルチパス環境において，受信局の場所が変わると電波伝搬の経路も異なり，伝搬路特性も異なるものとなる（マルチパスフェージングの場所依存性）．これより，Fig. 1 において場所が異なる盗聴局（Eavesdropper）と正規局（B 局あるいは A 局）では，測定した伝搬路特性は非常に相関の低いものとなる．

これら電波伝搬の特徴により，伝搬路特性の情報は正規局間（A 局―B 局間）でのみ共有可能となる．そこで，この情報に 2 値化処理を行って秘密鍵を生成すると，鍵の配送をすることなく秘密鍵の共有が可能である．

2.2. 秘密鍵生成手順

電波を活用した秘密鍵共有方式における秘密鍵生成手順を Fig. 2 に示す．Fig. 2 では，まず，秘密鍵を共有する局同士で伝搬路特性測定用信号の送受信を繰り返し行い，秘密鍵を生成するのに必要な長さの伝搬路特性の系列を得る．そして，得られた伝搬路特性の系列に 2 値化処理を行って鍵候補を生成する．ここで，伝送路における雑音などの影響

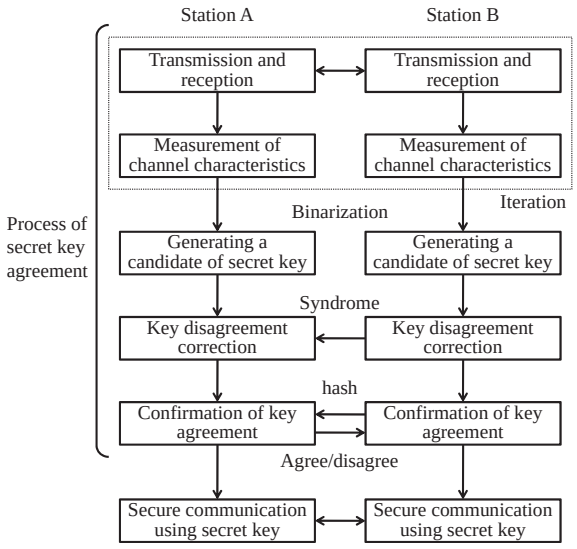


Fig. 2. Procedure of secret key agreement.

により，互いの局で生成した鍵候補に不一致が発生することがある．この場合には鍵候補の不一致訂正を行い，訂正後の鍵系列を秘密鍵として暗号通信に使用する．

3. ビット誤り率変動に基づく秘密鍵共有方式

3.1. ビット誤り率変動に基づく秘密鍵共有方式

従来の方式 [5-7]では，秘密鍵を共有する局がそれぞれ RSSI を測定し，RSSI に対してその中央値などを閾値として 2 値化処理を行っていた．RSSI により秘密鍵を生成する場合，正規局同士と盗聴局が互いに直接波の到来圏内にあるなど支配的なパスが存在すると，RSSI 値も支配的なパスに依存してしまい盗聴局でも正規局で測定したものと相関の高い RSSI が得られる [12]．このように，正規局間と盗聴局で高相関になる RSSI に基づいて秘密鍵を生成すると，盗聴局でも正規局で共有している秘密鍵と同じものが生成される危険性がある．

そこで，本論文では秘密鍵の生成に RSSI を用いるのではなく，ビット誤りに基づいて秘密鍵を生成し共有する手法について提案する．

3.2. 擬似ビット誤りの秘密鍵生成への適用

ビット誤りを用いて秘密鍵を生成するには，伝送路で発生する劣化要因や伝搬路特性の変動などを

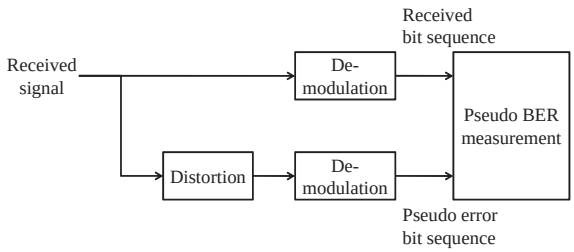


Fig. 3. Measurement of pseudo BER

ビット誤り率に反映させることが重要である．また，盗聴局に対して必要以上の情報を与えないという観点から，ビット誤りは受信側のみで検出できるものが望ましい．そこで本論文では，ビット誤りとして，受信時に人為的にビット誤りを発生させる擬似ビット誤り [14-20]を用いる．擬似ビット誤りは，情報信号伝送時の伝搬路特性を推定する手法の一つであり，伝搬路の劣化に応じた適応制御などに用いることが検討されている．

ここで，擬似ビット誤り発生システムのブロック図を Fig. 3 に示す．受信局において，受信した信号に人為的な歪みを与えて復調すると，受信ビット系列が劣化したような系列（擬似ビット誤り系列）が得られる．この擬似ビット誤り系列と，受信信号をそのまま復調したデータ系列（受信ビット系列）を比較することで得られるビット誤り率が擬似ビット誤り率である．この擬似ビット誤り率を秘密鍵生成の共有情報に用いることで，秘密鍵の生成および共有が可能になると考えられる．

ただし，従来検討されている擬似ビット誤り発生法では，雑音が非常に小さい環境において擬似ビット誤りが発生しない可能性がある．擬似ビット誤りを秘密鍵共有に用いる場合，適切な量の擬似ビット誤りが発生しないと，2 値化処理が不可能となり秘密鍵を生成することができない．そこで，擬似ビット誤りを秘密鍵生成に用いるためには，雑音の大きさによらず適切な量の擬似ビット誤りを発生させる必要がある．

3.3. 秘密鍵生成に用いる擬似ビット誤りの検討

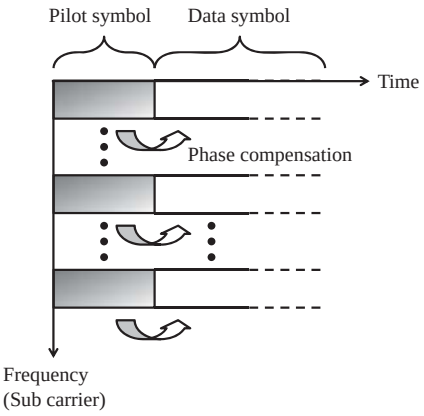
本論文で提案する擬似ビット誤りに基づく秘密

鍵共有方式では，雑音以外の伝送路の劣化要因に基づいて擬似ビット誤りを発生させる必要がある．そこで，ここでは擬似ビット誤り発生法について検討する．

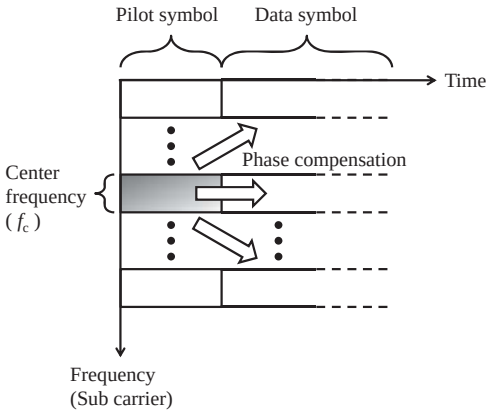
3.3.1. 信号の判定軸の誤りを用いた方法

擬似誤りを用いたビット誤り率推定法 [14-20]では，変調方式に PSK (Phase Shift Keying) を用いて，受信信号の復調時の判定軸にオフセットを与える方法や判定軸に位相回転を与える方法が検討されている．

これらの判定軸を誤らせるような方法を用いて，擬似誤りを発生させると，雑音による劣化を精度良く推定することが可能である．しかし，擬似ビット誤りの発生が雑音電力に依存し，雑音電力が小さい環境では擬似誤りの発生も少なくなるため秘密鍵の生成には適していない．そこで，雑音が小さい環境でも適度に擬似ビット誤りを発生させる方法が必要である．



(a) Regular phase compensation.



(b) Phase compensation for occurrence of pseudo BER.

Fig. 4. Phase compensation using pilot symbol.

3.3.2. 位相補償歪みを用いた方法

ここでは，OFDM (Orthogonal Frequency Division Multiplexing) 伝送 [21] を想定し，通常とは異なるパイロットシンボルを用いて伝送路歪みの補償を行い，擬似ビット誤りを発生させる方法について述べる．

通常の OFDM システムでは，各サブキャリアのデータシンボルの先頭に送受信局で既知であるパイロットシンボルを付加しておき，受信側で Fig. 4 (a) のように，パイロットシンボルに基づいて伝送歪みを推定・補償している．

ここで，各サブキャリアの周波数を f，送信情報を $s(f)$，伝搬路特性を $h(f)$，雑音を $n(f)$ とすると，受信側での OFDM における受信信号 $r(f)$ は，

$$r(f) = h(f)s(f) + n(f) \qquad (1)$$

となる．この信号に対して Fig. 4 (a) のような通常の方法で伝送路歪みの補償を行うと，補償後の信号 $y(f)$ は，

$$y(f) = s(f) + n(f)/h(f) \qquad (2)$$

となる．通常では，これを復調することで情報を得ることができる．

この伝送路歪みの補償の際に，誤ったパイロットシンボルを用いて歪み補償を行うと，擬似誤りを発生させることが可能である．誤ったパイロットシンボルを用いて位相補償を行う方法の一例として，Fig. 4 (b) のように OFDM の全サブキャリアのデータシンボルを，中心周波数 f_c のサブキャリアのパイロットシンボルを用いて歪み補償を行う擬似ビット誤り発生法を提案する．この方法を用いた場合，式(1)の受信信号に対して，

$$y_e(f) = h(f)/h(f_c)\,s(f) + n(f)/h(f_c) \qquad (3)$$

という歪み補償を行うことになり，擬似ビット誤り率に $h(f)/h(f_c)$ の影響を反映することができる．

本論文では，以降は中心周波数で歪み補償を行って発生させる擬似ビット誤りを用いる．

4. 計算機シミュレーション

4.1. シミュレーション諸元

提案方式の有効性を確認するため，無線 LAN のシステムを想定し，シミュレーションを行う．

シミュレーションで用いるパラメータを Table 1 に示す．伝搬環境は端末自体がゆっくりと移動する，あるいは周囲の人やものの移動により，常に伝搬環境が変動することを想定する．Table 1 に示すように，想定環境における遅延波の遅延時間は 0.1μs 刻みで，それぞれ相対電力が 0dB, -5dB, -10dB の 3 パスモデルとし，各パスは互いに独立なレイリーフェージング，あるいは，ライスフェージングとする．また，最大ドップラー周波数の標準値を 10Hz とするが，これを変化させる場合についても検討する．

パケット構成とタイムチャートは Fig. 5 に示すものを想定する．Fig. 5 および Table 1 に示すように，送信するパケットはパケット長が 400μs で，それぞれ 1ms 間隔で送受信を行うものとする．各パケットは，シンボル周期が 4μs の OFDM シンボルで，パイロットシンボル 20 シンボル (80μs) と，80 シンボルのデータシンボル (320μs) から構成されるとする．また，それぞれの局で測定用信号の送受信を行った後，片方のユーザで測定時間差を補償するための補間用のパケットの送受信を行う．この補間用のパケットを受信したユーザは，最初に受信したパケットと補間用のパケットを用いて線形補間を行い，測定時間差の影響を抑える．

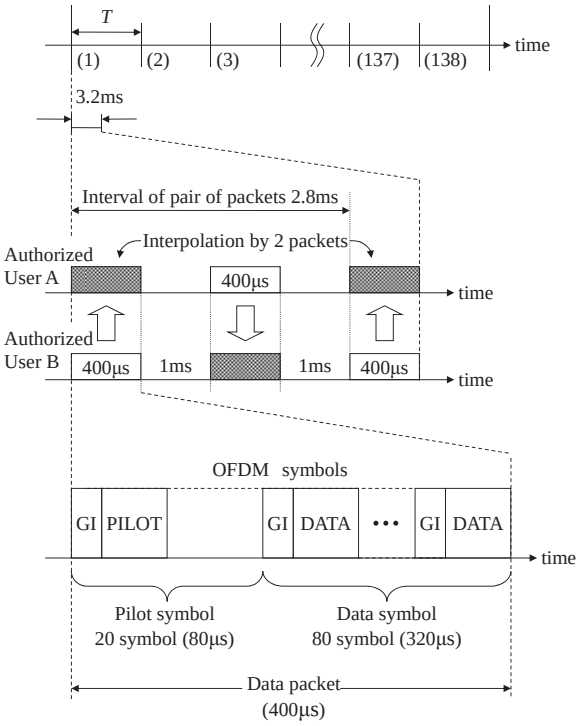


Fig. 5. Timing diagram and configuration of data packet.

測定用信号および補間用パケットの送受信および伝搬路特性測定処理は T 間隔で 138 回繰り返し行い，正規局でそれぞれ 138 個の擬似ビット誤り率系列を得る．この擬似ビット誤り率系列の中央値を閾値として 2 値化処理を行い，秘密鍵候補を生成する．生成した鍵候補系列のうち，閾値付近の擬似ビット誤り率を 2 値化したビットには，比較的多くの鍵不一致が発生する．そこで，閾値付近に該当するビットを 10 ビット取り除き，最終的に 128 ビットの鍵を生成する．

Table 1. Simulation parameters.

Modulation	OFDM QPSK (Quadrature Phase Shift Keying) Number of subcarriers: 48 Interval of OFDM symbol: 4μs Guard Interval: 0.8μs
Channel model	3-path Rayleigh model Independent Rayleigh fading Delay time difference : 0.1μs Relative power: 0dB, -5dB, -10dB Maximum Doppler frequency: 10Hz (nominal value) 3-path Rice model Independent Rice fading (rice factor: 10dB) Delay time difference : 0.1μs Relative power: 0dB, -5dB, -10dB Maximum Doppler frequency: 10Hz (nominal value)
Packet format	Length of a packet: 400μs Interval of a pair of packet: 2.8ms Measurement time difference: 1.4ms (Correction by linear interpolation using compensation packet)
Generation of key	Binary digitization by threshold of median value
Correction of key disagreement	Error correction within 5 bits by algebraic decoding method

4.2. 擬似ビット誤り率と秘密鍵の生成

ここでは，擬似ビット誤りの特性と，擬似ビット誤りから生成した秘密鍵の一例を示す．

まず，雑音が発生しない環境において，測定用信号の送受信を行うことを想定する．測定用信号を受信した正規局は，受信信号に擬似ビット誤りを発生させ，パケットごと擬似ビット誤り率を計算し，その系列から鍵候補を生成する．擬似ビット誤りの発生において，1 パケットあたりの擬似ビット誤り率を 0.1 区切りで分類し，それぞれの領域の発生確率を求めた分布特性を Fig. 6 に示す．Fig. 6 より，1 パケットあたりの擬似ビット誤り率が 0〜0.1 である場合が最も多く発生しており，0.35 程度であることがわかる．しかし，0.1 以上の擬似ビット誤り率も 0.65 程度発生していることから，系列は 2 値化処理が可能である．

次に，発生した誤り率から鍵を生成する一例を示す．パケットごとの擬似ビット誤り率の変動を Fig. 7 に示す． Fig. 7 の擬似ビット誤り率系列に対して閾値（系列の中央値）以上と閾値以下で 2 値化処理を行い，鍵候補系列を生成する．

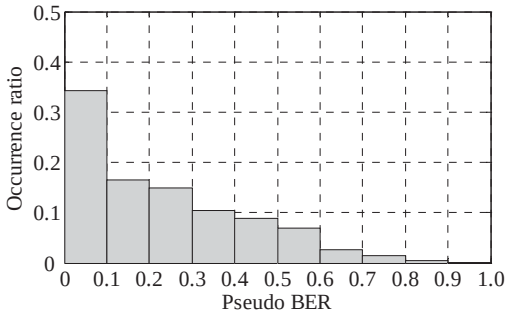


Fig.6. Occurrence distribution of BER.

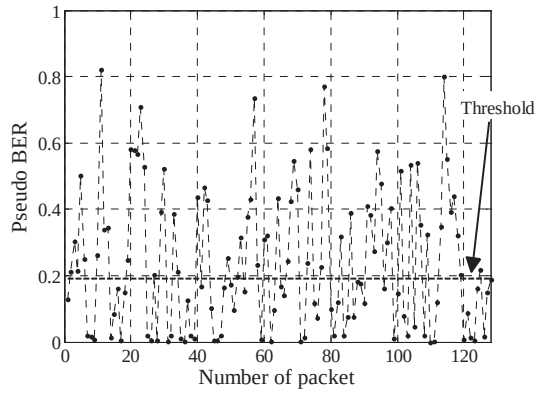


Fig. 7. An example of pseudo BER sequence.

4.3. 秘密鍵の生成時間と秘密鍵の安全性

Fig. 5 に示す T の値次第では，鍵の生成に莫大な時間がかかり，秘密鍵の生成効率が低下する．一方，T の値を過度に小さく設定すると，それぞれのビット誤り率に相関関係が生じ，生成した秘密鍵のビットのランダム性が低下する可能性がある．そこで，生成した秘密鍵を対象として，その鍵の自己相関を求め，T の設定値について検討する．

Fig. 8 に，T の値を変化させて生成した鍵系列に対して，鍵系列をビットごとスライドさせたものとの自己相関を計算した場合の特性を示す．T が 30 ms〜90ms の間は，自己相関特性にあまり変化がみられない．一方，T を 20 ms 以下に設定すると，鍵 1 ビット移動させた場合に自己相関が 0.2 以上になり，鍵系列に自己相関があることが確認できる．鍵系列に自己相関がある場合は，自己相関がない場合に比べて，盗聴局における秘密鍵の総当たりによる解読が容易になる可能性があり，秘密鍵として最適ではない．そこで本論文における，以降の検討は自己相関特性に差がみられない T = 30 ms を用いる．

4.4. 雑音に対する特性

雑音が提案方式を用いて生成した秘密鍵の共有に及ぼす影響について調べるため，雑音環境を想定し，シミュレーションを行う．Fig. 9 に，レイリー

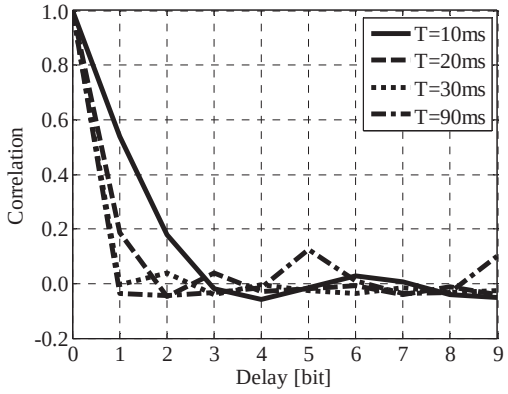


Fig. 8. Auto correlation of key sequence.

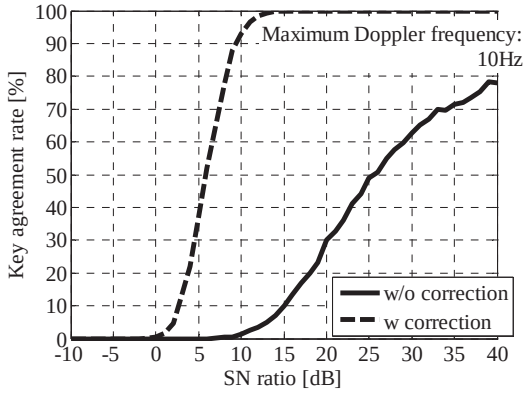
フェージング環境，および，ライスフェージング環境における，送信信号電力対雑音電力比（SN 比）に対する秘密鍵一致率特性を示す．なお，秘密鍵一致率は，生成した 128 ビットの秘密鍵が正規局間で完全に一致する割合，つまり，秘密鍵を共有できる確率である．また，Fig. 9 には，それぞれの環境で誤り訂正を適用する前と適用した後の特性を示している．ここでの誤り訂正は，5bit 以内の誤り（鍵不一致）なら確実に訂正できるという，理想的な訂正を行うものとする．

Fig. 9 のレイリーフェージング環境とライスフェージング環境の結果より，誤り訂正を行う前の状態では，生成した秘密鍵が必ずしも一致しない可能性があることが確認できる．しかし，SN 比が約 15dB 以上の環境では，誤り訂正を行うことで秘密鍵の共有が可能であることを示している．

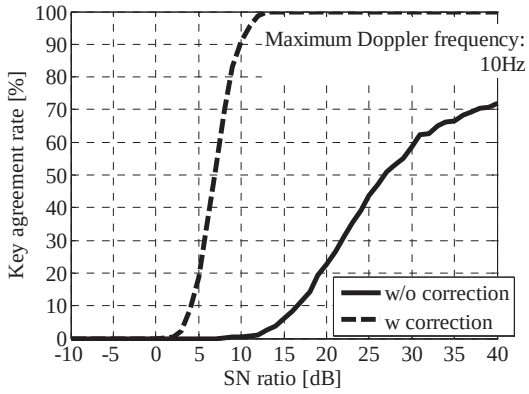
4. 5. フェージング変動に対する特性

測定信号の送受信間隔に対してフェージング変動の周期が短い場合，測定用信号の送受信の過程で伝搬路特性が変動してしまうため，両局の擬似ビット誤り率が異なり秘密鍵の共有が困難になると考えられる．そこでフェージング変動の周期が秘密鍵の共有に与える影響について検討する．SN 比が 20dB の環境を想定し，その環境下での最大ドップラー周波数ごとの鍵一致率特性を Fig. 10 に示す．

同図より，レイリーフェージング，ライスフェージングの両方のフェージング環境で，最大ドップラー周波数が 40 Hz 以下の場合に，生成した秘密鍵が一致することがわかる．2.4GHz 帯の無線 LAN を想

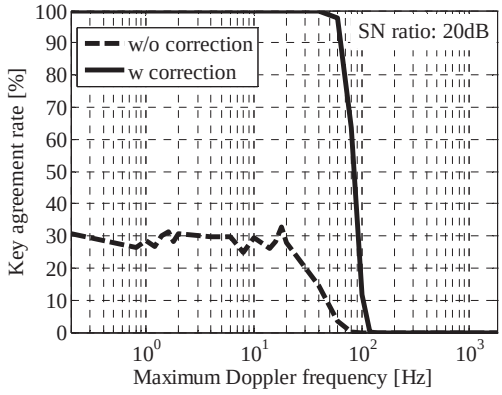


(a) Rayleigh fading environment.

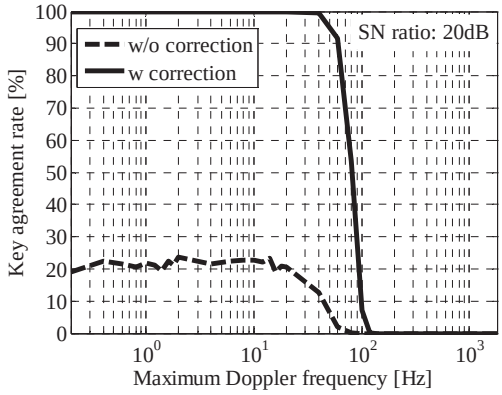


(b) Rice fading environment.

Fig. 9. Key agreement performance when SN ratio is changed.



(a) Rayleigh fading environment.



(b) Rice fading environment.

Fig. 10. Key agreement performance when maximum Doppler frequency is changed.

定する場合に，最大ドップラー周波数が 40 Hz となるのは，端末などの移動速度が約 5 m/s の場合である．無線 LAN では，端末の移動速度が 5 m/s となることを想定した設計がなされていないため，提案方式による秘密鍵共有は有効であるといえる．

5. まとめ

本論文では，電波を用いた秘密鍵共有方式において，人為的に擬似ビット誤りを発生させ，その擬似ビット誤り率を用いて秘密鍵を生成し共有する方式を提案した．

本論文では，まず秘密鍵生成が可能となる擬似ビット誤りの発生方法について検討した．擬似ビット誤りを秘密鍵共有方式に適用するには，雑音による劣化以外の劣化要因を擬似ビット誤りに反映させることが必要である．そこで本論文では，OFDM 伝送において，中心周波数のサブキャリアのパイロットシンボルを用いて，他のサブキャリアの歪み補償を行う方法を採用した．

提案方式について，無線 LAN 環境を想定したシミュレーションを行ったところ，レイリーフェージング，および，ライスフェージング環境下で SN 比が 15 dB 以下，最大ドップラー周波数が 40Hz 以下という環境において秘密鍵共有が可能であることを示した．

参考文献

1) 笠原正雄，境隆一，暗号，（共立出版，東京，2000）．
2) 岡本龍明，山本博資，現代暗号，（産業図書，東京，1979）．
3) J. E. Hershey, A. A. Hassan and R. Yarlagadda, “Unconventional cryptographic keying variable management,” IEEE Trans. Commun., vol. 43, pp. 1-6 (1995).
4) A. Hassan, W. E. Stark, J. E. Hershey and S. Chennakeshu, “Cryptographic key agreement for mobile radio,” Digital Signal Processing, vol. 6, pp. 207-212 (1996).
5) 岩井誠人，笹岡秀一，“電波伝搬特性を活用した秘密情報の伝送・共有技術，”信学論(B)，vol.J90-B，no.9，pp.770-783 (2007).
6) 北浦明人，笹岡秀一，“陸上移動通信における OFDM の伝送路特性に基づく秘密鍵共有方式，”信学論(A)，vol. J87-A，no.10，pp.1320-1328 (2004)．
7) T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, “Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels,” IEEE Trans. Antennas Propag., vol. 53, No. 11, pp. 3776-3784 (2005).
8) W.C. Jakes, Microwave mobile communications, John Wiley & Sons (1974).
9) 唐沢好男，ディジタル移動通信の電波伝搬基礎，（コロナ社，東京，2003）．
10) 大平孝，飯草恭一，“電子走査導波器アレーアンテナ”，信学論(C)，Vol.J87-C，no.1，pp.12-31 (2004).
11) 清水崇之，岩井誠人，笹岡秀一，“エスパアンテナを用いた秘密鍵共有方式における盗聴耐性向上の検討，”信学技報，AP2008-43，pp.41-46 (2008).
12) 川村俊一，清水崇之，岩井誠人，笹岡秀一，“エスパアンテナを用いた秘密鍵共有方式における盗聴耐性向上の検討，”信学技報，RCS2009-34，pp.37-42 (2009).
13) T. Kitano, A. Kitaura, H. Iwai, H. Sasaoka, “A Private key agreement scheme based on fluctuations of BER in wireless communications,” Proc. ICACT 2007, 8B, pp.1495-1499 (2007).
14) D. J. Gooding, “Performance monitor techniques for digital receivers based on extrapolation of error rate,” IEEE Trans. Commun. Technol., vol.COM-16, pp.380-387 (1968).
15) S. Takenaka, T. Katoh, “Bit error monitor for four phase PSK system,” ICC'80 Conference record, pp.251-256 (1980).
16) E. A. Newcombe, S. Pasupathy, “Error rate monitoring for digital communication,” Proceedings of IEEE, vol.70, no.8, pp.805-828 (1982).
17) I. M. Kostić, “Pseudo error rate of a PSK system with hardware imperfections, noise and cochannel interference,” IEE Proceedings, vol.136, Pt. I , no.5, pp.333-338 (1989) .
18) J. M. Keelty, “On-line pseudo-error monitors for digital transmission systems,” IEEE Trans. Commun., vol.26, no.8, pp.1275-1282 (1978).
19) 岩井誠人，渡邊貴志，高井信人，笹岡秀一，“擬似誤りに基づくビット誤り率の推定法，”信学技報，AP2006-15，pp.35-40 (2006).
20) 石崎俊輔，岩井誠人，笹岡秀一，“擬似誤りに基づくビット誤り率推定法の高精度化に関する検討，”同志社大学理工学研究報告, 49, pp. 100-107 (2008).
21) 伊丹誠，OFDM 変調技術，（トリケップス，東京，2000）．