平成 25 年 1 月 8 日

電気・電子情報工学専攻	学籍番号	093435
申請者氏名	吉田斉史	

指導教員氏名	大平　孝

論　文　要　旨（修士）

論文題目	エスパアンテナ無線秘密鍵生成システム秘匿性向上技術

無線通信は有線通信と比較し利便性が高い反面，電波を周囲に放射しているため，暗号通信が必須である．しかし，暗号通信に多用されている秘密鍵暗号方式は盗聴局に知られることなく秘密鍵を共有することが難しい．この問題の解決策として，両端末にエスパアンテナを用いた無線秘密鍵共有方式が研究されている．

両端末にエスパアンテナを用いた無線秘密鍵共有方式では可変指向性アンテナの一種であるエスパアンテナを使用する．正規両端末は指向性を同時に変化させ電波の送受を繰り返すことで複雑な変動を持つ受信信号強度(Received Signal Strength Indicator:RSSI)履歴を得ることができる．電波伝搬の相反性により正規局間では同じRSSI系列が得られ，電波伝搬の場所依存性により盗聴局は，正規局と同じRSSI系列を得ることはできない．そのため，RSSI履歴を元に秘密鍵を作れば安全に秘密鍵を共有できる．しかし，盗聴局に直接波を傍受されると秘密鍵の推定が容易となり，秘密鍵の秘匿性が低下する．

本稿では信号処理により秘匿性を向上させる手法として固有値を除去する手法を提案する．提案する 2 種の固有値生成方法の 1 つが式(1)である．両端末で得られる受信信号振幅y_nを 9 つ順番に取り出し，式(1)で固有値分解する．その後，式(2)のように再計算する．

図 1 のシミュレーション環境により提案する手法の 1 つで効果があることを確認した．図 2 がシミュレーション結果であり，実際の雑音環境であるTNR110dBで直接波ありと比較してImac14 ポイントの向上，従来手法の高レベルRSSI削除手法と比較してImac1 ポイントの向上を確認した．また，ほぼ無雑音であるTNR130dBで直接波ありと比較してImac19 ポイントの向上，高レベルRSSI削除手法と比較してImac8ポイントの向上を確認した．これにより，提案手法オプション 2 が実雑音の環境及び雑音の少ない環境で従来手法より効果的な手法であると示すことが出来た．また，提案手法の効果を実証するために実機実験を行ったが使用したアンテナの性能が不十分であり，効果を実証できなかった．

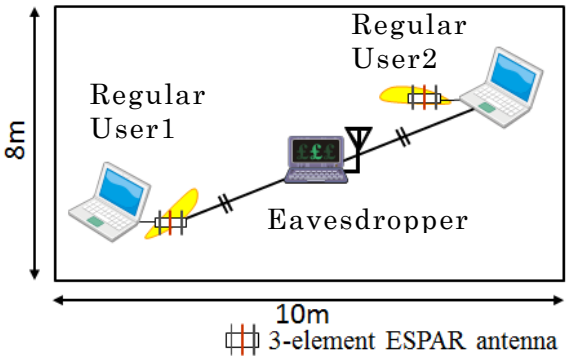

図 1　シミュレーション環境

$$Y=\begin{bmatrix} y_1 & y_4 & y_7 \\ y_2 & y_5 & y_8 \\ y_3 & y_6 & y_9 \end{bmatrix}=P_r\begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{bmatrix}P_t^H \quad \text{式(1)}$$

$$Y'=P_r\begin{bmatrix} 0 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & 0 \end{bmatrix}P_t^H=\begin{bmatrix} y'_{11} & y'_{12} & y'_{13} \\ y'_{21} & y'_{22} & y'_{23} \\ y'_{31} & y'_{32} & y'_{33} \end{bmatrix} \quad \text{式(2)}$$

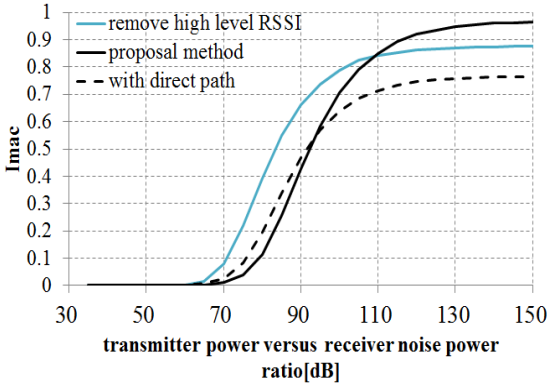

図 2　提案手法と従来手法の比較