混信状態を活用した安全性と大容量化を両立する無線ネットワークの創出

代表研究者　　田久　修　　信州大学 学術研究院（工学系）　准教授

１．はじめに

本研究調査は、災害時などにおける無線端末を利用した一時的な無線ネットワークを確立する際、他端末の中継処理における情報の搾取を回避するため、信号の混信状態を活用した通信方法を検討した。

近年、スマートフォンの普及発達に伴い、生活の様々なシーンでスマートフォンを通した無線通信の利用が進んでいる。さらに、Internet of Things（IoT)に代表されるように、あらゆるモノの状態情報をインターネットに集約することによって、新たな付加価値を見出そうとする検討も進められている。このように、無線通信が生活のあらゆるところで利用されていることに伴い、無線通信の生活基盤としての重要性が高まってきている。その結果、取り扱う情報がよりプライベート性が高まってきており、その情報が外部に漏洩することにより、生活の安全性が脅かされる深刻な状況になる恐れがある。また、生活基盤としての重要性が高まる中、災害時などにおける重要な情報の収集や救助のための情報発信ツールとしても利用が期待されている。しかし、携帯基地局が破損する大規模災害となると大規模な不通状態が生じる可能性がある。そのため、無線通信の持続的な通信環境の提供が必要不可欠である。

このように、無線通信の安全面の向上と持続的な通信環境の提供が今後の無線通信に求められる重要な要件として考えられる。そこで、近年実用が期待されているのが、他の無線端末を利用した中継伝送という方法である。基地局が停止した場合には、他端末を利用した信号の中継伝送により、代替となる通信経路の確立が可能になる。特に、スマートフォンが普及する現在においては、中継伝送を実施する装置は面的な普及率が極めて高く、中継伝送が確立できる環境にあるといえる。しかし、不特定の他端末を中継する際に、情報が搾取される恐れがあり、安全面の低下が問題視されている。

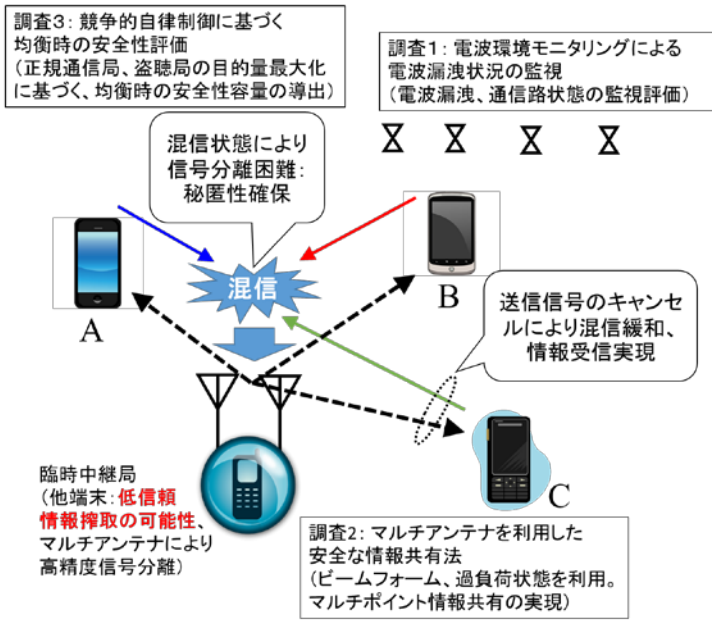
情報漏洩に対する安全面を確保するための対策として、暗号化技術の適用が検討されている。暗号化技術では、情報を暗号文と呼ばれる別の情報系列に変換する。そして、暗号文から元の情報に復元する際、復号鍵と呼ばれる情報が無い場合には、一つの情報に特定することが困難になるため、復号できないことが基本原理となっている。暗号化技術は情報漏洩対策に極めて有効であるが、本来の情報に比べて伝送する情報量が増えてしまい、伝送効率が低下する。特に、スマートフォンなどの端末を経由した情報転送では、端末の電源が少なく制限されており、伝送情報量の拡大に起因する消費電力の拡大は許容できない場合がある。また、IoT などの状態情報を伝送する場合には、伝送する情報自身が極めて小さく、暗号化に必要な情報ビットの付加が相対的に大きなオーバーヘッドとなり、電力消費の拡大が無視できなくなる。そこで、暗号化に加えた新たな安全通信の確立が求められると考えられる。

無線通信における通信の特徴を利用した秘匿性を確保する方法として、物理層セキュリティ技術がある。無線通信はディジタル化に伴い、一定の品質を達成しない場合には、所望とする情報が復調できなくなる。これを、ディジタル通信におけるスレッショルド効果と呼ばれている。スレッショルドとは一定の品質を指す閾値を指し、その品質を達成しないとき、情報が正しく得られない。この特徴を利用することで、正規の通信者に対してのみ正しい情報を伝送し、その他の無線機には復調を困難にする方法が確立される。これを物理層セキュリティ技術という[1]。物理層セキュリティでは、正規の通信者に対して、受信品質を高めるように、アンテナ指向性制御、送信電力制御、符号化などを適用することにより、他者が情報復調に必要な所要品質を高く上げる。また、同時に、他者に対しての品質を落とすため、人工的な雑音信号（人工雑音）を放射することにより、他者の品質を下げる。このように、正規通信者の品質を高め、他者の品質を下げる、品質差を設けることで、他者に対する情報復調を困難にすることが可能になる。

そこで、本研究調査では、持続的な無線通信の確立と他の無線端末による中継及び電波の漏洩に対する情報漏洩対策として、混信状態を活用した中継伝送法について着目した。具体的な方法を図 A に示す。図に示すように、複数の無線機が同時に端末に信号を送信することで、信号の混信状態を生成し、他端末への秘匿性を維持する。一方、中継局は、混信情報を周辺局に報知する。各局は、自局がアクセスした信号を、混信信号から差し引くことで、混信状態を緩和し、復調が可能になる。その結果、他端末への情報漏洩の回避を実現するだけでなく、高効率な情報交換を可能にする。このような同時アクセス環境は、一方の信号が他方

の信号の復調を困難にする保護信号とらえることができ、中継局以外に対する電波漏洩に起因した情報漏洩に対する対策にも有効である。そこで、本研究調査では、混信状態を活用した安全な無線ネットワークを確立するため、三つの研究調査に取り組んだ。

一つ目は、多数端末の同時アクセスによる混信状態を利用した電波漏洩対策効果を明らかにした。ここでは、多数の信号の同時アクセスや人工的な雑音を放射することによって、混信状態を生成することで、電波が室外へ漏洩した際の情報漏洩に対する回避効果を検討した。また、電波センサを用いた電波漏洩の監視体制を確立し、センサを通信区間や周辺区間に網羅的に配置することで、電波漏洩の危険度を通知することや、センサの空間的な分布を考慮した、安全性を高める人工雑音の放射方法について検討した。二つ目は、二端末以上の無線端末及び複数アンテナを利用した、混信状態を活用した安全な情報交換を確立する、多数アンテナ技術（Multiple Input Multiple Output: MIMO）のプレコーダー技術による情報交換法を検討した。三つ目は、中継局による無線システムの運用をかく乱する攻撃的な情報搾取行為に対する耐性評価を明らかにするため、ゲーム理論の原理を取り入れた均衡状態を導出し、本システムの安全性評価を進めた。各調査の成果を以下に報告する。



図A 本研究調査の基本原理と個別調査の関係

２．調査１：電波モニタリングによる電波漏洩状況の監視

２－１：生活センサによるモニタリングを利用した電波利用頻度予測

本調査では、無線通信ネットワークを確立した際の電波漏洩に起因する情報漏洩の可能性について検討を進めた。その基本となる観測として、実際の電波の利用頻度をモニタすることによって、電波の使用状況を観測し、電波が漏えいする危険性を統計評価により明らかにする。その際、電波の使用が部屋内の人物に限られることに着目し、人の生活の様子を表す、温度や湿度、照度などを観測する生活用途向けセンサによるモニタリングを実施し、電波利用状況との関係性を明らかにした。実験の様子を図 B(a)に示す。ここでは、生活センサの配置と同時に、電波利用状況をモニタするスペクトラムアナライザを併用した。生活センサによるモニタとスペクトラムアナライザの時刻同期を確立することで、生活の変化の様子と電波の利用関係が時刻を通して結び付けられるようにした。実験では、5GHz 帯の IEEE802.11 規格の無線 LAN の部屋内のすべての電子機器に接続し、すべてが無線通信経由でインターネットと接続する環境を整備した。また、アクセスポイントを一局に集中することで、アクセスポイントで無線環境の一括観測ができるようにした。さらに、アク

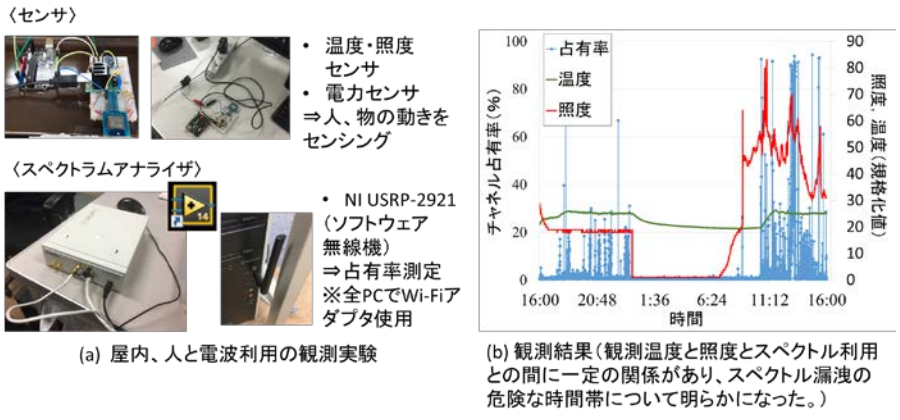


図 B 生活センサ（温度・湿度など）とスペクトル利用率の関係評価
（電波発生頻度（占有率）の明確化）

セスポイントに近接するようにスペクトラムアナライザを配置することで、アクセスポイントから発せられる信号は高感度に検出できる。実験結果を図 B(b)に示す。この結果は、ある 1 日の温度、照度及び一定時間間隔における電波の利用割合（占有率）の結果を示した図である。図より、電波が高頻度に利用されていることを示す高占有率の値のとき、照度が上昇している様子がわかる。それゆえ、人の活動を示す照明の調光が、電波利用に強く関係していることが認められた。一方で、本観測結果とは別に、照度が低い状況においても高い占有率を発生することが観測された。これは、計算機におけるインターネットを経由したソフトウェアアップデータの更新であることを確認した。それゆえ、Internet of Things (IoT)などのような人を介在しない無線通信の確立と人を介した無線通信の確立を区別するためには、生活モニタリング結果と電波の観測結果を比較することで、無線通信利用の差異が顕著に表れ区別が可能になると考えられる。そこで、特に人利用による高いプライベート性のある情報伝送を生活モニタリングの観測結果から識別することで、効果的に漏洩対策をとることができる。なお、本研究成果が応用され、環境モニタリング結果と電波の利用頻度の関係を示す関係モデリングを確立する検討なども進められている[2]。

２－２：多数の電波センサを用いた電波漏洩量の実験

次に、実際の屋内部屋環境における電波センサを用いた電波漏洩量評価を実施した。測定環境を図 C に示す。図中央の円形の部屋において、無線ネットワークが確立された場合、部屋を行き来する廊下において、不特定の人物が出入りすることが想定される。そこで、廊下における電波漏洩量を観測する。その際、無線通信エリアの境界面及び、周辺の部屋の壁面上に電波の漏洩量を観測するセンサを多数配置した。このセンサでは、電波の強度だけでなく、反射波が到来する際に、伝搬遅延に起因した電波の広がり（遅延広がり）も測定できると想定している。このように、通信エリア及び周辺の部屋の壁面上に多数のセンサを廊下周辺に網羅的に配置することによって、廊下上での電波の漏洩量を予測する方法を確立した。具体的な予測方法は次のとおりである。

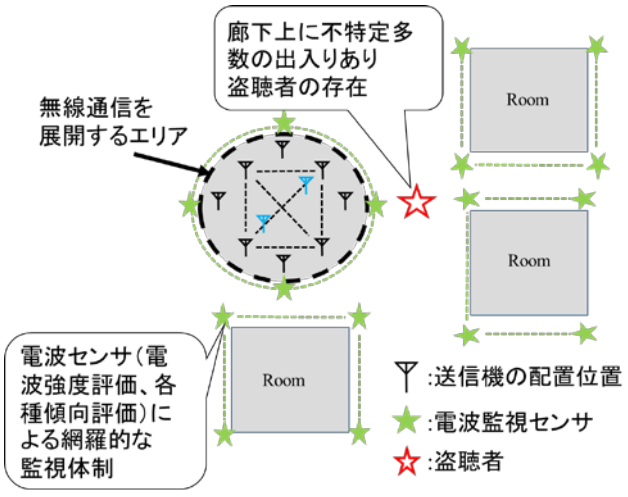


図 C 多数の電波センサを用いた電波漏洩量観測

まず、廊下上に電界強度計を配置し、通信エリアから漏洩する電力量を測定する。その際、壁面上のセンサも同時に漏洩量及び遅延広がりを観測する。その結果、漏洩量に対する各センサの観測量が紐づいた、観測ベクトルが構築される。この観測ベクトルは、通信エリア内の送信機の位置が変化するごとに生成する。その結果、室内の観測数に等しい観測ベクトルが生成される。次に、電波の漏洩状態を複数段階にレベル分けする。その際、クラスタリング技術を用い、各レベルの平均値の探索と観測データの分類わけを進める。その結果、各レベルの平均値に対して、各センサの該当データが紐づけされた新たな観測ベクトルが生成される。以上を、事前観測に基づく学習期間と呼ぶ。学習期間後、廊下に配置した電界強度計を外す。その際、通信エリア内の任意の送信位置において信号を放射した際、廊下での漏洩電力量を予測する。まず、各センサでは、センサを通過する電波の電界強度及び遅延広がりを観測する。各観測結果に対して、学習期間で生成した観測ベクトルと比較し、最も近接するレベルを選択する。各センサが独自にレベルを選択し、全センサの選択結果を集約する。その際、最も高頻度に選択されたレベルの漏洩電力量を推定値とする。観測結果を図 D に示す。本評価実験では、レイトレーシングシミュレータによる評価実験で実施している。レイトレーシングシミュレータは、電波を線分でモデル化し、電波の物体に対する反射、屈折、回折などの物理現象を模擬する。ただし、物理現象の回数の増加や電波の広範囲に放射する様子を再現するため線分の数を増やすと、各回数の増加に対して計算機処理の複雑さが指数関数的に増加する。本研究調査では、現実の計算量で評価するため、各パラメータを少なく限定している。そのため、現実の無線環境との間に一定の差異が生じる可能性があり、その差異を克服するための補間方法については継続的な研究調査となっている。室内の無線 LAN 環境を想定するため、2.4GHz の周波数帯域での評価を進めた。図 D より、レベル区分が 5 パターンにおいて観測したところ、学習期間で生成したレベル結果と実際の盗聴者の受信レベルが高精度に推定でき

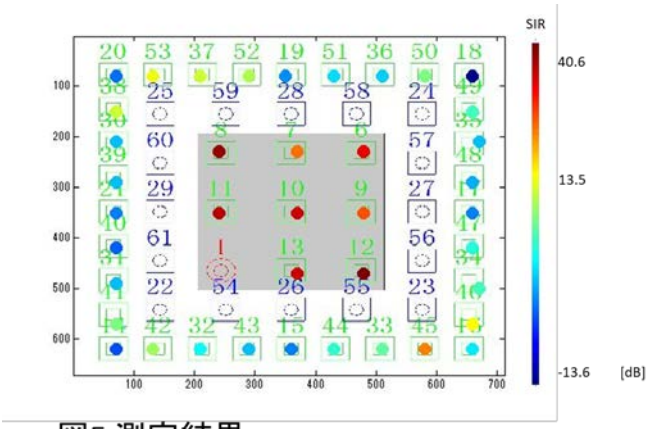
ることがわかる。また、受信レベルに加えて、遅延広がりの観点でレベル選択をした場合にも、同様の結果が認められており、高い推定精度を達成している。それゆえ、今回の評価実験を通し、電波漏洩量の推定に対して、漏洩量を直接的に差し示す電力量だけでなく、関連するデータである遅延広がりも用いることができる可能性を明らかにした。

ダイポールアンテナ				
3パターン				
送信機の位置	オフセット1		オフセット2	
	受信レベル	遅延スプレッド	受信レベル	遅延スプレッド
危険度小(-44.42dBm)	11	15	35	34
危険度中(-40.53dBm)	14	8	8	6
危険度大(-35.77dBm)	21	23	3	6
オフセット時の盗聴者の受信レベル	-38.85dBm		-45.14dBm	
5パターン				
送信機の位置	オフセット1		オフセット2	
	受信レベル	遅延スプレッド	受信レベル	遅延スプレッド
危険度1(−48.09dBm)	2	3	16	9
危険度2(−45.98dBm)	9	12	19	25
予想される危険度	14	8	8	6
危険度4(−38.81dBm)	20	18	2	5
危険度5(−33.94dBm)	1	5	1	1
オフセット時の盗聴者の受信レベル	-38.85dBm		-45.14dBm	

予測される危険度から
実際の受信レベルが高精度に推定可能

受信レベルに加え
遅延スプレッドにおいても
受信レベルに高い相関関係

図D レイトレーシングシミュレーターによる評価結果
(事前測定結果による危険度評価(事前学習)を進め、
観測結果の近似性を使った漏洩量予測を実施)結論:信号漏洩の予測には、受信レベルだけでなく関係信号(遅延スプレッド)などの考慮が有効



図E 測定結果
人工雑音源は、破線の円が示す箇所であり
合計16か所である。中央の四角い通信エリアに対して
外向きにアンテナ指向性を設計し、人工雑音
を放射することで、通信エリア内(灰色内)のSIRは
高く維持し、それ以外(白色部分)では低いSIRとなった。

２－３：人工雑音信号との混信を利用した漏洩対策

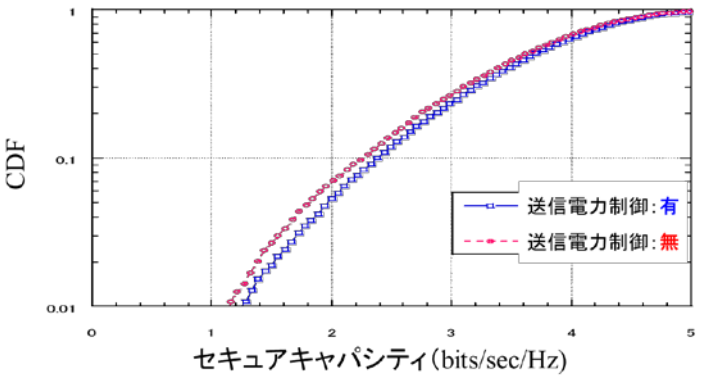
人工雑音を用いた混信状態を利用した秘匿性について評価した。人工雑音の放射は、盗聴者の受信信号電力対干渉雑音電力比（SINR）を低減するが、正規通信局に対しても深刻な干渉となり、SINR を低下させる。そのため、正規通信局の復調に必要な SINR が低下するため、盗聴局に対して復調に必要な SINR が低下し、復調困難性が低下する。その結果、人工雑音に対して、盗聴局の受信 SINR の低減と正規通信局の SINR の向上の両立が不可欠である。そこで、本研究調査では、通信エリアに対して垂直外向きにアンテナ指向性を向けるように配置した。その結果、通信エリア外の SINR の削減を実現し、盗聴局の復調困難性を向上させると同時に、正規通信局の所要 SINR の向上を両立している。また、本研究調査の提案法では、人工雑音発信源に電波受信結果を観測する電波センサ機能を取り付けている。これは、室外に向けた電波漏洩状況を観測し、適応的に送信電力を制御するためである。その結果、過剰な送信電力の増加による、消費電力の削減や正規通信者に対する、SINR の低下を回避している。また、室外に向けた電波漏洩量を予測するため、距離に比例した簡易な外挿方法を取り入れている。図 E に、レイトレーシングシミュレータを利用した SIR 評価結果を示す。ここでは、雑音を 0 としているため、評価結果を SIR としている。図より、人工雑音の指向性制御により、通信エリア内の SIR を高く維持している一方で、通信エリア外の SIR を効果的に抑制していることがわかる。それゆえ、人工雑音を利用した混信状態の確立によって、一定の電波漏洩対策が可能であることを確認している。

３．調査２　マルチアンテナを利用した安全な情報共有法

3-1 空間ブロック符号化（STBC）を活用した、安全な情報共有法の確立

三つの無線機において、一つが中継器、残りの二つが情報交換を実施する無線機とした場合の情報交換方法は、物理層ネットワークコーディング（PLNC）を活用した方法により、実現できることは明らかになっ

ていた[3]。そこで、無線機が三局以上における情報交換方法を確立した。単純化のため、中継局のアンテナ数を 3、無線局数を 3 として、相互に情報交換を実施する。まず、三局が同時に中継局に信号を送信する。その結果、中継局では、3 つの信号が混信する信号を二つのアンテナで受信する。ここで、各アンテナの通信路状態は統計的に独立と仮定した。その結果、各アンテナでは 3 種類の送信信号が異なる伝達関数を通過して受信され、合成されている。そこで、中継局では、この合成された二つの信号を送信信号と見立て、二つの信号を二つのアンテナで並列送信する STBC を適用した。STBC を適用した後の受信信号を、中継局から３つの無線局へ報知する。その際、ブロック符号化のため送信すべき信号が二種類となり、時間分割で送信する。その結果、信号送信に時間を消費する。この結果、各無線局は 3 つの信号が合成された混信信号を 2 種類受信する。



図F STBCを用いた低信頼中継局を利用した端末間情報交換法の安全性を考慮した通信容量
（送信電力制御の適用により、通信容量の改善を確認）

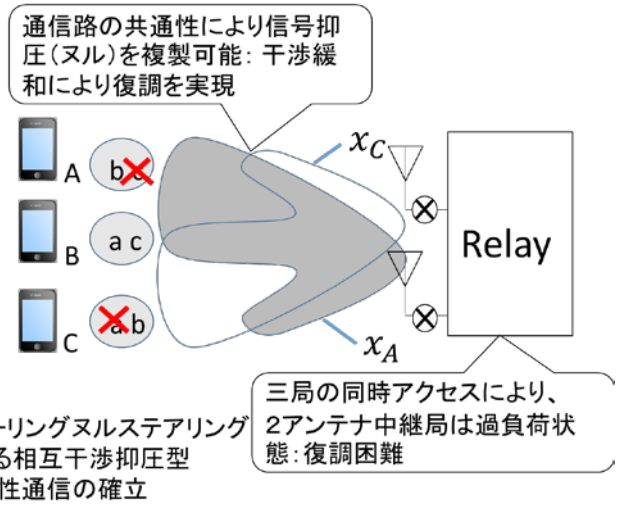
復調方法は次の通りである。まず、自局が送信した信号は既知であるため受信信号から差し引く。そして、残りの信号は、STBC 復号処理後に Zero Forcing フィルタ処理（処理のイメージ：連立方程式の解を導出する方法と等価）を適用する。その結果、三種類の信号の分離復号が可能になる。一方、中継局では、三つの信号が合成されて二つのアンテナで受信をするため、送信信号数に比べて受信アンテナ数が少ない過負荷状態となり、線形的な復調処理では分離することができない。また、干渉キャンセラーや最尤復号法（MLD）などを活用することで、無線機から送信された信号の電力差が大きく生じた場合に、復調できる可能性が高まる。そのような復調可能性を回避するため、各送信局では中継局へのアクセスの際、適応送信電力制御を適用した。送信電力制御では、各局の通信路状態情報に適応した電力を制御することによって、中継局で受信した信号の電力差が生じないように設計する方法が考えられる。しかし、各端末に伝搬した受信状態で決定される所要 SINR が大きくなる場合にも、中継局での復調が困難になる。そのため、中継局の SINR の低下だけでなく、各無線局の SINR の向上が、復調困難性をより高くすることができる。そこで、送信電力制御を各端末間伝送容量から中継局に対する情報漏洩量を差し引いた安全性を考慮した通信容量を定義し、通信容量を最大にする送信電力制御を適用した。その結果、提案送信電力制御法を適用することで安全性の向上が達成される。図 F に、安全性を考慮した通信容量に対する累積分布確率（CDF）を示す。この評価では、各無線端末と中継局間の距離は等距離と仮定し、通信路をレイリーフェージングでモデル化している。通信路容量の導出においては、シャノンの情報容量定理に基づく公式により導出している。計算機シミュレーションによる評価の結果、送信電力制御を適用した提案法が高い通信容量を達成し、安全性の確保と通信容量の拡大を実現している。

３－２ミラーリングヌルステアリングを用いた、安全な情報共有法の提案

３－１の STBC による安全な情報共有では、中継局で二種類の送信信号を伝送するため、信号送信に必要となる時間数が増え、伝送効率が低下する。一方、各無線局において利用者が WEB コンテンツを利用している途中などコンテンツを利用している最中においては、伝送すべき情報が必ずしもない場合がある。そこで、一つの無線端末が残りの二つの無線局に情報を共有する高効率な方法としてミラーリングヌルステアリングを用いた MIMO 中継伝送法を確立した。

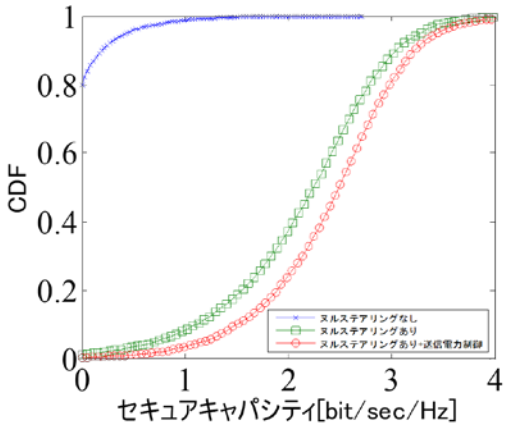
提案法では、一つの無線局は情報を、残りの二つの無線局では伝送すべき情報がないため、中継局での復調可能性を回避するため、人工雑音を用いた疑似信号を送信する。中継局は二つのアンテナを想定する。中継局では、二つのアンテナを三つの無線局から信号を同時に受信するため、過負荷状態となり復調困難になる。次に、中継局では、二つの中継局アンテナで放射した信号が受信アンテナで合成されるとき、信号がキャンセルされるように送信重みを割り当てる。これをヌルステアリングという。その際、人工雑音を放射した二つの信号はそれぞれが通過した無線通信路の伝達関数が、各端末間で受信された信号において共通であ

る特徴がある。その結果、一方の信号に対して設計したヌルステアリング（例えば A 局から C 局に対しての信号伝搬に対するヌルステアリング）が、他方の信号に対して設計したヌルステアリング（例えば、C 局から A 局に対しての信号伝搬に対するヌルステアリング）と同じ設計重みとなるため、ヌルが各々の人工雑音局に向けることができる。そのイメージ図を図 G に示す。このように、二本のアンテナでありながら対称関係により、ヌルが二つ形成される現象をミラーリングヌルステアリングと称する。その結果、各無線局に対して、人工雑音を 1 つ打ち消すことができる。よって、第 3 局（B 局）が信号を伝送するため、中継局へ信号を伝送する。その際、A 局と C 局が人工雑音を放射することで、3 種類の信号（二種類の人工雑音と B 局の所望信号）が混信されて中継局に受信される。



図G 混信状態を利用した情報交換法
（ミラーリングヌルステアリングを用いた方法、盗聴困難性を高める人工雑音をヌルステアリングを利用して除去。安全な端末間情報共有実現）

中継局では、ミラーリングヌルステアリングにより伝送することで、A 局では C 局から伝送された信号がキャンセルされて打ち消される。一方、A 局自身が送信した人工雑音は、自局の信号としてキャンセル可能である。その結果、B 局の信号を復調することができる。同様の理由で C 局においても、B 局の信号を復調できる。その結果、B 局の信号を STBC とは異なり一つの送信信号伝送できるため、伝送時間の短縮を達成し、伝送効率の向上を実現している。図 H に計算機シミュレーションによる評価結果を示す。通信路環境として、レイリーフェージング通信路を仮定し、各端末と中継局の距離は互いに等しいと仮定した。図に示す通り、ヌルステアリングを用いることで、安全性セキュリティが高く維持することができることがわかる。また、中継局での復調困難性を維持するため、調査３－１と同様に送信電力制御を適用したところ、安全性を考慮した通信容量の拡大に成功している。



図H 安全性セキュリティ評価結果
提案（赤の特性）が高い安全性セキュリティを実現（ミラーリングヌルステアリングによる干渉制御、送信電力制御による、低信頼中継局への安全性確保）

４．調査３： 競争的自律制御に基づく均衡時の安全性評価

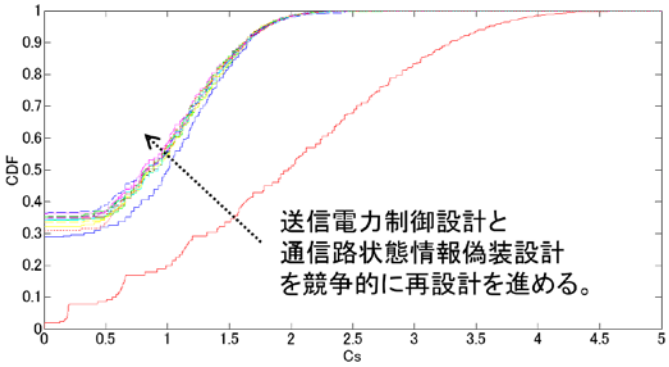
調査２において混信状態を活用することによって、低信頼の中継局を利用した場合にも、安全性の高い端末間の情報交換が可能になることを明らかにした。しかし、調査 2 における安全性を実現するため、二つの処理が行われている。まず、送信電力制御を適用することで、中継局における受信電力差が最小になるようにした。その結果、偶発的な信号の電力差の発生に伴う、中継局での復調可能性を回避している。次に、各中継局の送信アンテナでは、ミラーリングヌルステアリングを形成するため、送信プレコーダーに基づく、送信ウェイトを設計している。しかし、これらの実現には、通信路の状態情報を示す、通信路状態情報（CSI）が必要になる。特に、無線端末が送信電力制御を適用するためには、受信機である中継局が伝達関数を推定し、それを別チャネルで端末に通知しなければならない。その際、悪意ある中継局の場合、CSI を偽装することで、送信電力制御の設計を狂わせ、中継局における受信電力差が生じるように、誘導することが可能になる。これを、CSI 偽装を用いた、中継局での情報搾取法という。

これまでに、CSI 偽装における情報搾取法に対して、中継局が情報搾取できる情報量を最大化し、その際正規通信者に偽装を気づかれないように最適に CSI を偽装する方法を提案している[4]。ここでは、CSI の偽

装を正規通信局が認知しない基準として、CSI の統計分布の維持を用いている。CSI は、レイリー分布やライス分布などの確率分布に従う乱数でモデル化される。そこで、偽装した CSI の通知においても、無限時間観測した結果の統計量が同じ分布に従うことで、偽装された CSI と実際の CSI の統計量に明確な差は生じることがない。そこで、CSI 統計量を維持することによって、正規通信局が偽装を認知することがないという仮定を設けた。このような CSI 偽装方法は、実際の CSI から偽装する CSI へと線形変換された関係としてモデル化できるため、情報搾取量を最大化する線形計画問題として CSI 偽装法は確立されている。一方、送信電力制御に対しては、調査 2 で検討しているように、安全性セキュリティを最大にするように最適設計している。一般に、安全性を考慮した通信容量は、対数関数などによる非線形関数で与えられる。また、送信電力は無線機機能の限界に伴い、一定電力以上を出力できない。それゆえ、総送信電力の限界の制約のある非線形計画問題として、安全性を考慮した通信容量最大化問題として確立され、送信電力は設計されている。

図I 低信頼中継局と正規通信局の各目的量最大化に基づくナッシュ均衡解の導出

正規通信局：安全性通信容量を最大化する送信電力制御最適化
低信頼中継局：情報搾取容量を最大化する通信路状態情報の最適偽装



図J 安全性通信容量の特性結果

均衡状態に向けて、安全性容量に収束傾向（ただし、状態は二安定的（安全容量と搾取容量の最適値を交互に移動）で振動傾向もあり）

これらのシステム関係を整理すると図 I のようになる。つまり、正規通信者は、安全性を考慮した通信容量を最大化するため、総送信電力に限界が設けられた、制約付き最適化問題として送信電力制御を確立している。一方、盗聴者の立場では、情報搾取量を最大化し、同時に正規通信局に偽装を気づかれないという制約下での CSI 偽装として最適化問題として確立される。このように、二つの独立したシステムが共通のリソースに対して各々の目的量を最適化する問題は、ゲーム理論に基づく各種理論を適用することができる。特に、二つのシステムが最大化の戦略を設計し、各目的量が変動せず不動となる状況をナッシュ均衡という[5]。そこで、本研究では、このナッシュ均衡を達成する状態における、安全性セキュリティの評価を実施した。最初に、安全性セキュリティを最大にする最適送信電力設計を確立する。その結果、CSI 通知と最適設計パラメータ（重み）との関係性を確立できる。そこで、中継局は情報搾取量を最大化するように、CSI の通知を偽装する。そして、真の CSI に対する偽装された CSI 通知との関係性が与えられる。この関係性は、正規通信局にも既知であるため、その関係性を考慮したうえで、情報搾取量をゼロとするように送信電力制御を再設計する。再設計された送信電力制御に基づき、再び CSI の偽装関係を再設計する。このように、送信電力制御と CSI の偽装方法の再設計を繰り返すことで、安全性を考慮した通信容量あるいは情報搾取量が一定となる均衡状態へと移行していき、均衡状態における、各種通信容量が本システムの安全性を考慮した通信容量としてとらえられる。

このような検討システムに対する影響を計算機シミュレーションにより評価した。評価環境として二つの無線機における情報交換を想定した。また、中継局のアンテナ数は 1 とした。通信路環境としてレイリーフェージングを仮定し、中継局と各無線局間の通信距離は等しいと仮定している。また、無線局間は直接信号を伝送することはできないと仮定し、通信路状態情報の通知にたいして、中継局が偽装することによる変化はあるが、推定誤りに起因する通信路状態情報の推定結果の変化は生じないと仮定した。さらに、中継局の

送信電力量の制約は設けないとして、通信路状態情報の偽装と実際との間の差異に起因した、復調困難性は克服できるとする。

具体的な評価結果を図 J に示す。この結果では、横軸に安全性を考慮した通信容量を縦軸に、横軸を下回る確率（CDF）を示している。図より、設計を繰り返すことで、安全性を考慮した通信容量がある一定の値に収束する様子が確認できる。このように、一定の安全性を確保したうえで、伝送できる確率が 60%程度確保できることがわかる。しかし、この結果から、二つの調査が明確になっている。まず、40%のうち、CSI の偽装を再設計した直後においては、約 10%の割合で情報搾取ができることがわかっている。しかし、その後送信電力を再設計することで、10%が搾取される割合は 0 となる。そのため、情報搾取量が 0 に安定するのではなく、0 と 10%を振動する状態となっている。この結果は、検討したシステムでは、10%の情報搾取が機能限界として明らかになったと考えられ、それを克服するためには、暗号化等による別のセキュリティ技術が必要になる。しかし、このように情報搾取が 10%生じることが明らかになったことにより、過度な暗号化を適用する必要がなくなり、高効率な伝送が確立できたと考えることができる。

５．まとめと今後の研究課題

本研究課題では、信号の混信状態を利用することで、無線ネットワーク上での復調困難性を確保し、混信状態前の部分信号を有する受信者だけが、信号受信を可能にする安全性の高い通信を確立する方法について検討を進めた。検討では、三つの個別課題を設けた。一つ目の課題では、電波漏洩に対して多数の電波センサによる監視方法、および監視結果を利用した人工雑音発射により、正規通信者の発した信号と混信することで、復調を困難にするエリア展開を確立できることを明らかにした。二つ目の課題では、複数アンテナを有する中継局に対して、複数の無線端末において、中継局に対する情報漏洩を回避しながら情報交換をする、マルチアンテナ技術の確立を進めた。本課題の成果により、無線機数の拡大や、アンテナ本数の拡大を実現しており、無線ネットワークを構成するネットワークハブ機構としての役割を担うことが可能になり、安全性の高いネットワーク展開を可能にしている。三つ目の課題では、実際の中継局が悪意ある利用者により、通信制御をかく乱するように、通信路状態情報を偽装する攻撃に対して、混信を利用した通信方法の安全性について評価した。この課題では、ゲーム理論による理論検討を取り入れ、正規通信者と盗聴者との間で、各目的量を最大化する競争モデルを導出し、均衡状態を引き出すことで、検討する無線通信ネットワークの安全性について定量的に明らかにした。この結果により、情報漏洩の可能性について明らかにするとともに、漏洩を回避するために必要となる暗号化方法についての設計を示すことができると考えられる。

三つの個別研究課題の実施により、混信状態を活用した無線ネットワークについて安全性が明らかになったといえる。しかし、安全性を確保するための通信容量の低下や、通信制御のための通信路状態情報の伝送によるオーバーヘッドについては議論されていないため、引き続き検討が必要である。加えて、ゲーム理論による議論展開から、一定の情報漏洩の危険性が明らかになった。その対策として、強い制約を設けることが考えられ、現状の通信路状態情報の統計的分布の維持という制約は、通信路状態情報の連続性を維持することは保証されていない。そこで、時間連続性など、通信路状態情報の偽装に対する正規通信者の認知方法を高感度化することによって、より情報搾取は困難になると考えられる。それゆえ、偽装方法の検出精度の高感度化が今後の重要な研究課題となっている。

【参考文献】

[1] Matthieu Bloch, Joao Barros, Physical-Layer Security, Cambridge University Press, 2011
[2] 藤井威生、田久修、太田真衣、クラウドソーシングを用いた多次元環境認識による先進的無線ネットワークの研究開発、総務省受託研究費 SCOPE 平成 28 年度課題
[3] Kazuma Yamaguchi, Osamu Takyu, et al.,``Physical layer network coding with multiple untrusted relays for physical layer security,” in proc IEEE APSIPA ASC, 5 pages, Dec. 2014
[4] Osamu Takyu, et al., ``Optimal impersonation of CSI for maximizing leaked information to untrusted relay in PLNC,” in proc IEEE WCNC 2016, 5 pages, April 2016
[5] 小島寛之、松原望、戦略とゲームの理論、東京図書 2011 年 9 月

〈発　表　資　料〉

題　　名	掲載誌・学会名等	発表年月
PLNC 無線通信システムにおける低信頼中継局による CSI 偽装への対策	電子情報通信学会　無線通信システム研究会（ＲＣＳ）	2016 年 6 月
低信頼中継局における情報搾取量を最大にする CSI 偽装の再設計	電子情報通信学会　ソサイエティ大会	2016 年 9 月
低信頼中継局による MIMO スイッチングにおける STBC と PLNC を用いた物理層セキュリティ	電子情報通信学会 総合大会	2017 年 3 月
低信頼中継局における MIMO プレコーダを利用した安全な情報共有法	電子情報通信学会　無線通信システム研究会（ＲＣＳ）	2017 年 7 月
マッシブ無線センサを用いた電波漏洩モニタリングの検討	電子情報通信学会 スマート無線研究会（ＳＲ）	2017 年 7 月