様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２７　年　　６　月　　３　日現在

機関番号：　１２６１２
研究種目：　基盤研究(B)
研究期間：　2012～2014
課題番号：　２４３６０１４７

研究課題名（和文）学習を活用した物理層セキュリティ技術によるセキュアコグニティブ無線

研究課題名（英文）Secure Cognitive Radio using Physical Layer Security with Learning

研究代表者
藤井　威生（Fujii, Takeo）

電気通信大学・先端ワイヤレス・コミュニケーション研究センター・教授

研究者番号：１０３２７７１０

交付決定額（研究期間全体）：（直接経費）　　14,000,000円

研究成果の概要（和文）：本研究課題では、多様な無線資源をダイナミックに活用し、周波数の有効利用を図るコグニティブ無線環境で、物理層セキュリティ技術を核とした通信セキュリティの向上を目指す研究を進めた。ここでは、干渉に関する制約を満足した上でセカンダリ通信の品質向上と周波数有効利用を図るため、新たなマルチチャネル選択法、スペクトラムの貸し出しを考慮したビームフォーミング法、低信頼中継局を用いた場合の秘匿性向上法などの検討を行いその有効性を確認した。

研究成果の概要（英文）：In this research, in order to dynamically utilize various types of spectrum resource for improving the spectrum efficiency based on cognitive radio, we focus on physical layer security techniques for the research of improving communication security. Here, we consider a novel multi-channel channel selection method, a beamforming algorithm suitable for spectrum leasing, improving security under a relay networks including unreliable relay node and so on. Finally, the effectiveness of the proposed methods are confirmed.

研究分野：　移動通信

キーワード：　コグニティブ無線　物理層セキュリティ　学習

１．研究開始当初の背景

周波数資源不足の抜本的な対策として、現在利用されている無線システムと周波数を共用し、利用可能な周波数資源を格段に増やすコグニティブ無線技術が検討されている。このような周波数共用環境では、複数の高機能無線機が同一の帯域に多数共存することから、常に自分の無線通信信号を他の無線機が受信できる環境にさらされることとなり、秘匿性を保持した通信が脅かされる恐れがある。通信の秘匿性は情報の暗号化などにより保護されてきたが、一度暗号が解読されると常に盗聴のリスクにさらされる問題や、暗号、復号に大きな演算量を必要とするなど課題が多い。そこで、これらの課題を解決する方法として、情報理論の通信路容量の限界を活用し、信号の復号を妨げることで秘匿性を確保する物理層セキュリティ技術が注目されている。物理層セキュリティは、信号電力と干渉電力および雑音電力(SINR:信号対干渉＋雑音電力比)によって定義されるシャノンの通信路容量を活用し、正規の受信ユーザの通信路容量を盗聴者の通信路容量より大きく保つことで、理論的に盗聴者が情報の復号をできなくする技術であり、通信方式の工夫によりセキュリティの向上をもたらすことが可能となる。

そこで、本研究課題では、周波数共用環境における秘匿性向上のために物理層セキュリティ技術の活用を目指した。そのためには、秘匿性確保のため、周囲への人工雑音の発生や、意図的な送信ビームの変形により秘密保持容量を拡大する必要がある。これらの信号生成は、周囲の干渉電力を増加させることから、周波数共用環境ではプライマリシステムの干渉保護に反する働きをしてしまう。本研究課題は、周波数共用のための干渉回避と、SINR を一定以下に保つことによる秘密保持領域の確保というトレードオフ関係にある二つの規範を拘束条件として満足させた上で、安全で高速・大容量なコグニティブ無線の実現を目指して研究した。

２．研究の目的

本研究課題では、多様な無線資源をダイナミックに活用し周波数の有効利用を図るコグニティブ無線において、物理層セキュリティ技術を核とした通信セキュリティの向上を目指し、以下の具体的な目標を掲げて研究を行った。

１．コグニティブ無線ならではの多様な無線資源を活用した秘密情報分散化による秘匿性向上

２．ノードが観測可能な統計量情報を活用した学習によるセカンダリ最適伝送

３．既存システム干渉保護と盗聴ノードに対する人工雑音付加による秘匿性向上の両立

４．複数の分散ノードを協調活用することによる適応的な通信品質および秘匿性向上

このように、本研究はコグニティブ無線の多様性に着目し、干渉に関する制約を満足した上でセカンダリ通信の品質向上と周波数有効利用を図ることが可能な新たな無線ネットワークを創ることを目的としている。

３．研究の方法

本研究課題では周波数共用における干渉保護と物理層セキュリティによる秘匿性保護を両立するための研究として、周波数共用および秘匿性保護条件下でセカンダリ無線システムの通信路容量を最大とする最適条件を明らかにすることを目指し、その実現手法に関して検討した。ここでは以下のように課題を設定し、研究代表者、研究分担者、連携研究者が互いに役割分担して研究活動を行った。

協調通信および分散無線による干渉および秘匿性保護手法の検討：プライマリ受信機の干渉量を一定以下に保ちつつ、セカンダリ通信の通信路容量を改善したうえで盗聴者の SINR を最小化するように周囲の分散ノードを制御する手法の検証、さらに、複数帯域・複数ルートを活用した秘密情報の分散化効果を活用した秘匿性向上の検討

統計量情報に基づく学習理論を用いた干渉および秘匿性保護領域設計手法の検討：セカンダリの秘匿性保持とプライマリの干渉保護を両立するため観測可能な統計量を用いたパラメータの最適設計に関する検討

実証実験による干渉および秘匿性保護性能の検証：検討の総括として干渉および秘匿性保護性能の確認のため、ソフトウェア無線プラットフォームを活用した実証試験の実施

これらの課題に対して研究に携わる研究者および大学院学生の研究協力者が連携して検討を行った。本報告では多数の研究成果の中から代表的な研究成果を抽出して報告するものとする。

４．研究成果

（１）コグニティブ無線環境下での通信秘匿性向上のためのチャネル選択を考慮したマルチバンド伝送法

コグニティブ無線では、一次ユーザ(PU: Primary User)が利用していない空間的・時間的空きチャネル(WS：White Space)に二次ユーザ(SU: Secondary User）がアクセスすることで周波数共用による周波数利用効率の向上を目指す。一方、コグニティブ無線では、SU がチャネルを共用することで、意図しないユーザへの情報漏えいの可能性が高まる。本研究では、SU 通信において、盗聴者(Eve)の計算能力を問題としない物理層セキュリティの導入を考える。物理層セキュリティは、正規送信機(Tx)が盗聴リンク(Tx-Eve)間の通信路容量を超える伝送レートで通信することで、Eve による低い誤り率での復号を阻止する。その指標として Tx-Rx 間の通信路容量と Tx-Eve 間の通信路容量の

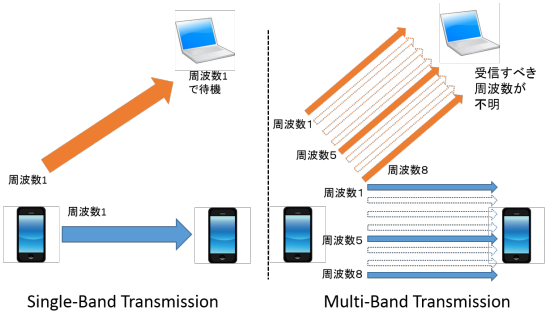

図 1　シングルバンド伝送とマルチバンド伝送

差で定義される秘密保持容量を定義し、正の秘密保持容量による通信を実現することで安全性が保たれる。ここで Rx は正規受信機とする。本研究では、PU 存在下での秘匿伝送手法として、チャネル選択を考慮したマルチバンド伝送を提案する。本手法により、マルチバンドでの同時伝送による周波数軸上での情報分散と、通信路応答と PU 利用状況を加味したチャネル選択による秘密保持容量の向上を狙う。

マルチバンド伝送では、送信機が L 個の周波数チャネルから n 個の周波数チャネルを選び、それぞれ異なる秘密情報を n チャネルで受信機へ分散させて同時送信する。これによって、盗聴者がある周波数を盗聴しているとき、周波数軸での情報の分散効果が望める。マルチバンド送信機が利用する周波数チャネルは、1 つの周波数帯を分割した帯域幅を持つサブチャネルで構成される。それに対し、シングルバンド伝送では、分割されていない 1 つの周波数チャネルを利用する。このとき、盗聴者が各伝送のチャネルを j チャネル盗聴可能としたときの、シングルバンド伝送とマルチバンド伝送の各伝送方式の概要図を図 1 に示す。

マルチバンド伝送を利用した秘密保持容量の向上のため、L 個のサブチャネルから SINR が大きい順に n 個のチャネルを SU 通信用に選択する。ただし、PU と周波数共用するチャネルの場合は与干渉電力制約を満たす送信電力で送信を行うものとして SINR を計算する。PU が存在しない WS チャネルを利用する場合は、送信可能電力で送信を行い、PU からの干渉電力項は 0 となる。

シングルバンド伝送とマルチバンド伝送による秘密保持能力の違いを検証するため計算機シミュレーションを行った。シングルバンド伝送では、10 個の 5GHz 帯の周波数チャネルから分割されていない 1 個の周波数チャネルを選んで情報送信し、マルチバンド伝送では、5GHz 帯で 1 個のシングルバンド伝送に用いた周波数チャネルをそれぞれ 3 分割した合計 30 個のサブチャネルから 3 個のサブチャネルを選び 3 サブチャネル並列で情報を送信するとした。

ここで、PU 利用状況を加味した SINR に基づくチャネル選択(SINR-based-CS)と SU のチャネル状態のみを考慮したチャネル選択(H-based-CS)によるマルチバンド伝送の比較を行った。各手法は PU チャネルを選択時は PU 保護を行っている。送受信機がそれぞれ(0,0), (50,0)の位置にあるモデルを考え、送信機と盗聴者の距離を 0[m]から 150[m]まで変化させ、秘密保持容量を n=3 としてシミュレーション評価した。シミュレーション諸元は表 1 の通りである。セカンダリユーザ送信機は PU の保護用件を満足した上での SINR の最大化によってチャネル選択するため、Eve の情報は利用しない。Eve は各伝送で SU が利用するチャネル数と帯域幅と同じ数、大きさだけ盗聴できるとする。Eve の盗聴方法は、ランダムにチャネルを盗聴するとした。ここで、j 本盗聴される確率を $P_r(j)$とし、ランダムに盗聴される際の $P_r(j)$を表 2 にまとめた。図 2 に、PU チャネル利用率 50%における SINR-based-CS と H-based-CS の比較を示した。各カーブは j 本盗聴されたときの秘密保持容量となっている。図 2 より、PU 利用状況を含めた SINR ベースでチャネル選択することで、最大で約 12%秘密保持容量を向上できることを確認した。

表 1　シミュレーションパラメータ

Total transmitted power	10[dBm]
PU's transmitted power	10[dBm]
PU channel usage	0～30
Allowed interference power at PU	-90[dBm]
AWGN	-108[dBm/MHz]
Fading	Rayleigh
Avalable freqency band	5.18～5.36[GHz]
Reference distance	10[m]
Pass loss index	3

表 2　シングルバンド伝送、マルチバンド伝送の盗聴確率（ランダムチャネル盗聴の場合）

$P_r(j)$ \ j	0	1	2	3	
P_{Single}	0.9	0.1			Total=1
P_{Multi}	0.72	0.26	0.02	0.0003	Total=1

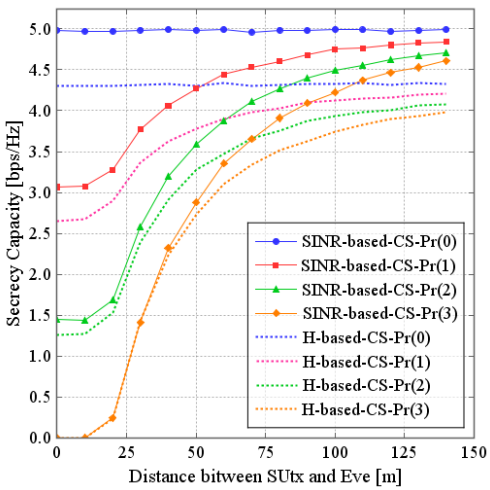

図 2　チャネル選択法による秘密保持容量

（2）プライマリ安全通信のためのスペクトルリーシングにおける複数セカンダリ送信ビームフォーミングの検討

コグニティブ無線において、プライマリが、所有する周波数帯域の一部を、セカンダリシステムに貸与し、その代償として、協調通信を要求するスペクトルリーシングが検討されている。一方、無線通信は、有線通信と比べ盗聴の危険性が高い。従来、計算量的安全性に基づく暗号化により、セキュリティを確保している。しかし、計算機性能が十分に高い場合、復号・解読される危険性がある。そこで、計算の複雑さに基づかずに、安全な通信を実現する物理層セキュリティへの関心が高まっている。正の秘密保持容量を達成するための一手法に、複数アンテナを利用し、電波の指向性を制御するビームフォーミング（BF : BeamForming）を用いた手法がある。代表的な BF に、非所望ユーザへヌルを形成するゼロフォーシング（ZF : Zero Forcing）BF 及び所望ユーザの受信信号電力を最大にする最大比伝送（MRT : Maximal Ratio Transmit）BF がある。従来文献では、盗聴者存在下で、プライマリ安全通信のためのスペクトルリーシングが検討された。セカンダリシステムは、ZF-BF 及び MRT-BF から生成するビームフォーミングを用いて、プライマリの秘密保持容量保証と自身のデータ送信を実現した。しかし、従来のシステムモデルでは、セカンダリは一対に限定されている。また、MRT-BF に電力を割り当てることで、プライマリに対して干渉が発生してしまい、プライマリ通信の安全性が保証できる場合でも、プライマリスループット特性は、劣化しまう可能性がある。

そこで、本研究では、図 3 に示すようにセカンダリが複数存在するモデルを検討し、プライマリに対して干渉を発生させない直交ビームフォーミングを用いた協調通信について検討した。セカンダリ間での協調の有無を考慮し、グラムシュミット直交化及びチャネルインバージョンを利用した直交ビームフォーミングを協調通信に用いて、プライマリ安全通信を実現する。本手法の有効性を確認するため、プライマリ通信安全性及びセカンダリスループットを計算機シミュレーションにより評価し図 4-6 に結果を示す。

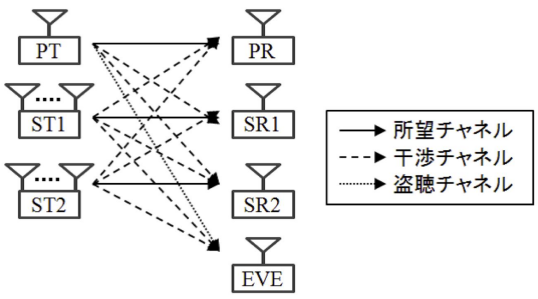

図 3　システムモデル

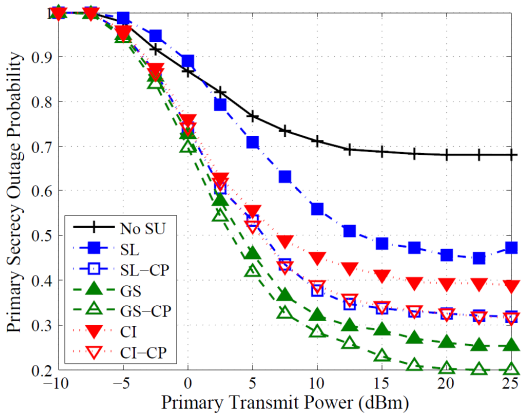

図 4　PU 秘密保持容量アウテージ確率

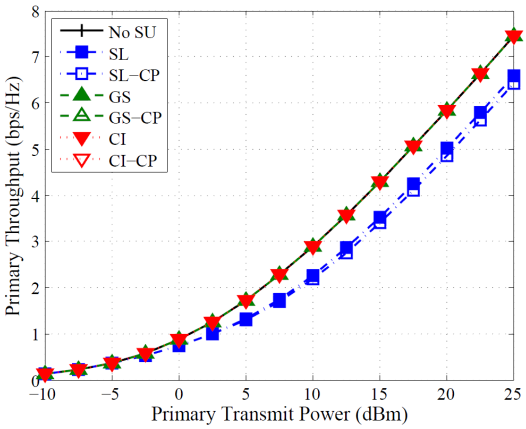

図 5　PU スループット特性

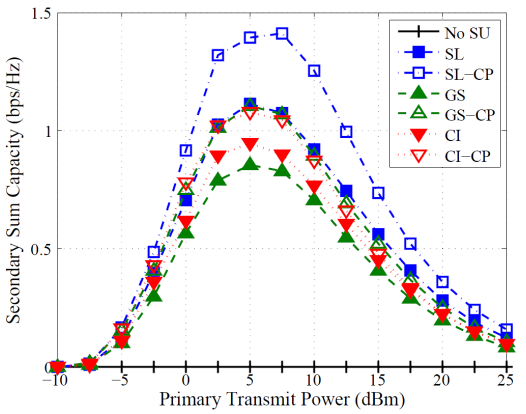

図 6　SU 総スループット特性

これらの結果より、スペクトルリーシングにおいて、直交ビームフォーミングを用いた協調通信は、プライマリスループットの劣化を防ぎ、プライマリの通信安全性を改善することを示した。

（3）低信頼中継局を利用した物理層ネットワークコーディングによる秘匿通信の検討

オフィスなどで一時的な無線通信ネットワークを構築する際、他の無線機を中継局として利用するアドホックネットワークが簡易接続性や高い柔軟性の観点から注目されている。しかし、上位クラスの情報にアクセ

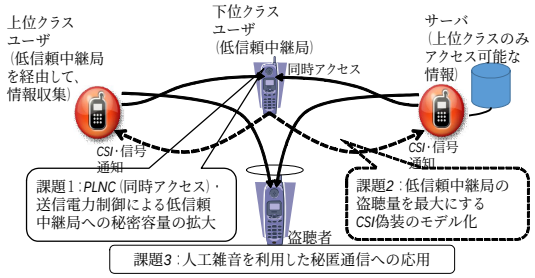

図7　低信頼中継局を利用した物理層ネットワークコーディングによる秘匿通信の検討

スできるユーザが下位クラスのユーザを中継局として利用した場合、下位クラスのユーザに情報が漏洩する恐れがある。このようなユーザを低信頼中継局と呼ぶ。低信頼中継局に対する秘匿通信を確立するため、物理層ネットワークコーディング（PLNC）に注目した。PLNC は、二つの無線拠点が同時に中継局にアクセスすることで、相互の信号が干渉となり中継局では復調が困難になる。一方、各拠点は自身が送信した信号を中継信号から取り除くことで、他拠点が送信した信号を復調することができる。PLNC における秘匿通信を実現するため、本研究では、図 7 に示す三つの課題に取り組んだ。1 つ目は秘密保持容量を最大化する準最適送信電力制御である。中継局に同時に受信される信号の電力差が大きくなると、一方の信号が強く現れ復調が可能になるキャプチャ効果が働く。キャプチャ効果を抑制するため、各拠点の送信電力制御を最急降下法により準最適化する電力設計を導出した[1]。低信頼中継局が復調困難である安全性を確保した上で情報を伝達できる通信容量（秘密保持容量）の観点で、提案法は既存法（MRT、ZF）と比較して高い秘密保持容量を達成することを図 8 に明らかにした。二つ目は、CSI 偽装により搾取可能な情報量を最大化する盗聴モデルを導出した。最適な送信電力設計では低信頼中継局が通知する通信路状態情報（CSI）に依存するため、低信頼中継局が情報搾取に優位になるように CSI を偽装する恐れがある。そこで、CSI が確率モデルに適合することを各拠点が偽装識別子として用いることを前提としたとき、搾取できる情報量を最大にする CSI 偽装法を制約条件つき線形計画問題としてモデル化した。シンプレックス法により問題解決をした結果、具体的な偽装方法が明らかになった。三つ目は、PLNC を応用し、一方の拠点が発する信号を人工雑音に置き換えたとき、ネットワーク外の無線局に対する情報漏洩に対する抑制効果を秘密保持容量の観点で定量評価した。

[1] 田久修、山口和馬、藤井威生、大槻知明、笹森文仁・半田志郎、``低信頼中継局を利用した PLNC における秘密保持容量を拡大する送信電力制御の準最適設計、” 電子情報通信学会 無線通信システム（RCS）研究会、2015 年 5 月

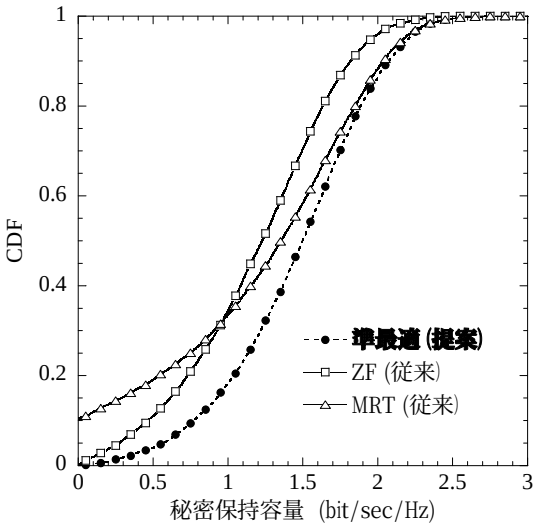

図 8　課題 1 における準最適送信電力制御（提案法が高い秘密保持容量を達成）

5．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計２件）

① F.H. Panahi, T. Ohtsuki, ”Optimal channel-sensing scheme for cognitive radio systems based on fuzzy Q-learning,” IEICE Trans. on Communications, vol.E97-B, no.2, pp.283-294, Feb. 2014.

② M. Jilani and T. Ohtsuki, “Joint SVD-GSVD precoding technique and secrecy capacity lower bound for the MIMO relay wire-tap channel, “ EURASIP Journal on Wireless Communications and Networking, Dec. 2012.

〔学会発表〕（計３５件）

① K. Matsumoto, O. Takyu, T. Fujii, T. Ohtsuki, F. Sasamori, S. Handa, “Evaluation of information leak by personated CSI in PLNC considering physical layer security,” IEEE RWS 2015, 2015 年 1 月 25 日～28 日、サンディエゴ（米国）

② A. Ida, T. Fujii, “Physical layer security using multi-band transmission considering channel selection for cognitive radio network, APSIPA ASC 2014, 2014 年 12 月 10 日、シェムリアップ（カンボジア）.

③ M. Endo, T. Ohtsuki, T. Fujii, and O. Takyu, “Secondary transmit beamformings for spectrum leasing in CRNs in the presence of eavesdropper,” IEEE PIMRC 2014, 2014 年 9 月 2 日～5 日、ワシントン DC

（米国）

④ K. Tsukada, T. Suzuki, T. Fujii, O. Takyu, T. Ohtsuki、” Secondary node cooperation with enhancing secure capacity under existence of primary system, “ IEEE APWCS 2013, 2013年8月22日～23日、ソウル（韓国）

⑤ F.H. Panahi, T. Ohtsuki, “Optimal channel-sensing policy based on fuzzy Q-learning process over cognitive radio systems,” IEEE ICC, 2013年6月9日～13日、ブタペスト（ハンガリー）

他３０件

６．研究組織

(1)研究代表者

藤井　威生（FUJII, Takeo）
電気通信大学・先端ワイヤレス・コミュニケーション研究センター・教授
研究者番号：１０３２７７１０

(2)研究分担者

大槻　知明（OHTSUKI, Tomoaki）
慶應義塾大学・理工学部・教授
研究者番号：１０２７７２８８

(3)連携研究者

田久　修（TAKYU, Osamu）
信州大学・工学部・准教授
研究者番号：４０４５３８１５