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 ２８ 年　 ６ 月　 ９ 日現在

機関番号：１５４０１
研究種目：基盤研究(C)（一般）
研究期間：2013～2015
課題番号：２５４２０３７１

研究課題名（和文）物理層においてもセキュアな無線通信の実現

研究課題名（英文）Realization of a secure wireless communication at physical layer.

研究代表者
大野　修一（Shuichi, Ohno）

広島大学・工学（系）研究科（研究院）・准教授

研究者番号：７０２７３９１９

交付決定額（研究期間全体）：（直接経費）　　4,000,000円

研究成果の概要（和文）：無線通信の基地局が複数の送信アンテナを持つ場合、それぞれのアンテナに重みをつけることで送信信号の指向性を制御することができる。一方、受信側が複数の送信アンテナを持つ場合、それぞれのアンテナの受信信号に重みをつけることで受信信号の品質を向上することができる。本研究では、複数の盗聴端末が共謀して最適な受信ビームフォーミングを行ったときの受信強度が盗聴可能となるレベルより小さくなるよう基地局が情報信号と妨害電波を送信する手法を考案した。また、通信路情報に不確定性がある場合であっても所望の性能を確保できる方法を提案している。

研究成果の概要（英文）：If a base station of a wireless communication system has multiple transmit antennas, it is possible to control the direction of its transmitted signal by using beamforming. On the other hand, if the receiver has multiple receive antennas, it is possible to enhance the received signal by using beamforming.
We consider a wireless LAN, where the base station utilizes beamforming to combat colluding eavesdroppers with multiple antennas and transmitting artificial noises. The beamformer and the artificial noises are optimally designed to achieve the prescribed signal to interference and noise ratio (SINR) at the legitimate receiver and the maximum allowable SINR at the eavesdroppers.

研究分野：通信・ネットワーク工学

キーワード：物理層セキュリティ　ビームフォーミング　盗聴

１．研究開始当初の背景

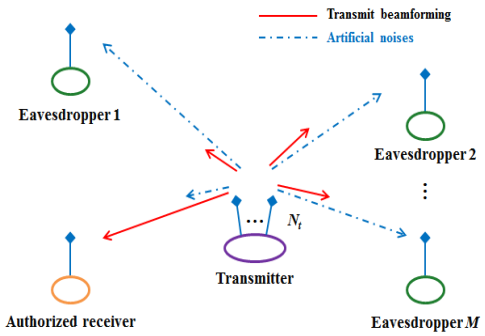
高度情報化社会の時代となり、無線通信ネットワークが広く普及している。携帯端末などによる個人の無線通信の利用が必要不可欠となっている。一方、無線通信は、空間を通して伝達する性質上、電波の傍受が容易である。そのため、盗聴や不正使用を防ぐための情報セキュリティの確保が重要となってきている。

送信機と正規受信機の一般的な盗聴対策として、秘密鍵を利用した暗号化通信が利用されている。さまざまな暗号化方式が提案されているが、暗号化は送信機と受信機間での暗号に関する情報のやりとりが必要である。そのため、暗号を用いる秘密通信は、秘密鍵をいかに安全に伝達し共有するのかが問題となる。また、暗号化は通信プロトコルの上位層にあるため、情報セキュリティが下位層においても確保されているとはいえない。そのため、下位層における安全性確保の研究が注目を集め始めた。

送信機と正規受信機の通信路容量が、送信機と盗聴機の通信路容量より大きければ、安全な秘密通信が可能であることが理論的に示されている。しかし、信号処理などの物理層における技術で安全性を保障した秘密通信は十分には研究されていなかった。

一方、近年、高速データ通信を目的とした複数送受信アンテナ (MIMO) システムが実用化されている。複数送受信アンテナを用いると単一送受信アンテナでは不可能であった技術が利用できるようになる。そこで、複数送受信アンテナを用いた物理層における秘密通信の理論的研究が盛んになり、物理層における秘密通信の試みがなされるようになっていた。

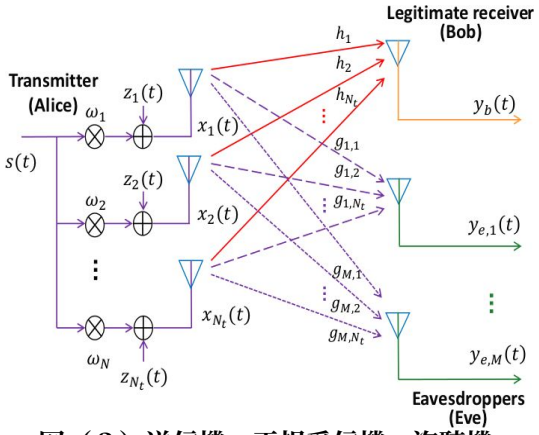
２．研究の目的



図（１）システムモデル

図(1)の無線通信システムにおいて、複数のアンテナを持つ送信機(アリス:Alice)から、正規受信機(ボブ:Bob)への無線通信を他のＭ個の端末(イヴ：Eve)が盗聴することを考える。複数の送信アンテナが利用できれば、送信機は送信ビームフォーミングにより正規受信機に送信したい秘密信号を向けることができ、盗聴機に人為的ノイズである干渉信号を向けることができる。一方、複数の盗聴者は共謀し受信ビームフォーミングを用いて盗聴能力を向上することができる。情報の安全性を確保するには盗聴機にもっとも都合のよい状況であっても盗聴機による秘密情報の復元が困難な方法が必要である。そこで、送信機がビームフォーミングと干渉信号送信を効果的に利用することにより盗聴に耐性与え、物理層においても安全性の高い無線通信方法を開発することを目的とする。

３．研究の方法



図（２）送信機、正規受信機、盗聴機

図（２）に本研究で考える送信機、正規受信機、盗聴機を示している。通信路はすべてフラットフェージングであると仮定する。単一アンテナを持つ盗聴端末が複数ありそれぞれが情報を共有し共謀し盗聴することは、複数アンテナを持つひとつの盗聴機で盗聴することと等しくなるため、複数アンテナを持つひとつの盗聴機による盗聴を考える。

送信機は秘密にしたい情報 s(t)を Nt 本のアンテナから送信する。正規受信機と盗聴機への通信路の係数をそれぞれ $\mathbf{h}_n$ と $\mathbf{g}_{n,m}$ とする。送信機は通信路の情報をもとに i 番目のアンテナで秘密信号に重み w_i を乗算したのち干渉信号 s(t)を付加し送信する。

受信信号から送信信号の復元性能は、信号対干渉ノイズ比で評価できる。正規受信機では秘密信号が復元できるよう信号対干渉ノイズ比がある閾値 r_b より大きくなければならない。盗聴機は複数アンテナをもつので信号対干渉ノイズ比を受信ビームフォーミングで最大にすることができる。このもっとも条件のよい場合の信号対干渉ノイズ比を、ある小さな値 r_e より小さくなるよう重みと干渉信号を設計すれば、秘密情報を正規受信機にのみ送信できることになる。

干渉信号は秘密信号と独立なガウスノイズを利用する。正規受信機における信号対干渉ノイズ比 $SINR_b$ は通信路、秘密信号の分散、干渉信号の相関行列で表現できる。一方、盗聴機の最適受信ビームフォーミングは送信機と盗聴機間の通信路から一意に決定できる。そのため、盗聴機における最適受信ビームフォーミング後の信号の号対干渉ノイズ比 $SINR_e$ も通信路、情報信号の分散、

干渉信号の相関行列で表現できる。
以上より、秘密信号の分散と通信路が与えられているとき正規受信機における信号対干渉ノイズ比の条件

$$SINR_b > r_b$$

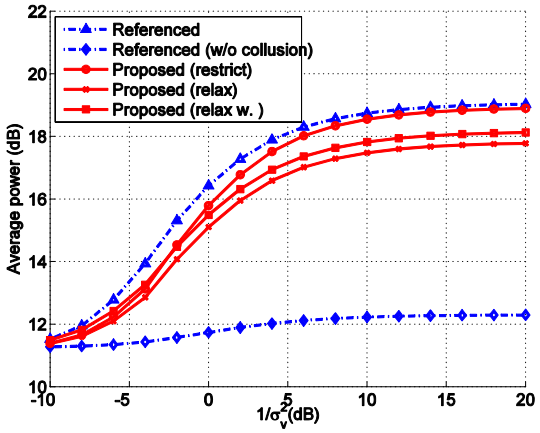
と盗聴機における信号対干渉ノイズ比の条件

$$SINR_e < r_e$$

を満足する送信ビームフォーミングと干渉信号を設計すればよい。さらに、できるだけ少ない送信電力によりこれらの条件を満たすことが望まれる。そこで、送信ビームフォーミングの係数と干渉信号の相関行列を変数、送信電力を目的関数とし、ふたつの条件のもとで送信電力の最小化を行う。
この問題を定式化すると凸でない最適化問題となり、そのままでは解くことができない。そこで条件を緩和することで凸最適化問題に帰着させ、最適な送信ビームフォーミングと干渉信号を数値的に求めることを考える。
通常、推定により通信路を求める。そのため得られた通信路には誤差が含まれる。上で述べた設計法は通信路の真値を利用しており、推定誤差に対応できない可能性がある。通信路推定誤差がある場合であっても、信号対干渉ノイズ比に関する条件を満たす送信ビームフォーミングと干渉信号を、凸最適化問題として定式化することで設計する。

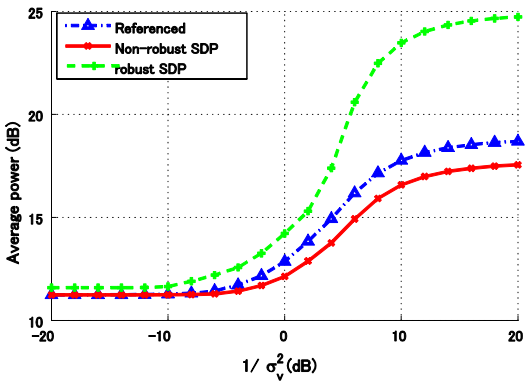
４．研究成果

まず、通信路の真値が利用できる理想的な場合において最適な送信ビームフォーミングと干渉信号の設計を最適化問題として記述した。送信ビームフォーミングの係数は要素数 Nt のベクトルとして表現されている。これを Nt 行 Nt 列の行列に緩和すると、凸最適化問題となることを示した。さらに、この凸最適化問題の解は要素数 Nt のベクトルの積となるため、緩和問題の最適解からもとの凸でない最適化問題の解が得られることを明らかにした。
提案法で設計した通信方法を既存の方法と比較した。既存の方法として複数の端末が共謀を行わずそれぞれの端末において信号対干渉ノイズ比の制約を課したもの（Referenced w/o collusion）とその制約に共謀盗聴による信号対干渉ノイズ比の制約を追加したもの(Referenced)を用いた。図（３）に提案法(Proposed (relax))と提案法に各アンテナにおける信号対干渉ノイズ比の制約を追加したもの(Proposed (relax w.))の信号対干渉ノイズ比条件を満たすための必要送信電力を示している。横軸は受信機におけるノイズの分散の逆数としている。比較手法(Referenced w/o collusion)がもっとも小さい送信電力となっているが、これは共謀盗聴を考慮していないためである。共謀盗聴を考慮する手法の中では提案法(Proposed (relax))がもっとも小さい送信電力で共謀盗聴に対応できている。



図（３）盗聴を防ぐために必要な送信電力

通信路の推定誤差がある場合、実際には真値はわからない。そこで、推定誤差量がある値以下であれば誤差があっても信号対干渉ノイズ比制約を満たす送信ビームフォーミングと干渉信号が設計できる方法を提案した。真値が利用できる場合の最適化問題に推定誤差量に関する制約を付加した最適化問題を考え、この問題を緩和により凸最適化問題として定式化した。そのため最適解を数値的に求めることを可能にしている。
図（４）に誤差がある場合の送信電力を比較している。Non-robust SDP は真値が利用できる場合であり、Robust SDP は推定誤差がある場合である。推定誤差がある場合は、真値が利用できる場合より大きな送信電力が必要であるが、誤差があっても信号対干渉ノイズ比制約を満たすことができ、共謀盗聴を防ぐことができる。
以上のように、本研究は、無線通信の送信機が複数の送信アンテナを持つ場合、アンテナに重みをつけ干渉信号を送信することで、複数の端末が共謀して盗聴する場合であっても正規受信機に安全に情報を伝達する技術を確立している。また、実際の応用において、通信路誤差があってもロバストに対応できる手法を提案している。提案法は通信レイヤーにおける物理層の技術を利用しているため、物理層における通信の秘匿性を向上する技術であり、今後の発展が期待できる。



図（４）通信路誤差がある場合の送信電力

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　0　件）

〔学会発表〕（計　3　件）

３．鄒京博 大野 修一 物理層における秘匿性向上のためのロバストビームフォーミング 信学技報 115(396), 243-246, 2016-01-18

２．Shuichi Ohno and Yuji Wakasa, Robust beamformer and artificial noises for MISO wiretap channels with multiple eavesdroppers, Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 3133-3117, Brisbane, Australia, April 20-24, 2015

１．Shuichi Ohno, Yuji Wakasa, Shui Qiang Yan, and Emmanuel Manasseh, Optimization of transmit signals to interfere eavesdropping in a wireless LAN, Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 6093-6097, Florence, Italy, May 4-9, 2014

〔図書〕（計　0　件）

〔産業財産権〕
○出願状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
ホームページ等

６．研究組織
(1)研究代表者
大野　修一（OHNO SHUICHI）
広島大学・工学研究科・准教授

研究者番号：７０２７３９３１

(2)研究分担者
（　　）

研究者番号：

(3)連携研究者
（　　）

研究者番号：