様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成２５年５月　２９日現在

機関番号：34310
研究種目：基盤研究(C)
研究期間：2010～2012
課題番号：22560397
研究課題名（和文）　複数アンテナ送受信による電波伝搬特性変動を用いた電波信号秘匿方式

研究課題名（英文）　Radio Signal Hiding Scheme Based on Fluctuation of Radio Propagation Characteristics Using Multiple Transmitting and Receiving Antenna

研究代表者
笹岡　秀一（SASAOKA HIDEICHI）
同志社大学・理工学部・教授
研究者番号：70309194

研究成果の概要（和文）：電波を用いた情報セキュリティ技術の分野において、電波信号の複数アンテナ送受信により、秘密情報を伝送する電波信号を秘匿する方式の実現性を検討した。その結果、信号を複数に分割して複数アンテナ送受信により伝送する方式が信号秘匿に有効であることが分かった。また、安全性が盗聴者の場所に依存することに課題があることが明らかになった。
研究成果の概要（英文）：Feasibility of radio signal hiding scheme using multiple transmitting and receiving antenna is studied in a radio-layer information security. As a result, it is found that the scheme of the separated signal transmission using multiple antenna system is useful for signal hiding.　It also found that improvement of anti-attack performance against eavesdropper is further studies.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2010 年度	1,000,000	300,000	1,300,000
2011 年度	1,100,000	330,000	1,430,000
2012 年度	700,000	210,000	910,000
年度			
年度			
総　計	2,800,000	840,000	3,640,000

研究分野：工学
科研費の分科・細目：電気電子工学、通信・ネットワーク工学
キーワード：暗号・セキュリティ

１．研究開始当初の背景

無線通信は電波の傍受により盗聴される危険性があるため、盗聴や不正アクセスなどが問題となっている。この対策として公開鍵暗号方式や共通鍵暗号方式が一般的で、移動通信の場合に端末での処理演算量の制約から共通鍵暗号方式が用いられることが多い。しかし、共通鍵暗号方式は鍵管理や鍵配送が必要なこと、端末の紛失・盗難の危険性のあることが問題である。これらの従来方式と異なり、情報理論的な複雑性を安全性の根拠とする暗号技術も研究されている。これらには、使い捨て鍵（ワンタイムパッド）を用いる暗号方式（シャノンの暗号方式）、雑音のある通信路を用いた鍵配送（盗聴通信路を用いた鍵配送）、相関情報を用いた秘密鍵共有などがある。

一方、通信路特性を活用する点が共通しているが、より現実的なものとして移動通信路特性を用いた秘密鍵共有と秘密情報伝送が提案されている。ここで、秘密鍵共有の原理は、電波伝搬路の可逆性により正規ユーザ間で相関性の高い秘密情報を共有する一方で、電波伝搬路の場所依存性により盗聴者での

情報推定を阻止することである。また、秘密情報伝送の原理は電波伝搬特性を活用して、正規の送受信者間と盗聴者間との通信品質に格差をつけることである。これらの研究が米国や日本などで盛んに行われている。

また、最近、この分野に属する新しい技術として、電波伝搬特性を活用した通信秘匿（電波スタガノグラフィ）が提案され、その有効性が示されている。この電波ステガノグラフィの概念は、秘匿情報を伝送する電波信号（秘匿信号）を別の公開情報を伝送する電波信号（カバー信号）で覆い隠し、秘匿信号の存在自体を検出不能にする一方で、正規の受信者には電波伝搬特性を活用することで情報を抽出できるものである。一方、最近、複数アンテナを用いた秘密鍵共有や秘密通信に関する研究も行われている。

２．研究の目的

本研究の実施者は、これまで物理層（電波層）情報セキュリティ技術の分野において、電波伝搬特性を用いた秘密鍵共有と秘密通信の分野で研究成果を上げてきた。また、最近、電波ステガノグラフィという新しい概念の技術の研究に着手した。この初期検討を行った方式は、電波ステガノグラフィの実現性を初めて示した点で評価できるが、秘匿信号の伝送効率と安全性が十分とは言えない。その原因の一つは、初期検討を行った方式が電波伝搬特性を十分に活用した方式になっていないことである。

そこで、電波伝搬特性を用いた秘密鍵共有や秘密通信によく用いられる複数アンテナ送受信を活用した新しい方式を検討することにした。これにより、方式の性能が画期的に向上することが期待できる。研究達成目標は、複数アンテナ送受信による電波伝搬特性変動を用いた電波信号秘匿の可能性を明らかにするとともに、その具体的な実現法について検討することであり、以下の三つ研究内容からなる。

・各種の要素技術を組合せた新方式を提案。
・計算機シミュレーションによる特性評価。
・評価結果に基づく課題抽出と方式改良。

本研究は、従来の電波層（物理層）における情報セキュリティ技術と異なり、秘密鍵共有や秘密通信の実施自体及び使用する電波信号自体が検出されない方式を対象としている。このような情報セキュリティ技術は、悪意の第三者からの攻撃により情報セキュリティが損なわれる可能性が少ない。また、物理層での情報セキュリティ技術であり、暗号化の適用が困難な場合にも有効である。

３．研究の方法

研究目的を達成するため、下記の研究項目を順次実施する。①各種の要素技術を効果的に組合せた新しい方式を提案し、簡易な特性評価を行う。②電波伝搬特性の詳細な模擬を含めて忠実な計算機シミュレーションを実施し、提案方式の実環境での特性評価を行う。③初期の結果が得られなかった場合も含めて、提案方式の課題の抽出と改良方式の提案を行う。

研究項目①について、各種の要素技術の効果的な組合せの検討は、関連分野の研究成果を活用できる。しかし、未着手の新方式を対象とするので、従来の要素技術を単に組合せるだけでは、十分に良好な特性をもった方式を構成できない可能性が高い。それゆえ、従来の手法のままでは、電波信号の存在自体を秘匿する電波ステガノグラフィに適用できない。そこで、電波信号の秘匿に適した複数アンテナ送受信方式を考案する。また、その効果を簡易なシミュレーション評価を併用しながら検討し、問題点を把握しながら方式検討を深める。

研究項目②については、送受信信号と電波伝搬特性の忠実な模擬が必要となる。単一送受信アンテナの場合、電波伝搬特性の模擬を統計的伝搬モデルにより実施する。しかし、複数送受信アンテナの場合、複数経路間の電波伝搬特性の場所依存性も正確に模擬する必要があるが、統計的伝搬モデルによる模擬が難しい。そこで、レイトレース法による電波伝搬特性の詳細評価などが必要となる。

研究項目③については、評価結果に基づいて提案方式の課題を抽出するとともに、所期の特性が得られない場合にその原因を解明する。また、その対策を検討し、改良方式を提案する。これには、既存の要素技術に基づく新たな工夫により対応する。

４．研究成果

(1)研究成果の概要

複数アンテナ送受信を用いた電波信号秘匿方式の検討の手始めとして関連の既存技術の評価検討を行った。複数アンテナ送受信を用いた秘密情報伝送方式、秘匿信号の多重による無線ステガノグラフィ方式については、その有効性を評価するとともに安全性の脅威となる攻撃法の可能性を明らかにした。また、複数アンテナ送受信を用いた信号分散手法による電波信号秘匿方式の検討を行い、この方式に基づいた電波信号秘匿の可能性が示された。さらに、無線中継システムにおける秘密鍵共有方式の検討を行い、その有効性を確認した。

次に、電波伝搬特性の忠実な模擬によりその場所依存性と安全性との関連を詳細に評価した。この検討の一環として電波伝搬特性の実測を行い、位置識別方式を検討した。その結果、攻撃耐性の場所依存性が明らかとなった。さらに、攻撃耐性が強いと考えられた

信号分散手法を用いた方式においても課題があることが分かった。その結果に基づいて対策技術の検討を行い、その有効性を確認した（未発表、今後発表予定)。

これらの研究成果は、新規性の高く有効性の高いものであり、今後、この分野の発展に寄与することが期待される。

(2) MIMO を用いた秘密情報伝送方式

MIMO 固有ビーム空間分割多重伝送における秘密情報伝送に関しては、下記のような研究成果を上げた。提案方式では、MIMO 固有ビーム伝送において固有値の大きいパスで秘密情報伝送を行い、固有値の小さいパスを用いて盗聴を妨害することで秘密情報の安全性を向上させている。計算機シミュレーションの結果、提案方式の有効性を確認できた。しかし、通信秘匿の観点からは十分とは言えず、逆に固有値の小さいパスで秘密情報を伝送するなどの工夫が必要となる。

(3)信号分散を用いた秘密情報伝送方式

MIMO システムにおける信号分散を用いた秘密情報伝送方式に関しては、下記のような研究成果を上げた。提案方式では、送信信号を複数のサブストリームに分散して伝送し、受信局で簡易な信号処理により信号を復元する。また、正規の受信局で打ち消されるような人工的な干渉信号を送信側で付加し、盗聴耐性の向上を図っている。計算機シミュレーションにより想定される盗聴手段に対する盗聴耐性を評価し、提案方式の有効性を確認した。しかし、盗聴局が独立成分分析を用いた場合の盗聴耐性が不十分となる場合があることが明らかとなったので、その対策が今後の課題となった。

(4)無線信号秘匿方式

ディジタル移動通信における直接拡散信号の埋込による無線ステガノグラフィ方式に関しては、下記のような研究成果を上げた。提案方式では、カバー信号と秘匿信号の他に雑音を付加することで、秘匿信号の検出の危険性を軽減している。計算機シミュレーションにより提案方式の有効性と信号秘匿の可能性が確認できた。しかし、秘匿性能の空間的評価が課題であることも明らかとなった。

(5)無線中継による秘密鍵共有方式

電波伝搬特性に基づく無線中継システムにおけるグループ秘密鍵共有方式に関しては、下記のような研究成果を上げた。提案方式では、単純な中継（信号増幅と再送信）でなく、盗聴耐性を高めるため信号合成と中継、多元接続と中継の手法を提案し、計算機シミュレーションで提案方式の有効性を確認している。

(6)電波伝搬特性を用いた位置識別方式

電波伝搬特性を用いた位置識別に基づく相手認証方式の特性評価に関しては、下記のような研究成果を上げた。提案方式では、アンテナ指向性を変化させて取得した受信信号強度変動の時系列の場所依存性に基づき、時系列間の相関係数により位置識別を行う。計算機シミュレーションと実環境下での実験により位置識別の可能性を評価した。

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　４件）

①笹岡秀一、尾谷尚宣、岩井誠人、電波伝搬特性を用いた位置識別に基づく相手認証方式の特性評価、電子情報通信学会論文誌 B、査読有、採録決定、2013。

②清水崇之、岩井誠人、笹岡秀一、Group Secret Key Agreement Based on Radio Propagation Characteristics in Wireless Relaying Systems、電子情報通信学会論文誌 EB、査読有、Vol.E95-B、No.7、2012、pp.2266-2277。

③北野隆康、岩井誠人、笹岡秀一、ディジタル移動通信における直接拡散信号の埋込による無線ステガノグラフィ方式、同志社大学理工学研究報告、査読有、第 52 巻、第 2 号、2011、pp.127-134。

④北野隆康、岩井誠人、笹岡秀一、MIMO 固有ビーム空間分割多重伝送における秘密情報伝送、電子情報通信学会論文誌 B、査読有、Vol.J94-B、No.2、2011、pp.85-93。

〔学会発表〕（計　１件）

①田中智、清水崇之、北野隆康、岩井誠人、笹岡秀一、MIMO システムにおける信号分散を用いた秘密情報伝送方式、電子情報通信学会技術研究報告、Vol.RCS2010-282、2011、pp.195-200。

６．研究組織

(1)研究代表者

笹岡　秀一（ SASAOKA HIDEICHI ）

同志社大学・理工学部・教授

研究者番号：70309194

(2)研究分担者

岩井　誠人（IWAI HISATO ）

同志社大学・理工学部・教授

研究者番号：70411064

(3)連携研究者

（　　）

研究者番号：