様式 C-19

科学研究費補助金研究成果報告書

平成　２３年　５月１１日現在

機関番号：24402
研究種目：基盤研究（C）
研究期間：2007～2010
課題番号：19500059
研究課題名（和文）　一般化直交変調のセキュリティ評価に関する実証的研究

研究課題名（英文）　Security Criteria for General Orthogonal Modulations

研究代表者
岡　育生（OKA IKUO）
大阪市立大学・大学院工学研究科・教授
研究者番号：80160646

研究成果の概要（和文）：秘匿性の高い変調方式として，直交ＣＤＭＡなどすべてのブロック直交変調を表現できる一般化直交変調を取り上げ，その変調パラメータ推定を通して秘匿性の強度を明らかにした．受信信号点にクラスタリングを適用して変調方式の基準ベクトルを推定し，推定した変調方式の誤り率を明らかにした．その結果，帯域信号では搬送波再生が困難であり秘匿性が高いが，ベースバンド信号では受信機においてシンボル同期とブロック同期が推定できれば変調方式の識別が可能であることが明らかとなった．

研究成果の概要（英文）：General orthogonal modulations are examined as secure modulations, which are hardly demodulated without modulation parameter information. The new identification method is proposed based on the clustering of received signals for basis vector estimation. The method is applied to general orthogonal modulations to demonstrate that the modulation can be identified by some amount of received samples with the knowledge of carrier frequency, block timing and symbol timing in a receiver.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2007 年度	1,000,000	300,000	1,300,000
2008 年度	800,000	240,000	1,040,000
2009 年度	700,000	210,000	910,000
2010 年度	800,000	240,000	1,040,000
総　計	3,300,000	990,000	4,290,000

研究分野：情報通信工学
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：一般化直交変調、変調方式推定、識別誤り率、余弦モーメント、振幅モーメント

１．研究開始当初の背景

通信のセキュリティを確保するため，公開鍵暗号をはじめとして多種の暗号化技術が実用化され，さらに解読が困難な方式を目指して研究が進められている．これらは，暗号化後の２値情報である０と１の系列が盗聴されても，鍵がない限り元の情報が復号できないことを利用している．一方，０と１の系列が盗聴できないように変調方式自体に秘匿性を持たせることも可能である．例えば，符号分割多元接続方式（ＣＤＭＡ）では，各ユーザに割り当てられた拡散符号が不明であれば，変調信号は復調されず雑音状のままである．しかしながら，この場合でも，２値系列からなる拡散符号の探索を行えば復調が可能となっている．セキュリティ強化のた

めに変調方式を用いるには，各種の変調方式の秘匿性を明らかにする必要がある．

２．研究の目的

通信のセキュリティを確保するために用いられる公開鍵暗号をはじめとする多種の暗号化技術の多くは鍵がない限り元の情報が復号できないように設計されている．ここで，鍵を広義にとらえ，変調方式における変調パラメータを鍵とすれば変調方式自体が秘匿性を有すると考えられる．一般化直交変調は，多次元空間の回転を用いて変調方式を定義するもので，回転平面と回転角の系列が変調パラメータとなることから，秘匿性との整合性が極めて良い変調方式であり，また，すべてのブロック変調を記述することができる利点を有している．本研究の目的は，一般化直交変調で表されるブロック直交変調のセキュリティ機能の評価を実証的に行うことにある．一般化直交変調を用いて高いセキュリティ機能を有する変調方式を開発すると共に，その盗聴可能性の程度を，変調方式の識別誤り率の理論解析，ならびに計算機シミュレーションを用いて明らかにする．

３．研究の方法

(1)　ブロック直交変調のパラメータ推定

任意のブロック直交変調は多次元立方体で表される信号点の回転によって表現できる．一般化直交変調を推定するには，まず，受信信号の標本を，それぞれの情報に応じてクラスタリングする必要がある．N 次元空間における情報シンボルには 2^N 通りのパターンが存在する．それらはN次元空間における立方体の頂点に位置し，送信信号の系列はこの立方体を回転させたものとなる．図１に３次元空間における受信信号の例を示す．図において，白い円が送信信号を，黒い点が雑音を付加された受信信号を表す．受信信号の標本をクラスタリングし，各クラスタの平均をとれば，送信信号点の推定値が得られるが，次元数Nが大きい場合には信号点数が膨大となり計算不可能となる．そこで本研究では図１に示すN個の基準ベクトル h_1, h_2, h_3 のみをクラスタリングにより復元し，各基準軸の送信情報を判定する．なお，信号点のクラスタリングを用いて信号の基準ベクトルを推定する場合には，任意の回転に対してパラメータ推定の手順ならびにその特性が不変であるため，座標軸と信号が一致した立方体配置を用いてパラメータ推定を行う．このようにしても推定の一般性を失わない．受信信号のクラスタリングには k-means 法を適用する．k-means 法ではその特性が初期値に大きく依存するため，初期値を繰り返し変更して初期値依存を軽減する．

次に，情報ビットの判定を行うには，クラスタリングで得られた 2^N 個の送信信号点の推定値に対し，2進数のラベル付けを行う必要がある．本研究では，信号点のラベルで各シンボルの位置関係がわかるように，新たにグレイ符号によるラベル付け法を開発する．実際に送信機で用いたラベル付けを，復元した信号点のみから推定することは，信号点の回転による自由度のため困難となる．このため，本研究ではこの自由度がないものと仮定することにより，基準軸の推定誤りに起因するビット誤りで推定結果を評価する．

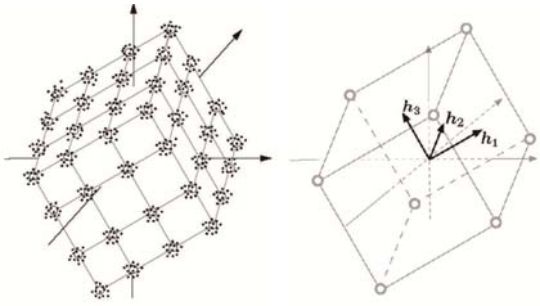

図１　受信信号点と基準ベクトル

また，各次元が担う信号点の多値数が未知である場合に，変調多値数を正規性検定を用いて推定する方法を開発する．

さらに，解析的に推定した変調方式のビット誤り率の導出を行う．多次元空間における基準軸の角度誤差の確率密度関数を導出し，これを用いてビット誤り率の解析式を積分形式で表現する．

(2)　シンボルバイシンボル変調の識別

ブロック変調の一種である直交周波数多重（OFDM)の場合，ブロック変調としての識別特性と共に，各サブキャリアの変調方式の識別特性を明らかにすることも重要である．そこで，特に識別の難易度の高い直交振幅変調（ＱＡＭ）を識別の対象とする．本研究では実現の容易な識別法として，受信した信号の振幅モーメントならびに位相モーメントに関係する余弦モーメントの２つの判定変数からなる識別法を開発し，その特性の評価を行う．図２に，振幅モーメント（x_a：横軸）と縦軸の余弦モーメント（y_b：縦軸）を用いる１６ＱＡＭと６４ＱＡＭの識別におけるモーメントの例を示す．ここで，a は振幅モーメントの次数，b は余弦モーメントにおける位相の係数を表し，信号対雑音電力比（ＳＮ比）を１６ｄＢに設定している．それぞれのモーメントの値により，１６ＱＡＭの領域（S_{16}）と６４ＱＡＭ（S_{64}）に分離して識別を行う．なお，信号が小さい場合には，余弦モーメントは雑音の影響が大きく受ける．このため，受信信号レベルがRより小さい場合には小信号除去とし，その受信信号を識別

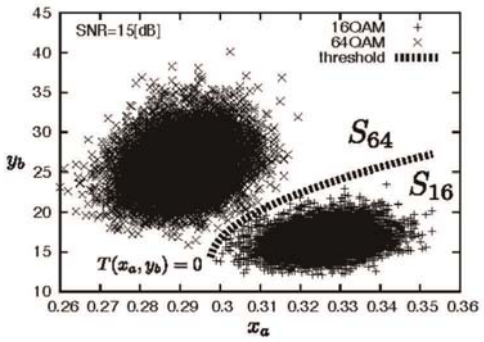

図２　振幅モーメントと余弦モーメントを用いたＱＡＭの識別

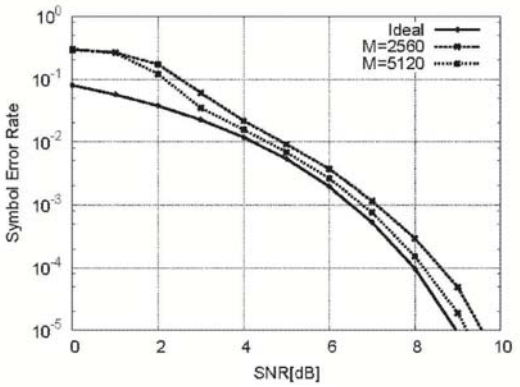

図３　推定した変調方式のシンボル誤り率

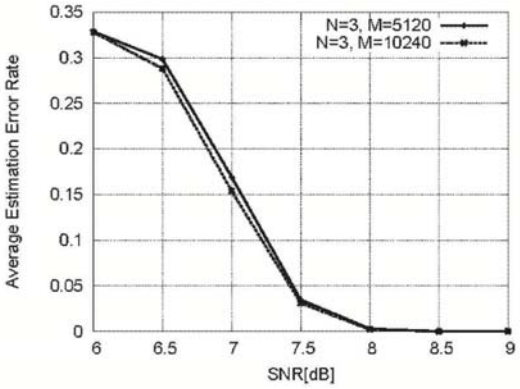

図４　多値数の推定誤り率

に用いないこととする．識別誤り率を計算機シミュレーションで求めるとともに，識別誤り率の解析式を導出する．

周波数オフセットΔが存在する場合には，受信した信号点が２πΔの角速度で回転することから，モーメントの値が変化して識別特性が劣化する．これに対処するため，受信点を一定の角度でシフトし，複数個に拡大することにより，周波数オフセットのモーメントへの影響を軽減する．

また，これまで，変調方式識別の研究では2者択一の識別が主となっていたが，大信号と小信号の２つの変調波が混在する場合に，その両方の変調方式の識別について検討する．まず，振幅モーメントを用いて大信号を識別し，続いて，識別した大信号のモーメント成分を取り除いて小信号を識別する．識別誤り率を計算機シミュレーションを用いて求める．

４．研究成果

(1)　ブロック直交変調のパラメータ推定

まず，一般化直交変調の次元数をN=3，各次元の多値数をQ=8として，クラスタリングで基準軸を推定した場合のシンボル誤り率を計算機シミュレーションで求め，その結果を図３に示す．図中，Ｍは受信信号の標本数を示す．標本数Ｍが大きくなれば，Ｍが無限大の理想的なシンボル誤り率に近づき，変調方式の推定に成功していることがわかる．次に，変調多値数の推定誤り率を図４に示す．ＳＮ比（ＳＮＲ）が８ｄＢ以上あれば，低い誤り率で多値数を推定できることがわかる．また，次元数Ｎが３と４の場合に対してシンボル誤り率の解析式を導出し，その数値計算結果が計算機シミュレーションの結果と一致することを確認した．

本研究では，変調信号の搬送波が受信側で既知であるとして評価を行った．帯域信号の場合には，現在のところ受信機で搬送波情報がない場合の変調識別は困難であり，その秘匿性は高いといえる．一方，ベースバンド信号におけるブロック直交変調については，受信機でシンボル同期とブロック同期が推定できれば，ある程度の受信信号の標本数があれば識別が可能であることがわかった．

(2)　シンボルバイシンボル変調の識別

周波数オフセットがない場合，振幅モーメントと余弦モーメントを用いた場合の１６ＱＡＭと６４ＱＡＭの識別誤り率の解析結果を図５に示す．なお，図５の結果は計算機シミュレーション結果と一致していることを確認している．ここで，小信号除去レベルR，ならびに振幅モーメント次数a=12と位相モーメント係数B=12は最適値を用いている．図５より,受信信号の標本数5000において，振幅モーメントと余弦モーメントの両方を用いる提案手法の識別誤り率は，従来の振幅モーメントあるいは余弦モーメントを単体で用いる場合より，優れた誤り率となっていることがわかる．

次に，周波数オフセットが１シンボルあた

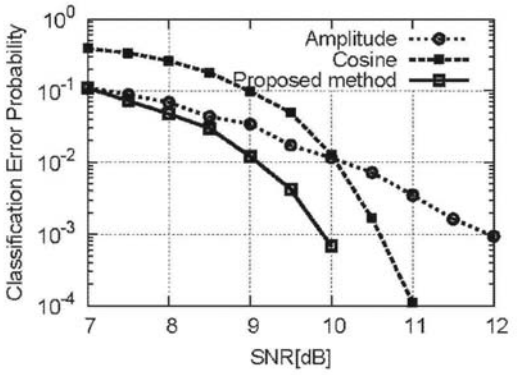

図５　ＱＡＭの識別誤り率(N=5000)

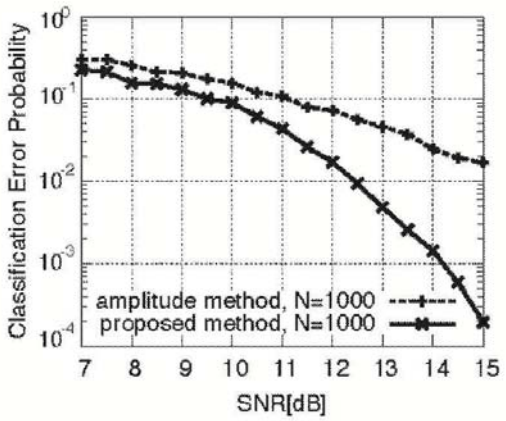

図６　ＱＡＭの識別誤り率

り１度の場合に，受信点シフトによる信号点の拡大を用いる提案手法と従来の振幅モーメントのみを用いた識別法の誤り率を，計算機シミュレーションを用いて求めた結果を図６に示す．なお，周波数オフセットが大きい場合でもほとんど識別特性に変化はない．図６より，提案手法は，周波数オフセット存在下においても振幅モーメントを用いる方法より低い識別誤り率を呈することがわかる．さらに，提案手法の識別誤り率の解析式を導出した．

また，ディジタル位相変調（ＰＳＫ）とＱＡＭが同時に存在する場合に，受信信号の振幅モーメントを用いて，これら両方の変調方式の識別を行った．その結果，２つの信号にある程度の電力差があれば識別が可能であることを示した．なお，この電力比が既知であれば識別誤り率を大きく改善することが可能である．

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）

〔学会発表〕（計 12 件）

① Shinji Ohara, Ikuo Oka, Shingo Ata, Robust QAM Classification by Moments and Its Error Probability Analysis, Proc. 2011 IEEE Radio and Wireless Symposium, January 18, 2011, Phoenix
② Yu Morishima, Ikuo Oka, Shingo Ata, Pulse Interference Mitigation Techniques for QPSK and QAM using Viterbi Decoding, Proc. 2010 International Symposium on Information Theory and its Applications, October 20, 2010, Taichung
③ Takahiro Yamamoto, Ikuo Oka, Shingo Ata, Signal Identification of Block Orthogonal Modulations, Proc. 2010 IEEE Radio and Wireless Symposium, January 12, 2010, New Orleans
④ Shinji Ohara, Masato Kita, Ikuo Oka, Shingo Ata, Modulation Classification Based on Amplitude and Cosine moments, Proc. 2009 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing, August 25, 2009, Victoria
⑤ Shinji Tani, Ikuo Oka, Shingo Ata, Capacity and Cutoff Rate of Binary Tree Network Composed of BSC, Proc. 2009 International Conference on Advanced Technologies for Communications, October 13, 2009, Hai Phong
⑥ Masato Kita, Ikuo Oka, Shingo Ata, Classification Error Probability of Cosine Moment Method with Small Signal Rejections, Proc. 2009 IEEE Radio and Wireless Symposium, January 20, 2009, San Diego
⑦ Shinji Tani, Ikuo Oka, Shingo Ata, Path Diversity Effects of Binary Tree Network Composed of Binary Symmetric Channels, Proc. 2008 International Symposium on Information Theory and Its Application, December 08, 2008, Auckland
⑧ Takahiro Yamamoto, Ikuo Oka, Shingo Ata, Clustering and Labeling of Orthogonal Signals for Modulation Identification, Proc. 2008 International Symposium on Information Theory and Its Application, December 08, 2008, Auckland
⑨ Takahiro Yamamoto, Ikuo Oka, Shingo Ata, Error Probability of Orthogonal Modulation Estimation by Clustering, Proc. 2008 Joint Conference on Satellite Communications, November

08, 2008, Busan
⑩ Tomoya Katayama, Ikuo Oka, Shingo Ata, Modulation Identification by General Orthogonal Modulations, Proc. 2008 International Conference on Advanced Technologies for Communications, October 08, 2008, Hanoi
⑪ Masato Kita, Ikuo Oka, Shingo Ata, QAM Classification Based on Cosine Moments Excluding Small Signals, Proc. 5th International Conference on Information Technologies and Applications, June 24, 2008, Cairn
⑫ Ken Hashimoto, Ikuo Oka, Shingo Ata, An Application of Error Correcting Codes to Network Coding, Proc. 2007 Hawaii and SITA Joint Conference on Information Theory, May 31, 2007, Honolulu

６．研究組織

(1)研究代表者

岡　育生（OKA IKUO）
大阪市立大学・大学院工学研究科・教授
研究者番号：80160646

(2)研究分担者

なし

(3)連携研究者

笹野　博（SASANO HIROSHI）
近畿大学・理工学部・准教授
研究者番号：00122052

阿多　信吾（ATA SHINGO）
大阪市立大学・大学院工学研究科・准教授
研究者番号：30326251