様式 C-19

科学研究費補助金研究成果報告書

平成２１年　６月１５日現在

研究種目：　基盤研究（Ｃ）
研究期間：2006～2008
課題番号：　18560391
研究課題名（和文）　センサネットワークの多端子情報理論と
決定理論によるモデル化と最適化
研究課題名（英文）　Modeling and optimization of the sensor networks
based on the multiterminal information theory and decision theory

研究代表者
松嶋　敏泰（MATSUSHIMA, Toshiyasu）
早稲田大学・理工学術院・教授
研究者番号：30219430

研究成果の概要：本研究では，センサネットワークを含むネットワーク分散処理の問題に対して，多端子情報理論と統計的決定理論に基づいた基礎モデルを構築し，構築したモデル上での最適解の導出及び最適解またはその近似解を実現するアルゴリズムを設計した．

交付額

（金額単位：円）

	直接経費	間接経費	合　計
２００６年度	1,500,000	0	1,500,000
２００７年度	1,200,000	360,000	1,560,000
２００８年度	800,000	240,000	1,040,000
年度			
年度			
総　計	3,500,000	600,000	4,100,000

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：情報理論，センサネットワーク，多端子情報理論

１．研究開始当初の背景

ネットワーク上の分散情報を処理する問題について多くの研究が行われていた．分散し配置されたセンサー等によって集められた多様な情報をネットワーク経由で伝送し，それらを統合することで何らかの決定や制御を行うセンサネットワークの問題などである．この研究分野では，問題に対する数理的基礎モデルが無く，最適性や性能限界に関する議論がなされておらず，また最適解や限界が示されても，それを達成するアルゴリズムを構築することが困難であるということが原因となり，なかなか研究の進展が得られていなかった．

２．研究の目的

本研究では，センサネットワークを含む分散処理における基礎的な理論研究を中心に，大きく次の 2 つのステップで研究を行い，それぞれのステップを研究の目的とした．

(1) ネットワーク上に分散した情報の伝送と決定・制御に関する基礎モデルを構築し，構築したモデル上での最適解や理論的性能限界についての定式化を行う．

(2) 定式化した最適解またはその近似解を実現するアルゴリズムをグラフ上のメッセージ伝搬アルゴリズム等を用いて設計し，その性能や計算量の評価を解析的・実験的に行う．

３．研究の方法

(1) ネットワーク分散情報の処理に関する基礎モデルの構築

基礎モデルの構築に際して，センサネットワークなどのネットワーク分散処理の分野における主問題の調査及び整理を行った．この調査結果をもとに，多端子情報理論・統計的決定理論を融合・応用することで基礎モデルの構築を行った．

(2) 構築されたモデル上の理論的性能限界・最適決定・制御方式の導出

構築されたモデルにおける性能限界については，多端子情報理論で研究されてきた成果を応用することで研究を進めた．また，最適な決定・制御については統計的決定理論及び学習理論の成果を応用することで研究を進めた．

(3) 定式化された最適解や理論的性能限界を達成するアルゴリズムの設計

LDPC 符号やターボ符号で理論的性能限界に迫る性能を示した，sum-product 復号法やターボ復号法に代表される，メッセージ伝搬アルゴリズムを発展させることで研究を行った．また，データ圧縮・統計的決定理論における効率化手法を発展させることで効率的な決定・制御方式の設計を行った．

４．研究成果

(1) Capacity 計算アルゴリズム

暗号分野の１つの問題として，秘密情報を持つ Broadcast Channel に対する符号化・復号法に関する研究がある．従来，この問題の限界に関する議論があり，理論限界が導出されていた．しかし，導出されていた理論限界は関数形が導出されていたに過ぎず，その値を具体的に計算する方法については議論がされていなかった．

本研究では，通信路符号化の問題において同様の計算を行うアルゴリズムである，有本の算法を拡張することで，秘密情報を持つ Broadcast Channel における理論限界値を計算するアルゴリズムを提案した．

また，この研究を拡張することで，より一般的に，関数の最小値を計算するアルゴリズムを提案した．これにより，一部のレートひずみ関数などの関数の最小値を計算することが可能となった．

(2) 盗聴・改ざんに対して耐性を持つネットワーク符号化の理論限界の導出

従来のルーティングと比較して，より多くの情報をネットワーク上でやり取りが出来る技術としてネットワーク符号化に関する研究が盛んに行われている．ネットワーク符号化の問題において，悪意のある第三者による攻撃を未然に防ぐために，セキュアなネットワーク符号化の方法を構築することは重要である．従来，この問題に対して，第三者によりネットワークが盗聴されていても安全に通信が行えるようにする方法及び，第三者により情報の改ざんが行われてもそれが訂正できるようにする符号化法の研究が行われていたが，これらの攻撃が同時に行われるという問題は考えられていなかった．本研究では，ネットワーク内の通信路を盗聴し，さらにはその通信路を流れる情報を改ざんする攻撃者が存在する問題をモデル化し，そのような状況で安全に通信を行うことが出来る符号化効率の限界を導出し，その限界を達成する符号化法を提案した．

(3) 帰還通信路を有する通信路モデルにおける確率伝搬アルゴリズムに基づいた復号法とその性能の解析

雑音のある環境下で出来るだけ効率的に誤りなく通信を行うための研究として，通信路符号化・復号の問題が挙げられる．この問題における理論限界は古くから導出されており，この限界に近い性能を示す符号として LDPC 符号・ターボ符号が，それに対する復号法として，確率伝搬アルゴリズムに基づいた復号法がある．

通信路符号化の問題に対して，受信者も送信

者に対して，情報を送ることが出来る帰還通信路を有する通信路モデルにおける符号化・復号の問題がある．この問題については，理論的限界は帰還通信路が無い場合と同じであることが示されているが，帰還通信路があることで，同じ限界を，より少ない計算量で達成できる可能性がある．本研究では，確率伝搬アルゴリズムに基づいた復号法を，帰還通信路を有する通信路符号化の問題に適用した場合の性能をDensity Evolutionという解析手法を応用して解析を行った．また，受信信号の信頼度を利用した復号法を提案し，復号性能が向上することを数値実験により示した．

また，上記の研究では通信路のパラメータは既知である問題を扱っているが，このパラメータが未知である場合の限界に関する議論はあまりされていない．本研究では，このような問題の１つである，ブロック誤り率が未知である場合の選択再送ＡＲＱ方式における最適なアルゴリズムを提案し，この問題における理論限界を明らかにした．

(4) 記憶を有する通信路モデルに対する確率伝搬アルゴリズムに基づいた復号法の性能解析

通信路符号化の研究の多くは，通信路の状態は時間に依存せず独立であるという仮定を置くが，実際には通信の状況は時間によって徐々に変化し，現在の通信路状態は過去の通信路状態に依存するため，このような過程は成り立たない．これに対して，通信路の状態が過去の通信路状態に依存して変化するような，記憶を有する通信路モデルに対する符号化・復号法に関する研究が数多くされている．

従来，このような通信路モデルに対して，確率伝搬アルゴリズムに基づいた復号法の性能をDensity Evolutionという解析手法により解析を行う研究がされていたが，本研究では，この解析における数値計算の精密化を行った．

(5) 確率伝搬アルゴリズムに基づいたCDMAマルチユーザ検出器の提案

CDMA方式は，移動体通信の重要な基盤技術である．CDMA方式を用いることにより，複数のユーザが同一の通信路を共有する通信システムの実現が可能となる．これは，情報理論では多元接続通信路と呼ばれる通信路モデルの一種である．従来，多元接続通信路の限界値は，多端子情報理論の分野で導出されており，特に符号化を固定したCDMA方式における理論限界も導出されていたが，具体的にこの理論限界に近い性能を示すような復号法は存在しなかった．

本研究では，通信路符号化の分野で，理論限界に迫る復号法の基盤であった確率伝搬アルゴリズムを，CDMA方式の復号に応用することで，非常に良い性能が得られることを数値実験により示した．また，さらにこの復号法を拡張することで，より一般的な通信路においても適用可能であることを示した．

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17件）

① Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, “Fingerprinting code for multimedia data against averaging attack,” IEICE Trans. Fundamentals, Vol.E-92-A, No.1, pp.207-216, 2009, 査読有

② 須子統太、松嶋敏泰、平澤茂一、”外れ値データの発生を含む回帰モデルに対するベイズ予測アルゴリズム，”情報処理学会論文誌数理モデル化と応用，Vol.1，No.1，pp.17-26，2008，査読有

③ 安井謙介、須子統太、松嶋敏泰、”拡張された有本－Blahutアルゴリズムの大域的収束性について，” 電子情報通信学会論文誌, Vol.91-A，No.9，pp.846-860，2008，査読有

④ Manabu Kobayashi, Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, “Density evolution analysis of robustness for LDPC codes over the Gilbert Eliott channel,” IEICE Trans. Fundamentals, Vol.E-91, No.10, pp.2754-2764, 2008, 査読有

⑤ Gou Hosoya, Toshiyasu Matsushima, Shigeichi Hirasawa, “A combined matrix ensemble of low-density parity-check codes for correcting a solid burst erasure,” IEICE Trans. Fundamentals, Vol.E-91, No.10, pp.2765-2778, 2008, 査読有

⑥ Kazuhiko Minematsu, Toshiyasu Matsushima, “Improved MACs from Differentially-Uniform Permutations, ”IEICE Trans. Fundamentals, Vol.E90-A, No.12, pp.2908-2915, 2007, 査読有

⑦ Ryo Nomura, Toshiyasu Matsushima, Shigeichi Hirasawa, “A note on the epsilon-overflow probability of lossless codes,” IEICE Trans. Fundamentals Vol.E90-A, No.12, pp.2965-2970, 2007, 査読有

⑧ Daiki Koizumi, Naoto Kobayashi, Toshiyasu Matsushima, Shigeichi Hirasawa,

“Reliability-Based Hybrid ARQ Scheme with Encoded Parity Bit Retransmissions and Message Passing Decoding,” IEICE Trans. Fundamentals, Vol.E90-A, No.12, pp.2908-2915, 2007, 査読有

⑨ Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "A generalization of the parallel error correcting codes by allowing some random errors," IEICE Trans. Fundamentals, Vol.E90-A, No.9, pp.1745-1753, 2007, 査読有

⑩ 野村亮, 松嶋敏泰, 平澤茂一, "無歪み情報源符号化におけるオーバーフロー確率について," 電子情報通信学会論文誌, Vol.J90-A, No.4, pp.292-304, 2007, 査読有

⑪ Tomohiko SAITO, Toshiyasu MATSUSHIMA, Shigeichi HIRASAWA, "A Note on Construction of Orthogonal Arrays with Unequal Strength from Error-Correcting Codes," IEICE Trans. Fundamentals, Vol.E89-A No.5, pp. 1307-1315, 2006, 査読有

⑫ Naoto KOBAYASHI, Toshiyasu MATSUSHIMA, Shigeichi HIRASAWA, "Transformation of a Parity-Check Matrix for a Message-Passing Algorithm over the BEC," IEICE Trans. Fundamentals, Vol.E89-A No.5, pp. 1299-1306, 2006, 査読有

⑬ Naoto KOBAYASHI, Daiki KOIZUMI, Toshiyasu MATSUSHIMA, Shigeichi HIRASAWA, "A Note on Error Correction Schemes with a Feedback Channel," IEICE Trans. Fundamentals, Vol.E89-A No.10, pp. 2475-2480, 2006, 査読有

⑭ 新家稔央, 松嶋敏泰, 平澤茂一, "判定基準LR+Thを用いたブロック符号の帰還誤り指数の改善," 電子情報通信学会論文誌, vol.J89-A, no.12, pp.1168-1174, 2006, 査読有

⑮ Gou Hosoya, Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "A Modification Method for Constructing Low-Density Parity-Check Codes for Burst Erasures," IEICE Trans. Fundamentals, vol.E89-A, no.10, pp.2501-2509, 2006, 査読有

⑯ Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "Fast Algorithm for Generating Candidate Codewords in Reliability-Based Maximum Likelihood Decoding," IEICE Trans. Fundamentals, vol.E89-A, no.10, pp.2676-2683, 2006, 査読有

⑰ Takashi Ishida, Masayuki Goto, Toshiyasu Matsushima, Shigeichi Hirasawa, "Properties of a Word-Valued Source with a Non-Prefix-Free Word Set," IEICE Trans. Fundamentals, vol.E-89A, pp.3710-3723, 2006, 査読有

〔学会発表〕(計 42 件)

① Tomohiko Saito, Toshiyasu Matsushima, Shigeichi Hirasawa, “A Note on Automatic Construction Algorithms for Orthogonal Designs of Experiments Using Error-Correcting Codes,” Pre-ICM International Convention on Mathematical Sciences, 2008 年 12 月, Delhi, India

② Tota Suko, Toshiyasu Matsushima, Shigeichi Hirasawa, “Asymptotic Property of Universal Lossless Coding for Independent Piecewise Identically Distributed Sources,” Pre-ICM International Convention on Mathematical Sciences, 2008 年 12 月, Delhi, India

③ Ryo Nomura, Toshiyasu Matsushima, Shigeichi Hirasawa, “An Information Spectrum Consideration on the Universal Joint Source-Channel Coding,” Pre-ICM International Convention on Mathematical Sciences, 2008 年 12 月, Delhi, India

④ Gou Hosoya, Toshiyasu Matsushima, Shigeichi Hirasawa, “Construction and performance analysis of irregular low-density parity-check code ensemble for correcting a single solid burst erasure,” Pre-ICM International Convention on Mathematical Sciences, 2008 年 12 月, Delhi, India

⑤ 浮田善文, 松嶋敏泰, 平澤茂一, “実験計画法における効果の推定の計算量削減に関する一考察,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木

⑥ Tomohiko Saito, Toshiyasu Matsushima, Shigeichi Hirasawa, “A Note on Automatic Construction Algorithms for Orthogonal Designs of Experiments Using Error-Correcting Codes,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木

⑦ Shunsuke Horii, Toshiyasu Matsushima, Shigeichi Hirasawa, “A Note on the Iterative Interference Cancellation and Decoding for Coded CDMA,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木

⑧ Naoto Kobayashi, Toshiyasu Matsushima, Shigeichi Hirasawa, “An Accurate Density Evolution Analysis for a Finite-State Markov Channel,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木
⑨ 須子統太, 松嶋敏泰, 平澤茂一, “区間で一定なパラメータを持つ非定常情報源の漸近的な性質について,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木
⑩ 前田康成, 吉田秀樹, 藤原祥隆, 松嶋敏泰, “ブロック誤り率が未知の場合の選択再送 ARQに関する一考察,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木
⑪ 細谷剛, 松嶋敏泰, 平澤茂一, “ソリッドバースト消失の訂正に適した非正則LDPC符号について,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木
⑫ Ryo Nomura, Toshiyasu Matsushima, Shigeichi Hirasawa, “On the Overflow Probability of Lossless Codes for Mixed Sources,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木
⑬ Manabu Kobayashi, Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, “On designing irregular LDPC codes using accurate densitied for Gilbert-Elliott channel,” 第 31 回情報理論とその応用シンポジウム, 2008 年 10 月, 栃木
⑭ Shunsuke Horii, Tota Suko, Toshiyasu Matsushima, Shigeichi Hirasawa, “Multiuser Detection Algorithm for CDMA based on the Belief Propagation Algorithm,” IEEE 10th International Symposium on Spread Spectrum Techniques and Applications, 2008 年 8 月, Bologna, Italy
⑮ Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, “Error control codes for parallel channel with correlated errors,” 2008 IEEE Information Theory Workshop, 2008 年 5 月, Porto, Portugal
⑯ Ryo Nomura, Toshiyasu Matsushima, Shigeichi Hirasawa, “A Note on the Weak Universal Joint Source-Channel Coding,” 電子情報通信学会技術報告IT, 2008 年 1 月, 東京
⑰ Shunsuke Horii, Tota Suko, Toshiyasu Matsushima, Shigeichi Hirasawa, “A Note on Multiuser Detection Algorithms for CDMA based on the Belief Propagation Algorithms,” 電子情報通信学会技術報告 IT, 2008 年 1 月, 東京
⑱ Kazuhiko Minematsu, Toshiyasu Matsushima, "Tweakable Enciphering Schemes from Hash-Sum-Expansion," INDOCRYPT 2007, 8th International Conference on Cryptology in India, 2007 年 12 月, Chennai,INDIA
⑲ Toshiyasu Matsushima, Shigeichi Hirasawa, "A Class of Prior Distributions on Context Tree Models and an Efficient Algorithm of the Bayes Codes Assuming it," IEEE International Symposium on Signal Processing and Information Technology, 2007 年 12 月, Cairo, Egypt
⑳ 堀井俊佑, 松嶋敏泰, 平澤茂一, "盗聴・改ざんに対して耐性を持つネットワーク符号化について," 第 30 回情報理論とその応用シンポジウム, 2007 年 11 月, 三重
⑳ 小林学, 松嶋敏泰, 平澤茂一, "Gilbert-Elliott通信路に対するLDPC符号のロバスト性に関する密度発展法による解析," 第 30 回情報理論とその応用シンポジウム, 2007 年 11 月, 三重
21 Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "Error control codes for parallel channel with correlated errors," 第 30 回情報理論とその応用シンポジウム, 2007 年 11 月, 三重
22 Gou Hosoya, Toshiyasu Matsushima, Shigeichi Hirasawa, "A combined matrix ensemble of low-density parity-check codes for a solid burst erasure," 第 30 回情報理論とその応用シンポジウム, 2007 年 11 月, 三重
23 Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "Improved collusion-secure codes for digital fingerprinting based on finite geometries," 2007 IEEE International Conference on System, Man and Cybernetics, 2007 年 10 月, Montreal Canada
24 Yasunari Maeda, Noya Ikeda, Hideki Yoshida, Yoshitaka Fujiwara, Toshiyasu Matsushima, "A Note on Morphological Analysis Methods based on Statistical Decision Theory," SICE Annual Conference 2007, International Conference on Instrumentation, Control and Information Technology, 2007 年 9 月, Kagawa, Japan
25 Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "Short concatenated fingerprinting codes for multimedia data," Forty-fifth Annual Allerton Conference on Communication, Control, and Computing, 2007 年 9 月, Illinois, USA
26 Takashi Ishida, Masayuki Goto, Toshiyasu Matushima, Shigeichi Hirasawa, "Word segmentation for the sequences emitted

from a word-valued source," IEEE 7th International Conference on Computer and Infromation Technology, 2007 年 8 月, Fukushima, Japan
27 Kensuke Yasui, Tota Suko, Toshiyasu Matsushima, "An Algorithm for Computing the Secrecy Capacity of Broadcast Channels with Confidential Messages," 2007 IEEE International Symposium on Information Theory, 2007 年 6 月, Nice, France
28 Ryo Nomura, Toshiyasu Matsushima, Shigeichi Hirasawa, "On the epsilon-overflow probability of lossless codes," 2007 IEEE International Symposium on Information Theory, 2007 年 6 月, Nice, France
29 Naoto Kobayashi, Toshiyasu Matsushima, Shigeichi Hirasawa, "A Note on Error Correction Schemes using LDPC codes with a High-Capacity Feedback Channel," 2007 IEEE International Symposium on Information Theory, 2007 年 6 月, Nice, France
30 Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "Shotening methods of collusion-secure codes for digital fingerprinting," 2007 Hawaii and SITA Joint Conference on Information Theory, 2007 年 5 月, Hawaii, USA
31 Gou Hosoya, Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "An adaptive decoding algorithm of LDPC codes over the binary erasure channel," 2007 Hawaii and SITA Joint Conference on Information Theory, 2007 年 5 月, Hawaii, USA
32 安井謙介, 須子統太, 松嶋敏泰, "秘密情報を持つ Broadcast Channel の Secrecy Capacity 計算アルゴリズム," 第 29 回情報理論とその応用シンポジウム, 2006 年 11 月, 北海道
33 増井陽一, 小林直人, 松嶋敏泰, "記憶のある通信路に適した誤り訂正符号の構成法に関する研究," 第 29 回情報理論とその応用シンポジウム, 2006 年 11 月, 北海道
34 Naoto KOBAYASHI, Toshiyasu MATSUSHIMA, Shigeichi HIRASAWA, "A Note on Transmission Schemes with Unequal Error Protection Codes and a Feedback Channel," 第 29 回情報理論とその応用シンポジウム, 2006 年 11 月, 北海道
35 吉田隆弘, 松嶋敏泰, 平澤茂一, "相互通信可能な情報源符号化に関する一研究," 第 29 回情報理論とその応用シンポジウム, 2006 年 11 月, 北海道
36 Ryo NOMURA, Toshiyasu MATSUSHIMA, Shigeichi HIRASAWA, "A Note on overflow probability of lossless codes," 第 29 回情報理論とその応用シンポジウム, 2006 年 11 月, 北海道
37 Gou Hosoya, Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "Performance of Low-Density Parity-Check Codes for Burst Erasure Channels," 2006 International Symposium on Information Theory and its Applications, 2006 年 10 月, Seoul, Korea
38 Hideki Yagi, Toshiyasu Matsushima, Shigeichi Hirasawa, "New Traceability Codes against a Generalized Collusion Attack for Digital Fingerprinting," 2006 International Workshop on Information Security Applications, 2006 年 8 月, Jeju Island, Korea
39 Shunsuke Horii, Tota Suko, Toshiyasu Matsushima, "Multiuser Detection Algorithms for CDMA based on the Massage Passing Algorithms," 電子情報通信学会技術研究報告IT, 2006 年 5 月, 奈良
40 Daiki Koizumi, Naoto Kobayashi, Toshiyasu Matsushima, Shigeichi Hirasawa, "The Reliability based Hybrid ARQ Scheme with both the Encoded Parity Bit Retransmissions and Message Passing Decoding," 電子情報通信学会技術研究報告IT, 2006 年 5 月, 奈良
41 Tomohiko Saito, Toshiyasu Matsushima, Shigeichi Hirasawa, "On Factorial Effects Corresponding to Orthogonal Arrays with Unequal Strength," 電子情報通信学会技術研究報告IT, 2006 年 5 月, 奈良

６．研究組織

(1)研究代表者

松嶋　敏泰 (TOSHIYASU MATSUSHIMA)
早稲田大学・理工学術院・教授
研究者番号：30219430

(2)研究分担者

該当なし

(3)連携研究者

平澤　茂一 (SHIGEICHI HIRASAWA)
早稲田大学・理工学術院・教授
研究者番号：30147946