学位論文審査報告

藤原, 修平

張, 雪峰

華, 景煜

趙, 亮

他

出版情報：九州大学大学院システム情報科学紀要. 18 (1), pp.31-62, 2013-01-25. 九州大学大学院システム情報科学研究院
バージョン：
権利関係：

学 位 論 文 審 査 報 告

氏　　名　藤 原 修 平
学 位 記 番 号　シ情　博甲第 471 号（工学）
学位授与の日付　平成 24 年 8 月 31 日
学位論文題名　電力系統の不平衡解析手法の開発に関する研究
論文調査委員
（主　査）　九州大学　教　授　村 田 純 一
（副　査）　〃　〃　末 廣 純 也
〃　〃　〃　庄 山 正 仁

論 文 内 容 の 要 旨

電力系統解析は，系統構成の策定，機器の制御・保護方式の設計など様々な検討に必須である．検討においては出来るだけ実系統での現象を再現できるように，三相平衡状態のみならず三相不平衡状態を考慮した解析も実施するのが望ましい．そこで従来は三相不平衡の発生状況を的確に捉えた前提条件を設けることで，現象を適切に模擬してきた．例えば実効値による定常解析（潮流計算）では「三相不平衡状態は無視出来る」として平衡で模擬を，実効値による動特性解析（安定度計算）では「送電配電設備の事故を対象にすれば十分である」として，送電線の不平衡故障や単相再閉路などを主な検討対象としてきた．また瞬時値の動特性解析においては，従来から三相での解析を実施してきたが，計算時間の制約から検討対象の簡略化等が必要となる場合もあった．

しかし，近年の電力系統の構成の変化に伴い上記の方針では対応出来ないケースが発生してきている．例えば実効値による定常解析においては，非撚架送電線による三相不平衡を検討する必要がでてきた．しかし従来の計算方法では，三相不平衡を考慮した場合，大規模系統では収束性が悪くなり解を得られない課題がある．また，実効値による動特性解析においては，太陽光発電等の単相機器や静止型無効電力補償装置等のパワエレ機器の影響が大きくなるにつれて，それらの機器が三相不平衡状態に与える影響を検討するニーズがでてきている．これらの機器はその三相不平衡状態が動的に変化するが，従来の解析手法では解析が困難である課題がある．また，三相不平衡状態を模擬する場合，解析規模の増大に伴う計算時間の増大と計算精度の悪化も課題として存在している．瞬時値による動特性解析についてはＥＭＴＰが広く使われており，計算手法に関する検討の必要性は低いが，瞬時値解析は多大な計算時間を要する場合が多いため，計算時間の短縮については実務上の要望が多い．

そこで本論文は，上記の課題に対する検討を報告する．まず実効値による定常解析については，潮流計算の方程式を電流で表現し，さらに非接地系統のノード方程式に零相の条件式を導入することを発案した．また実効値による動特性解析については，まず計算時間の増大と計算精度の悪化を解決するため，陽的ルンゲクッタ埋め込み法の適用と，適用時の課題である代数微分方程式の計算方法，不連続要素を精度良く扱う方法を発案した．さらに動的な三相不平衡状態の解析が困難である課題については，不平衡故障を複数組み合わせたブランチと電流源による模擬手法を発案した．最後に瞬時値による動特性解析についても検討を実施し，課題である計算時間を短縮すべく，電力変換器の解析モデルの高速化を実現した．

本論文は上記の課題に対する検討を纏めたもので，６章で構成されている．第１章は緒言，第２章は電力系統の三相不平衡解析手法と本研究の目的，第３章～第５章が本論で，第６章は結言である．

第３章は実効値による定常解析（潮流計算）に関する報告である．

本件の課題である難収束を解決するために①潮流計算の方程式を電力方程式ではなく電流方程式を用い，変圧器中性点等の解が零付近となる母線の電圧を安定して求め，②ノード方程式に零相に関する条件を導入し，非接地系統の電圧解が不定になる事を防止するとともに，③直角座標系の採用により浮遊母線のノード方程式を線形化し，計算速度と収束性を向上させることで課題を解決した．発案した手法を実規模の系統に適用して反復回数と残差を確認し，安定して収束することを確認すると共に，ＥＭＴＰと計算結果を比較し，十分な計算精度であることを確認した．この結果，これまでは 200 母線程度のきわめて小規模の系統しか解を得ることが出来なかったが，本発案により 1000 母線規模の解析でも安定して解を得ることが可能となり，これまでは解析できなかった規模の大きい実系統を対象とした三相不平衡の検討が可能となった．

第４章は実効値による動特性解析（安定度計算）に関する報告である．

実効値による動特性解析において三相不平衡を取り扱う際には，(1) 計算時間の増大と計算精度の悪化，(2) 動的な三相不平衡状態の解析が困難である の２つの課題がある．(1)の課題については，①可変刻み幅と誤差の定量評価が可能な陽的ルンゲクッタ埋め込み法を適用し，②適用時の課題である代数微分方程式の扱いについては代数方程式と微分方程式を交互に求解し，③精度悪化の要因となるリミッタ等の不連続要素については不連続点を通過するタイミングで解析解を補間する方法を発案する事でこの課題を解決した．発案した手法を実規模の系統に適用し計算精度と計算速度を評価し，同程度の計算精度の場合，計

算速度向上(解析規模 1026 母線，許容誤差 0.1%の場合,計算時間は約 40%に短縮)が図れることを確認し，その有効性を示した．もう一つの課題 (2)は，①まず数値計算上安定して多地点の三相不平衡状態が計算可能な手法を発案した．この手法は正相回路の故障点間に故障等価インピーダンスを作成し正相回路に挿入することで実現する．この発案により，まず静的な模擬ではあるが多地点に接続される複数機器の三相不平衡状態を扱う事が可能となった．②次に，前述の手法を用いて動的な三相不平衡状態を解析する手法を発案した．この手法は三相不平衡発生地点に不平衡故障を複数組み合わせたブランチと正相電流源を接続し逆相・零相の電流源を実現する方法である．さらに発案した手法をＥＭＴＰの計算結果と比較し十分な計算精度を有することを確認した．結果として，動的な三相不平衡状態の解析が可能となり，これまで困難であったパワエレ機器等の動的な三相不平衡成分を含む機器の解析が可能となった．

第５章は瞬時値による動特性解析に関する報告である．本件についてはＥＭＴＰが広く使われており，計算手法に関する検討の必要性は低い．しかし瞬時値解析は多大な計算時間を要するため計算時間の短縮については実務上の要望が多い．このために今後電力系統への大量導入が見込まれる電力変換器の高速計算用解析モデルを発案し，多数台連系解析を可能とした．検討の対象として風力発電機を対象にモデルの検討を行い，計算精度を維持しながらも高速化が可能方法について提案を行うと共に詳細モデルとの比較により有効性を明らかにした．

以上，本論文では非撚架送電線やパワエレ機器の増大などによる電力系統の構成の変化に伴い解析のニーズが出てきたが，従来の計算手法では扱うことが難しい電力系統の三相不平衡現象を模擬する事に取り組み，『三相不平衡を考慮した実効値による定常解析』『動的な三相不平衡状態の解析が可能な実効値による動特性解析』『瞬時値による電力変換器の高速計算用解析モデル』を実現した．

論 文 調 査 の 要 旨

電力系統の数値解析は，電力系統構成，電力機器および電力系統制御・保護方式の設計に必須である．電力系統では三相平衡状態のみならず三相不平衡状態の解析も必要であるが，従来，実効値を対象とした不平衡解析は解の収束性，解析精度および計算時間に問題があるため，実用面では三相平衡を仮定した解析が主として実施されてきた．また，瞬時値を対象とした解析では汎用の計算手法である EMTP (Electro Magnetic Transients Program)を用いることによって三相不平衡状態を取り扱うことが可能であるが，計算時間の増大が課題であった．これに対し，近年の非撚架送電線やパワーエレクトロニクス機器の増大などによる電力系統の構成の変化に伴い，三相不平衡状態の解析の必要性は著しく高まってきており，実用的な不平衡解析手法が望まれている．

本論文は，上記の課題に対し，電力系統解析を，実効値による定常解析，実効値による動特性解析および瞬時値による動特性解析に分類し，その各々についての課題解決策を提案したものである．

まず実効値による定常解析すなわち潮流計算において，不平衡解析は，正相回路だけを取り扱う平衡解析と比べて規模が大きい非線形方程式を解く問題となることから，解の不定性や難収束の課題が発生し，これらは対象系統規模が大きくなるほど顕著になる．これに対し，著者は，ノード方程式に電流方程式を導入して浮遊母線電圧を正しく求め，非接地系統のノード方程式に零相電流の条件式を導入することによって電圧解が不定になることを防止するとともに，電圧表現に直角座標系を採用して浮遊母線の方程式を線形化し収束性を向上させている．これらによって上記課題を解決し，従来，200 母線程度が実効値解析で取り扱える上限規模であったのに対し，909 母線を含む大規模系統である国内の 154kV 以上全系統について，汎用解析手法である EMTP の結果と良く合致する正確な不平衡解析が行えることを示している．

次に，実効値による動特性解析では，大規模な非線形微分方程式の数値解を求めることになり，計算時間と計算精度が大きな課題となる．また，実務者が取り扱やすい不平衡機器の解析手法が存在していなかった．そこで，陽的ルンゲクッタ埋め込み法を適用することにより，その可変刻み幅による計算時間短縮と誤差の定量評価による精度保証を両立させ，さらに，実務者が取り扱いやすい対称座標法に基づく多地点に存在する動的な非線形不平衡機器の解析手法を開発している．これらを適用することによって，1000 母線程度の大規模系統において同一精度の場合に計算時間が従来に比べて 40%まで削減でき，また，多地点に存在する動的不平衡機器の動特性解析を EMTP の結果と合致する高い精度で行うことができることを示している．これにより，従来は実効値解析では不可能であったパワーエレクトロニクス機器等の動的な三相不平衡機器を含む解析を可能としている．

最後に，瞬時値による動特性解析について，解析モデルの簡略化による解析の高速化を実現している．瞬時値解析については EMTP が広く用いられており，計算手法に関する検討の必要性は低い．しかし瞬時値解析は多大な計算時間を要するためその短縮の要請は強い．そこで，今後電力系統への大量導入が見込まれる電力変換器について，基本波に着目して電圧源・電流源で表現する高速計算用解析モデルを開発している．これを，風力発電機コンバータモデルに適用した結果，詳細なコンバータモデルを使用した場合と比較して実用上十分な精度の解析が 1%の計算時間で得られることを示している．

以上要するに本論文は，電力系統の構成の変化に伴い必要性が著しく高まってきているにもかかわらず，従来の計算手法では扱うことが難しかった電力系統の三相不平衡解析を，高速かつ高精度に行う方法の開発に取り組み，三相不平衡機器の持つ本質的特性，および数値計算手法の特性の両面から考察することによって，その方法を開発，確立したものである．この成果は実用化され，三相不平衡を考慮した電力機器の設計や電力系統側の対応策の検討を容易にしている他，今後の太陽光発電や風力発電の大量導入計画の実現に大いに貢献するものであり，電気電子工学上価値ある業績である．よって，本論文は博士（工学）の学位論文に値するものと認める．

氏　　名　張　雪峰
学位記番号　シ情　博甲第 472 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　Hybrid Particle Swarm Optimization for Flow Shop and Job Shop Scheduling Problems
（フローショップ及びジョブショップスケジューリング問題におけるハイブリッド粒子群最適化）

論文調査委員
（主　査）　九州大学　教　授　長谷川　隆　三
（副　査）　〃　〃　横　尾　　真
〃　〃　〃　冨　浦　洋　一
〃　〃　准教授　峯　　恒　憲

論 文 内 容 の 要 旨

Scheduling problem is one of the most critical issues in the planning and managing of manufacturing processes. The difficulty of finding the optimal schedule depends on the shop environment, the process constraints and the performance indicator. The main objective of scheduling problems is an efficient allocation of shared resources over time to competing activities. Emphasis has been on investigating machine scheduling problems where jobs represent activities and machines represent resources. The problem is not only NP-complete, but also has a well-earned reputation of being one of the most computationally difficult combinatorial optimization problems considered to date. The most difficult problems in this area are the Flow Shop Scheduling Problem (FSSP) and Job Shop Scheduling Problem (JSSP).

Over the past decades, FSSP and JSSP have attracted many outstanding researchers, efforts have been devoted to finding high-quality global solutions in a reasonable computation time by heuristic optimization techniques. The traditional methods include Tabu Search method (TS), Ogbu and Smith's Simulated Annealing algorithm (SA), Reeves's Genetic Algorithm (GA), Adams, Balas and Zawack's Shifting Bottleneck procedure (SB) and Eberhart's Particle Swarm Optimization algorithm (PSO), and Ant Colony (ACO). In recent years, most studies indicate that a single technique cannot solve this stubborn problem. Since hybrid methods can provide high-quality solutions within reasonable computing times, a variety of works have been done on hybrid methods including several techniques, such as GA, TS, SA and SB, etc. A comprehensive survey of hybrid methods on scheduling techniques can be seen. In addition, the research on the PSO algorithm is one of current hot topics. It combines the local search and the global search together, such that it is able to achieve a better search efficiency.

In order to refrain from the premature convergence and being easily trapped into local optimum, in this thesis, motivated by these perspectives, we propose an efficient hybrid intelligent algorithm for the FSSP and JSSP based on PSO, TS, SA and GA, which are evolution computation techniques. They exhibit implicit parallelism and contain certain redundancy and historical information of past solutions. Moreover, TS, SA and GA also have better local search features. Therefore, the proposed hybrid PSO algorithm also effectively exploits the capabilities of distributed and parallel computing of swarm intelligence approaches to achieve the better solution for FSSP and JSSP.

Specifically, this thesis is organized as follows:

In Chapter 2, the basic concepts and notations of the FSSP and JSSP are described, such as the semi-active, the disjunctive graph representation and critical path. The main focus throughout this thesis is the minimum-makespan problem, in which makespan, maximum completion time of all the operations, is used as an objective function to be minimized. Moreover, we introduce searching mechanism and algorithm processes of PSO. Then, PSO has been demonstrated as an optimization technique in real-number spaces.

In Chapter 3, the concept of neighborhood search is described as a widely used local search technique to solve combinatorial optimization problems and is extended to include meta-heuristics. Especially, it is shown that TS and SA can be considered as advanced meta strategies for neighborhood search to avoid local optimum. PSO combines local search (by self-experience) with global search (by neighboring experience), achieving a high search efficiency. TS uses a memory function to avoid being trapped at a local

minimum, and has emerged as an effective algorithmic approach. This method can also be referred to as calculation of the horizontal direction. SA employs certain probability to avoid becoming trapped in a local optimum and the search process can be controlled by the cooling schedule (also known as calculation of vertical direction). By reasonably combining these three different search algorithms, we develop two robust, fast and simply implemented hybrid optimization algorithms (HPTS and HPTS with parameter selection approaches). Based on the HPTS algorithm, an improved HPTS algorithm called IHPTS is also proposed, which will enhance the particle swarm computing performance by GA operation to solve FSSP. In addition, we propose a new multi-layer hybrid particle swarm optimization model, which brings the new research direction and inspiration for the hybrid algorithms.

In Chapter 4, through extensive experiments on different scale benchmarks, we validate the effectiveness of our approaches (HPTS, HPTS with parameter selection approaches and IHPTS algorithms). 30 instances for FSSP of 10 different sizes taken from Taillard's benchmark have been selected to test our three proposed approaches. This benchmark contains some instances that have been proven to be very difficult to solve in the sense that the best solutions found so far are through the use of a very lengthy Tabu-search heuristic. On the other hand, 43 instances for JSSP are taken from OR-Library as test benchmarks to test HPTS. The proposed approaches was coded in MATLAB programming language and run on a 2.27 GHz Intel(R) Core(TM)2 Duo CPU, RAM 4GB personal computer. Each instance is executed for 10 runs. The experimental results reveal the effectiveness of our approaches, compared with other well-established methods.

Finally, **in Chapter 5**, the study in this thesis is summerized and the future directions are suggested.

論 文 調 査 の 要 旨

スケジューリング問題は計画立案や製造過程の管理における重要な課題の１つである．ここでスケジューリング問題とは，複数のジョブを複数のマシンで処理する際，最大完了時間を最小にするようにマシンとジョブの割当を決定する問題であり，組合せ最適化問題の中でも，最適解を得ることが困難とされている問題である．スケジューリング問題はマシンでの処理順序や条件により分類され，すべてのジョブでマシンの処理順序が同じであるフローショップスケジューリング問題(FSSP)，および，そのような制約がなく，ジョブごとにマシンの処理順序が異なって良いジョブショップスケジューリング問題(JSSP)などがある．

過去数十年，FSSP と JSSP は多くの研究者を惹きつけており，発見的最適化技法により，妥当な計算時間で高質な大域解を見つける努力がなされてきた．近年，鳥や魚の群れの振る舞いを工学的に摸倣した粒子群最適化(PSO)が様々な組合せ最適化問題に用いられてきており，とりわけ，タブー探索(TS)，焼鈍し(SA)や遺伝的アルゴリズム(GA)などの進化型計算アルゴリズムをそれぞれ個別に組み込んだ，ハイブリッド PSO アルゴリズムが FSSP や JSSP に適用され，成功を収めている．しかしながら，既存のアルゴリズムは粒子群の多様性を考慮に入れておらず，初期収束が起きやすい．また，近傍の探索能力が満足のいくものではなく，このため探索の初期に局所最適解に陥ってしまう，などの問題を抱えている．

本論文は，これらの問題を解決するハイブリッド組合せ最適化アルゴリズムを提案し，その効果を実験検証したものであり，以下の点で評価できる．

第一に，著者は，FSSP および JSSP を解くために，PSO, TS, SA を組み込んだ効率的なハイブリッドアルゴリズム HPTS を提案している．PSO は（個々の粒子の経験に基づく）局所探索と（近傍粒子群の経験を取り込んだ）大域探索を組合せて探索を効率化する．TS はタブーリストというメモリ機能を利用して，同じ解の探索や局所最適解に陥ることを回避する．SA は局所探索の強化版であり，確率的遷移と冷却スケジュールにより，局所最適解に陥ることを回避する．さらに TS と SA の導入によって増加した可能な解の組み合わせが，粒子群の多様性を生みだしている．PSO の性能はパラメータ設定に非常に敏感に左右される．著者は，質量と加速度という２つのパラメータの選択法を提示し，提案手法により，HPTS の大域探索能力と収束性が向上することを実験を通じて明らかにしている．

第二に，著者は，GA の導入により粒子群計算性能の向上を図った,HPTS の改良アルゴリズム IHPTS を提案している．IHPTS では，GA の各繰り返し過程において，1）粒子群の中から適応度に応じて２つの親個体を選び，これらに２点交叉を施し，新たな子個体を生成する．2）ある確率で単一の個体に２点突然変異を施し，個体を変更する．PSO は大域探索能力を持つが，初期収束したり大域収束を遅らせたりする欠点がある．GA の交叉および突然変異は，粒子群の多様性を増し探索空間を拡大する効果的な方法である．さらに，IHPTS では，PSO と GA を並行動作させ，一方が局所最適解に陥ると他方がそれを防ぐ，相互補完手法が提示されている．

第三に，著者は，異なるスケールのベンチマークを用いた広範な実験を行い，提案手法の有効性を実証している．提案手法の評価のため，FSSP 用に Taillard のベンチマークから３０例が，JSSP 用に OR ライブラリから４３例が選ばれた．他の有力な方法と比較して，既知の最良記録に匹

敵するかそれを上回る解がより多く得られており，未解決問題の上限値の更新にも成功している．例えば，FSSP 用３０例中７例で，JSSP 用４３例中６例で，新上限値が HPTS により得られている．また，IHPTS により，FSSP 用３０例中１８例で，新上限値が得られている．これらの成果は既存手法を凌駕しており，高く評価できる．

以上要するに本論文は，フローショップやジョブショップ問題などの組合せ最適化問題の高質な解を求める方法として，進化型計算アルゴリズム PSO，TS，SA，GA を効果的に組み合わせたハイブリッド組合せ最適化アルゴリズムを提案し，異なるスケールのベンチマークを用いた広範な実験を通じてその有効性を示したものであり，情報学に寄与する所が大きい．

よって，本論文は博士（工学）の学位論文に値すると認める．

氏　　名　華　景煜
学位記番号　シ情　博甲第 473 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　A Study on Anomaly-Based Countermeasures Against Malware Constructing Botnets
（ボットネット構築マルウエアへの異常検知に基づく対策に関する研究）
論文調査委員
（主　査）　九州大学　教　授　櫻　井　幸　一
（副　査）　〃　〃　福　田　　晃
〃　〃　准教授　堀　　良　彰

論文内容の要旨

Botnet, i.e. a collection of compromised computers that are remotely controlled by hackers, is one of the biggest threats against the Internet security. To construct a botnet, hackers usually have to integrate various malware techniques for handling different tasks: firstly, they need some malware propagation technique to locate and infect as many vulnerable hosts as possible. Then, to make the bot-malware parasitic in the victims, they have to adopt some concealment techniques to conceal malware traces and even disable security software on the target machines. Finally, to let the attackers remotely control their hijacked machines, they have to establish an efficient and stealthy command and control (C&C) channel. In this dissertation, we study three real malware techniques that are being or will be widely used for the above tasks in botnet construction, and propose anomaly-base countermeasures against each of them.

Specifically, this dissertation proposal is organized as follows:

Chapter 1 presents the background and motivation of this research. It also summarizes our main works and contributions in this chapter.

Chapter 2 first makes a quick review of existing malware techniques in botnet construction. In this process, it discusses the merits and demerits of each technique and illustrates the positions of the three targeted techniques: Google Hacking, Kernel Rookits, and SMS-based C&C. It then introduces the existing works on these three techniques and summarizes the challenges to defense against them. Finally, it presents the principle and the challenge of designing anomaly-based countermeasures.

Chapter 3 studies Google Hacking, a new malware propagation technique that uses malicious search-engine queries to locate vulnerable machines. This technique has been proved efficient by real malware but receives very little attention. Existing signature-based query filtering countermeasures cannot deal with neutral or 0-day malicious queries. According to our analysis, the maliciousness of a query is not determined by the query itself but what the searcher does against search results. The only normal behavior of a searcher is requesting web pages appeared in search results, and any other actions against search results can be regarded as abnormal. We leverage this observation to design a Google Hacking Defense System (abbr. GHDS). It makes a search engine randomly insert some fake results that point at honeypots within search results of suspicious queries. Then, attackers can be captured when their abnormal behaviors against fake results are drawn to honeypots. The practical and theoretical evaluations demonstrate that this anomaly-based system has the ability to capture neutral and 0-day malicious queries, and can well prevent Google Hacking attacks in different scenarios with a small insert-rate of honey pages.

After attackers locate vulnerable machines, their next step is to exploit application vulnerabilities (e.g. buffer-overflow) to inject malicious codes for the malware infection. Once a program is exploited and injected malicious codes, its runtime behaviors must deviate from its original intents. We leverage this point to design a model-based intrusion detection system against code injecting in **Chapter 4**. It uses a statically-constructed state transition table (STT), which records expected transitions among system calls as well as their stack states (return address lists), as a normal behavior model to perform anomaly-detection. According to our analysis, the STT model greatly improves the space

efficiency of the classic VPStatic model without decreasing its high precision and time efficiency.

Chapter 5 studies kernel rootkits, which is the toughest malware concealment technique. Because they conceal malware by directly subverting the kernel, it's hard to prevent them with traditional antivirus tools that rely on the information provided by the kernel. We find that the root of kernel rootkits is at the lack of isolation among OS kernel modules: they can access each other's memory without any restriction. So, we present Barrier: a lightweight hypervisor, to isolate kernel modules into different spaces. As a result, kernel rootkits can be captured when they access text or data outside their spaces without obeying some predefined normal behavior rules (models). The evaluation results show that this anomaly-based hypervisor can well capture the current kernel rootkits without bringing unaffordable performance overheads.

Chapter 6 mainly studies the possibilities to use Short Message Service (SMS) to construct an efficient and stealth C&C channel. Recently, many Internet threats including botnet are moving to mobile devices. Although many existing control techniques in the desktop world can be easily adapted to the mobile environment, special features of mobile phones such as SMS provide hackers additional ways to perform remote control. We present a SMS-based C&C using a simple flooding algorithm, and prove its effectiveness both theoretically and experimentally. We then propose countermeasures that can well prevent this emerging threat.

Chapter 7 concludes the results of this research, and discusses some future works.

論 文 調 査 の 要 旨

ネットワーク化された多数の計算機から構成される情報基盤に対する新たな脅威が出現している．脆弱性を有する計算機に悪意あるソフトウェアであるマルウェアを侵入させ遠隔操作を提供するプログラムであるボットを用いた攻撃への対策は重要である．ボット群の遠隔制御ネットワークであるボットネットは，脆弱性を有する計算機の侵入，迷惑メール乱発，マルウェアの拡散，サービス不能攻撃の温床となっており，その対策は技術的・社会的な課題である．

本研究は，ボットネットの構築において重要なネットワーク化された計算機へのマルウェアの侵入，その計算機上でのマルウェアの稼働，さらにそれらのネットワーク化によるマルウェアの連携に着目している．マルウェア侵入と稼働を阻止する防御システム，マルウェアが攻撃対象とする計算機における侵入後の検知システム，モジュール化されたオペレーティングシステムカーネル部に侵入するマルウェアに対する対策，携帯電話網を利用したショートメッセージサービスを用いた新たなボットネットの構築挙動の解析とその対策を論じたものである．これらのボットネット構築に関する４つの課題を解決したもので，以下の点で評価できる．

第一に，検索エンジンへの問合せに基づく脆弱性を有する計算機の発見手法についての解析と対策を行った．検索エンジンを用いた攻撃手法は，実環境において脅威でありながら，従来の研究ではマルウェアのコードパタンの特徴情報との照合による対策にとどまっており，未知の脆弱性に対する攻撃への対策が課題であった．著者は，悪意を持って行われる検索エンジンへの問合せのみならず，問合せ者のその他の挙動を解析することによって，異常検知を用いて未知の脆弱性に対する攻撃の検知手法を考案した．加えて，検索エンジンの応答に模擬攻撃対象であるおとりシステムへのリンクを挿入し，攻撃者に確率的におとりを攻撃させることにより攻撃者の異常挙動を発見し防御を行う手法を考案した．さらに，本手法を適用した際のおとりシステムへのリンク挿入度と本手法の適用前と適用後のマルウェア侵入比を数値解析により導出した．本手法の適用により，ボットネットからの攻撃の際におとりシステムへのリンク挿入度を 2%とした場合，95%以上のホストの感染を防止できることを明らかにした．

第二に，脆弱性を有する計算機に侵入したマルウェアを対象とするモデルベースの侵入検知システムを考案した．従来の方法では，検知精度を上げるには，状態遷移空間を広げる必要があり，結果として処理効率が落ちるという課題があった．著者は，計算機上のプロセスが呼出すシステムコールの種別とその時のスタック状況のハッシュ値から決まる状態について，正常な状態遷移との比較による異常検知手法を考案した．さらに実験により，従来方式（VPStatic model）と同等の精度を維持し，半分以下のメモリにて実現できることを示した．

第三に，オペレーティングシステムのカーネル部に侵入するマルウェアへの対策技術を考案した．一般プロセスから隠ぺいするために，カーネル部に実行コードを置くマルウェアへの対策は，ユーザプロセスで稼働するセキュリティソフトウェアでは困難である．特に，カーネルの一部がモジュール化され動的構成を行うオペレーティングシステムにおいて，カーネルモジュールの挙動把握に基づく検知および対策は課題であった．著者は，個々のカーネルモジュールに独立したメモリ空間を提供することでアクセス可能なメモリ領域を制限可能なハイパーバイザを考案した．従来の技術で実現していなかったカーネルモジュールによるカーネル空間のデータ取得を含む挙動把握を可能にし，カーネルモジュール型マルウェアへの対策を実現した．さらに，実システムにおける試験実装によりオペレーティングシステムに標準で備わっているプログラムを

用いてそのオーバヘッドの量を実験的に評価し，提案手法の有効性を検証した．

第四に，スマートフォンを攻撃対象とするボットネットの構成方法とその解析を行った．従来の携帯電話端末は利用開始後の機能追加には制限があり，マルウェアの侵入対象ではなかった．しかしながら，機能追加が容易な汎用性を有するスマートフォンを攻撃対象とするボットネットは現実の脅威となっている．著者は，携帯端末間での直接の通信チャネルであるショートメッセージサービスを用いたボットネットの制御に着目し，通信チャネル形態の数理解析とシミュレーションによる解析を基に，その脅威を初めて定量的に解明するとともに，その対策について論じた．特に，アンドロイドＯＳではユーザから隠されているショートメッセージ挙動のユーザへの提示による対策手法の詳細設計を行った．

以上要するに，本論文は，ボットネットを構築するマルウェアの挙動解析とその対策について新たに出現するボットネットを含む対策技術を論じたものであり，情報工学上寄与するところが大きい．よって本論文は，博士（工学）の学位論文に値すると認める．

氏　　名　趙　　亮
学位記番号　シ情　博甲第 474 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　A Study on Security Analysis of Image Encryption Algorithms
（画像向け暗号方式の安全性解析に関する研究）

論文調査委員
（主　査）　九州大学　教　授　櫻　井　幸　一
（副　査）　〃　名誉教授　香　田　　徹
〃　〃　教　授　内　田　誠　一
〃　〃　〃　高　木　　剛

論 文 内 容 の 要 旨

With the development of the computer and network technology, digital media information is used in many fields more widely, e.g., the industry, medical treatment and academic research. As a result, the corresponding security problem of the digital media information becomes increasingly significant. Moreover, to reduce the volume of the information for the transmission, the digital media information, in general, does the compression as one procedure. Based on this background, there are three kinds of methods for the secure communication of the digital media information. The traditional way is that the digital media information is first compressed to reduce the redundancy, and then encrypted to mask its meaning. However, in some application scenarios, the sender of the digital media information hopes encrypting the original data firstly and the network provider may compress the encrypted information without knowing any knowledge on the original and the corresponding data. Therefore, the second method which does the encryption followed by the compression has been attracted as the considerable research interest recently. Specially, for the second method, the research of the corresponding encryption algorithms is one of the main research topics in the digital media security. The third method is that the compression of the digital media information and the corresponding encryption can be achieved simultaneously. This research always considers the revision of the traditional compression algorithm (e.g., the Huffman coding and arithmetic coding). The purpose of it focuses on the reduction of the time and computation of each operation (i.e., the compression and encryption), and this kind of research makes the system flexible for the advanced digital media processing.

According to the above analysis, it can be found that the second method and the third method are two interesting topics in the field of the digital media security. In fact, there have been many encryption algorithms belonging to these two methods which are proposed for protecting the secrecy of the digital media information. Correspondingly, the security analysis of the proposed algorithms also becomes important before they are employed in practice. In this thesis, we investigate the security of some encryption algorithms about the digital media. In particular, as the still image is one of the main vehicles of the digital media information which causes that there have been many proposed image encryption algorithms, our security analysis primarily focuses on the still image related encryption algorithms. In our analysis, we try to identify some properties in the different encryption algorithms which can be exploited to break the corresponding ciphers.

In this thesis, there are 6 chapters as follows:

Chapter 1 provides the general outline on this research. We present the motivation and main contributions of this thesis in this chapter. Moreover, the organization of this thesis is also described.

Chapter 2 includes the introduction of two main branches on our research. On one hand, the basic information about the digital media security is provided. We introduce the concept and the application of the digital media firstly. Then, the background, motivation and corresponding research

progress about the digital media security are presented. On the other hand, a short review about the security analysis of the digital media encryption is given. We provide the categories of the security and the target of the adversary in this chapter. Moreover, the classification of the attack scenarios and the measurement of the attack are also introduced. Finally, some examples about the security analysis of image encryptions are presented.

Chapter 3 presents a scrambling analysis of image spatial scrambling encryption algorithms. As the image scrambling algorithms (e.g., the Arnold cat map and Fibonacci transformation) are widely used to encrypt the digital image, the scrambling degree of the corresponding ciphertext image should be measured. In this chapter, an evaluation method based on the bit-plane has been proposed. Specially, the bit-plane theory is the core of this evaluation method. In the evaluation step, the spatial distribution entropy and centroid difference for the bit-plane are used to measure the scrambling degree of each bit-plane. As the relationship between the original image and most significant bit-plane to least significant bit-plane reduces gradually, we set a level decreasing-based weight for each bit-plane when the final scrambling degree is computed. The experiment results show that this evaluation method can find the scrambling degree for the image scrambling algorithms.

Chapter 4 addresses a security analysis of an image encryption algorithm of pixel bits and provides the comparison with the previous state of the art. We use the chosen-plaintext attack for an image scrambling encryption algorithm of pixel bits which was provided by Ye published on *Pattern Recognition Letters* in 2010. Our attack reveals the encryption vectors which can substitute for the secret keys. Compared with the former analysis work achieved by Li and Lo which was published on *Signal Processing* in 2011, our attack has the lower complexity which implies that our attack is more efficient than Li and Lo's attack. Moreover, a suggested improvement against our attack is presented in details. In fact, we introduce the self-correlation which comes from the idea of the self-adaptive encryption, proposed by Chen et al. published on *Journal of Software* in 2005, into the original algorithm to enhance the security. The final simulations show that the suggested improvement may be better than the original algorithm.

Chapter 5 is concerned with a security analysis of the randomized arithmetic codes based on the Markov model and the further analysis on the corresponding improvement. The randomized arithmetic code is a kind of symmetric-key algorithm which can achieve the encryption and the compression for the digital media information simultaneously. In this chapter, we first put forward a formal definition of a randomized arithmetic code based on the Markov model (ACMM) which is proposed by Duan et al. published on *Communications in Nonlinear Science and Numerical Simulation* in 2011, and then explore the security of ACMM. Our analysis shows that ACMM is insecure under the ciphertext-only attack (COA) even if a new pseudorandom bit sequence is used for the encryption of each message. Moreover, an enhanced algorithm which combines ACMM with the randomized arithmetic coding (RAC), introduced by Grangetto et al. and published on *IEEE Transactions on Multimedia* in 2006, is presented. However, the security analysis also shows that ACMM+RAC is insecure under the COA. Finally, we present the simulation results to confirm the proposed attacks.

Chapter 6 summarizes the results of this thesis and describes some corresponding future works.

論 文 調 査 の 要 旨

コンピュータとネットワーク技術の発展に伴い，音声や画像などデジタルメディアの情報は広く多くの分野で使用されている．同時に，著作権保護をはじめとするメディア情報に対応するセキュリティ上の問題はますます重要となっている．応用先の要件としては，処理速度を重要視する場合もあり，カオス原理などを利用した高速暗号が適用される場合も多い．しかし，安全性の検討が不十分な場合には容易に解読されたり，暗号アルゴリズムの提案のみが先行し安全性評価指標の確立が遅れているという状況にある．

著者は，画像暗号での要素技術である撹乱処理，置換暗号，圧縮符号を用いた暗号系に着目した．膨大な画像データに必要な高速処理に加えて，画像の符号化，視覚特性に関わる暗号化処理の制約など，通常のテキスト文書とは別の画像暗号固有の課題がある．本研究は，これら画像暗号方式に対する安全性解析と強度評価を論じたものであり，以下の点で評価できる．

第一に，著者は画像の空間スクランブル暗号に対する評価方法を与えた．スクランブルは広くデジタル画像を暗号化する基本要素であるため，暗号強度評価として処理後の画像のスクランブ度を測定する必要がある．このスクランブル暗号は，単純な非線形関数の繰り返しを利用する．このため関数の周期が，画像の撹乱に影響することはよく知られている．また，完全な周期でなく周期の 1/2 や 1/3 などの分周期でも，撹乱度が弱く画像暗号に適さないことがある．従来の評価においては，空間分布のエントロピーと重心の差異を用いて，各ビットプレーンのスクランブル度を測定しているが，分周期の特性まではつかめていないと

いう課題がある．これに対して著者は，最後のスクランブリング度を計算する際，ビットプレーンに関する重みを設定する指標を提案し，分周期におけるスクランブル画像の脆弱性を評価することに成功した．さらに複数の画像に用いて実験を行い，筆者の評価方法が画像のスクランブリング度を測定するための基準の１つにできることを明らかにした．

第二に，離散カオス乱数を利用したピクセルビット置換に基づく既存の画像暗号化アルゴリズムの解析を行った．置換は暗号処理の基本関数の１つであるが，視覚的特性を隠すために，画像暗号でも重要な構成要素である．この暗号は，２分木を用いた解析により，置換行列そのものが露呈することが既存研究により指摘されている．これに対して本研究では，攻撃者が画像を自由に選択できる環境を仮定し，置換乱数鍵を入手する解読手法を開発した．復元された画像は，元の画像と同一のものとなることも実験的に確認した．この解析手法は，攻撃者が選択するわずか画像８枚のみで実行可能であり，かつ従来の攻撃より少ない計算時間で可能である．さらに著者は，この暗号に自己相関関数を導入し，これまでの攻撃に対して堅固な改良方式も提案し，解読された本来の暗号方式の基本アイデアの有効性も主張した．

第三に，算術符号に基づく暗号に対する解析を行った．算術符号は，本来データ圧縮に利用される．この算術符号に秘密鍵を組み込み，圧縮と暗号を同時に行う手法が提案されている．しかし，これまでほとんどの手法は解読されている．著者は，誰も解読に成功していないマルコフモデルに基づく算術符号暗号に対する解読を行った．異なる鍵が異なるメッセージの暗号化のために使用されるという条件の下での暗号文攻撃を与えた．またメッセージごとにこのマルコフモデルに基づいた算術符号とランダム化とを組み合わせて使用する方式の安全性についても解析し，この複合暗号化方式でも安全ではないことを示した．この解析には，複雑な確率計算が必要となるが，著者は計算すべき確率の区間を分割する手法を導入し，効率よい解析手法を開発した点が評価できる．

以上要するに，本論文は，画像向け暗号方式における撹乱処理，置換，算術符号の安全性解析と評価を行ったものであり，情報工学上寄与するところが大きい．よって本論文は，博士（工学）の学位論文に値すると認める

氏　　名	Ghazal Abdelaty Fahmy Atia
学位記番号	シ情　博甲第 475 号（学術）
学位授与の日付	平成 24 年 9 月 24 日
学位論文題名	Development of Delta –Sigma Modulator for Broadband Wireless Communications 広帯域無線通信のためのデルタ・シグマ変調器の開発

論文調査委員

（主　査）	九州大学	教　授	吉田　啓二
（副　査）	〃	〃	林　　健司
〃	〃	准教授	金谷　晴一

論文内容の要旨

Analog-to-digital converters (*ADC*) are very important building block of digital wireless communication systems and in particular, more challenging for software defined radio implementation to operate in different signal bandwidths and channel conditions. Such systems require the *SNR* and bandwidth to be reconfigurable while requiring minimum modification of the system hardware.. Therefore, a flexible *ADC* with the ability to adjust its design parameters for adaptive and multi-mode operation with efficient use of the available power is required. Delta-sigma modulator provides very flexible architecture based on digital circuitry and trade-off between *SNR* and bandwidth. By varying the oversampling ratio (*OSR*), loop filters order, and quantizer resolution, different output SNR and bandwidth for a delta-sigma modulator could achieve. This research is to explore efficient techniques for the design of delta-sigma *ADC*, specifically for multi-standard wireless transceivers. We present different re-configurable delta-sigma modulators, and techniques for low power optimization. the *KT/C* has considered to selected the sampling capacitor that required to realize the suitable dynamic range for wireless applications. Moreover, clock generator designed to generate non-overlapped clock and buffered to feed the entire system avoiding the clock skew. In this work, we present a new design for comparator, Opamp, and three different architectures for delta-sigma modulator. All these design explained in the following paragraphs.

Since the comparator is one of important block in delta-sigma modulator, we proposed a latched comparator with high speed and low power suitable for high speed *ADC*. A low power *CMOS* latched comparator has been designed in *TSMC* 0.18μm. The neutralization technique for reducing Kickback Noise has provided. The simulation results illustrates that it works at 1GHz, suitable for high-speed applications. Measurement results prove that the latched comparator consumes 246 μW with a power supply of 1.2v at *10MHz*. A simulation method for accurately determining dynamic offset in latched comparator was presented.

Typical and proposed recycling folded cascade (*RFC*) amplifier designed and fabricated in *TSMC* 0.18μm. Simulated

and measured results were compared. Proposed *RFC* demonstrate an enhancement on *DC* gain by *5dB* almost for the same power consumption and bandwidth. Moreover, it realized less input referred noise than typical. Split-length devices (*SLD*) method applied on proposed (*RFC*) to create a low impedance node employed in indirect feedback compensation. Realization of two-stages recycling folded cascade amplifier using indirect feedback compensation method has designed. The proposed two-stages amplifier delivers open loop gain 83dB enhanced by 20dB over typical one, gain bandwidth product is 187MHz and slew rate is 74 V/μs which is required for reconfigurable.

The design of a third orders delta-sigma modulator exploited shared Opamp technique in order to reduce number of Opamps required, consequently the total power consumption for the modulator decreased, as well as, required area decreased too. The architecture relaxed comparator speed appropriate for wireless applications. First and second stages are sharing one Opamp in integration and sampling phase. The proposed circuit has designed on *TSMC* 0.18μm CMOS technology. *2MHz* Bandwidth, 50dB Peak Signal-to-Quantization-Noise Ratio (*SQNR*), which is suitable for *WCDMA*, have achieved. It consumes 2.4mW with power supply 1.2v and area is 0.3mm^2.

A third order delta-sigma modulator has designed using single Opamp for wireless applications. The behavioral model simulated using *MATLAB* to determine the modulator parameters that meet the *GSM/WCDMA* specifications. A comparison between conventional and proposed circuit has provided. The proposed circuit has achieved low power consumption compared to conventional one. The proposed circuit has been design using a 0.18μm TS*M*C technology. The proposed circuit achieves 70dB *SNR* and 8mW for analog part at *2MHz* bandwidth and *64MHz* sampling frequency.

Design multi-bits second order delta-sigma modulator using shared Opamp technique has provided. The target for this design is to meet the requirement of *GSM* and *WCDMA* applications. The basics building blocks in the delta- sigma modulator designed and explained in details. The modulator designed and fabricated in 0.18μm *TSMC CMOS* process at 1.8v supply voltage. *CMOS* complementary switches employed in entire architecture, the aspect ratio (*W/L*) selected to achieve low on-resistance and decrease the charge injection. The proposed modulator achieved 81/60 dB *SNDR* for *GSM/WCDMA* applications.

論 文 調 査 の 要 旨

スマートフォンや無線 LAN 等の様々な無線機器の高度化により，いつでもどこでもブロードバンド通信が可能となってきた．更なる無線通信の高度化のためソフトウェア無線(Software Defined Radio: SDR)技術が注目を浴びている．アナログディジタルコンバータ（Analog to Digital Converter: ADC）は，上述の無線通信システムにおいて，きわめて重要な回路ブロックである.特に SDR においては，ハードウェアの小型化および低消費電力化はもとより，様々な周波数帯域やチャネル条件で動作可能な広帯域化およびマルチモード化が必要である．したがって，マルチモード動作のため，各アプリケーションで動作可能な柔軟な ADC が必要となる．

著者は，本論文において，ADC のアーキテクチャのうちの１つである，デルタシグマ ADC に着目し，SDR 通信システムを実現するため，量子化器の分解能，オーバーサンプリング比，およびループフィルタの順序を変化させることによって，種々の周波数帯と高 SN 比を実現するための設計手法を提案している．更に回路シミュレータを用いて回路設計を行い，ファウンドリにより試作したチップを計測・評価することにより広帯域無線通信用デルタシグマ ADC の開発に成功している．

本論文では，まず第 1 章で無線通信用 ADC の現状およびデルタシグマ ADC の研究課題について述べている．

第 2 章では，デルタシグマ ADC を構成するブロックの１つである，コンパレータにおいて，キックバックノイズを減少する回路を導入している．

第 3 章ではフィードバック構造を用いた電流再利用型カスコードアンプを開発し，従来型と同一の消費電力および，周波数帯域において，5dB の利得向上を実現している．

第 4 章では WCDMA(Wideband Code Division Multiple Access) および GSM (Global System for Mobile Communications)用 ADC として，オペアンプを共通化した新しい構造のデルタシグマ ADC を開発している．まず，ADC の積分経路を 3bit 構成としたデルタシグマ ADC を開発している．次に１つのオペアンプで動作するコンパレータを多ビット化することで，高い SN 比を有するデルタシグマ ADC を設計し，試作・評価している．

第 5 章では，本研究のまとめおよび今後の課題について記述している．

本論文の成果の中でとりわけ以下の２点で評価できる．

第 1 に，デルタシグマ ADC を構成するブロックの１つである，ラッチ型コンパレータにおいて，コンパレータのトランジスタから出る雑音を，差動構成にしたキャパシタ対により相殺し，キックバックノイズの削減を行った．設計したラッチ型コンパレータは TSMC 社(Taiwan Semiconductor Manufacturing Company Limited)の 0.18 μm CMOS(Complimentary Metal-Oxide Semiconductor)プロセスにより試作し，実験結果より周波数 10MHz，バイアス電圧 1.2V において世界最高クラスの低消費電力 246μW を

実現した.

第 2 に, WCDMA 用 ADC において 1 次と 2 次の積分器のオペアンプを共通化し, 1 つのコンパレータを用いることで周波数 2MHz において SQNR(Signal to Quantization Noise Ratio)値 50dB の低雑音特性を達成し, 合わせて回路面積を削減することにより世界最高の FoM(Figure of Merit)を達成した.

以上要するに, 本研究は, ソフトウェア無線などのマルチバンド移動体通信システム実現に不可欠な低消費電力デルタシグマ・アナログディジタルコンバータの開発に成功したものであり, 電子工学上価値ある業績である. よって本論文は博士（学術）の学位に値するものと認める.

氏　　名　Prapto Nugroho
学位記番号　シ情　博甲第 476 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　DEVELOPMENT OF RADIO FREQUENCY RING OSCILLATORS IN STANDARD CMOS TECHNOLOGY
（CMOS 技術を用いた RF リング発振器の開発）

論文調査委員
（主　査）　九州大学　教　授　吉　田　啓　二
（副　査）　〃　〃　浅　野　種　正
〃　〃　准教授　金　谷　晴　一

論 文 内 容 の 要 旨

As the wireless communication market booming, Phase Locked Loops (PLLs) has found their importance role for frequency synthesis in high frequency communication systems as well as in high speed clock generators in microprocessor applications. A typical PLL consists of a phase/frequency detector (PFD), a charge pump, a low-pass loop filter, a voltage controlled oscillator (VCO) and a frequency divider. Among those components, VCO or oscillator is the most importance component since it is the biggest phase noise source outside the PLL Loop bandwidth.

There are two promising candidate for CMOS based oscillator design in current technology. They are LC oscillator and ring oscillator. LC oscillators have a better phase noise performance, but the tuning range is smaller compared with Ring oscillator. LC oscillators also need larger chip area because of the inductor they used. As CMOS technology getting advanced, digital blocks are becoming miniaturized with every generation of the CMOS technology whereas the size of analog blocks remains unchanged due to the lack of scalability of RF blocks. One of the major reasons of this is the existence of passive components like spiral inductors which are indispensable to design the RF components like oscillators, amplifiers, matching circuits and so on. Therefore, designing inductorless RF blocks like ring oscillator is very attractive.

Other advantages of a ring oscillator are its wide tuning range, compact size and scalability to integrate with back-end devices to realize a true system-on chip (SoC) in CMOS compared its Inductor-Capacitor (LC-) counterparts. However, because ring oscillators suffer from high phase noise, a relatively small number of research result has been reported for the wireless communications. Therefore, phase-noise reduction is the biggest challenge for the CMOS ring oscillator`s research Beside the phase noise, power consumption and quadrature output are becoming next important issue in ring oscillator research, especially for data transfer, image rejection receivers, half-rate clock recoveries and multiphase processor clock.

The first objective of this research is to design, fabricate and test a low power and wide tuning range Voltage Controlled Oscillator using for 5.9 GHz output frequency. The proposed designs employed a three stage ring oscillator whose output controlled using current or we can call it current controlled oscillator (CCO).

The second objective is to design, fabricate and test a low-noise Quadrature output ring oscillator for 4 GHz output frequency. The design use sub-feedback loop technique to increase the frequency output. It is tune using analog method.

The third objective is to design some Digitally Controlled Oscillators (DCOs). First DCO modify the previous analog quadrature VCO for 1 GHz and 2.4 GHz. All are employs 14 bit digital control. Second DCO use the same 14 bit digital control circuits but has a new delay cell circuits. It resulted in wide tuning DCO. The third DCO controlled by 8 bit digital control word. It has low power characteristics.

Chapter 1 and 2, of this thesis describes the background for the use of digitally control oscillator for radio frequency communication applications and different type oscillator topology and their characteristics with applications, respectively. The next chapters explore possibilities of the ring type DCO for next generation wireless systems. Current Controlled Ring Oscillator which have capabilities of low power, wide tuning range, and low chip size area, but due to poor phase noise limited its application, It has also non quadrature output. To overcome the problem of limited maximum frequency and power dissipation we designed a quadrature output ring oscillator that employs sub-feedback topology or coupled oscillator. This design has a low phase

noise and wide tuning range.

Due to scaling technology, there will be difficulty on tuning the frequency, so finally, in chapter 5, we come up with the designs of ring type DCO for next generation wireless standards in 0.18 um CMOS technology. Firstly, 14 bit digitally controlled oscillators were designed. First 14 bit DCO design explore the best phase noise performance that resulting a lowest phase noise in ring oscillator design. But it has to consumes high power and has a low frequency about 1 GHz. The Second DCO is designed to have best Figure of Merit that resulting in 2.4 GHz DCO with low phase noise and lower power. To reduce the power, we change the topology from coupled inverter to interpolating inverter and proposed new delay circuits. There are two designs with interpolating topology. They use 8 and 14 bit digital control. The prototypes consume lower power than the previous design.

論 文 調 査 の 要 旨

無線通信の急速な需要拡大に伴い，一つの無線端末で複数の通信規格を満たし，さらに低消費電力なマルチバンド携帯無線機器の開発が必要となっている．また，小型化・低コスト化のため，ディジタル回路と整合性の高い CMOS(Complimentary Metal-Oxide Semiconductor)プロセスにより高周波集積回路(Radio Frequency Integrated Circuit: RFIC)を実現し，ディジタル回路と高周波アナログ回路をワンチップ化する研究が盛んに行われている．

複数の通信規格で動作するためには，広帯域で動作する電圧制御発振器(Voltage Controlled Oscillator: VCO)または，電流制御発振器(Current Controlled Oscillator: CCO)が必要不可欠である．CMOS プロセスにより実現される発振器には，LC 発振器と，リング発振器がある．LC 発振器は，優れた位相雑音特性を持っているが，インダクタの占有する面積が極めて大きいことや，単一の LC 発振のため広帯域化が難しい点があげられる．また，インダクタのサイズはプロセスの微細化によらず使用周波数により決まるため，微細な CMOS プロセスを用いても小型化が困難である．一方，リング発振器は，遅延によるポジティブフィードバックにより発振するため，インダクタが不要であり小型化が可能である．さらに，遅延素子を容易に導入できるので周波数可変範囲が極めて広くできるという特徴があり，無線機器のマルチバンド化というトレンドを考えた場合，極めて魅力的である．しかしながら，これまでリング発振器には電力消費及び位相雑音が大きいという問題が知られており，これらの問題を解決することが喫緊の課題であった．

著者は，本論文において，低消費電力かつ，広い周波数範囲をカバーする新しい高性能リング発振器の開発に成功した．即ち，PSK(Phase Shift Keying)に適した 4 位相出力高性能リング発振器，及び発振周波数のディジタル制御が可能な新しいリング発振器の開発に成功した．

本論文では，まず第 1 章で，無線通信用発振器の現状について，第 2 章では発振器の原理およびリング発振器の研究課題について述べている．

第 3 章では，インバータ回路を奇数個接続した従来型リング発振器において，各位相に対応する出力端子を設けることで 4 位相出力が可能な，新しい電流制御リング発振器を開発した．第 4 章では，偶数個のインバータをプッシュプル型に接続した広帯域 4 位相リング発振器,第 5 章では，周波数同調回路にディジタル制御回路を導入することにより，新しい広帯域 4 位相ディジタル制御リング発振器を開発した．

第 6 章では，本研究のまとめおよび今後の課題について記述している．

本論文の成果の中でとりわけ以下の２点で評価できる．

第 1 に，4 位相リング発振器において MOS トランジスタの 3 次のトランスコンダクタンスを制御することで，素子のばらつきを抑え，低位相雑音特性を実現した．設計したリング発振器は TSMC 社(Taiwan Semiconductor Manufacturing Company Limited)の 0.18μm CMOS プロセスにより試作し，実験結果との比較により設計理論の妥当性を示している．本発振器の周波数可変範囲は，1.23～4.17GHz，発振器の性能を示す FoM (Figure of Merit)は，-163.8(dBc/Hz)の世界最高値を達成した．

第 2 に，リング発振器の同調周波数のディジタル制御回路において，周波数分解能を高めるため，同調方法として粗同調から微同調へ 3 段階とし，各段階にビット列を分離配置する新しい同調方式を提案した．その結果 0.6～4GHz という極めて広い周波数帯域での周波数制御を実現することに成功した．

以上要するに，本研究は，移動体通信システム実現に不可欠な低消費電力かつ，広い周波数範囲をカバーする高性能リング発振器の開発に成功したものであり，電子工学上価値ある業績である．よって本論文は博士（工学）の学位に値するものと認める．

氏　　名	西　　竜　三
学位記番号	シ情　博甲第 477 号（工学）
学位授与の日付	平成 24 年 9 月 24 日
学位論文題名	A Study of Key Distribution Schemes using Matched Filters for Wireless Communications （整合フィルタを用いた無線通信に適した鍵配送方式に関する研究）

論文調査委員

（主　査）　九州大学　教　授　櫻　井　幸　一
（副　査）　〃　〃　竹　内　純　一
〃　〃　准教授　堀　良　彰

論 文 内 容 の 要 旨

無線通信は，新たな配線工事を必要とせず，利便性の高い通信インフラである．これには２つの本質的な課題がある．一つ目は伝送路が不安定であることである．これは，伝送路上で暗号鍵更新メッセージが失われる可能性が高いことを意味する．二つ目は信号の届く範囲内で伝送路が第三者と共有されていることである．これは通信が物理層(MAC 層含む）に対するサービス停止攻撃（DoS 攻撃）に脆弱であることを意味し，これらが大きな課題である．

無線通信路上の情報の守秘性を確保する為に，無線 LAN 標準 IEEE802.11 で最初に採用した暗号においては多くの脆弱性が発見されて，今では数分程度で暗号鍵が推定される．そこで，IEEE は，無線 LAN セキュリティの改善版を新たに採用した．しかしこれについても既に脆弱性が指摘されている．このように，特に，計算量の多さを安全性の根拠とした計算量的安全性を持つ暗号については，計算機の進歩も考慮すれば，どのような暗号方式でも限界があり，これも大きな課題である．

本研究では，このような背景のもと，伝送路の不安定性，DoS 攻撃への脆弱性および計算量的安全性を持つ暗号の限界を課題として，特に暗号鍵の配送における対策について取組んでいる．対策案としては整合フィルタを用いる．整合フィルタは従来，主に無線 LAN 等において周波数拡散通信に用いられていた．従来の使用例との大きな違いは，今回は周波数帯域幅を変えていない点である．これによりノイズへの耐性および通信容量を高めると共にシステム全体に大きな影響を与えることがなく，実装が容易という効果がある．

本論文は，以下の６章からなっている．

第１章では，本研究の背景と目的，および，得られた研究成果について述べる．

第２章では，無線通信を使った場合のホームネットワークのセキュリティ上の課題について分析する．具体的には，様々な種類の機器が混在するホームネットワークにおいては，統一的な対応をとることが困難であるという課題がある．そこで，機器の種類毎，具体的には，制御系，AV 情報機器系，コミュニティ通信に分けて，課題やリスク，求められる対策を検討して体系的に整理すると共に，無線通信と有線 LAN や電力線通信等とのセキュリティ上の差異についても整理する．

第３章では，不安定な伝送路でも高い伝送信頼性を有する鍵配送方式を提案する．無線通信路の伝送路の不安定性に起因して，暗号鍵更新メッセージが失われた場合には，その後の通信は不可能になるという課題があった．対策として整合フィルタの送受既知情報として直交シフト M 系列を使う．従来研究として誤り訂正符号を用いる場合に，信号伝送速度が雑音帯域幅よりも大きい通常の場合では，冗長度の長さや方式に関らず伝送信頼性は最大でも BER $\fallingdotseq 10^{-6}$ 程度であることを示し，提案方式はこれを BER$=10^{-15}$まで改善することを示した．

第４章では，物理層に対する DoS 攻撃に対して高い伝送信頼性を有する鍵配送方式を提案する．伝送路が第三者と共有されていることに起因して，物理層への DoS 攻撃に対して脆弱性であるという課題があった．物理層に対する DoS 攻撃は悪意のあるものだけでなく，可用性という観点から見れば他の無線通信等による干渉等も同様の影響を有する．対策として送受既知情報として乱数を使うが，受信信号判定の閾値を最適化することで，DoS 攻撃下で BER $=10^{-9}$まで改善することを示した．

第５章では，計算量的安全性を持つ暗号の限界に関する対策として，暗号鍵の推測を理論的に不可能にする情報理論的に安全な手法を検討する．しかし情報理論的な手法には制約が課されることが多い．今回は情報理論的に安全な手法としてセキュリティ通信路容量の概念（正規受信機の通信容量と盗聴受信機通信容量との差）を用いる．この手法では，盗聴可能範囲が正規の通信範囲より広いという大きな課題がある．従来の研究例の一つとして，誤り訂正符号を用いた手法により，盗聴範囲を狭くするという改善例があった．この手法では，正規の通信は屋内であることを前提にしつつ，狭くなった盗聴可能範囲でも 58m に達し，この課題を解決していない．そこで提案方式では，盗聴可能範囲を狭くすべく，整合フィルタの送受既知情報として乱数を用いると共に送信電力を小さくする．これにより正規受信機の受信信号品質は変らないまま盗聴受信機の受信信号品質は受信不可能なレベルまで低下する，このような非常に実装が容易な手法により，盗聴可能範囲が正規の通信範囲より狭くなるだけでなく，ある条件のもとでは，正規の通信範囲を変えることなく，従来の盗聴可能範囲が半径１４ｍ時のケースを，提案方式により４ｍまで大幅に狭くできることを示した．この手法は屋内で用いるコードレス電話のような用途に非常に有効である．

第６章では，これまでの研究をまとめ，今後の課題と将来の展望について述べる．

論 文 調 査 の 要 旨

無線通信機器は近年の普及と共に，電子商取引等の個人情報を扱う応用も広がり，セキュリティ上の脅威が高まっている．無線通信では，物理層とリンク層の構造が有線通信と異なる為，無線通信特有の脅威が存在する．有線伝送路では伝送媒体や伝送装置に対する物理的なアクセス制御が可能であるが，無線伝送路ではこの様な制御が困難で

ある為,妨害電波などによるDoS攻撃(Denial-of-Service, サービス停止攻撃）に脆弱であり，その対策は技術的な課題である.

本研究は，無線伝送路上の雑音，DoS 攻撃への脆弱性および計算量的安全性を持つ暗号の限界という３つの課題に取組んだ．無線伝送路上の雑音によるビット誤り率の改善には，従来誤り訂正符号が用いられるが，復調後のビット列に対する適用であるためビット誤り率の改善は不十分である.また,物理層に対するDoS攻撃への対策として，スペクトラム拡散通信があるが，拡散符号の安全な共有は課題である．計算量的安全性を持つ暗号の限界への従来の対策としては，送信情報と同じ長さの鍵を用いる情報論的安全性を備えた手法があるが，その鍵は使い捨てでなければならない問題がある．著者は，これら３つの課題解決の為に，秘密情報を予め共有している送信者からの信号のみを 選択的に受信できる整合フィルタを導入した．この整合フィルタを用いた通信方式は通信の冗長度が高くなる．しかし，著者は暗号鍵のような伝送量をあまり必要としない通信では，この問題が現実的には障害とならないことに着目し，暗号鍵配送方式を提案した．本研究は以下の３つの点で評価できる.

第一に，雑音の多い伝送路でも高い伝送信頼性を有する鍵配送方式を提案した．無線通信路の雑音に起因して，暗号鍵更新情報が失われた場合には，その後の通信が不可能になるという課題がある．従来用いられている復号されたビット情報に誤り訂正符号を適用する方式では，ビット列復調時の非線形処理によりアナログ信号が有する情報の一部は失われる．著者は，受信機における出力ビット列復号以前に整合フィルタを用いる方式を提案し，無線伝送路の悪条件下でも通信を可能にした．提案手法は，アナログ信号の処理段階では非線形処理を含まず，ビット誤り率は送受既知情報長に対して線形に改善される．提案方式では,整合フィルタの送受既知情報として擬似乱数M系列を用いた．128 ビット長の M 系列を使えば，受信信号誤り率 1%のガウス雑音下の無線伝送路で，復号後の信号誤り率を 10^{-15} 以下まで改善できることを理論解析により明らかにした.

第二に，物理層への攻撃を含むDoS攻撃に対して高い伝送信頼性を有する鍵配送方式を提案した．無線通信では,伝送路が第三者と共有されていることに起因して，物理層へのDoS攻撃に対して脆弱であるという課題がある．従来研究としては，物理層に実装されたスペクトラム拡散通信を用い妨害電波を遮断することで，DoS 攻撃対策をおこなう手法がある．これに対して，著者は，乱数列をなす秘密情報を予め共有した送信者からの信号のみを選択的に受信できるフィルタを提案した．受信信号判定の閾値を最適化することで，同時攻撃の攻撃者の全信号電力が正規の信号電力以下の DoS 攻撃下で，正規化閾値 0.8，秘密情報長 64 ビットの場合に，正規の信号を見逃す確率および非正規信号の誤検出確率が共に 10^{-9} 以下まで改善することを理論解析により明らかにした.

第三に，Wyner が提案したセキュリティ通信路容量を用いて，実用性を確保しつつ情報理論的安全性を確保可能な鍵配送方式を提案した．情報理論的安全性の確保には，正規の受信機における受信信号の SN 比が盗聴者の受信機における受信信号の SN 比を上回る状況が必要である．しかし，実用的な場面でこのような状況を作り出すことが課題である．従来研究には，符号化を用いたノイズ付加により，SN 比が小さい場合のビット誤りを増加させる手法があるが，情報理論的盗聴可能な領域の縮小範囲は十分ではない.これに対し，著者は情報理論的盗聴可能範囲を数ｍ以内とし,無線 LAN やコードレス電話に適用可能な守秘性を実現する方式を提案した．整合フィルタの送受信機共有情報として乱数列を用いる通信方式に，正規受信機の受信信号品質を制御しつつ送信電力を小さくする手法を導入した．これにより正規受信機の受信信号品質を変えないまま，盗聴受信機の受信信号品質を受信不可能なレベルまで低下させることが可能になった．提案方式により，無線 LAN における高速伝送時の変調方式 64QAM を用いる場合，送受既知情報長 128 ビットの場合に,盗聴可能範囲を送信者より 14ｍの範囲から 4ｍの範囲へ改善できることを明らかにし，提案方式の実用性を示した.

以上要するに，本研究は，無線通信の有する課題すなわち伝送路上の雑音，DoS 攻撃への脆弱性，伝送路上の情報の守秘性についての課題の解決の為に，整合フィルタを用いた方式を提案すると共にその有効性を論じたものであり，情報工学上寄与するところが大きい．よって本論文は，博士（工学）の学位論文に値すると認める.

氏　　名	Mohamed Saber Saber Elsayes
学位記番号	シ情　博甲第 478 号（工学）
学位授与の日付	平成 24 年 9 月 24 日
学位論文題名	CIRCUIT DESIGN AND IMPLEMENTATION FOR CARRIER SYNCHRONIZATION IN DIGITAL RECEIVERS （搬送波同期のためのディジタル受信回路設計と実装）

論文調査委員

（主　査）　九州大学　准教授　實　松　　豊
（副　査）　〃　教　授　吉　田　啓　二
〃　〃　〃　竹　内　純　一

論 文 内 容 の 要 旨

ディジタル無線通信では情報信号の伝送に先立ち，送信器と受信器の周波数及び位相を同期させる必要がある．同期の確立と保持に幅広く用いられるのが位相同期回路（Phase Locked Loop; PLL）である．従来の PLL は，対応できる周波数の誤差が中心周波数の 10%程度以内に限られ，通信端末が高速で移動し大幅なドップラー周波数推移が発生する環境に対応できない．したがって，10%を超えるドップラー周波数に対応できる周波数推定器が必要であり，近年の移動体無線通信における解決すべき課題の一つとなっている．既存の周波数推定法として，最尤推定に基づく方法がよく知られているが計算量が膨大なので低消費電力が要求される移動端末へ実装するのは困難である．本研究の目標は，周波数と位相を高速かつ高精度で推定するディジタル回路を，移動端末に搭載可能な面積と消費電力で実現することである．

一般に PLL は可変周波数発振器，位相比較器，ループフィルタの 3 つの要素からなる．位相比較器は，入力信号と発振器の位相差を出力する．その出力に含まれる高周波成分をループフィルタで遮断し，得られた位相差信号を用いて発振器の周波数を制御することにより同期を保持する．PLL は現在ディジタル回路により実装されるのが一般的であるが，ディジタル可変周波数発振器が使用する三角関数のルックアップテーブルが大きな回路面積を占める問題と，ループフィルタの高周波除去能力を向上させるためフィルタの次数を上げると PLL システムが不安定化する問題があった．

まず著者は，従来の PLL の性能を改善するため，位相比較器で発生する第 2 次高調波成分を直接減算する回路を位相比較器の前に設置する手法を提案した．また，提案法の性能評価のため FPGA (field programmable gate array) 回路への実装を行った．提案法を実装した回路は，ループフィルタへ入力される第 2 次高調波成分を約 10 分の 1 に削減し，PLL の周波数推定能力を向上させた．次に，回路規模と消費電力を抑えるため，三角関数のルックアップテーブルを区分線形関数で近似する回路に置き換えた．この手法により提案回路の消費電力は，従来法に比べ約 25 パーセント削減された．PLL 出力に含まれる所望の周波数成分と，近似により発生する偽周波数成分の比である Spurious-Free Dynamic Range (SFDR)は 59.8dB であり十分な精度を実現した．

さらに著者は，大幅なドップラー周波数に対応するため，入力信号を未知の振幅，周波数，位相をもつ正弦波であると仮定した場合に入力信号とその時間微分との間に成立する関係式を用いる新しい周波数推定回路を提案した．提案法はまず入力信号の振幅を推定し，次いで入力信号の同相成分と直交成分それぞれの標本値と単位時刻前の標本値との差分を計算する．得られた同相成分と直交成分の差分同士の差を電力の推定値で除することにより，周波数を推定する．著者は提案法を実装した FPGA 回路の使用面積と消費電力は上述の PLL 回路と同程度であるので十分省電力と考えられる．従来の PLL は発振器の中心周波数の 10%を超えるドップラー周波数に対応できなかったが，提案法は中心周波数と関係なく，アナログ・ディジタル(A/D)変換器のサンプリング周波数の半分の周波数まで対応できる．提案法は送信信号の振幅が途中で変化しても位相の追尾が可能であり，白色ガウス雑音を付加した状況でも高い精度での周波数の推定が可能であった．

最後に著者は，周波数推定器と PLL の 2 つの提案法を複合した回路を FPGA に実装し，符号分割多元接続(CDMA)通信の受信器に応用した．他ユーザの信号との間の干渉が発生する環境下でも周波数の推定ができることを示した．

論 文 調 査 の 要 旨

ディジタル無線通信では，情報信号の伝送に先立ち送信器と受信器の周波数及び位相を同期させる必要がある．同期の確立と保持に幅広く用いられるのが位相同期回路(Phase Locked Loop: PLL)である．PLL は，位相の同期を保持するのが本来の役割であるが，中心周波数の 10%程度以内であれば周波数の推移にも対応できる．しかしながら周波数推移がそれを超える場合には PLL では対応できず，周波数を推定する回路が別途必要となる．通信端末の高速移動に伴うドップラー効果により発生する周波数推移(ドップラー周波数)への対応は，近年の移動体無線通信における解決すべき課題の一つとなっている．既存の周波数推定法として最尤推定に基づく方法がよく知られているが，計算量が膨大であるため低消費電力が要求される移動端末へ実装するのは困難である．本研究の目標は，周波数と位相を高速かつ高精度で推定するディジタル回路を，移動端末に搭載可能な面積と消費電力で実現することである．

一般に PLL は可変周波数発振器，位相比較器，ループフィルタの 3 つの要素からなる．位相比較器は入力信号と発振器の位相差を出力する．その出力に含まれる高周波成分をループフィルタで遮断し，得られた位相差信号を用いて発振器の周波数を制御することにより同期を保持する．PLL は現在ディジタル回路により実装されるのが一般的であるが，ディジタル可変周波数発振器が使用する三角関数のルックアップテーブルが大きな回路面積を占める問題と，ループフィルタの高周波除去能力を向上させるためにフィルタの次数を上げると PLL システムが不安定化する問題があった．

まず著者は，従来の PLL の性能を改善するため，位相比較器の出力に含まれる第 2 次高調波成分を直接除去するための回路を位相比較器の前に設置する手法を提案した．また，提案法の性能評価のため FPGA (field programmable gate array)回路への実装を行った．提案法を実装した回路は，ループフィルタへ入力される第 2 次高調波成分を約

10 分の 1 に削減し，PLL の位相追尾能力を向上させた．次に，回路規模と消費電力を抑えるため，三角関数のルックアップテーブルを区分線形関数で近似する回路に置き換えた．提案法は従来法に比べ，論理回路の規模(スライス数)を約 40 パーセント，消費電力を約 25 パーセント削減した．実装回路から出力される正弦波は，想定するディジタル受信器として十分な精度であることを確認した．

さらに著者は，大幅なドップラー周波数に対応可能な新しい周波数推定回路を提案した．著者は，入力信号は時間変化する未知の振幅および時間変化しない未知の周波数と位相をもつ正弦波であるというモデルを立て，このとき入力信号とその時間微分との間に成立する関係式を用いた．提案法は，まず入力信号の振幅を推定し，次いで入力信号の同相成分と直交成分それぞれについて，最新の標本値と一つ前の標本値との差分を計算する．得られた同相成分と直交成分の差分同士の差を振幅の推定値の二乗で除したものが周波数の推定値となる．著者は提案法を FPGA 回路に実装し，その使用面積と消費電力が想定する受信器に搭載可能であることを示した．従来の PLL は発振器の中心周波数の 10%を超えるドップラー周波数に対応できなかったが，提案法は中心周波数と関係なく，推移後の周波数がアナログ・ディジタル(A/D)変換器のサンプリング周波数の二分の一以上であれば対応できることを示した．提案法は，入力信号の周波数は固定であるとの仮定に基づくが，実験では，周波数が変化してもこれを追尾できることを示した．また，モデルは雑音の存在を仮定していないが，提案法は白色ガウス雑音を付加した状況でも高い精度での周波数の推定が可能であることを確認した．

最後に著者は，周波数推定器と PLL の 2 つの提案法を複合した回路を FPGA に実装し，符号分割多元接続(CDMA)通信の受信器に応用した．他ユーザの信号からの干渉が存在する環境下でも，提案法は周波数と位相を推定することが可能である事をシミュレーションにより明らかにした．

以上，要するに，本論文は，大幅なドップラー周波数推移に対応可能なディジタル受信器の設計問題に取り組み，まず第 2 次高調波減算回路を提案して位相同期回路の性能を向上させ，次にルックアップテーブルを用いずにディジタル可変周波数発振器を実現して消費電力と回路面積を大幅に削減し，最後に入力信号の振幅推定器と入力信号の同相成分と直交成分に対する 2 つの微分回路を用いた新しい周波数推定回路を提案し，その有効性を示したものである．本研究成果は，情報通信のための回路設計の発展に寄与するものである．よって本論文は博士(工学)の学位論文に値するものと認める．

氏　　名　趙　　来 平
学 位 記 番 号　シ情　博甲第 479 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学 位 論 文 題 名　Algorithmic Aspects in Cloud Computing
（クラウドコンピューティングのアルゴリズム的研究）
論文調査委員
（主　査）　九州大学　教　授　櫻 井 幸 一
（副　査）　〃　〃　山 下 雅 史
〃　〃　准教授　日下部　茂

論 文 内 容 の 要 旨

Cloud computing changes the traditional computation pattern into an Internet based service providing mode. Users submit job requests to the cloud providers through accessing the Internet interface, whereas cloud providers fulfill user requests with respecting specific Quality-of-Service (QoS) goals using a local resource scheduling policy. Because of the new characteristics of cloud computing, like Internet based service providing, pay-as-you-go, on-demand resource provision and service level agreement, traditional algorithms for distributed systems cannot be applied into cloud directly. To this end, we focus on the algorithmic aspects in cloud, and promote the algorithm design in cloud environment with considering these characteristics.

We specifically address two problems: resource scheduling and service selection. Considering resource scheduling as an optimization process, there have been many algorithms proposed for optimizing performance of traditional distributed systems. However, we show that there emerge new problems in terms of cloud environment. In particular, scheduling algorithms for improving the reliability with less resource usage is able to increase the system resource utilization and helps to save energy; scheduling algorithms for increasing the cloud provider's revenue could benefit the provider, and possibly reduce the price of services, hence further promote the development of cloud. Considering the service selection in cloud, learning algorithms for recommending services could ease user from complex service selection work, and facilitate the interactions between user and broker.

Our main contributions are summarized as follows.

Chapter 1 presents the background of our proposals. We introduce the concept of cloud computing, and describe the features which distinguish cloud computing from traditional distributed systems.

Chapter 2 states the two major problems discussed this thesis, i.e., resource scheduling, which is discussed in terms

of a centralized scheduler model, and service selection, which is discussed based on a user-broker-provider model. We also present a brief introduction on three practical distributed systems that are commonly employed in cloud.

Chapter 3 presents our study on reducing the resource usage for reliable workflow scheduling. As scheduling workflow applications in heterogeneous systems, either for optimizing the reliability or for minimizing the makespan, is NP-complete, we alternatively consider the specific reliability and deadline requirements in the scheduling. In particular, we analyze the reliability of a given schedule using two important definitions on reliability: Accumulated Processor Reliability (APR) and Accumulated Communication Reliability (ACR). Given a schedule, we can compute the upper bound and lower bound of a range that the reliability of the schedule is within. Inspired by the reliability analysis, we propose two algorithms on reliable workflow scheduling with replicas: RR algorithm (Two ”R”s are for ”Reliability” and ”Resource” respectively) is a greedy algorithm that assigns tasks to machines according to the computation on APR and ACR. DRR algorithm extends RR algorithm by further respecting the deadline requirement. The experimental results show that RR and DRR algorithm are able to satisfy user's requirements on reliability and deadline with less resource usage.

Chapter 4 presents our study on the problem of increasing provider's revenue in cloud. Cloud providers usually sign a contract, named as Service Level Agreement (SLA), to state the service quality. SLA violation frequently occurs in a cloud system due to the frequent failures, thereby affecting the normal operation of job requests and incurring high penalty cost. We formally define the problem of maximizing expected revenue with respecting capacity requirements, and then propose First-Fit and Harmonic algorithms to the problem. Our analysis shows that both algorithms are not performing well in their worst cases, but approach to the optimal under some specific situations.

Chapter 5 discusses our second problem: service selection. As a large number of service providers have created an intense competitive world of business, selecting the appropriate services for a job becomes a big challenge for user. To this end, we consider the broker model which is independent from user and provider, but works for user to find the best services for his jobs. Different with existing algorithms that requires users to have an explicit approximation on their preferences, we recommend a list of services to user, and facilitate the service selection process using learning algorithms. We show the feasibility of preference learning in service selection using experiments.

Chapter 6 concludes the results of this thesis, and discusses our future works.

論 文 調 査 の 要 旨

クラウドコンピューティングにより，ネットワークに接続された計算資源を使って，プロバイダがユーザに計算サービス，情報やアプリケーションなどを提供するサービスが普及してきている．ユーザはプロバイダへのジョブ要求を提出し，プロバイダはユーザが指定したジョブをサービス品質を考慮しながら実行する．これによって，ユーザはハードウェアやソフトウェアといった計算資源を所有せずとも計算ジョブの実行が可能となるなど，新たな社会的計算サービス基盤として注目されている．

クラウドコンピューティングは，いくつかの特徴を持つ．たとえばインターネットベースのサービスの提供，pay-as-you-go，オンデマンドの資源提供，サービス品質保証契約などが挙げられる．本研究は，これらの特徴を考慮してクラウド環境における計算，通信，そしてサービスに焦点を当てアルゴリズム設計と解析を行った．特に，ジョブ実行のプロセスに関して，資源スケジューリングとサービス選択という二つの問題を取り上げ，これらを解決する効率よいアルゴリズムを提案したもので，以下の３つの点で評価できる．

第一に，低い資源使用率で信頼性を向上させるためのワークフローに対するスケジューリングアルゴリズムを設計した．従来の方法では，信頼性を向上させるために，動的レプリケーションスキームを直接適用し，結果として多くの資源を必要とする．著者は，スケジューリングに対する評価基準として，蓄積処理信頼性と累積通信信頼性の２つに注目し，これらの指標に基づく貪欲アルゴリズムを提案した．従来の動的レプリケーションを直接適用するアルゴリズムと同等の計算時間で，より高い信頼度を達成することを，理論解析により明らかにした．さらに提案アルゴリズムは，資源使用量を 40%減らすことを実験的に確認した．

第二に，プロバイダの収益を増加させるアルゴリズムを設計した．プロバイダとユーザは通常，サービス品質を保証するために保証契約を結ぶ．この時，スケジューリングの失敗が，ジョブリクエストの通常処理に悪影響を及ぼし，プロバイダが高い契約違反コストを負う場合がある．著者は，期待される収益を最大化する問題を定式化し，よく知られる組み合わせ最適化問題との関連に着目し，First-Fit と調和分割という２つのアルゴリズムを，著者の定式化問題に適用した．設計した２つのアルゴリズムそれぞれの競合比に対して厳密な下界を与え，最悪の場合には一致することを，理論解析によって明らかにした．さらに平均的にジョブの到着率が 0.2 より高い場合には，調和

分割法が 2%程度の高収益を獲得することも実験的に確認した．

第三に，サービス選択のための学習アルゴリズムを設計した．プロバイダの大規模化は企業間の激しい競争を作り出し，同時に希望するジョブに対して適切なサービスをユーザが選択することは，大きな課題となっている．著者は，ユーザとプロバイダの間に独立したブローカが介在するモデルを取り上げ，ユーザがジョブを実行する際に，最適なサービスをブローカが勧めるシステムを取り上げた．ここではユーザへサービスのリストを推薦するために，ブローカがユーザの好みを効率よく学習するアルゴリズムが必要となる．著者は，既存の最急降下法と Hedge という二つのアルゴリズムをベースにし，さらにサービスの属性値を配慮した独自の学習アルゴリズムも提案した．実験解析により，これら 3 つの学習アルゴリズムの比較特徴付けを行い，サービス選択における学習アルゴリズムの効果を明らかにした．

以上要するに，本論文は，クラウドコンピューティングにおける資源スケジューリングとサービス選択に対するアルゴリズムの設計と評価を行ったものであり，情報工学上寄与するところが大きい．よって本論文は，博士（工学）の学位論文に値すると認める．

氏　　名　蔡　　文　杰

学位記番号　シ情　博甲第 480 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　Studies on Online Multi-Stroke Character Recognition
（オンラインマルチストローク文字の認識に関する研究）
論文調査委員
（主　査）　九州大学　教　授　内　田　誠　一
（副　査）　〃　〃　谷　口　倫一郎
〃　〃　准教授　諸　岡　健　一

論 文 内 容 の 要 旨

本論文は，漢字のような多画文字を対象としたオンライン文字認識に関する．オンライン文字認識とは，タブレット上のペン先位置の時系列として入力された文字データを対象とした認識手法である． 1960 年代から現在に渡って 50 年の歴史を持つが，昨今の Tablet PC を代表とする電子機器の普及によって応用は急激に広がっている．例えば，Tablet PC や PDA(電子手帳の類)では，キーボードに変わる文字入力手段としてオンライン文字認識が利用されている．また，そこで培われた技術は，タブレットやタッチパネルを具備したゲーム機器類や携帯端末のためのマンマシンインタフェースの基盤技術として活用されている．

オンライン文字認識に関する様々な技術課題のうち，本論文では筆順変動問題に取り組む．同問題は，時系列データを扱うオンライン文字認識に独特な問題である．すなわち，筆順が変わると，見かけ上同じような文字形状であっても，時系列的には一部のデータが通常とは異なる部位に移動してしまう．その結果，例えば時系列順に沿ったマッチングを行うと，その字形の標準的な時系列データと大きく異なってしまい，誤認識を生ずる．例えば「女」の標準データは「く」「ノ」「一」の順であるが，もし入力が「一」「く」「ノ」の順に筆記されたとすれば，両者を単純に照合しても，全く異なる文字と判断されてしまう．

本論文の主たる貢献は，(1)この筆順変動問題への対処法の調査・分類および実験的比較検討，ならびに(2)部首レベル処理の導入による計算量低減法の提案，の 2 点に集約される．

第一の貢献に関する具体的検討内容は以下の通りである．まず従来の筆順変動対処法を網羅的に調査，分類した．そしてそれら分類の上で最も精度的に期待できるものとして，画対応探索法の重要性を強調した．ここで画対応探索法とは，例えば 2 つの画系列「く」「ノ」「一」と「一」「く」「ノ」の間に適切な対応関係を定める方法を指す．基盤となる数学的定式化並びに解探索原理が全く異なる 5 種類の画対応探索法 — cube search (CS), bipartite weighted matching (BWM), individual correspondence decision (ICD), stable marriage (SM), deviation-expansion model (DE) — を特に採り上げ，それらの原理を比較，吟味した．その上で，それらの詳細な計算量および精度の比較を，教育漢字を対象とした認識実験を通して行った．その結果，原理的に大局的最適化能力を持つ CS と BWM が最も高い画対応精度を示し，相対的な優位性を確認した．また，計算量の側面においては，BWM，ICD，SM に優位性があることを実証した．加えて，高速化のために枝刈りを組み込んだ CS は，原理的には近似解しか得られないものの，現実的には精度と速度を両立可能なことを実験により示した．

第二の貢献に関する具体的検討内容は以下の通りである．この部首レベル処理の着想は，ほとんどすべての筆順変動が，部首内，もしくは部首単位で起こりうることに基づく．すなわち例えば「桜」に起こる筆順変動は，「木」内部や「女」内部で起こるもの，および「木」全体が「ツ」「女」の後に書かれるといった部首単位のものが主要であり，「木」と「ツ」にまたがったような筆順変化は少ない．このような制約を上記の画対応探索法に組み込むことで，解探索空間を圧縮でき，結果的に計算量を低減できる．具体的には，こうした制約との相性が良い CS に基づいた手法を提案し，実際の認識結果を通して，速度面での改善が

得られたことを実証している．さらに，副次的に精度の向上も図れていることを示している．

論 文 調 査 の 要 旨

本論文で扱うオンライン文字認識とは，一般に，タブレット等のタッチパネルを介してペン入力された文字データの認識手法である．この文字データは，ペン先の運動軌跡すなわちペン先座標の時系列として表現される．従って，その認識のために，画像データを対象とする文字認識すなわち光学的文字認識(OCR)とは異なった要素技術が開発されてきた．

オンライン文字認識においては，次の三つの問題に対処する必要がある．すなわち，非線形時間変動問題，筆順変動問題，画数変動問題である．このうち筆順変動問題は，漢字のような多画文字において特に重要である．筆順変動が起こると，見かけ上同じような文字形状であっても，時系列的には一部のデータが通常とは異なる部位に移動してしまう．その結果，時系列順に沿った照合を行うと，その字形の標準的な時系列データと大きく異なってしまうため，誤認識を生ずる可能性が高い．例えば「く」「ノ」「一」の筆順を標準とする「女」について，もし入力が「一」「く」「ノ」の順に筆記されたとすれば，両者を単純に照合しても，全く異なる文字と判断されてしまう．

本論文は，この筆順変動問題の対処法について，網羅的かつ詳細な比較実験および筆順変動の傾向を利用した計算量低減法を提案しており，以下の点で評価できる．

第一に，この筆順変動問題の対処法について調査・分類および比較実験を行った点である．具体的には，まず従来の筆順変動対処法を網羅的に調査，分類した．そしてそれら分類を通して，画対応探索法が最も精度的に期待できることを示した．ここで画対応探索法とは，例えば 2 つの画系列「く」「ノ」「一」と「一」「く」「ノ」の間に適切な 1 対 1 の画対応関係を定める方法である．次に，代表的な 5 種類の画対応探索法 ― cube search (CS), bipartite weighted matching (BWM), individual correspondence decision (ICD), stable marriage (SM), deviation-expansion model (DE) ― を採り上げ，それらの計算量および精度の詳細な比較を，教育漢字を対象とした認識実験を通して行った．その結果，原理的に大局的最適化能力を持つ CS と BWM が最も高い画対応精度を示し，それらの優位性を確認した．また計算量の側面においては，BWM, ICD, SM に優位性があることを示した．加えて，高速化のために枝刈りを組み込んだ CS は，原理的には近似解しか得られないものの，現実的には精度と速度を両立可能なことを実験により示した．

第二に，部首レベル処理の導入による計算量低減法を提案した点である．具体的には，まず手書き漢字約 1 万 7 千サンプルの筆順を調査し，ほとんどすべての筆順変動が，部首内，もしくは部首単位で起こりうること明らかにした．すなわち例えば「桜」に起こる筆順変動は，「木」「ツ」「女」の各部首内で起こるもの，および「木」全体が「ツ」「女」の後に書かれるといった部首単位のものが主要であり，「木」と「ツ」に跨るような筆順変動は少ない．次に，この性質を上記の CS に制約として組み込んだ手法を提案した．同制約により CS の解探索空間は圧縮され，原理的に高速化が図られる．認識結果を通して，この高速化を実証するとともに，認識精度も副次的に向上することを示した．

以上要するに，本研究は，オンライン文字認識における筆順変動問題について，様々な解法の比較評価実験を行い，さらに部首レベル処理の導入の有効性を実験的に証明したものであり，情報知能工学上寄与するところが大きい．よって本論文は博士（工学）の学位論文に値するものと認める．

氏　　名　久永　聡
学位記番号　シ情　博甲第 481 号（情報科学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　GIS アプリケーションにおける景観表示の再現性を優先する空間データ処理方式に関する研究
論文調査委員
（主　査）　九州大学　教　授　岡村耕二
（副　査）　〃　〃　内田誠一
〃　〃　〃　志堂寺和則
〃　〃　准教授　岡田義広

論 文 内 容 の 要 旨

地理情報システム（GIS: Geographic Information System）とは，地理情報を空間データ（地球上の地理位置と対応付いた図形情報）と関連付けた地理空間情報を蓄積して利用するシステムである．初期の GIS における空間データは，航空写真，等高線，地理情報を線にて表現するベクトルデータが用いられていた．近年，コンピュータの性能向上により，空間データとして街並みを撮影した映像，及び建物や道路の立体形状を表現した 3 次元データが扱われるようになってきた. GIS を利用する環境にも変化が見られた．近年，各種ソフトウェアを実行可能な携帯電話やスマートフォンが普及し，モバイル環境にて GIS アプリケーションを利用する環境が整った．また，携帯電話の普及にあわせて, 2006 年に事業用電気通信設備規則が改正され緊急警報機能の充実のために携帯電話への GPS（Global Positioning System）モジュールの内蔵が義務付けられたため，モバイル環境にて GIS を使用するために重要な位置情報の取得が

可能になった．さらに，GPS の測位精度の高精度化および GPS 利用範囲の可用性向上が進み，屋外において高精度に位置情報の取得が可能になった．このような空間データの進歩およびモバイル環境の変化により，活用される GIS アプリケーションの形態にも新たな可能性と課題が生じた．従来の典型的な各種業務向け GIS アプリケーションでは，利用する空間データの種類やデータ量が端末の表示性能に適して選択されていた．また，事前に端末に空間データを蓄積して利用するため，大容量の空間データの表示に伝送は不要であった．これに対して，モバイル環境において，各種空間データが空間データの種類や端末性能，及び回線の速度に制約を受けずに表示可能になれば，地理空間情報を必要とするより多くの利用者へ各種情報の提供が可能になり，GIS アプリケーションの用途も特定業務用途から様々な用途への拡大が期待できる．例えば，道案内の用途では，3 次元データや動画データを用いて目の前の景観と同じ景観を再現して表示すると，2 次元地図による表示と比較して誰もがより直感的に理解しやすい道案内が可能になる．また，災害発生時に航空機から取得した地上の状況を携帯端末へ即座に送信して表示できれば，いち早く災害発生場所付近の住民へ状況を伝えるサービスの実現が可能になる．

しかしながら，モバイル環境において空間データを表示する携帯電話やスマートフォン等の端末には，端末の表示性能や回線速度に制約がある．特に，映像や 3 次元データは大容量であるため，モバイル環境にて利用するのは困難であった．従来，データ容量が大きな 3 次元空間データの表示課題に対して，表示範囲を制限する LOD(Level Of Detail)が適用されていた．しかし，この方式では，表示可能な景観の範囲を制限して表示するデータ容量を削減する方式であるため，十分な範囲の景観を表示できない課題があった．

これに対して，本論文では，端末や回線の性能に適したデータ容量の 3 次元空間データと，歩行者ナビゲーションに適した表示範囲の景観を再現可能なパノラマ画像とを同時に配信して，端末において 3 次元空間データとパノラマ画像を合成表示する表示方式を提案した．パノラマ画像と 3 次元空間データとの合成表示により，景観を劣化せずにデータ量を 1/70 に削減する表示方式を開発した．さらに，この表示方式には，モバイル環境に応じて 3 次元空間データの範囲を変化させることにより，異なるモバイル環境においても，3 次元空間データによる自由な視点位置，視点方向による景観表示と同時に，パノラマ画像により遠景の景観表示も可能である特徴がある．また，この方式が実際の GIS アプリケーションにおいて効果的かどうかを，歩行者ナビゲーションをモチーフとした実証実験により検証した．空間データの整備が進んでいない屋内においても，多くの利用者が GIS アプリケーションを利用可能とするために，屋内データの表示に必要な空間データの取得方式を研究し，モバイル環境における屋内空間データの利用を可能にした．一般に形状が複雑な屋内空間を全て 3 次元モデルで表現するのは困難であるので，3 次元モデルを構築し易い通路形状の空間については，表現に自由度の有る 3 次元空間データを構築して表示する方式を適用し，モデル構築が難しい複雑な空間については，景観再現性が高いイメージベースレンダリング方式を適用した．通路形状の空間データ構築方式には，測定時にセンサの自己位置を求めるための距離計と通路の形状を取得するレーザレンジスキャナとを併用することにより，通路の形状にランドマークとなる特徴が得られない空間でも通路区間中の自己位置の取得と 3 次元モデルの構築を可能として，3 次元モデル構築を可能にした．また，イメージ空間データの構築には，測位環境の無い屋内空間において，景観から特定のランドマークを得難い空間において，景観全体を特徴として照合する方位推定方式を開発し景観画像取得位置の取得を可能にした．さらに，従来の形態の空間データである航空機から取得した空間データを新しいモバイル環境において有効に活用するための空間データ処理技術を開発した．航空機から取得する空間データには，光学画像，パンクロマチック画像，マルチバンド画像，さらに合成開口レーダ画像が挙げられる．中でも合成開口レーダ画像は，全天候にて取得が可能であるので，災害発生時に航空機から地上の状況を観測する目的で使用できる．このため，航空機から取得した合成開口レーダ画像をいち早く地上のモバイル端末へ伝送できれば，災害発生時の情報収集に役立つと考えられる．しかしながら，合成開口レーダ画像は，画素値がハイダイナミックレンジの値をとるため，人が見て理解し易く表示することが困難であり，データ容量も膨大（1 画素 8byte）である．これを携帯端末へ伝送表示するには，データ量を削減する必要があるため，景観を劣化させずにデータ量を削減するデータ圧縮方式を開発した．このデータ圧縮方式は，空間データを一様に圧縮する方式ではなく，必要な情報がある範囲と，それ以外の範囲を分離して，必要な情報のある範囲の視認性を保存してデータを削減する手法により，地表面の特徴の再現性を維持しつつデータ量の削減を可能にした．結果，災害状況の把握に適した構造物を自動的に検出して，構造物の輝度分布に応じて輝度を変換する処理により，画像全体の構造物を視認し易く表示するとともに，データ量を削減（1 画素 8bit）した．

これらの研究により，GIS の新しい環境であるモバイル環境において，景観の再現性を維持しつつ，屋外，屋内，および広域の空間データの活用が可能になる．これは，従来一部の業務システムにおいて利用されていた地理情報を幅広く多くの利用者に活用可能とする技術の進歩と考える．

論 文 調 査 の 要 旨

地理情報システム（GIS: Geographic Information System）とは，地理情報と空間データからなる地理空間情報を蓄積して利用するシステムである．近年の空間データは従来の航空写真，等高線，地理情報を線にて表現するベクトルデータから，街並みを撮影した映像，及び建物や道路の立体形状を表現した３次元データと変化してきた．GIS を利用する環境にも変化が見られ，各種ソフトウェアを実行可能なモバイル端末が普及し，モバイル環境にて GIS アプリケーションを利用する環境が整ってきた．一方，従来の GIS アプリケーションでは空間データが端末に予め蓄積されることを前提にして開発されているため，二次記憶容量が小さいモバイル端末ではそのまま利用することはできない．そこで，GIS アプリケーションが端末と独立して設計され，様々な場所で取得された空間データが伝送され，モバイル端末で共通的に利用できれば，より多くの利用者へ各種情報の提供が可能になると考えられる．例えば，航空機から取得したレーダの画像をいち早く地上の任意の端末へ伝送し景観を表示できれば，災害発生時の情報収集に役立つようになる．本論文は GIS の新たな利用環境であるモバイル環境において，景観の再現性を維持しつつ，屋外，屋内，および広域の地理空間データの活用を可能にしたもので，以下の点で評価できる．

第一は，通信速度が限られる屋外のモバイル端末における空間データの取得，表示のために，3 次元地理空間データの一部をパノラマ画像として送信し，残りの３次元地理空間データと合成表示する方式を考案したことである．本研究ではパノラマ画像として送信する適切な空間データの範囲を実証実験によって決定し，さらに，歩行者ナビゲーションアプリケーションによる実用性の評価を行なっている．

第二は，屋内において，形状が複雑で３次元モデルだけでは全体を表現することが困難である場合に，距離測定による３次元空間データとスキャンした画像を併用して屋内データの表示に必要な空間データを構築する方式を考案したことである．画像をスキャンする場合には，景観から特定のランドマークを得難い屋内空間においても，景観全体を特徴として照合する方位推定方式を開発し，景観画像取得位置の取得を可能にしている．

第三は，合成開口レーダ画像中に含まれる景観の情報を維持したままデータ圧縮する方式を考案したことである．このデータ圧縮方式は，空間データを一様に圧縮する方式ではなく，必要な情報がある範囲と，それ以外の範囲を分離して，必要な情報のある範囲の視認性を保存してデータを削減する手法により，地表面の特徴の再現性を維持しつつデータ量の圧縮を実現している．

以上を要するに本論文は，GIS の新しい環境であるモバイル環境において，景観の再現性を維持しつつ地理空間データの活用を可能にする方式として，屋外における３次元地理データとパノラマ画像を同時に送信し合成表示を行う方式，屋内における距離測定と画像スキャンを併用した空間データの取得方式，合成開口レーダ画像中に含まれる景観の情報を維持したままデータ圧縮する方式を考案し，実証実験によりその実用性を明らかにしたもので，空間データ工学に寄与するところが大きい．よって，本論文は博士(情報科学)の学位論文に値するものと認める．

氏　　名	Heru Sukoco
学位記番号	シ情　博甲第 482 号（工学）
学位授与の日付	平成 24 年 9 月 24 日
学位論文題名	Study on Network Migration over Fairness Networks （公平性のあるネットワーク上でのネットワーク移動に関する研究）

論文調査委員

（主　査）	九州大学	教　授	岡村耕二
（副　査）	〃	准教授	天野浩文
〃	〃	〃	堀　良彰

論 文 内 容 の 要 旨

Internetworking, also known in abbreviated term as Internet, has evolved rapidly in a few decades. It has experienced significant changes and affected our daily life in many areas such as communication, business, education, and entertainment. There are 2 technologies currently running on the Internet namely IPv4 and IPv6 which have a function as a communication protocol or packet transfer procedure of the Internet with 32-bits space addressing and 128- bits space addressing, respectively. The Internet is a technology with multi-purpose services and communication infrastructures such as routing function, node interconnection, address resolution, flow control, and congestion control. We can connect to this enormous network through dozens of different devices and technologies. However the IPv4 provides unreliable, best effort, and connectionless packet delivery services.

Future Internet is a general term for research activities on new architectures for the Internet. In the future, Internet is consuming and creating information more pervasive over high-speed network infrastructures and many new technologies. Many researchers are interested in such topics to improve current Internet technologies and services including network management, migration, virtualization, and

protocols. Content-based applications are the one of the dominant technologies which occupy the future Internet e.g. real-time and multimedia live streaming.

The distribution of those applications in the Internet has rapidly increased in the Internet and commonly they rarely use congestion control and do not fairly share provided network capacity with TCP-based applications such as HTTP, FTP and emails. Therefore, Internet communities will be threatened by the increase of non-TCP-based applications that the likely cause a significant increase of traffics congestion and starvation. I propose a set of mechanisms to establish friendliness for both Non-TCP-based and TCP-based applications when sending multicast traffics. I use Receiver-driven Layered-Multicast (abbreviated as RLM) protocol with 6 layered multicast transmission to handle the fairness on the networks. Fairness is an essential aspect of any transport protocol so that traffics are equally shared and distributed between applications in a network. By using 8 scenarios of simulations with background traffic Pareto (the shape factor 1.5), I evaluate several key performance metrics such as throughput, delay /latency, jitter, TCP friendliness, packet loss ratio, and convergence time. The study shows that non TCP traffics behave fairly and respectful of the coexistent TCP-based applications that run on shared link transmissions even with background traffic. Another result shows that the simulation has low average values of throughput (314 kbps for TCP and 240 for non TCP), vary in jitter (0-10ms), and packet loss ratio (PLR) is greater than 3%. It was also difficult to reach convergence time quickly when involving only non TCP traffics.

Another problem arises from the networks especially a router when managing the packets. It may not failures when it deals with network virtualization technology such as Openflow protocol or virtual networks. The author provides an alternative scheduling optimization in maintaining packet queues on virtual routers. It uses Genetic Algorithm (GA) to reduce a cost of network resources such as memory and time process on routers. They will use to overcome traditional scheduling algorithms such as weighted fair queuing (WFQ) and recursive round robin (RRR) which are not capable of a virtual network due to traffic flows in aggregated and tunneled sessions. GA offer an effective and optimal technique to solve those problems and define WFQ-like model to predict minimum queue length needed by a router. I evaluate the performance of GA by running simulations in several conditions such as various evolution values, population, packet sizes, and number of packets. The simulation results an average of slot number is 106.20 with a standard deviation of 82.51. It uses a crossover probability and mutation probabilities are 0.90 and 0.05, respectively.

Finally, the growth of networks bears the other problem when our network systems are failures because of outside influences such as a natural disaster and mobility. Network migration and virtualization technology are excellent tools to salvage network resources. Network virtualization isolates multiple network technologies while using the single hardware infrastructure and network migration is one solution to keep the system alive. The previous researches use a different approach to establish network migration. They used network paging-based technique and Locator/ID Separation Protocol (LISP)-based without paying attention to path selection before doing migration. My network migration scheme proposed network segmentation method and considered Genetic Algorithm (GA)-based path selection to solve a shortest path problem before doing network migration. This purpose is getting the most minimum cost of a way to a destination site. GA is a heuristic algorithm which can learn from previous historical data. Combining GA-based path selection and network segmentation approaches can be implemented in any condition both topology and technology.

論 文 調 査 の 要 旨

インターネットが古くから構造的に持つ公平性や通信資源管理といった諸問題を根本的に解決することを目標にした新世代ネットワークにおいて，ネットワークをより柔軟に利用可能とする仮想ネットワーク技術の研究開発は非常に重要なテーマである．近年，ハードウェア命令をソフトウェアでエミュレートし物理的に一つのハードウェア上で仮想的に複数のシステムの実行を支援できる仮想環境が実用化されてきた．インターネットを構成するルータも仮想化が可能となり，物理的に一つのネットワーク上で複数の仮想ネットワークを同時に運用できるようになってきた．多様化する通信要求に対して，動的に公平性を保つためには通信資源のスケジューリングが必須である．ハードウェアをソフトウェアで実行している仮想ネットワークでは通信資源の割り当てを柔軟に行うことができる．本論文は，ネットワークの公平性の定量化を可能にし，遺伝的アルゴリズムを応用して仮想ネットワークのための通信資源方式，仮想ネットワーク上でのネットワーク移動のためのアルゴリズムを考案したもので，以下の点で評価できる．

第一は，TCP による通信と，TCP と親和性の高い非 TCP による通信が混在しているネットワークで，それぞれのトラフィックの比率を用いて算出されるネットワークの公平性の値を考案し，公平性の定量化を可能にしたことであ

る．考案した公平性の値を利用することで，TCP 通信，非 TCP 通信およびマルチキャスト通信等の混在する複雑なネットワークに対して，公平性の検証が定量的に行えることをシミュレーションにより，示した．

第二は，遅延時間，最大パケットサイズや出力のバンド幅などの要件を満たす，遺伝的アルゴリズムを応用したパケット転送スケジューリングの決定手法を考案し，シミュレーションにより本方式による通信資源利用の効率化を明らかにした点である．本研究ではパケット転送に対して通信資源をスケジュールする従来の複数のキューを用いる方式と比較して，遺伝的アルゴリズムを用いることにより容易に通信資源スケジューリングを導出できることが示されている．

第三は，通信資源のスケジューリングと多様な通信要求を満たす経路設定を，遺伝的アルゴリズムを用いて導出する手法を考案したことである．本研究の手法では，経路情報を集約し処理の高速化を図っている．本手法を用いることで，移動元と同等な通信資源を確保し，同等な通信特性を提供する経路設定を行うことができるネットワークの候補を他の手法よりも高速に導出できることをシミュレーションにより，示した．

以上要するに本論文は，ネットワークの公平性を定量化する方式，遺伝的アルゴリズムを用いた通信資源のスケジューリング方式と仮想ネットワーク上でのネットワーク移動のための方式を考案し，それらの有用性の評価により，広域ネットワークにおける公平性と通信資源管理に関して論じたものであり，通信工学に寄与するところが大きい．よって，本論文は博士(工学)の学位論文に値するものと認める．

氏　　名　姫　　艶　麗
学位記番号　シ情　博甲第 483 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　Recognition of Human Actions using Visual Local Features
（局所特徴を用いた動画像中の人間動作認識）
論文調査委員
（主　査）　九州大学　教　授　谷　口　倫一郎
（副　査）　〃　〃　倉　爪　亮
〃　〃　准教授　長　原　一

論文内容の要旨

Recognition of human actions in videos is a process of naming actions which are captured by cameras, usually in a simple form of an action verb. Action recognition is an attractive research topic, and its application fields are not limited to video surveillance, human-computer interaction, sport video analysis, computer motion animation, and so on. However, human action recognition is still a challenging problem because of two reasons. One reason is owed to quite a lot of appearance variations in human actions, such as various action classes, different physiques of humans and a variety of clothing styles and colors. Furthermore, camera based action recognition need to overcome some difficulties brought by occlusion, view point changes, scale variation of video screen, etc..

Is this thesis, the author aims to recognize human actions captured by cameras from basic to complex situations. For the target, we propose a method for local feature calculation, and design a recognition system using these local features. Furthermore, we propose a local feature based method to solve the problem of more complex action recognition: human interaction.

Firstly, a new local feature calculation method is proposed for human action representation. In the method, FAST detector is extended to spatio-temporal space to detect feature points from videos. Then a compact descriptor is proposed which represents actions with compact peak kept histograms of oriented spatio-temporal gradients (CHOG3D). It is calculated in a small spatio-temporal support region around the candidate feature point in order to obtain a compact descriptor. It employs the first order gradient in spatial and temporal orientations for descriptor calculation. In addition, it keeps the peak value of orientation quantized gradient to make the descriptor CHOG3D being able to represent actions more exactly and being distinguished more easily. The efficiency of peak kept is certified by comparing with threshold setting method for action recognition. By parameter training, the optimal parameters for CHOG3D are determined. The local features calculated with FAST and CHOG3D are applied for action recognition using SVM. Based on the computation cost comparison and performance evaluation, the compact descriptor CHOG3D performs well on human action recognition, and it has a lower computation cost. Though CHOG3D has the limitation of containing less information, a proper quantity of feature points help to overcome the disadvantage.

Secondly, a self-organizing map (SOM) based recognition system is proposed for local feature used human action recognition. In the proposed system, the compact descriptor CHOG3D is adopted for local feature calculation to represent human actions. Then the SOM is employed to train local features and extract key features of actions because of its advantage in mapping data into a low dimension. After

training, the key features are assigned action labels of the training data. For action recognition, we adopt k-Nearest Neighbor algorithm (k-NN) to classify features of a testing action sequence into different action classes. By calculating the statistics of feature classification, the action class of the testing sequence is determined. We search for the optimal map size of SOM for training and the proper value κ for k-NN classification. With the optimal parameters, we test the proposed method for action recognition on three datasets, KTH, Weizmann and UCF sports datasets and the results certify the efficiency of the proposed recognition system.

Finally, we extend our research to recognize complex human actions, i.e. interactive actions, and propose a contribution estimation method for improving interactive action recognition. Unlike previous algorithms using both of two participants action information, the proposed algorithm estimates the action contribution of participants to select the major participant action for correct interaction recognition. To estimate contributions, we construct contribution interaction model for each interaction category in which both of two participants do major actions. Then we design a method making use of these contribution interaction models to estimate the contribution of participants and classify interaction samples to “co-contribution” or “single-contribution” interactions. Furthermore, we determine the major action in a “single-contribution” interaction. If a given interaction is determined to be “co-contribution,” the actions of both the two participants are adopted for recognition. While for “single-contribution” interaction, the major action is selected for recognition. Experiments show that the method is effective for human interaction recognition, which outperforms other methods.

論 文 調 査 の 要 旨

画像認識により人間の動作を認識する技術（以下，動作認識）は，近年盛んに研究が行われている．例えば，映像によるサーベイランス，ヒューマンインタフェース，スポーツ映像の解析などへの応用が期待されている．しかし，カメラにより撮影された人物の動作の見えは，動作の種類だけでなく，対象人物の体格や着衣の種類により大きく変化するため，画像認識としては必ずしも容易な問題ではない．また，動作の様態に関しても，単一人物だけの動作だけでなく，複数人物による相互に作用する動作（インタラクション）も認識の対象とする必要がある．本論文は，このような観点から，新たな局所画像特徴に基づき，一人の動作および二人のインタラクティブな動作を正確かつ高速に認識する手法について述べたものであり，以下の点で評価できる．

第一に，より正確かつ高速に動作認識を実現するための新たな局所画像特徴を提案した点である．局所画像特徴による手法は，対象の切り出しを陽に行う必要がなく，比較的複雑な背景でも安定に動作するという利点がある．提案手法では，まず，２次元画像の特徴点検出器である FAST (Features from Accelerated Segment Test)を時空間画像で利用できるように拡張し，撮影された映像から特徴点を検出する．その上で，検出した特徴点において CHOG3D (Compact Histogram of Oriented Gradient 3D) と呼ぶ局所画像特徴を計算する．CHOG3D は，特徴点の近傍領域における時空間微係数を量子化し，その局所的な最頻値をヒストグラム化したものである．CHOG3D によって得られた局所画像特徴集合と標準的な認識アルゴリズムである SVM (Support Vector Machine)を利用した認識が，従来良く用いられていた HOG3D (Histogram of Oriented Gradient 3D) によるものよりも認識率が高いことを実験的に示し，CHOG3D の有効性を確認している．

第二に，自己組織化写像(SOM, Self Organizing Map)を通して得られる固有局所画像特徴を用いて，認識率が高く，高速な動作認識システムを開発した点である．学習時には，学習用動作映像から得られた局所画像特徴集合の自己組織化写像を求め，自己組織化写像の各ノードに対応づけられた動作ラベルの頻度に基づいて，各動作における固有局所画像特徴を抽出する．一方，認識時には，入力から得られた局所画像特徴の集合を学習された自己組織化写像に投影し，入力に現れる固有局所画像特徴の頻度を求めて動作の種類を識別する．実験では関連研究で良く用いられる KTH, Weizmann, UCF sports の３つのデータセットで性能評価を行い，従来手法に比べて認識率，認識時間の点で優れていることを実験的に示している．

第三に，二人のインタラクティブな動作の認識をより正確に行う手法を開発した点である．本手法では，正確な認識を実現するために，パンチやキックといった片方の動作者のみが積極的な動作を行うものと握手やハグなどのように両方の動作者が共に積極的な動作を行うものに分類する．前者の場合，積極的な動作者の相手は定まった動きを行わないので，動作認識の有効な特徴として利用できない．そのため，定まった動作を行う積極的な動作者の局所画像特徴を，非協調動作，対称的協調動作，非対称的協調動作の３つのテンプレートモデルに基づいて選択的に利用して認識を行う．関連研究で良く用いられる UT interaction dataset および著者が独自に作成した LIMU interaction dataset を用いて，従来手法より認識率が高くなることを実験的に示している．

以上要するに，本研究は，映像中の一人の動作および二人のインタラクティブな動作の認識を正確，高速に行うための，局所画像特徴に基づいた動作認識の実現法を提案し，実験を通してその有効性を示したものであり，情報知能工

学上価値ある業績である．よって，本論文は博士（工学）の学位論文に値するものと認める．

氏　　名　張　　棟翔
学位記番号　シ情　博甲第 484 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　Robust global localization using laser reflectivity
（レーザ反射率を用いたロバストな大域的位置同定手法に関する研究）
論文調査委員
（主　査）　九州大学　教　授　倉　爪　　亮
（副　査）　〃　　〃　　長谷川　　勉
〃　　〃　　准教授　諸　岡　健　一

論文内容の要旨

移動ロボットにおける位置同定問題は，前時刻の位置などの事前知識を用いない大域的位置同定（Global localization）と，前時刻での位置や局所移動量などの事前知識を利用する位置追跡(Tracking)に大別される．このうち大域的位置同定は，多くのアプリケーションで必須の基本的な機能であるが，外界センサにより得られた周囲の環境情報のみから自己位置を推定する必要があり，広域な環境では困難な問題である．一方，ロボットの位置同定にはカメラやレーザレンジファインダ，超音波センサなどが用いられるが，特にレーザレンジファインダを用いた位置同定は，高精度かつ低価格なセンサが近年数多く開発され，最も実用的で信頼性の高い位置同定手法として標準的な手法になりつつある．これまでレーザレンジファインダによる位置同定では，計算量や距離データの取り扱いの容易さから，床面と平行にレーザを走査して得られる移動経路の断面形状を用いた 2 次元位置同定が主であった．しかし 3 次元計測が可能なレーザスキャナやステレオカメラが開発され，高さも含む 3 次元位置同定も可能になりつつある．一般的な 3 次元大域的位置同定では，あらかじめ人手やロボットにより獲得され保存された広域な 3 次元環境構造モデル（環境マップ）と，移動ロボットが移動中に獲得した部分的な 3 次元環境構造モデル（部分マップ）を比較し，ICP (Iterative Closest Point)法などを用いて，両者が最も一致する環境マップ内の部分マップの位置を繰り返し探索する．しかし 3 次元データを用いた探索は計算コストが高く，また正確に真値へ収束するには，探索の初期位置がある程度真値に近くなければならなかった．

そこで本論文では，レーザレンジファインダによる移動ロボットの 3 次元大域的位置同定を，レーザ計測の副産物であるリフレクタンス画像を利用して高速かつ頑健に行う手法を提案している．レーザレンジファインダには，レーザ光源から投射されたレーザ光が，物体へ反射し再びセンサへ戻るまでの伝達時間から距離を測定する Time-of-Flight 方式がよく用いられるが，この方式では距離データとともにレーザ光の反射強度であるリフレクタンス値が同時に得られる．このリフレクタンス値は対象表面の反射率やレーザの入射角度に応じて変化し，各点のリフレクタンス値を並べて表示すると，写真と非常に似たリフレクタンス画像が得られる．そこで，環境マップ構築時のレーザ測定毎にリフレクタンス画像を同時に計測，保存し，位置同定時に得られる部分マップのリフレクタンス画像と比較することで，3 次元データを用いずに環境マップ中の部分マップの位置の候補を効率よく求めることができる．本論文では，一般物体認識で用いられる Bag-of-features の手法を用いて，環境マップ計測時のリフレクタンス画像と部分マップ計測時のリフレクタンス画像を比較し，部分マップ計測位置の大まかな推定値を得ている．本手法の特徴は，リフレクタンス画像は距離データの取得の副産物として得られ，リフレクタンス画像取得のための新たな計測やカメラなどが不要であること，環境の明るさに無関係に安定して画像が得られることなどである．

本論文は５章から構成される．第１章は序論である．第２章では提案するリフレクタンス画像を用いた位置同定手法の原理を説明し，屋内外での大域的位置同定実験によりその有効性を確認している．第３章では，第２章の手法と ICP 法を組み合わせ，より高精度な位置同定を実現する手法を提案している．第４章では，パーティクルフィルタと組み合わせて頑健な位置同定を行う手法を提案し，類似した環境情報が多く得られる屋内廊下で実験を行い，位置同定性能の向上を確認している．第５章では結論として本論文で得られた結果を総括し，今後の展望について述べている．

論文調査の要旨

移動ロボットの位置同定問題は，前時刻での位置や局所移動量などから自己位置を推定する位置追跡と，それらの知識を用いない大域的位置同定に大別される．このうち大域的位置同定は，外界センサにより得られた周囲の観測情報のみから自己位置を推定するため，広域な環境や特徴的な手掛かりが得られにくい場所では困難な問題である．また位置追跡も，局所移動量の積算による累積誤差の増加を防ぐためには，大域的位置同定と同様に外界センサの利用は欠かせない．一方，近年，高精度かつ低価格なレーザレンジファインダが数多く開発され，実用的で信頼性の高い位置同定を実現するセンサとして利用されている．レーザレンジファインダを用いた位置同定では，あらかじめ人手やロボットにより獲得された広域な環境構造モデル（環境マップ）と，移動ロボットが位置同定時に獲得した部分的

な環境構造モデル（部分マップ）を比較し，Iterative closest point (ICP)法などを用いて，両者が最も一致する環境マップ内の部分マップの位置を繰り返し探索する．しかし 3 次元点を用いた 3 次元位置同定は計算コストが高く，また安定に真値へ収束するには，探索の初期位置がある程度真値に近い必要があった．

本論文は，レーザスキャナによる移動ロボットの 3 次元位置同定に対し，レーザ計測の副産物であるリフレクタンス画像を利用することで，計算コストの低減や位置探索の安定性を向上する手法を提案しており，以下の点で評価できる．

第一に，リフレクタンス画像に対して一般物体認識で用いられる Bag-of-features を適用し，環境マップ構築時のリフレクタンス画像と位置同定時のリフレクタンス画像を比較することで，3 次元点を直接比較することなく大まかな自己位置を推定する手法を開発した点である．レーザスキャナは，レーザ光源から投射されたレーザ光が，物体へ反射し再びセンサへ戻るまでの伝達時間に基づいて距離を測定する．このとき距離データとともにレーザ光の反射強度であるリフレクタンス値が得られる．このリフレクタンス値は対象表面の反射率や対象までの距離，レーザの入射角度に応じて変化し，各計測点のリフレクタンス値を並べて表示すると，計測位置に固有のリフレクタンス画像が得られる．そこで提案手法では，環境マップ構築時にリフレクタンス画像を計測，保存し，位置同定時に得られるリフレクタンス画像と比較することで，3 次元点を用いずに環境マップから自己位置の候補を効率よく求めることができる．

第二に，上述の手法で得られた環境マップ中の候補から，リフレクタンス画像間の類似性に基づき少数の初期位置を効率よく選択し，ICP 法を適用して真値を探索することで，安定かつ高精度な 3 次元大域的位置同定を実現した点である．リフレクタンス画像は，通常のカメラ画像と異なり，同時に計測された距離画像と一意に対応付けることができる．そこで，ICP 法で問題となる計測点の誤対応を防ぐため，リフレクタンス画像間の光学的類似性に加えて，対応する距離画像の幾何拘束を考慮した投票による対応点判定法を提案している．レーザスキャナを搭載した移動ロボットによる屋内外での位置同定実験により，その有効性を確認している．

第三に，開発した大域的位置同定と局所移動量を用いたパーティクルフィルタを組み合わせ，頑健な 3 次元位置追跡を実現した点である．類似した環境情報が多く得られる屋内廊下で実験を行い，パーティクルフィルタにより候補位置を絞り込むことで，パーティクルフィルタを用いない場合に比べて位置追跡の成功率が 53%から 94%へ向上することを確認している．

以上要するに，本研究は，レーザスキャナによる移動ロボットの 3 次元位置同定に対し，レーザ距離計測と同時に得られるリフレクタンス画像を利用することで，計算コストの低減や位置探索の安定性を向上させる手法を提案し，実験を通してその有効性を示したものであり，ロボット工学上価値ある業績である．よって，本論文は博士（工学）の学位論文に値するものと認める．

氏　　名　河 村 晃 宏
学位記番号　シ情　博甲第 485 号（工学）
学位授与の日付　平成 24 年 9 月 24 日
学位論文題名　Dynamic Grasping and Manipulation of an Arbitrary Object by a Multi-Fingered Hand-Arm System
（多指ハンドアームシステムを用いた任意物体の動的把持および操作）
論文調査委員
（主　査）　九州大学　教　授　倉 爪　　亮
（副　査）　〃　〃　長谷川　　勉
〃　〃　〃　山 本 元 司
〃　〃　准教授　田 原 健 二

論 文 内 容 の 要 旨

人と共生し，日常生活環境で様々な生活支援を行うロボットには，日用品や取っ手など日常生活で用いられる多種多様な対象物を，安定かつ巧みに把持し，操作する高度な能力が求められる．これまでに様々なロボットハンドによる物体把持・操作手法が提案されているが，その多くは材質や形状，剛性，質量，質量中心位置など，把持対象に関する正確な情報が既知であることを前提としている．一方，日常生活環境では，把持対象に対する事前知識が全くない，あるいは不正確な情報しか得られない状況が頻繁に生じる．把持対象の情報には，形状などロボットに搭載したレーザやカメラにより，把持開始前に非接触で得られるものもあるが，正確な情報の獲得には多くの計測時間が必要であり，また質量や摩擦，剛性など把持開始前では獲得不可能な情報も多く存在する．従って，把持対象に関する事前知識が与えられない場合でも，多様な物体を安定に把持し，操作する手法の開発が課題となっている．また，物体把持後の操作においては，所望の制御目標を精度良く実現するために，ロボットに搭載した視覚センサや触覚センサ，力センサなどの外界センサにより把持対象の状態を計測し，制御目標との差をフィードバックするサーボ制御法が広く用いられる．特に視覚センサは，非接触かつ短時間で物体の位置姿勢情報の取得が可能であるが，照明条件の変化やオクルージョンの発生などにより正確な情報が得られない場合も多く，このような状況が頻繁に発生した場合でも安定な視覚サーボ制御法の開発が望まれている．

本論文では，形状や質量中心位置が未知の任意多面体に対する安定な把持，操作手法，およびオクルージョンや時間遅れに対しても頑健な視覚センサを用いた未知の任意多面体の操作手法を提案している．

本論文は７章から構成される．第１章は序論である．第２章では，本論文で対象とする多指ハンドアームシステムおよび把持物体に対して，指先-物体間の転がり接触拘束を考慮した動力学モデルを導出している．第３章では，ハンドやアームの関節エンコーダから得られる関節角度および関節角速度のみを用いた，形状や質量中心位置，指先接触位置などが未知の任意多面体に対する安定把持手法を提案している．また安定性に対する理論的検討，数値シミュレーションおよび実機実験により，本手法の有効性を検証している．第４章では，第３章で示した物体把持手法を拡張した，未知の任意多面体の操作手法を提案している．本手法では，関節エンコーダに加えて，視覚センサから得られる把持物体の位置・姿勢情報を用いて，未知の任意多面体に対する位置・姿勢制御を実現している．本手法の有効性は，安定性に対する理論的検討および数値シミュレーションにより確認している．第５章および第６章では，第４章で提案した操作手法を拡張し，オクルージョンによるセンサ情報の欠損あるいは大きな時間遅れにも頑健な，未知の任意多面体の位置・姿勢制御手法を提案している．本手法では，ハンドの指先位置・姿勢により定義される仮想フレームを用い，視覚センサによって得られる実物体の位置・姿勢情報と仮想フレームを用いた制御を組み合わせることで，情報欠損や時間遅れにも頑健な物体の位置・姿勢制御を実現している．さらに数値シミュレーションおよび実機実験により，本手法の有効性を確認している．第７章では結論として本論文で得られた結果を総括している．

論 文 調 査 の 要 旨

人と共生し，日常生活環境で様々な生活支援を行うロボットには，日用品や取っ手など日常生活で用いられる多種多様な対象物を，安定かつ巧みに把持し，操作する高度な能力が求められる．これまでにもロボットハンドに対する様々な物体把持・操作手法が提案されているが，その多くは材質や形状，剛性，質量，質量中心位置など，把持対象に関する正確な情報が既知であることを前提としている．一方，日常生活環境では，把持対象に対する事前知識が全く与えられない，あるいは不正確な情報しか得られない状況が頻繁に起こり得る．この際，例えば物体形状は視覚センサ等で計測可能であるが，質量や剛性，質量中心位置は非接触では計測不可能である．従って，把持対象に関する事前知識が与えられない，あるいは不正確な場合でも，多様な物体を安定に把持し，操作するロボットハンドの制御手法の開発が求められている．また，物体把持後の操作においては，所望の制御目標を精度良く実現するために，ロボットに搭載した視覚センサや触覚センサ，力センサなどの外界センサにより把持対象の位置姿勢を計測し，目標位置姿勢との差をフィードバックするサーボ制御法が広く用いられる．特に視覚センサは，非接触で物体の位置姿勢情報の取得が可能であるが，照明条件の変化やオクルージョンの発生などにより計測に失敗する可能性がある．また取得されるデータが大量であり，プロセッサの処理能力が低いと画像の取得から計測結果の出力までに大きな時間遅れが生じる．従って，計測失敗や出力に遅れが生じた場合でも安定な視覚サーボ制御法の開発が望まれている．

本論文は，形状や質量中心位置などが未知の任意多面体に対する安定な把持，操作手法，およびオクルージョンや時間遅れに対しても頑健な視覚サーボ制御法を提案しており，以下の点で評価できる．

第一に，ハンドやアームの関節エンコーダから得られる関節角度および関節角速度のみを用いた，形状や質量中心位置などが未知の任意多面体に対する安定把持手法を提案した点である．本手法は，ハンド指先の位置姿勢から安定把持を実現する制御目標を決定することで，指先接触位置などが未知な場合でも安定把持を実現する．動力学モデルの構築と安定性に対する理論的検討，数値シミュレーション，および実機実験を通して，その有効性を検証している．

第二に，上述の物体把持手法を拡張した，未知の任意多面体の操作手法を提案している点である．本手法では，関節エンコーダに加えて，視覚センサから得られる把持物体の位置・姿勢情報を用いて，未知の任意多面体に対する位置・姿勢制御を実現している．動力学モデルに基づく解析的検討，および数値シミュレーションにより，その有効性を確認している．

第三に，提案した物体把持，操作手法を拡張し，オクルージョンによるセンサ情報の欠損あるいは大きな時間遅れにも頑健な視覚サーボ制御法を提案している点である．本手法では，ハンドの指先位置・姿勢により定義される仮想フレームを用い，視覚センサによって得られる実物体の位置・姿勢情報と仮想フレームから得られる位置・姿勢情報を適応的に切り替えることで，情報欠損や時間遅れにも頑健な未知の任意多面体の位置・姿勢制御を実現している．さらに数値シミュレーションおよび実機実験により，その有効性を確認している．

以上要するに，本研究は，生活支援ロボットの実現に向け，日常生活環境に存在する多種多様な対象物を安定に把持し，外乱に対して頑強に操作可能なロボットハンドの制御手法を提案し，実験を通してその有効性を示したものであり，ロボット工学上価値ある業績である．よって，本論文は博士（工学）の学位論文に値するものと認める．

氏　　名　Emad Mohamed Ahmed Mahmoud
学位記番号　シ情　博甲第 486 号（学術）
学位授与の日付　平成 24 年 10 月 31 日
学位論文題名　New Maximum Power Point Trackers Using Digital Control Techniques in Photovoltaic Systems
（ディジタル制御技術を用いた太陽光発電システム用新方式最大電力点追従装置に関する研究）
論文調査委員
（主　査）　九州大学　教　授　庄　山　正　仁
（副　査）　〃　〃　村　田　純　一
〃　〃　〃　岩　熊　成　卓

論 文 内 容 の 要 旨

In recent years, there has been an increasing interest of using Photovoltaic (PV) systems to supply electricity for various consumers due to their many merits, such as cleanness, little maintenance and no noise. However, the output power of PV panels varies with atmospheric conditions (solar irradiance level and temperature) as well as their output voltage and current. It is crucial to operate the PV energy conversion systems near the maximum power point (MPP) to increase the power yield of the PV system. Maximum power point tracking (MPPT) algorithms are usually implemented in the power electronic interface between the PV panel and an energy storage device or load for this purpose.

Although, various MPPT methods have been proposed in the literature, the commonly used MPPT algorithms are the power based methods, which include the hill-climbing (HC) method, perturb-and-observe (P&O) method, and the incremental conductance (INC) method. The HC and P&O methods achieve the same fundamental thought in different ways. These two methods are widely applied because their simplicity: nevertheless, they can fail under rapidly changing atmospheric conditions. The INC algorithm can track the maximum power point more accurately than the HC and P&O methods; however, it is relatively complicated to implement. Almost all tracking algorithms usually use a fixed iteration step size of the duty cycle of the converter in tracking MPP. Therefore, the steady state performance of the PV system exhibits steady state oscillations around the MPP. These oscillations properly increases as the tracker step size perturbation increased. On the other hand, tracking accuracy and tracking speed are highly depending on this fixed step perturbation: selecting small step size perturbation increases tracker accuracy and decreases tracker speed, and vice versa. Thus, the designed MPPT should satisfactorily address the tradeoff between the dynamics and steady state oscillations. This only can be done using variable step size algorithms. This step size would be automatically tuned according to the inherent PV array characteristics. If the operating point is far from MPP, it increases the step size which enables a fast tracking ability. If the operating point is near to the MPP, the step size becomes very small that the oscillation is well reduced contributing to a higher efficiency. Moreover, reducing the total number of the tracking sensors is a critical point of view. Because reducing tracker sensors means reducing the tracker size, increasing tracker robustness, increasing power density, and reducing the overall price of the tracker unit.

The above-mentioned tracking limitations and restrictions are tackled in this thesis and some novel algorithms and analysis are proposed. The thesis consists of six chapters. These chapters can be summarized as follows:

Chapter one introduces an overview about MPPT, and the main function of MPPT from circuit point of view. Moreover a literature review of MPPT different techniques is presented. And finally the motivation and the scope of this work are included.

Chapter two investigates the importance of the DC-DC boost converter with renewable energy (marine and tidal current) conversion systems. A simulation model for the conversion system has been developed. The effect of including DC-DC boost converter on the cut-in speed has been addressed. Moreover, the effect of including boost converter on the total harmonic distortion (THD) has also been introduced.

Chapter three proposes two variable step size MPPT algorithms that using only a single current sensor for stand-alone battery storage PV systems. These methods utilize only the relationship between the PV array measured current and the converter duty cycle to automatically adapt the step size in the duty cycle to reach the maximum power point of the PV array. Detailed analyses and flowcharts of the proposed methods are included. Moreover, a comparison has been made between the proposed methods to investigate their performance in the transient and steady states are also introduced. Finally, experimental results with field programmable gate arrays (FPGAs) are presented to verify the performance of the proposed methods.

Chapter four offers a novel stability study of variable step size incremental resistance (INR) MPPT. The main contribution of this analysis appears in developing the overall small signal model of the PV system. Therefore, by using

linear control theory, the boundary value of the scaling factor can be determined. The theoretical analysis and the design principle of the proposed stability analysis have been endorsed using numerical simulations, and experimentally using a fixed point digital signal processor.

Chapter five proposes a simple current-sensorless MPPT with DC-DC boost converter for a PV battery charging systems. The proposed tracker eliminates the use of the current sensor by using only the voltage sensor: The current sensor is substituted with a new quantity that employs both of the input voltage and the duty ratio of the converter. An empirical observation is used to develop a theoretical proof for this quantity. The proposed tracker is designed with a numerical simulator and implemented using a fixed-point DSP 2812. Moreover, a breadboard circuit has been built-up for testing the use of the proposed tracker with a DC-DC boost converter operating in continuous conduction mode. Experimental results show that the proposed tracker attains good dynamic and steady-state performances comparable to that obtained with the conventional MPPTs.

Chapter six includes both the final conclusions outline for this thesis and the future work.

論 文 調 査 の 要 旨

近年，クリーンで保守が容易，騒音を出さない等の特長を持つ太陽光発電システムが注目されている．太陽電池パネルの出力電力は，太陽の照射量や気温などの自然条件はもとより，その出力電圧や出力電流などの電気的動作条件によっても変化するため，常に最大電力点付近で動作するように電力変換器を制御することが大切である．そのため，太陽電池パネルにつながれる電力変換器には，ディジタル技術を用いた最大電力点追従（Maximum Power Point Tracking: MPPT）制御アルゴリズムが実装されている．

これまでに数多くの MPPT 手法が提案されてきたが，一般に用いられている方法は，「山登り法（HC）」，「摂動観測法（P&O）」，「コンダクタンス増分法（INC）」や「抵抗増分法（INR）」など，電力計算に基づく手法である．このうち，HC と P&O は簡単である理由から広く応用されているが，これらは太陽の照射量が急変すると追従に失敗する恐れがある．INC や INR はこの問題を改善したものであるが，実装が複雑になる欠点がある．

また，殆どの MPPT 制御アルゴリズムは，電力変換器に用いられるコンバータの時比率のステップ幅が固定であるため，最大電力点付近で振動現象を生じ，追従精度を悪化させる．これはステップ幅が大きいほど激しい．ステップ幅は追従精度と追従速度の両方に大きく影響し，ステップ幅を小さくすると追従精度は上がるが，追従速度が低下する．ステップ幅を自動的に変化させることにより，この問題は解決できる．すなわち，現在の動作点が最大電力点から大きく離れていればステップ幅を大きくして追従速度を上げ，逆に最大電力点の近傍であればステップ幅を小さくして振動現象を抑えるように制御する．また，MPPT 制御を実現するために使用するセンサの数をできるだけ減らすことも，電力変換器のサイズを小形化し，電力密度を上げ，コストを低減する観点から重要である．

本研究では，以上の改善方針に着眼し，具体的な実現方法として，いくつかの新しい MPPT 制御アルゴリズムを提案し，解析と実験により検証した成果をまとめたものであり，次の諸点で評価できる．

(1) バッテリー充電機能を備えた太陽光発電システムにおいて，コンバータの出力電圧が既知であることを利用して電圧センサを省き，電流センサのみを用いて実現した可変ステップ幅方式 MPPT 制御アルゴリズムを提案している．これらの制御アルゴリズムにおいて，太陽光パネルの出力電流とコンバータの時比率との関係を利用して最大電力点を求めており，ステップ幅を可変にすることにより，追従精度と追従速度の両方を向上させている．詳細な動作解析と FPGA を用いた実験により提案手法の有効性を確認している．

(2) 従来の INR をもとに，ステップ幅可変の MPPT 手法を新しく提案し，その安定性について検討している．太陽光発電システム全体の小信号モデルを導き，それをもとに安定性の理論解析を行っている．この解析結果を反映させた設計手順の妥当性を，数値計算によるシミュレーションと DSP を用いた実験により確認している．

(3) バッテリー充電機能を備えた太陽光発電システムにおいて，DC-DC 昇圧形コンバータを用い，電流センサを使わずに簡単な電圧センサのみで MPPT を実現する方法を提案している．提案した MPPT 手法によりシミュレーションを行い，DSP を使ってインダクタ電流不連続モードで動作する DC-DC 昇圧形コンバータを試作し，提案手法が動特性も定常特性も良好であることを示している．

以上要するに，本論文は，太陽光発電システムに用いられる最大電力点追従制御において，追従精度と追従速度の向上，センサ数の低減の観点から改良を加えた新しいディジタル制御アルゴリズムを提案し，解析と実験により，それらの有効性を示したものであり，電気電子工学に寄与するところが大きい．よって，本論文は博士（学術）の学位論文に値するものと認める．

氏　　名	阮　　娜
学位記番号	シ情　博甲第 487 号（工学）
学位授与の日付	平成 24 年 10 月 31 日
学位論文題名	Design and Analysis of Key Management and Authentication in

Wireless Sensor Network and Vehicular Ad-hoc Network
（無線センサーネットワークと車両アドホックネットワークにおける鍵管理と認証方式の設計と解析）

論文調査委員
（主 査） 九州大学 准教授 堀 良彰
（副 査） 〃 教 授 櫻井幸一
〃 〃 〃 古川 浩

論 文 内 容 の 要 旨

Wireless communication plays an important role in these days in the sector of telecommunication and has huge importance for future research. There has been an exponential growth in wireless communication due to the development of different devices and applications. In addition, there is an explosive increase in integration and convergence of different heterogonous wireless networks to ensure effective and efficient communication. These technologies primarily equal to Wireless ad hoc networks, which include mobile ad-hoc networks (MANETs), wireless mesh networks (WMNs) and wireless sensor networks (WSNs). Specially, the development of Vehicular Ad-Hoc Networks (VANETs) is growing fast recent years. VANET is a technology that uses moving cars as nodes in a network to create a mobile network. We can understand VANETs as subset of MANET.

Since many WSN and VANET will be deployed in critical applications, security is essential. Unfortunately, security may be the most difficult problem to solve in ad-hoc networks. It is the most important motivation for us to do some study on the security protocols in both WSN and VANET.

Specifically, this dissertation is organized as follows:

Chapter 1 presents the background and motivation of this research. We also summarize our main works and contributions in this chapter.

Chapter 2 makes a quick review of existing security problems in wireless ad hoc networks. In this process, we discuss the merits and demerits of each special wireless ad hoc network. Also illustrate why choose to study key management schemes and authentication Protocols in WSN and VANET. Before use Analytic Hierarchy Process (AHP) in chapter 3, we introduce it in this chapter as preliminaries.

Chapter 3 studies a method for the evaluation of Key Management Schemes (KMs) in WSNs. Wireless sensor networks (WSNs) have been widely used in various applications. Since their sensor nodes are resource-constrained and their security primitives need to store a set of security credentials to share a secure channel, key management is one of the most challenging issues in the design of WSN. Currently, various efficient lightweight key management schemes (KMs) have been proposed to enable encryption and authentication in WSN for different application scenarios. According to different requirements, it is important to select the trustworthy key management schemes in a WSN for setting up a fully appropriated WSN mechanism. In this context, adaptive methods are required to evaluate those schemes. This is one motivation of our work. Our proposal is Analytic Hierarchy Process aided. Comparisons between different case studies are provided. We exploit Analytic Hierarchy Process (AHP) to help with the complex decision. Specifically, we consider the following performance criteria: scalability, key connectivity, resilience, storage overhead, processing overhead and communication overhead. Two case studies are added for verifying our proposal. Via the two case studies, it is verified that our method can help selecting a suitable scheme for given requirements.

In addition, we use the proposed method to analyze characteristics of KMs in WSNs. Under given network scenarios, we enumerate all permutations for the importance scale of preference on the criteria. To achieve security for wireless sensor networks (WSNs), key management is one of the most challenging issues in design of WSN due to resource constrained sensor nodes. Various key management schemes (KMs) have been proposed to enable encryption and authentication in WSN for different application scenarios. We analyze the characters of abundant KMs intuitively. Experimental analyses on 43 exits KMs are presented, as all permutations of the five criteria which include 120 types' situations. During the analysis of all kinds of the situations, some interesting conclusions are extracted.

Chapter 4 studies Elliptic Curve ElGamal Threshold-based Key Management scheme against Compromise of Distributed RSUs for Vehicular Ad Hoc Networks (VANETs). In VANETs, the vehicular scenario requires smart signaling, smart road maintenance and other services. A brand new security issue is that the semi-trusted Road Side Units (RSUs) may be compromised. In this chapter, we propose an Elliptic curve ElGamal Threshold system based key management scheme for safeguarding VANET from the compromised RSUs and their collusion with the malicious vehicles. We analyze the packet loss tolerance for security performance demonstration, followed by a discussion on the threshold. After discussion of the feasibility on privacy and processing time, overhead analysis is presented in terms of two types of application scenarios: Emergency Braking

Notification (EBN) and Decentralized Floating Car Data (DFCD). Our method can promote security with low overhead in EBN and does not increase overhead in DFCD during the security promotion.

Chapter 5 studies DoS attack-tolerant TESLA-based broadcast authentication protocol in Internet of Things. The Internet of Things (IoTs) is an emerging concept referring to networked everyday objects that interconnect to each other via wireless sensors attached to them. TESLA is a source authentication protocol for the broadcast network. Scalability of TESLA is limited by its unicast-based initial parameter distribution. Low energy consumption version of TESLA is μTESLA, which is designed for wireless sensor network (WSN), while cannot tolerate DoS attack. TESLA++ is the DoS-tolerant version and is designed for VANET. TESLA++ cannot be accepted by WSN because of its higher power consumption. To realize secure and robust DoS attack in the hybrid-vehicle-sensor network, we provide a TESLA-based protocol against DoS attack with lower power consumption. Analysis results demonstrate that using our protocol is better than using μTESLA or TELSA++, individually.

Chapter 6 concludes the results of this research, and discusses some future works.

論 文 調 査 の 要 旨

無線アドホックネットワークは，動的にネットワークを構成する手法であり，接続する対象に応じて無線センサーネットワークや車両アドホックネットワークに分類できる．センサーと車両を接続することで，路面情報を車両に伝達し適切な制御を行う新たな応用が期待できる．これらのネットワークにおけるセキュリティ機能の実現は，社会基盤を構築する際の重要な要件となっている．無線通信は，有線通信よりも外的要因による伝送路品質への悪影響を受け易いことから，セキュリティ機能の実現にあたっても，それを考慮したプロトコル設計を行う必要がある．

本論文は，無線センサーネットワークと車載ネットワークにおいて暗号鍵を適切に共有するための鍵管理機能および認証機能の設計と評価について論じている．無線ネットワーク上で適切に動作するセキュリティ機能の設計には，通信路特性を前提に安全性要件を満たす必要がある．著者は，無線センサーネットワークにおける暗号鍵管理手法の特性評価，安全な車両間通信を実現するための分散型無線基地局（RSU：Road Side Unit）と車両間の暗号プロトコル，サービス不能（DoS：Denial of service）攻撃耐性と省電力性を同時に実現する一対多通信認証方式の設計を論じた．これらは，無線センサーネットワークと車両ネットワークにおける鍵管理および認証に関する３つの課題を解決したもので，以下の点で評価できる．

第一に，無線センサーネットワークにおける鍵管理プロトコルの特性評価を行った．低速な計算資源，低メモリ資源さらに低電力性が要求される無線センサーネットワーク用の暗号鍵管理プロトコルは，数十種類もの方式が考案されている．実ネットワークへの適用にあたっては，多数の候補から，センサーノードの計算資源，無線伝送路の通信品質，セキュリティ等の要件を満たす度合を比較し，目的とする特定の応用に対して最も適切な方式を選択することが課題である．この課題解決のため，Sally によって提唱されている階層分析法を鍵管理プロトコルに適用することで，鍵管理プロトコルが有する複数特性の重要度に従った重み値から導出される総合評価値に着目した．著者は，鍵管理プロトコルが有する各特性間の重要度に，すべての組み合わせを与えることにより導出される総合評価値の比較により，高評価値を得る際の組合せを分析し適切な鍵管理プロトコルの選択手法を与えた．さらに，実環境における応用を想定した条件下で，43 種類の鍵管理プロトコルの比較に本手法を適用した．その結果，センサーネットワーク用に設計された一対多認証方式μTESLA を用いた鍵管理プロトコルが適していることを示した．

第二に，安全な車両間通信を実現する分散型 RSU と車両間の暗号プロトコルを設計した．安全な車両間通信を実現するためには，道路脇で設置され車両間通信を仲介する装置である無線基地局（RSU）の安全性の担保が課題である．従来，安全な車両間通信実現のため RSU の仲介による方式が研究されているが，単一装置によるパケット損失と装置への攻撃が課題である．著者は，パケット損失耐性と RSU への攻撃耐性を併せ持つ，秘密分散法を適用した分散 RSU と車両間の暗号プロトコルを設計し，過半数に満たない数の分散 RSU が攻撃された場合でもシステムとして耐性を有することを示した．さらに，計算機シミュレーション下で，分散 RSU 数および秘密分散閾値と通信成功率を導出し，パケットロス率が 0.3 であっても 15 台の分散 RSU を用い秘密分散閾値を 6 に設定することで，99%の通信成功率を達成できることを明らかにした．

第三に，DoS 攻撃耐性と省電力性を同時に実現する一対多通信における認証方式を設計した．センサーネットワークと車両ネットワークとの統合ネットワークは，センサーと車両の通信基盤である．単一の始点から多数の終点への一対多通信におけるメッセージ認証手法には，従来，検証情報をパケット毎に付加する DoS 攻撃耐性を高めた手法，ハッシュ連鎖に基づく認証情報により検証情報を送出しない低消費電力性を有する手法が提案されている．検証用メッセージをパケット毎に付加する手法は検証情報増を招く一方で，単一ハッシュ連鎖を用いる手法は DoS 攻撃に脆弱であることから，DoS 攻撃耐性と低消費電力性を両立させることが課題である．著者は，第一のハッシュ連鎖から生成される第二のハッシュ連鎖による認証情報生成に

より，検証情報を削減可能な DoS 攻撃耐性と低消費電力性を有する一対多認証手法を設計しその評価を行った．本手法は，記憶域消費型と計算資源消費型の両方の DoS 攻撃耐性を有する．さらに，数値解析により，受信バッファ数と認証のために必要なバンド幅の関係を導出した．

以上要するに，本論文は，無線センサーネットワークと車両アドホックネットワークにおける暗号鍵管理と認証方式の設計および安全性と性能を解析したものであり，情報工学上寄与するところが大きい．よって本論文は，博士（工学）の学位論文に値すると認める．