科学研究費助成事業　　研究成果報告書

平成　２６　年　　６　月　　６　日現在

機関番号：　１７１０２
研究種目：　若手研究(B)
研究期間：　2011～2013
課題番号：　２３７０００１９

研究課題名（和文）有限時間ビザンチン故障に対する耐故障分散アルゴリズムに関する研究

研究課題名（英文）A study on fault tolerant distributed algorithms for time-bounded Byzantine faults

研究代表者
山内　由紀子（YAMAUCHI, Yukiko）

九州大学・システム情報科学研究科（研究院・助教

研究者番号：１０５４６５１８

交付決定額（研究期間全体）：（直接経費）　　3,300,000円、（間接経費）　　990,000円

研究成果の概要（和文）：大規模分散システムの安定的な運用を実現するためには，計算機の故障に対して頑健性を保証する分散アルゴリズムが必要である．本研究では，従来の一時故障と永久ビザンチン故障に対し，両者の中間に位置する故障に着目し，自己安定アルゴリズム等の耐故障分散アルゴリズム設計手法の拡張，新しい設計手法の提案を目標とした．研究期間内には移動ビザンチン故障に着目し，合意問題を解く分散アルゴリズムを得た．また，期待収束時間に関して性能保証を持つ確率的自己安定アルゴリズムの設計手法や，個体群プロトコルモデルにおけるリーダー選挙問題のメモリ複雑度の解明など，自己安定アルゴリズムの設計手法に関する成果を多数得た．

研究成果の概要（英文）：Large-scale distributed systems require distributed algorithms that guarantee tolerance against faults at processes. We aim to propose a new fault model in between the transient fault model and the permanent Byzantine fault model, and extend existing design schemes for fault tolerant distributed algorithms, such as self-stabilization. We focused on the mobile Byzantine fault model, and we obtained distributed algorithms for the mobile Byzantine agreement problem. Additionally, we obtained results about design of self-stabilizing algorithms, such as probabilistically stabilizing algorithms with bounded expected stabilization time, memory complexity of the leader election problem in the population protocol model.

研究分野：　総合領域

科研費の分科・細目：　情報学・情報学基礎

キーワード：　分散アルゴリズム　ビザンチン故障　一時故障　自己安定アルゴリズム

１．研究開始当初の背景

インターネット，無線センサネットワーク，モバイルアドホックネットワーク等の普及に伴い，大規模な分散システムを安定的に運用する手法が必要とされている．このような大規模分散システムでは，スケーラビリティのために集中型の制御手法は困難であり，分散型の制御手法が必要とされている．さらに，個々の計算機の故障や参加，移動，離脱といった状況変化に対して計算機ネットワークが自動的に対応し，人間の介入なくシステムの長期運用が可能となるような，高度な頑健性，自律適応性が期待されている．

耐故障分散アルゴリズムは既に多くの研究が行われており，メモリのソフトエラー等を考慮した一時故障に対してシステムが自動的に復旧することを保証する自己安定アルゴリズム，アルゴリズムにかかわらず任意の振る舞いをする永久ビザンチン故障に対する耐ビザンチン故障アルゴリズムなどが提案されている．しかし，対極的な一時故障と永久ビザンチン故障に対し，中間的な故障モデルの研究は十分に行われていない．本研究では，有限時間ビザンチン故障などの一時故障と永久ビザンチン故障の中間に位置する故障モデルに対し，新しい耐故障分散アルゴリズムの設計手法を提案することを目標とする．

２．研究の目的

本研究の目的は，有限時間ビザンチン故障のような，一時故障と永久ビザンチン故障の中間に位置する故障モデルに対して，以下の 3 点を明らかにすることである．

(1)故障耐性の理論的限界（故障数，通信複雑性，時間複雑性）
(2)分散アルゴリズムの設計手法
(3)乱択化による高速化等の可能性

３．研究の方法

本研究では，分散システム内での情報伝搬に着目する．分散システムでは，各計算機はシステム全体の状況を把握できず，通信リンクで接続された計算機どうしが局所的に情報交換を行うことで協調動作を実現する．たとえば，一時故障に対する故障耐性を有する自己安定アルゴリズムは，各計算機が絶えず通信を行うことで，任意の数の一時故障からの自動的な復旧を実現している．しかし，永久ビザンチン故障は虚偽の通信を繰り返す可能性がある．さらに他の計算機が故障計算機を特定することは難しいため，故障計算機からの情報がシステム全体に伝搬し，分散システム全体での協調動作が実現できない可能性がある．

永久ビザンチン故障の振る舞いを定数時間に限定した有限時間ビザンチン故障に対しては，情報伝搬を遅延させることで，自己安定性，故障の影響の伝搬抑制を実現する手法が提案されている(Yamauchi ら, SSS 2001)．しかし，このような手法では計算時間が増大してしまう．本研究では，効率的に計算を行いながら，有限時間ビザンチン故障などの影響を抑制するための情報伝搬手法に着目し，2 に挙げた 3 つの研究目的を達成する．

４．研究成果

本研究では，ネットワーク中を移動する移動ビザンチン故障モデルに着目した．この故障モデルは，ネットワーク内をビザンチン故障エージェントが移動し，故障エージェントが滞在する計算機が任意の振る舞いを行う．移動ビザンチン故障は，計画段階で着目していた有限時間ビザンチン故障とは異なるが，各計算機にとっては一時的なビザンチン故障に相当し，さらに，エージェントが離脱した後の計算機の状態回復という，従来の永久ビザンチン故障モデルにはない難しさを備えている．研究期間内には分散システムの最も基本的な問題のひとつである合意問題に取り組み，一般のネットワーク上での移動ビザンチン合意問題を解くための必要条件，また，高信頼伝送アルゴリズムをもとにした合意アルゴリズムを得た．

また，耐故障分散アルゴリズムの乱択化については，弱自己安定アルゴリズムの乱択化によって得られる確率的自己安定アルゴリズムの期待収束時間を保証する手法を得た．さらに，研究期間内には自己安定アルゴリズムの性能限界，設計手法に関する多数の結果を得た．

研究目的(1)，(2)に対しては，移動ビザンチン故障に対する成果(1)によって達成されている．この成果をもとに研究目的(3)の成果を得られるよう取り組んでいたが，移動ビザンチン故障に対する研究目的(3)の達成には至らなかった．　本研究の結果をもとに，今後も継続的に研究を行うことが必要である．

1)一般のネットワーク上での移動ビザンチン合意問題

分散システム内の計算機が合意を形成する問題を合意問題と呼ぶ．故障がない分散システムでの合意問題は過半数計算などで解決できるが，永久ビザンチン故障が存在する分散システムでは合意形成は容易ではない．

本研究では，Garay が提案した移動ビザンチン故障(Garay, WDAG 1994)に着目し，合意問題を解くための故障計算機数の上限，通信ネットワークの形状に対する十分条件を示した．永久ビザンチン故障については，分散システム中の計算機数 n に対し，故障計算機数 $t<n/3$ とネットワーク連結度 $d>2t$ が合意問題を解く必要十分条件である(Dolev, J. of Algorithms, 1982)．学会発表①では，移動ビザンチン故障が永久ビザンチン故障を模倣できることをもとに，$6t<n$ が合意形成の必要条件であることを示した．さらに，完全 k 部グラフや，直径が短く点疎パスを多数含

む一部のネットワーク上で正常プロセス間が情報伝搬を行うための高信頼伝送アルゴリズムを提案し，このアルゴリズムをもとに移動ビザンチン合意アルゴリズムを得た．

2)確率的自己安定アルゴリズムの性能保証

分散アルゴリズムの実行は，各計算機の動作タイミングや通信遅延により，同一の初期状況から計算を開始しても一意には決まらない．自己安定アルゴリズムは任意の初期状況から始まる任意の実行で，分散システムがやがて目的の状況へ到達（収束）することを保証する．一方，弱自己安定アルゴリズムは，任意の初期状況に対して，収束する実行が少なくとも１つ存在することを保証する．

このように，弱自己安定アルゴリズムは分散システムが必ず目的の状況へ到達することは保障しないが，弱自己安定アルゴリズムを乱択化すれば，確率１で収束する確率的自己安定アルゴリズムに変換でき，より強力な故障耐性を保証できる(Gouda，WSS 2001)．しかし，このようにして得られた確率的自己安定アルゴリズムの収束時間の期待値が有限になることは，任意のアドバーサリに対しては保証できない．

学会発表⑪では，乱択化した場合に期待収束時間が有限となるための，弱自己安定アルゴリズムの構造の必要十分条件を示した．

3)個体群プロトコルモデルにおけるリーダー選挙問題のメモリ複雑度

個体群プロトコルモデルとは，匿名なエージェント群から成る分散計算モデルである．各エージェントは状態機械であり，2 個のエージェントがインタラクションを行うことで，互いの状態を変更し，個体群全体の計算が進行する．個体群の代表となるエージェント，つまりリーダーを計算するリーダー選挙問題を解くには，個体群内のエージェント数 n に対し，個々のエージェントが n 状態を必要とすることが知られている(Cai ら, Theor. of Comput. Sys. 2012)．

学会発表⑦では，k 個のエージェント間でインタラクションを行う拡張個体群プロトコルモデルを提案し，このような個体群プロトコルモデルでは，エージェントの状態数を (n-1)/(k-1)+1 に削減できることを示した．

4)全域木の変換問題

あるグラフ上の 2 つの全域木に対し，辺の交換を繰り返しながら一方の全域木から他方の全域木までをつなぐ全域木の系列を求める問題を全域木の変換問題と言う．通信グラフ上の全域木を使えば，効率の良い放送，情報収集が可能となるため，全域木を構成する多数の分散アルゴリズムが提案されている．モバイルアドホックネットワーク等の動的なネットワークでは，ネットワーク形状の変化に従い，通信バックボーンとしての全域木を再構成することが必要であるが，分散システムでの全域木の変換問題については現在まで研究が行われていない．

マトロイドの基交換公理より，逐次的な環境では全域木の変換問題は容易に計算できる．しかし，基交換公理は異なる頂点に接続する辺の追加，削除を許すため，分散環境には適用できない．学会発表⑭では，同一頂点に接続する辺の削除，追加に限定しても，全域木の変換問題は解くことができ，更に容易に分散環境に適用できることを示した．

5)自律移動ロボット群のパターン形成

観測，計算，移動を自律的に行うロボット群の分散制御において，もっとも基本的な問題は，与えられた目的パターンにロボットを配置するパターン形成問題である．ロボットの動作タイミング(同期性)，メモリの有無，視界などによりロボット群の持つ計算能力は異なることが予想されるが，パターン形成問題については，一点集合を除けば，完全同期，半同期モデルにおいて，メモリの有無にかかわらず同等なパターン形成能力を持つことが知られている(Suzuki ら， SIAM J. of Compt. 1999)．特に，メモリを持たないロボット群の分散制御アルゴリズムは自己安定性を持つため，従来から多数の研究が行われてきた．

学会発表⑩では非同期モデルにおいても，ロボット群が完全同期・メモリなしロボットとほぼ同等のパターン形成能力を持つことを示した．

５．主な発表論文等

（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 2 件）

① Yukiko Yamauchi, A survey on pattern formation of autonomous mobile robots: asynchrony, obliviousness and visibility, *Journal of Physics: Conference Series*, Vol.473, 012016, Dec. 2013. (査読有り)

② Yuichi Sudo, Junya Nakamura, Yukiko Yamauchi, Fukuhito Ooshita, Hirotsugu Kakugawa, and Toshimitsu Masuzawa, Loosely-stabilizing leader election in population protocol model, *Theoretical Computer Science*, Vol.444, pp.100--112, July 2012.（査読有り）

〔学会発表〕（計 17 件）

① Toru Sasaki, Mobile Byzantine agreement on arbitrary network, Proceedings of the 17th International Conference on Principles of

Distributed Systems (OPODIS 2013), pp.236--250 (Springer 2013, LNCS 8304), Nice, France, Dec.16-18, 2013. (Dec.16, 2013)

② Sayaka Kamei, An asynchronous self-stabilizing 6-approximation for the minimum connected dominating set with safe convergence, Proceedings of the 15th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2013), pp.251--265 (Springer 2013, LNCS 8255), Osaka, Japan, Nov.16-18, 2013. (Nov.16, 2013)

③ **佐々木徹, 移動ビザンチン合意アルゴリズムのための高信頼性伝送アルゴリズム, 2013 年度 冬の LA シンポジウム, 京都大学数理解析研究所, 2014 年 1 月 28 日-30 日.** (2014 年 1 月 29 日)

④ Yukiko Yamauchi, A survey on pattern formation by mobile robots: asynchrony, obliviousness, and visibility, ELC International Meeting on Inference, Computation, and Spin Glasses (ICSG2013), Sapporo University, Sapporo, Japan, July 28-30, 2013. (July 30, 2013)

⑤ **松川理拓, トップダウンな回転手法を用いたスプレー木の実験的性能評価, 平成 25 年度（第 66 回）電気関係学会九州支部連合大会, 熊本大学, 2013 年 9 月 24-25 日.** (2013 年 9 月 25 日)

⑥ **佐々木徹, 一般のネットワーク上の移動ビザンチン合意問題について, 第 143 回アルゴリズム研究会,** 1-8, **飯坂温泉伊勢谷.** (2013 年 3 月 1 日)

⑦ Xiaoguang Xu, On space complexity of self-stabilizing leader election in population protocol based on three-interaction, **第 143 回アルゴリズム研究会, 飯坂温泉伊勢谷.**（2013 年 3 月 1 日）

⑧ **山内由紀子, ビザンチン故障と分散制御, 最適化ワークショップ：拡がっていく最適化, 九州大学マス・フォア・インダストリ研究所主催, 九州大学, 福岡,** 2013 年 2 月 18 日-19 日.（2013 年 2 月 19 日）

⑨ Yukiko Yamauchi, Mobile agent rendezvous on a probabilistic edge evolving ring, Proceedings of the 3rd International Conference on Networking and Computing (ICNC 2012), pp.103--112, Okinawa, Japan, Dec.5-7, 2012. (Dec.5, 2012)

⑩ Nao Fujinaga, Asynchronous pattern formation by anonymous oblivious mobile robots, Proceedings of the 26th International Symposium on Distributed Computing (DISC 2012), pp.312--325 (Springer 2012, LNCS 7611), Salvador, Brazil, Oct.16-18, 2012. (Oct.18, 2012)

⑪ Yukiko Yamauchi, Brief announcement: Probabilistic stabilization under probabilistic schedulers, Proceedings of the 26th International Symposium on Distributed Computing (DISC 2012), pp.413--414 (Springer 2012, LNCS 7611), Salvador, Brazil, Oct.16-18, 2012. (Oct.18, 2012)

⑫ Tomoko Izumi, Brief announcement: Mobile agent rendezvous on edge evolving rings, Proceedings of the 14th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2012), pp.92--94(Springer 2012, LNCS 7596), Toronto, Canada, Oct.1-4, 2012. (Oct.2, 2012)

⑬ **佐々木徹, 完全 k 部グラフにおける移動ビザンチン合意問題アルゴリズムの提案, 平成 24 年度（第 65 回）電気関係学会九州支部連合大会, 長崎大学.** (2012 年 9 月 24 日)

⑭ **山内由紀子**, Transitivity in distributed systems using exchange property of matroid bases, **2012 年度 夏の LA シンポジウム, 宮津ロイヤルホテル**(2012 年 7 月 17-19 日). （2012 年 7 月 18 日）

⑮ Yukiko Yamauchi, Design and communication complexity of self-stabilizing protocols resilient to Byzantine faults, Proceedings of the 2nd International Conference on Networking and Computing (ICNC 2011), Workshop on Frontiers of Distributed Computing, pp.372--379, Osaka, Japan, Nov.30-Dec.2, 2011. (Dec. 1st, 2011).

⑯ **山内由紀子, 確率的スケジューラの下での確率的自己安定, 2011 年度 冬の LA シンポジウム,京都大学数理解析研究所**(2012 年 1 月 30 日-2 月 1 日). (2012 年 1 月 31 日)

⑰ **山内由紀子, 悪意あるユーザ存在下での自律復旧型ネットワーク, 日本オペレーションズ・リサーチ学会九州支部 平成 23 年度第 1 回講演・研究会, 福岡.** (2011 年 7 月 23 日)

〔図書〕（計 0 件）

〔産業財産権〕
○出願状況（計 0 件）

名称：
発明者：
権利者：

種類：
番号：
出願年月日：
国内外の別：

○取得状況（計　0　件）

名称：
発明者：
権利者：
種類：
番号：
取得年月日：
国内外の別：

〔その他〕
該当なし

６．研究組織
(1)研究代表者
山内由紀子（YAMAUCHI, Yukiko）
九州大学大学院システム情報科学研究院
研究者番号：10546518

(2)研究分担者
該当なし

(3)連携研究者
該当なし