様式 C-19

科学研究費補助金研究成果報告書

平成２３年　６月　１６日現在

機関番号：１３３０２
研究種目：基盤研究（C）
研究期間：2008 ～ 2010
課題番号：２０５０００３０
研究課題名（和文）リアルタイムソフトウェアのコンポジショナルな処理モデルとその構造検証
研究課題名（英文）Compositional models and its structural verification of real time software
研究代表者　小川　瑞史（OGAWA MIZUHITO）
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：40362024

研究成果の概要（和文）：本研究では、ソフトリアルタイムソフトウェア構造検証のモデル化の基礎として、プッシュダウンモデル検査の拡張・スケーラビリティ確保・およびそのツール実装を行った（雑誌論文 1，学会発表 1～3)。さらにアクセス制御の非同期多段処理の実験・ケーススタディとして、同期処理による限界を示し、web サーバにおけるセキュリティ制御やセキュリティプロトコルについて各個別なモデル化と検証手法を示した。(学会発表 4～8)。

研究成果の概要（英文）：Aiming compositional verification of soft real time software, as foundation of modeling, extensions, algorithms for scalability, and tool implementation of pushdown model checking are shown (Journal 1, Oral presentation 1~3). As an experiment and case studies of asynchronous multi stage processing, their modeling and formal verification methodology on security access control and protocols on a web server are investigated (Oral presentation 4~8).

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
２００８年度	1,500,000	450,000	1,950,000
２００９年度	1,000,000	300,000	1,300,000
２０１０年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,500,000	1,050,000	4,550,000

研究分野：計算機科学
科研費の分科・細目：情報学・ソフトウェア
キーワード：仕様記述、仕様検証、リアルタイムソフトウェア、非同期処理、モデル検査

１．研究開始当初の背景

近年、組込みシステムなどリアルタイムソフトウェアの高信頼化にむけた形式手法が注目されている。特にマルチコア CPU 環境下での高信頼化方法論は明確ではなく、形式的モデルの構成から始めることが必要である。リアルタイムソフトウェアでは、しばしば時間を定量的にモデル化する時間オートマトンなどのモデルが取り上げられるが、厳密な実時間性をもつハードリアルタイムでは必然的に外部との柔軟なインターラクションは制限され、汎用 OS やミドルウェアなどでは必ずしも適切なモデル化ではない。本研究の背景として、明確な実時間性の要求より、外部との柔軟なインターラクションが重視するソフトウェアリアルタイムを対象とした柔軟で検証しやすい定性的なモデルの探求を想定した。

２．研究の目的

本研究では、応答性と信頼性を両立させたソフトリアルタイムソフトウェアの多階層コンテキスト非同期処理モデルを定式化し、リアルタイムソフトウェアにおけるデザイン

上の選択とその必然的帰結を分離、さらに理論的制約条件や設計・実装デザインを明らかにすることを目的とした。その際、モデルはプッシュダウン状態遷移モデルを出発点とし、理論的基礎となるモデルの拡張および自動検査のスケーラビリティの拡張に焦点をあてた。さらに、実用面からはケーススタディを通じて妥当なモデル化の検討に焦点をあてた。

３．研究の方法

リアルタイムソフトウェア構造検証の基礎技術として、プッシュダウンモデル検査の実時間制約等の拡張、ならびにスケーラビリティ確保のための新たなアルゴリズム、およびそのツール実装など、理論的基礎を含む基礎技術については、研究代表者が中心となり、研究を進めた。

またフトリアルタイムソフトウェア構造検証のためのアクセス制御の非同期処理および多段処理のケースタディとして、web サーバにおけるセキュリティ制御を取り上げ、同期処理による限界を確認する実験、web サーバにおけるセキュリティ制御やセキュリティプロトコルについて各個別なモデル化と検証手法について、研究分担者が中心となり研究を進めた。

４．研究成果

プッシュダウンモデル検査の決定可能性を保つ拡張として、実時間制約（event-clock visually pushdown automata）および言語クラスの拡張（superdeterministic pushdown automata）を明らかにした。さらに条件付状態遷(conditional weighted pushdown model checking）を提案し、そのプッシュダウンモデル検査の決定可能性を示した。最終年度にスケーラビリティ確保のための新たなインクリメンタルアルゴリズムの提案およびそのツール実装を行った。

アクセス制御の非同期処理および多段処理のケースタディとして、クラウド環境下における web サーバにおけるセキュリティ制御を取り上げ、モデル化と形式検証法を各個別に提案した。

H20 年度には、研究代表者（小川）はリアルタイムソフトウェアの構造検証のための基礎技術として、プッシュダウンモデル検査の実時間制約への拡張（学会発表 3)、ならびに決定可能性の拡張（雑誌論文 1)、およびそのツールによる実装について研究を進めた。具体的には、プッシュダウンオートマトンの包含関係の成り立つ部分クラス（一般の場合は決定不能であることが知られている）を調査し、あるクラスについて実時間制約を扱えるよう拡張をしめした。また、その応用としてセキュリティプロトコル解析を取り上げ、検証ツール Maude によりプッシュダウンモデル検査の原理を用いた実装を行い、有効性をしめした。(学会発表 4)

研究分担者（小野）はソフトリアルタイムソフトウェアの構想検証のための非同期処理のケースタディとして、web サーバを取り上げ、並列処理環境と組合せ高いスケーラビリティを持つバシステムを構成する方式の検討を行った。具体的には 代表的な Web サーバである Apache サーバを分析し、従来の複数スレッドによる同期的処理（モノリシックな実装方法）の問題点を示した。そして、要求処理を性質の異なる複数フェーズに分解し、フェーズごとに適切な並列度をもつ非同期処理モジュールとして実装し、それらのモジュール相互を非同期キューで接続して構成するフェーズドアプローチモデルを提案し、IOCP を用いた実装方法を検討した。（学会発表 3)

H21 年度は、研究代表者（小川）はリアルタイムソフトウェアの構造検証のための基礎技術として、(重み付）プッシュダウンモデル検査のスケーラビリティのためのインクリメンタルアルゴリズム（学会発表 2 ）、文脈についての条件記述の拡張(学会発表 1)について研究を進めた。前者はモデル検査の手法でしばしば問題になるメモリオーヴァーフローなどを抑制するのに大きな効果がある。ここでは、ケーススタディとして、Java の文脈依存 points-to 解析を取り上げ、現状で 20 万行程度（2 万メソッド程度）のスケーラビリティを得ている。これらはシングルスレッドであるが、現在、マルチスレッドへの拡張（ナイーブに行うと決定不能問題）として relational な抽象化のアプローチや、実行列の制限によるアプローチを検討中である。

研究分担者（小野）はソフトリアルタイムソフトウェアの構想検証のための非同期処理のケースタディとして、web サーバを取り上げ、並列処理環境における非同期処理の高いスケーラビリティの実証と、同期処理におけるボトルネックを明示する実験を行った。具体的には、代表的な Web サーバである Apache サーバに対し、同期的処理（モノリシックな実装方法）ならびに非同期処理による応答処理を実装し、過負荷試験による応答速度低下の測定実験を行った。さらに web アプリケーションにおけるロール（セキュリティレベル）に応じたアクセス制御モデルを構築し、複数のアクセスが競合する環境下における Spin を用いた形式検証手法のケーススタディを進めた。(学会発表 7)

H22 年度は、研究代表者（小川）はリアルタイムソフトウェア構造検証のための基礎技術として、

１．重み付プッシュダウンモデル検査の漸増

的アルゴリズム、
２．シングル CPU 上のマルチスレッドの割込み処理モデル化について研究を進めた。
前者はモデル検査の手法で問題になるメモリオーヴァーフローの抑制に大きな効果がある。漸増的アルゴリズムのアイデア・実装は昨年度に既に得ていたが、漸増的収束判定の正しさについて確信が得られなかった。今年度は数学的証明を与え、実装上のバグと思われていた不整合が本質的なバグであったことを示した。(学会発表準備中) 後者は割込み処理の時間制約モデル記述として controller automaton に注目し、時間制約を非対角制約に制限した場合の時間プッシュダウンオートマトンへの変換可能性を発見し、現在、その正しさの証明および実装を含めた検討を進めている。
研究分担者（小野）はソフトリアルタイムソフトウェア構想検証のためのアクセス制御の非同期処理および多段処理のケーススタディとして、クラウド環境下における web サーバを取り上げ、１． web アプリケーションにおけるロール（セキュリティレベル）に応じたアクセス制御モデルの構築と、アクセス競合環境下におけるモデル検査形 Spin を用いた形式検証手法（学会発表 6)、２．クラウドコンピューティング環境において重要視されるアクセス制御の多段委任可能な SPKI という認証方式によるネットワーク間相互接続を行うための分散型オンデマンド仮想システム構築法（学会発表 5）についてケーススタディを行った。
ソフトリアルタイムシステムにおける、適切な多階層コンテキスト非同期処理モデルの設定は困難な課題であり、プッシュダウンモデル検査を基本としたアプローチをとったが、いまだ十分な解決を得たとは言いがたい。しかしながら、Microsoft の SLAM プロジェクトにおける Windows device driver の検証などはプッシュダウンモデル検査器などを用いて行われたときいており、このようなケーススタディを積み重ねて、実用上妥当なモデルに近づけていくことが必要である。現在、車載リアルタイムシステムの割り込み制御に関するモデル化として controller automata に注目し、そのプッシュダウン遷移モデルへの帰着可能性について注目しており、今回、十分に進めることのできなかった変換規約違反などの自動検証法について研究を進める予定である。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）
〔雑誌論文〕（計１件、うち査読付１件）
1. Nguyen Van Tang, Mizuhito Ogawa, Alternate Stacking Technique Revisited: Inclusion Problem of Superdeterministic Pushdown Automata, IPSJ Transactions on Programming Vol.1, 2008 （査読付）

〔学会発表〕（計８件、うち査読付４件）
1. Xin Li, Mizuhito Ogawa, Conditional Weighted Pushdown Systems and Applications, ACM SIGPLAN 2010 Workshop on Partial Evaluation and Program Manipulation (PEPM10), 2010 年 1 月 19 日, マドリッド. pp.141-150.
2. Xin Li, Mizuhito Ogawa, Stacking-based Context-Sensitive Points-to Analysis for Java, Haifa Verification Conference 2009 (HVC09), 2009 年 10 月 20 日, イスラエル. Springer LNCS 6405, pp.133-149.
3. Nguyen Van Tang, Mizuhito Ogawa, Event-Clock Visibly Pushdown Automata, 35th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM09)2009年1月27日,チェコ. Springer LNCS5404, pp.558-569.
4. Guoqiang Li, Mizuhito Ogawa, Authentication Revisited: Flaw or Not, the Recursive Authentication Protocol, 6th International Symposium on Automated Technology for Verification and Analysis (ATVA08) 2008年10月21日, 韓国. Springer LNCS 5311, pp.374-385.
（以上、査読付国際会議）

5. 濱田惇司、小野諭、分散型オンデマンド仮想システム構築法の提案、電子情報通信学会・インターネットアーキテクチャ研究会、2011 年 2 月 18 日、東京
6. 越智通宣、小野諭、機能ロールに基づいた動的職責分離の形式的検証手法, 電子情報通信学会・情報セキュリティ研究会, 2010 年 5 月 21 日、東京
7. 越智通宣、小野諭、動的職責分離を記述できるアクセス制御モデルの形式的検証手法、電子情報通信学会・情報セキュリティ研究会、2010 年 3 月 4 日、信州大学
8.森春紀、小野諭、スケーラブルな Web サーバ・ソフトウェア構成法の研究、電子情報通信学会・情報セキュリティ研究会 2008 年 12 月 17 日、東京
（以上、研究会報告）

〔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〕
ホームページ等

６．研究組織
(1) 研 究 代 表 者　小 川　瑞 史 （ OGAWA MIZUHITO)
北陸先端科学技術大学院大学・情報科学研究科・教授
研究者番号：40362024

(2)研究分担者　小野　諭（ONO SATOSHI）
工学院大学・情報工学部・教授
研究者番号：90407164

(3)連携研究者　なし