無限状態モデル検査を用いた高信頼性ソフトウェアの自動検証に関する研究

課題番号 18500023

平成１８年度～平成１９年度科学研究費補助金（基盤研究（C））
研究成果報告書

平成２０年５月

研究代表者　関　浩之
奈良先端科学技術大学院大学　情報科学研究科　教授

まえがき

金融オンライン、航空宇宙システム、情報セキュリティ等のミッションクリティカルと呼ばれる分野では、システムの不具合が社会に及ぼす影響が大きく、開発早期段階で不具合を発見するシステム検証技術の確立が急務となっている。特に、**モデル検査技術**は、有限状態系に対して検証の完全自動化が原理的に可能であるという特長をもつことから、理論研究から開発現場での事例研究へと実用化が進展しつつある。我々は、次の３点を目標として研究を行い、以下で述べるような成果を得た。

- 無限状態系に対するモデル検査技術について理論的考察を深める。
- その結果を利用して、特に情報セキュリティの観点から、ソフトウェア信頼性保証へのモデル検査技術の適用を検討する。
- モデル検査器の実装を通して提案手法の有効性を実証する。

(1) 再帰的プログラムのモデル検査に関する研究

我々が以前より取り組んでいる、実行履歴に基づくアクセス制御付きプログラム（HBAC プログラム）の安全性検証法において、種々の最適化を行うことにより、高速な検証が可能であることを実証した。我々のモデル検査アルゴリズムでは、検証対象のプログラムに対するモデル検査問題を、文脈自由文法(CFG)の空判定問題に帰着しており、一般にアクセス権の個数に対して指数的な検証時間を要する。そこで、CFG を構成する際、useless な規則（開始記号から到達しないか、または、終端記号列を一つも生成しない規則）の構成を防ぐ最適化法を提案した。Chinese-Wall ポリシとオンラインバンキングシステムの２つの例題について最適化の効果を実測した結果、どちらの検証例においても、最適化を行わない場合、アクセス権の数が 5 個程度までしか検証できなかったのに対し、最適化を行うことにより、前者の例ではアクセス権の数が 80 個のとき約 64 秒、後者の例では 60 個のとき約 0.01 秒で検証を行えた。

(2) 再帰的プログラムの情報フロー解析に関する研究

プログラムの実行による情報流出を解析する手法として情報フロー解析が有効である。本研究では、HBAC プログラムに対し、モデル検査に基づく新しい情報フロー解析法を提案した。提案手法を用いることにより、プログラムの実行完了時に出力の機密度(security class, SC）がどのようになるかだけでなく、「SC が τ であるような値を引数として関数 f が呼び出されたならば、いつか SC が τ' である値を引数として関数 g が呼び出される」のような、実行系列上に拡張された情報フローに関する性質を調べることができる。

また最近、自己合成法と呼ばれる情報フロー解析法が提案されている。自己合成法は従来の型推論に基づく解析法より解析精度がよいという特長をもつ。本研究では、自己合成法を一般の再帰プログラムに適用できるように拡張を行った。

(3) 実行履歴に基づくアクセス制御モデルの表現能力の比較に関する研究

Schneider のセキュリティオートマトン、Fong の狭履歴オートマトン、スタック検査、HBAC

のそれぞれをアクセス制御機構にもつプログラムクラスの表現能力を比較した。

(4) 実行履歴に基づくアスペクト折込み機能の形式モデルに関する研究

Aspect-J 等で採用されている PA (pointcut and advice) の形式モデル A-LTS を提案した。A-LTS と既存の計算モデルの表現能力を比較し、A-LTS の受理言語、決定性文脈自由言語、線形文脈自由言語のクラスはすべて互いに他を含まないことを証明した。その系として、A-LTS にはプッシュダウンシステムのモデル検査法が適用可能であることがわかった。

(3) その他

(a) 等式系と書換え系を内部に演繹系としてもつ木オートマトンの諸性質を明らかにし、XML 文書処理への応用についても考察した。

(b) 公開木戦略とよばれる信用交渉戦略 (DTS) が知られている。CFG によるモデル化を用いて DTS の計算量を明らかにし、妥当な前提条件のもとで効率良く動作する DTS 実行アルゴリズムを示した。

(c) CFG の構文解析法を応用し、相互作用をもつ RNA の２次構造予測法を提案した。

研究組織

研究代表者： 関 浩之 （奈良先端科学技術大学院大学情報科学研究科教授）

研究分担者： 高田 喜朗（高知工科大学工学部講師）

（研究協力者： 八木 勲， 王 静， 毛利 寿志）

交付決定額（配分額） （金額単位：千円）

	直接経費	間接経費	合計
平成 18 年度	1,800	0	1,800
平成 19 年度	1,600	480	2,080
総計	3,400	480	3,880

研究発表

（１） 学術論文誌

1. Isao Yagi, Yoshiaki Takata and Hiroyuki Seki: ``A Labeled Transition Model A-LTS for Histroy-based Aspect Weaving and Its Expressive Power," IEICE Transactions on Information and Systems, Vol.E90-D(5), pp.799-807, May 2007.
2. 高田喜朗, 王静, 関浩之: ``実行履歴に基づくアクセス制御の形式モデルと検証," 電子情報通信学会論文誌 D, Vol.J91-D(4), pp.847-858, April 2008.

（２） 国際会議発表

3. Jing Wang, Yoshiaki Takata and Hiroyuki Seki: ``HBAC: A Model for History-based Access Control and Its Model Checking," 11th European Symposium On Research In Computer

Security (ESORICS 2006), Hamburg, Germany, Sept. 2006, Lecture Notes in Computer Science 4189, pp.263-278.

4. Hitoshi Ohsaki and Hiroyuki Seki: ``Languages Modulo Normalization,'' 6th International Symposium on Frontiers of Combining Systems (FroCoS07), Liverpool, U.K., Sept. 2007, Lecture Notes in Artificial Intelligence 4720, pp.221-236.
5. Yoshiaki Takata and Hiroyuki Seki: ``Computational Complexity of the Disclosure Tree Strategy in Trust Negotiation,'' the 2007 International Conference on Next Era Information Networking (NEINE07), pp.323-328, China, Sept. 2007.
6. Yuki Kato, Tatsuya Akutsu and Hiroyuki Seki: ``A Grammatical Approach to RNA-RNA Interaction Prediction,'' 2007 International Symposium on Computational Models for Life Sciences (CMLS'07), pp.197-206, Gold Coast, Australia, Dec. 2007.

（３） 国内口頭発表

7. Jing Wang, Yoshiaki Takata and Hiroyuki Seki: ``An Efficient Model Checking Method for Programs with History-based Access Control,'' 電子情報通信学会技術研究報告, SS2006-38, Aug. 2006.
8. 王静, 伊藤信裕, 高田喜朗, 関浩之: ``実行履歴に基づくアクセス制御付きプログラムのモデル検査法による情報フロー解析,'' 電子情報通信学会技術研究報告, SS2006-72, Feb. 2007.
9. 王静, 高田喜朗, 関浩之: ``実行履歴に基づくアクセス制御モデルの表現能力の比較,'' 第 9 回プログラミングおよびプログラミング言語ワークショップ(PPL2007)論文集, p. 90, March 2007.
10. 王静, 伊藤信裕, 高田喜朗, 関浩之: ``HBAC プログラムのモデル検査の情報フロー解析への応用,'' 電子情報通信学会 2007 年総合大会, D-3-1, March 2007.
11. 高田喜朗, 関浩之: ``モデル検査による HBAC プログラムの情報流解析,'' 日本ソフトウェア科学会第 5 回ディペンダブルシステムワークショップ (DSW2007), pp. 17-27, July 2007.
12. Hiroyuki Seki and Yoshiaki Takata: ``Comparison of the Expressive Power of Language-based Access Control Models,'' 日本ソフトウェア科学会第 5 回ディペンダブルシステムワークショップ (DSW2007), pp. 69-73, July 2007. 改訂版：日本ソフトウェア科学会第 4 回システム検証の科学技術シンポジウム, 函館ワークショップ特別講演, Nov. 2007. http://unit.aist.go.jp/cvs/symposium/sympo-top.html
13. 伊藤信裕, 関浩之: ``自己合成法を利用した再帰プログラムの情報流解析について,'' 電子情報通信学会技術研究報告, SS2007-62, March 2008.