要 旨

履歴ベースアクセス制御プログラムに対するモデル検査の高速化法

勝山 雅彦

Java 仮想機械や共通言語ランタイム (CLR) などのプログラム実行環境にはスタック検査と呼ばれる動的アクセス制御機構が導入されている．近年，このようなアクセス制御機能を言語処理系に持たせることや，そのような機能を含むプログラムの自動検証法などの研究が広く行われている．その一例として，このスタック検査を拡張した履歴ベースアクセス制御 (HBAC) プログラムを対象とした検証技術の研究がある．その中で森田らが提案したアルゴリズムは，計算量が到達可能状態の数に比例するアルゴリズムであり，既存のプッシュダウンシステムモデル検査器を利用したものより高速化することに成功している．

しかし，このアルゴリズムは HBAC プログラム特有のアクセス権の特徴を利用して高速化したわけではない．本研究では，アクセス権の集合を表すのに二分決定図 (BDD) というデータ構造を利用することにより，HBAC プログラムの検証においてさらに高速化することを目的とする．

キーワード　モデル検査, 履歴ベースアクセス制御，二分決定図

Abstract

An Optimization Method of Model-Checking for History-Based Access Control Programs

Masahiko KATSUYAMA

Stack inspection is a runtime access control mechanism and is implemented in execution environments such as Java virtual machine and Common Language Runtime. The automatic verification of programs with such access control has been studied widely in recent years. Those studies include research of History-Based Access Control (HBAC) programs, which is an extension of stack inspection. Morita proposed a verification algorithm for HBAC programs which is faster than a tool that uses a well-known model checking tool for pushdown systems.

However, this altorithm was not optimized using the features of HBAC programs. In this thesis, we aim at the optimization of the verification of HBAC programs using Binary Decision Diagrams (BDDs).

key words Model Checking, History-Based Access Control, Binary Decision Diagrams