STSプロトコルの形式化と検証によるCafeOBJとCoqの比較

原 光太朗 (310088)

北陸先端科学技術大学院大学 情報科学研究科

2005年2月10日

キーワード: 形式手法, 検証, CafeOBJ, Coq, セキュリティプロトコル.

インターネットに代表される広域情報ネットワークの急速な普及および発展に伴い, セキュリティプロトコルを始めとした通信プロトコルの研究が広く行われている. セキュリティプロトコルは情報を暗号化し通信者間で秘密の通信を行うためのプロトコルで, 近年のネットワークセキュリティへの関心の高まりとともに盛んに考案が行われている. 交通システムや金融システムなど多くのシステムがネットワークを介して重要な情報のやり取りを行っている現在, 期待した通りの情報のやり取りが安全に行われるなどのセキュリティプロトコルの正しさを保証することの重要性が増してきている.

セキュリティプロトコルの解析と検証を行う方法としてはNSPKプロトコルの不具合が報告されたことなどから, 形式手法が有効であると考えられている. 形式手法による検証は, システムを数学的にモデル化し形式仕様の作成および仕様の検証を行う技法で, 厳密性・無矛盾性の点で優れておりシステムの高信頼性に効果が高い. このようなことから, セキュリティプロトコルの正しさを形式的に検証するための技法が広く研究され, 多くの方法が提案されている. 代表的なものに, 代数仕様言語を用いる方法, 証明支援系を用いる方法, 様相論理を用いる方法, モデル検査を用いる方法がある.

ここに一つの問題点が存在する. その問題点とは, それぞれの手法は独自の理論や論理体系に基づいており形式化や検証法は個々の形式手法に依存した特徴を持ったものになっているにも関わらず, 方法の提案や実例を扱う研究に比べその比較を扱う研究はあまり行われていないということである. その結果, 形式手法を用いる際のガイドラインがなく, 目的によって手法を使い分けたり併用したりすることができない.

そこで本研究では, セキュリティプロトコルの一つであるSTSプロトコルを例題として取り上げ, 正しさを保証する性質として安全性と信頼性を有していることを, 異なる二つの形式手法により検証する. 安全性と信頼性を示す性質として, 不正を働く主体のなりすまし等による攻撃によって誤った認証鍵の交換が行われないこと, およびプロトコルの正規の参加者である主体同士が正しく認証鍵を交換することを確かめる. また異なる二つの形式手法として, CafeOBJを用いる方法とCoqを用いる方法の二つを用いる. CafeOBJは仕様記述を主目的とした等式論理に基づく代数仕様言語である. 処理系において, 項書

き換えによる仕様の検証も行うことができる．一方 Coq は高階論理に基づく証明支援系で, 定理証明を主目的としている．その処理系である証明モードにおいて, 証明支援により検証を半自動に行うことができる．

仕様記述を行う際に必要となるシステムのモデル化には双方とも観測遷移機械 OTS (Observational Transition System) を用いる．OTS ではシステムがどのように振る舞うかを観察する．すなわち, システムに関連する値が実行に伴いどのように変化するのかを観測することで, システムのモデルを作成する．

本研究における STS プロトコルの形式手法による検証の流れを以下に示す．まず, STS プロトコルのモデルを OTS を用いて作成する．次に, 作成した STS プロトコルのモデルを CafeOBJ と Coq それぞれで記述することによって形式化し, STS プロトコルの CafeOBJ 仕様および Coq 仕様を作成する．続いて, 安全性と信頼性を表す性質を同じく CafeOBJ と Coq それぞれで記述する．最後に, その記述が正しいことを双方の処理系で示すことによって仕様の検証を行う．

本研究ではさらにこの STS プロトコルを対象とした形式手法による検証の具体例を通して, CafeOBJ と Coq 双方によるシステムの形式化および検証の手法についての比較を行う．具体的にはモデルの記述法や処理系における検証などに焦点を当て, 特徴を捉えることによって比較を行うことにより, CafeOBJ と Coq それぞれを用いる形式手法の長所・短所を明らかにする．さらに, 考察を加えることでシステムの正しさを保証することを目的とする形式手法に関しての新たな指針を示す．

本研究では比較の結果, 次のような特徴を捉えることが出来た．CafeOBJ を用いる方法は, 形式化や検証の結果の可読性が高く, 検証を容易に短時間で行える可能性のある．一方 Coq を用いる方法は, 人間による誤りを含むことなく, 検証者の意図した通りの検証を行うことができる．本研究ではこれらの特徴から, CafeOBJ を用いる形式手法はソフトウェア開発の上流工程である仕様段階の検証に用いるのに適しており, 一方の Coq を用いる形式手法は場合の数の多いシステムに対し専門家による検証を行う場合に用いるのに適しているという結論を出した．