On-the-fly Model Checking of Security Protocols

（セキュリティプロトコルにおけるオンザフライなモデル検査）

Guoqiang LI
北陸先端科学技術大学院大学 情報科学研究科

平成 20 年 3 月 6 日

論文の内容の要旨

セキュリティプロトコルの解析はおよそ 30 年に渡り活発な研究が行われている。多くの形式化手法がセキュリティプロトコルを記述するために用いられ、解析は様々なテクニックにより (半) 自動的に行われてる。しかしネットワークの複雑性ゆえ、セキュリティプロトコルの解析は困難な作業であると認識されている。セッション数、通信ユーザ数、侵入者や不正な主体が生成するメッセージ数などは非有界、つまり上限を定めることはできない。それゆえ解析手法は、これら無限の因子を有限で記述できるよう注意深く設計する必要がある。

無限の因子を扱うセキュリティプロトコルを解析するための方法を考えるとき、次のようなジレンマに陥いる。セキュリティプロトコルのモデルは実行において起こりえる状況—不正な攻撃を受けた場合も含め—を記述できる位に十分に強力な表現能力を備えている必要がある。しかし、強力な表現能力を持つモデル上の性質は決定不能な問題になりやすく、欠陥を自動検出する解析が有限時間で終わらなくなるおそれがある。

この論文では、セキュリティに関する様々な性質を与えられた仮定の下で解析するための健全かつ完全なモデル検査手法を提案する。すなわち、欠陥が検出されないのであれば、その仮定の下ではプロトコルが安全であることが保証される。セキュリティプロトコルの振舞を記述するため、Spi 計算の変種に基づくプロセス計算を導入する。演繹システムは自由に挿入でき、侵入者や不正な主体による無限の数のメッセージを表現できる。この計算に対するトレースセマンティクスは、可能なセキュリティプロトコルの実行が具体的なトレースによって明確に表現できるように選ばれる。

主たる貢献と成果は下記の通り。

- セキュリティプロトコルについての各種セキュリティの性質を異なる仮定の下で解析するとき、無限因子は様々なテクニックにより有限になるよう抽象化され、セキュリティの性質は以下のいずれかの仮定の下で、健全かつ完全なオンザフライモデル検査により自動的に検証できる。(i) 有界なセッションにおける秘匿性と認証性、(ii) 再帰的プロトコルに対する認証性、(iii) 有界なセッションにおける非否認性と公平性。このうち (ii) と (iii) はモデル検査法による初めての解析である。

- 秘匿性と認証性に対しプロトコル独立な仕様を提案する。このアプローチでは秘匿性と認証性の仕様は、プロトコルの記述から自動的に生成できる。対照的に他の、特にプロセス計算に基づくアプローチの場合は、与えられたセキュリティプロトコルに依存したセキュリティの仕様を、手動で定義する必要がある。

提案手法は Maude で実装されている。各性質は、Maude の `search` コマンドの機能によってモデルの生成時に検査できる。

キーワード: セキュリティプロトコル, オンザフライモデル検査, 秘匿性, 認証性, 非否認性, 公平性, 再帰的プロトコル, Maude