セキュリティプロトコルの代数モデルに基づく形式化

金城 直貴

言語設計学講座
北陸先端科学技術大学院大学 情報科学研究科

2001 年 2 月 15 日

キーワード: セキュリティプロトコル, NSPK Protocol, 仕様記述, CafeOBJ.

本研究の目的は、セキュリティプロトコルを検証するために提案された形式化を用いて、その仕様記述を行い、記述した仕様について検討することである。

セキュリティプロトコルとは、暗号技術を利用し、通信者間の秘密通信を目的とする通信プロトコルであり、ネットワーク上での安全な商取引や選挙への適用が期待され、多数提案されている。

セキュリティプロトコルを実用化する場合、あらかじめ、その安全性を保証することが必要である。セキュリティプロトコルの安全性は、そのプロトコルで用いられる暗号と切り放して議論する。これは、たとえ暗号が安全だとしても、プロトコルに欠陥があれば、悪意のあるユーザがその欠陥を利用して秘密情報を知り得るからである。

セキュリティプロトコルが安全であるという正当性は、しばしば人間の直感に頼っていた。しかし、良く知られたプロトコルの欠陥が形式手法を用いた検証によって発見されたことにより、セキュリティプロトコルの検証方法として形式手法の有効性が期待されている。

代数仕様言語 CafeOBJ は、順序ソート代数、書き換え論理、隠蔽代数を任意に組み合わせることで、仕様の意味定義を行う。特に近年、抽象状態機械を表現する場合、隠蔽指標と、それに関する等式を用いて、その仕様を記述する手法が取り入れられた。この隠蔽指標と等式によって記述される仕様を振舞仕様という。

セキュリティプロトコルの検証方法として形式手法への期待が高まり、それにともない、様々な形式化がなされた。その中でも本研究では、G.Denker、J.Meseguer、C.Talcott らによる Configuration を用いた形式化と、萩谷、戸田、福場らによる、ネットワークのシステム状態を定義した形式化の 2 つの形式化の枠組みを取り上げる。

Denker らが形式化に用いた Configuration は、並行分散システムを表現、分析するために提案された並行オブジェクト指向モデルを記述するために定義された。ネットワークプロトコルは、並行オブジェクト指向モデルで自然に表現することができる。Configuration 上には Object と Message が存在し、Object が Message を受信した際に Configuration の状態遷移が起きる。Configuration の遷移は、書き換え規則で表現される。Denker らは、Configuration を用いて代数仕様言語 Maude でいくつかのセキュリティプロトコルを記述した。

萩谷らはネットワークのシステム状態を定義した。ネットワーク状態は、通信を行う主体とネットワーク上を流れるメッセージの集合で表し、状態遷移はプロトコルのステップで行われる。主体は状態を持ち、特定の状態にあるときにメッセージの送受信を行う。ネットワーク上に流れるメッセージはプロトコルのフォーマットに依存する。

本研究では、代数仕様言語 CafeOBJ により、Configuration を用いた形式化を書き換え論理による仕様で記述し、ネットワークのシステム状態を定義した形式化を振舞仕様で記述する。

セキュリティプロトコルの例題として、Needham-Schroeder Public-Key Protocol (以降 NSPK Protocol と略記) を取り上げる。NSPK Protocol は公開鍵暗号方式を利用して、通信者相互の認証を目的とするプロトコルである。NSPK Protocol は、推測不可能でランダムに生成されるノンスと呼ばれる値を通信者がお互いに相手の公開鍵で暗号化して送受信し、値を交換する。ある公開鍵で暗号化したメッセージは対応する秘密鍵でしか復号できない。NSPK Protocol の認証は、自身で生成したノンスを通信相手の公開鍵で暗号化すれば、その内容を知っている、あるいは知ることができるのは、自身とその秘密鍵を持つ者のみであり、すなわち自身と通信相手のみであることを根拠とする。しかし、Gavin Lowe によって、NSPK Protocol の認証が反証された。それは、A が S と通信を開始し、その後、S が A から受信したメッセージのノンスを用いて、B と通信を始めると、意図した認証が行われない結果が得られることである。これを、Lowe's Attack という。Lowe は Lowe's Attack と同時に NSPK Protocol の改訂版も発表した。その改訂版に Lowe's Attack を試みても、通信は途中で終了し、間違った認証が行われることがない。

NSPK Protocol とその改訂版を書き換え論理と振舞仕様で記述し、その仕様を CafeOBJ の実行環境でシミュレートする。

書き換え論理による仕様は、ある Configuration を与えることでプロトコルが自動的に実行される。書き換え規則に認証が行われた状態、攻撃がなされた状態を記述することで、認証と攻撃を検知することができる。

振舞仕様による仕様は、あるネットワークの状態を与えることで、プロトコルの 1 ステップ毎の状態遷移を確認することができる。1 ステップ毎にネットワーク上の通信者が生成可能なメッセージを確認し、次に可能なステップを確認する。

両仕様ともに NSPK Protocol で Lowe's Attack を確認し、改訂版では Lowe's Attack が成立しないことを確認した。また、振舞仕様による改訂版の実行では Lowe's Attack が行われた場合、通信者がお互いに他人になりすましているという無意味な認証が行われる可

能性があることを確認した。

書き換え論理による仕様は、直感的に理解しやすいため、可読性が高い。また、状態遷移の書き換えが自動的に行われ、ある状態に到達可能かを検知することもできるという特徴を持ち、プロトコルの動作を確認するための有効なシミュレータとなる。しかし、状態遷移の書き換え規則を全て列挙することが困難であることから、セキュリティプロトコルに対する攻撃を検知することができなくても、その安全性を必ずしも保証することにはならない。

一方、振舞仕様での記述は、現時点ではシミュレータ、検証系としてもともに力不足であるが、検証系としての可能性が期待できるのではないかと考える。セキュリティプロトコルの安全性は、ある性質を満たすことをその根拠とする。セキュリティプロトコルが安全であるという性質から、プロトコルのどのステップによる遷移でもその性質を満たすことを証明すればよい。その方法として、ネットワークの状態に対する、プロトコルステップの帰納法が考えられる。しかし、その検証にはセキュリティプロトコルの安全性とその性質をどのように形式化するかという課題がある。