通信プロトコルのモデリングに関する研究

200612051　樋口　優輝

インターネットにかかわる技術仕様は，Internet Engineering Task Force(IETF)によりRequest For Comment(RFC)として公開されている．しかし，当初安全とみられていた仕様に脆弱性が発見される事例（SSH，DHCP等）も多数報告されている．仕様は，各動作のシナリオ，設定パラメタ，フレームフォーマットが自然言語で記載されている．挿入されている図面は，前述の一般的なシナリオに従ったタイムライン図および状態遷移図が主である．これらを読み取ることによって，プロトコルの概略は理解可能である．しかし，それがクライアント・サーバ間で常に安全に動作するか否かを読み取ることは困難である．また，RFCでは，実装に対する要求レベルとして‘MUST’，‘MUST NOT’，‘SHOULD’，‘SHOULD NOT’，‘MAY’の5レベルを設けており，これらの取り合わせによってはパフォーマンスの低下が生じることがある．

RFCを満たすようにC言語で実装し，テストを実施する方法も無くはないが，多数のホスト間で協調動作が必要な場合のテストは困難である．また，そもそも実装コードの作成には時間を要する．（比較的小規模なudhcpd-0.9.8でもソースコードサイズは約100kB）

そこで本研究では，仕様記述言語のひとつであるVDM-SLを用いて通信プロトコルのモデル化を試みる．仕様記述言語の特徴は，モデルの性質が静的に表現可能である点にあるこれによりモデルの性質は手続きを動的にたどることなく，集合論により一目で掌握できるようになることが期待される．

以上，仕様記述言語による通信プロトコルのモデル化が本研究の最終目標であるが，その前段階として自然言語で書かれた簡単な文書をVDM-SLで表現する訓練が必要である．中間発表では，VDM-SLの表現力を確認するために，大学入試センター試験問題を例にして，問題文のモデル化と解答の導出を行ったので報告する．

並列動作モデルの自動設計に関する研究

200612045　田村　英輔

現実のハードウエアはほとんどすべて並列動作モデルで設計する必要がある．信号機を例にすると，一方の信号が赤のときにもう一方の信号は赤または青でなければならない．各信号機のランプすべてから直接コントローラにケーブルを引くことができれば単一モデルでの実現も可能ではあるが，高コストで柔軟性の無いシステムとなる．このため，通常は，各車線の端末にメッセージを送りそのメッセージによってランプの点灯・消灯を行う設計の際にはメッセージの不達や端末の障害といった異常事態についても常に考慮して設計する必要がある．この設計はミューテックスを2つ導入することでの解決する．しかし，このような解を見つける作業には多くの経験が必要である．本研究の最終目標は，モデルの振る舞いを様相論理式で記述することにより，評価可能なコードを自動生成することである．これにより，モデルの設計を経験から数学に置き換えることを目指している．

様相論理式の一つである，線形時相論理(LTL)は，SPINモデル検査ツールにおいて，モデルそのものではなく，モデル検査オートマトンの生成に用いられている．本研究の第一段階では，従来の設計手法の定石をまとめ，第2段階ではそれらの論理式での表現方法について検討する．中間発表では，信号機の設計を例に既存のモデル設計手法と検証について報告する．