6A-03

モデル検査に基づくネットワーク機器製品の性能検証手法

大林　浩気
（株）日立製作所　研究開発グループ

１．はじめに

組込みソフトウェアにおいては，厳しいリソース制約下で応答時間などの性能要件を満たすことが要求される。しかし，従来の実機を用いたテストは不具合発覚時の手戻りが大きいという問題があった。

本稿では，上流工程で性能検証を可能とするために，モデル検査によって性能を検証する手法を提案する。また，提案手法をネットワーク機器製品のプロトコル制御機能の設計に適用した結果について述べる。

２．課題

組込みソフトウェア開発における性能評価手段として，従来は実機による性能テストがよく用いられている。しかし，実機によるテストはソフトとハードが揃う下流工程でないと実施できないため不具合発覚時の手戻り工数が大きく，また，処理の順序やタイミングに依存する不具合の発見が困難であるため，不具合の摘出漏れが発生しやすいという課題がある。

３．提案手法

上記課題を解決するため，上流工程でモデル検査を用いて性能を検証する手法を提案する。

モデル検査は，検証対象を有限状態機械としてモデル化し，その状態空間を網羅的に探索することによって，与えられた検証式が満たされるか否かを判定する検証手法である。検証にモデルを用いるため，動作するソフトウェアやハードウェア実機が存在しない上流工程においても検証を実施することができる。また，モデルの状態を網羅的に探索するため，実機によるテストやシミュレーションでは発見が困難な再現性の低い不具合を発見することができる。

提案手法は対象としてネットワーク機器製品のプロトコル制御機能を想定しており，プロトコルのモデル化においてはモデルに時間の概念が必要となる。そこで，モデル検査ツールSPIN[1]の離散時間機能拡張版である DTSPIN[2]を用いる。DTSPIN では，検証モデルを Promela と呼ばれるモデル記述言語で記述し，検証条件は LTL （線形時相論理）式やアサーションで記述する。また，タイマ命令を用いて時間の経過を表現することができる。

提案手法では，規格と仕様に対して満たすべき性能情報を付加した検証モデルと検証条件を Promela と LTL 式で作成し，DTSPIN によるモデル検査を実行することで検証結果を得る。提案手法の検証モデル作成手順は以下の通りである。

(1) プロトコル規格や製品仕様に基づき検証対象を Promela による状態遷移モデルで記述する。
(2) (1)のモデルに含まれる処理の実行に相当する箇所に対し，製品仕様や旧製品の実測値に基づいて処理時間を算出し，Promela 内の対応する処理の実行箇所に DTSPIN のタイマ命令による時間経過として埋め込む。
(3) 規格や仕様で定められている応答時間などの満たすべき性能要件を，LTL 式またはモデル内のアサーションで記述する。これらは，具体的にはタイマ変数に関する論理式として表現する。

図１は提案手法で作成する Promela の記述例のサンプルコードである。

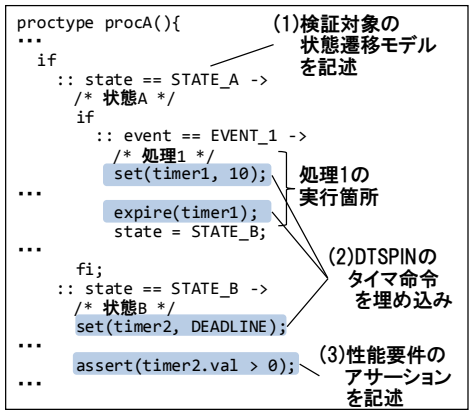

図 1　Promela の記述例

A Performance Verification Method Based on Model Checking for Networking Equipment Products
Hiroki Ohbayashi, Research & Development Group, Hitachi, Ltd.

４．手法の適用

あるネットワーク機器製品のプロトコル制御機能の設計を対象とし，提案手法を適用した。

対象プロトコルは，スイッチ間の通信経路の冗長化を目的とするリングプロトコルの一種である。リング内でリンク障害が発生した場合，リングに属するそれぞれのノードがプロトコルに従って制御メッセージの送受信，状態遷移，ポートの開閉などを実施することにより，リンクの切替が行われ，リングが再構築される。

対象プロトコルの規格書では，リンク障害が発生してからリンク切替が正常に完了するまでの時間が 50msec 以内でなければならないと規定されている。そこで，この性能要件を満たす設計を策定することを目的として提案手法による検証モデルを作成し，検証を実施した。

プロトコル制御機能の開発では，まずプロトコル規格書の読解を行い，開発関係者が規格について理解した後で基本設計に入り，実際の製品上でプロトコルをどのように実装するかを検討する。そこで本適用では，モデル化の粒度と範囲が異なる 2 つの検証モデルを作成した。一つは，規格書に基づき個々のネットワーク機器の状態遷移をモデル化した「規格ベース検証モデル」である。規格ベース検証モデルは規格書の読解フェーズで作成し，規格書の解釈の正しさを検証するために用いた。もう一つは，開発中の設計に基づき，モデルの範囲を一つのネットワーク機器内に限定して機器内の個々のハード/ソフトモジュールの状態遷移をモデル化した「設計ベース検証モデル」である。設計ベース検証モデルは基本設計フェーズで作成し，設計が規格や仕様の性能要件を満たすかどうかを検証するために用いた。

５．結果

検証の結果，規格ベース検証モデル，設計ベース検証モデルそれぞれの検証で，性能上の不具合を 1 件ずつ，合計 2 件発見することができた。以下はそれぞれの詳細である。

(1) リンク切替シーケンス中のあるタイミングにおいて隣接するノードがお互いに同時に制御メッセージを送信した場合，異常な状態遷移が発生し，さらに，予期しない不要な処理が引き起こされ，リンク切替性能が悪化するという問題があることが規格ベース検証モデルの検証により発見された。

(2) 対象ネットワーク機器製品では冗長化のため制御管理モジュールを主／副の 2 セットを持っており障害発生時に主／副の切替を行うことにより障害による被害を最小限にしている。この主／副の切替が特定のタイミングで発生すると，リング内の他ノードの状態遷移が正常に完了せず，リンク切替にかかる時間が大幅に長くなる問題があることが設計ベース検証モデルの検証により発見された。

発見された 2 件の不具合はどちらもタイミングに依存する再現性の低いものであった。(1)は設計で回避可能な問題であることが分かり，設計フェーズに入る前に不具合の作り込みを防止することができた。また，(2)も開発中設計の修正により手戻り無く摘出することができた。

６．評価

提案手法により削減することができた手戻りコストを見積もる。開発担当者へのヒアリングにより，発見された不具合 2 件はどちらも従来はテスト工程で摘出されるものであるということが分かった。また，テスト工程で摘出したと仮定した場合に仕様，設計や実装の修正などにかかる手戻りコストとして 7.5 人月/件という見積りを得た。一方，検証モデル作成，検証実施にかかったコストはおよそ 2.5 人月であった。

以上を元に今回の適用により削減することができた手戻りコストを見積もると以下のようになる。

7.5 人月/件×2 件 － 2.5 人月 ＝ 12.5 人月

上記結果は提案手法の手戻りコスト削減に対する有効性を示している。

７．おわりに

本稿では，手戻りコストを削減することを目的として，モデル検査技術を用いて上流工程で性能を検証する手法を提案した。提案手法をネットワーク機器製品のプロトコル制御機能の設計に適用した結果，タイミングに依存する再現性の低い性能上の不具合を 2 件発見することができ，12.5 人月の手戻りコスト削減効果を確認することができた。これらの結果は，提案手法の有効性を示していると考える。

参考文献

[1] Spin-FormalVerification,http://spinroot.com
[2] D. Bosnacki and D. Dams, Discrete-Time Promela and Spin, Proceedings of the 5th International Symposium on Formal Techniques in Real-Time and Fault-Tolerant Systems, SpringerVerlag, pp. 307-310, (1998)