7L−5

優先サービスを含む通信プロトコルの安全性の検証

玉井 順子　樋口 昌宏　関 浩之　嵩 忠雄

大阪大学基礎工学部情報工学科

1 まえがき

通信ソフトウェアの信頼性を高めるためには，通信プロトコルの正しさを検証することが重要である．実用のプロトコルには通信路の強制切断のように他のサービスより優先度の高いサービスを提供しているものが多い．優先サービスは通常動作を実行しているすべての状態から開始できるよう定義されるためプロトコルの規模の増大をまねき，その諸性質の検証を直接扱うのは検証時間の観点から適当でない．筆者らは，優先サービスを含むプロトコルについて優先サービス，通常サービスそれぞれを定義した2つのサブプロトコルが安全であれば合成したプロトコルの安全性が保証されるための一つの十分条件を示している[1]．本稿では，OSIセションプロトコル[2]の一部を対象に，筆者らの提案している検証法[3]に基づき，検証システムを利用して2つのサブプロトコルの安全性と上記十分条件の成立の検証，及び合成して得られたプロトコルの安全性の検証を行ない，それらの結果を比較し，サブプロトコル段階での検証の有効性について述べる．

2 プロトコルのモデル化

2.1 プロトコルモデル

通信系を，2つのプロトコル機械を双方向の長さに制限のないFIFOでモデル化した通信路で結合した系としてモデル化する．**プロトコル機械** PM を4字組 (S,Σ,δ,SI) で定義する．ここで，Sは状態の有限集合，Σはメッセージ送信にかかわるイベントの有限集合$\Sigma-$とメッセージ受信にかかわるイベントの有限集合$\Sigma+$ の和集合からなるイベントの有限集合，δは $S\times\Sigma$から 2^Sへの非決定性状態遷移関数であり，$SI(\subseteq S)$はプロトコル機械の初期状態の集合である．2つのプロトコル機械 $PM_A=(S_A,\Sigma_A,\delta_A,SI_A)$, $PM_B=(S_B,\Sigma_B,\delta_B,SI_B)$ について$\Sigma_A-=\Sigma_B+(=\Sigma_{AB})$, $\Sigma_B-=\Sigma_A+(=\Sigma_{BA})$ であるとき2字組$\Pi=\langle PM_A,PM_B\rangle$ を**プロトコル**と呼ぶ．通信系全体の状態は4字組 $\langle s_A,s_B,u_{BA},u_{AB}\rangle\in S_A\times S_B\times\Sigma^*_{BA}\times\Sigma^*_{AB}$で表し，通信系の**合成状態**と呼ぶ．

A Verification Example for Communication Protocol Including Priority Services

Junko TAMAI, Masahiro HIGUCHI, Hiroyuki SEKI, Tadao KASAMI
Osaka University

2.2 安全性

合成状態 $gs=(s_A,s_B,u_{BA},u_{AB})$ に対して u_{BA}(または u_{AB}) 上の先頭メッセージの受信に対する遷移関数が s_A(または s_B) で定義されていないときかつそのときのみ，gs は**未定義受信状態**であるという．また，2つの通信路上にともにメッセージが存在せず，s_A, s_Bにおいて送信動作が定義されていない合成状態 $(s_A,s_B,\varepsilon,\varepsilon)$ を**空チャネルデッドロック状態**という．さらに，PM_A(または PM_B) がエラー状態であると指定されるような状態 s_A(または s_B) に対して，合成状態 (s_A,s_B,u_{BA},u_{AB}) を**プロトコルエラー状態**という．

与えられたプロトコル$\Pi=(PM_A,PM_B)$に対して，PM_A, PM_Bがプロトコルで定義された送受信動作のみを行なうという仮定の下で，初期状態から上記の3つの状態に到達可能でないときΠが**安全**であるという．

3 優先サービスと通常サービスの合成

通常サービスを定義したプロトコル機械 $PM_N=(S_N,\Sigma_N,\delta_N,SI_N)$ と優先サービスを定義したプロトコル機械 $PM_P=(S_P,\Sigma_P,\delta_P,SI_P)$ から，PM_Nと PM_Pの双方の機能を含むプロトコル機械 $PM_C=(S_C,\Sigma_C,\delta_C,SI_C)$ の合成を以下のように定義する．ここで，(1)PM_Pの最終状態集合 $SF_P(\subseteq S_P)$ (2) 関数 $mi: S_N\to SI_P$ (3) 関数 $mr: SF_P\to S_N$ をパラメータとして用いる．但し，$S'_p=S_P-SI_P-SF_P$とする．

1 : $S_C=S_N\cup S'_p$

2 : $\Sigma_C=\Sigma_N\cup\Sigma_P$

3.a : $\forall_{s\in S_N,e\in\Sigma_N}\{\delta_C(s,e)=\delta_N(s,e)\}$

3.b : $\forall_{s\in S_N,e\in\Sigma_P}\{\delta_C(s,e)=\delta_P(mi(s),e)\}$

3.c : $\forall_{s\in S_{P'},e\in\Sigma_P}\{\delta_C(s,e)=$
$\{\delta_P(s,e)-SF_P\}\cup\{mr(\delta_P(s,e)\cap SF_P)\}\ \}$

3.d : $\forall_{s\in S_{P'},e\in\Sigma_N-}\{\delta_C(s,e)=\phi\}$

3.e : $\forall_{s\in S_{P'},e\in\Sigma_N+}\{\delta_C(s,e)=s\}$

4 : $SI_C=SI_N$

$\Pi_N=(PM_{A_N},PM_{B_N})$, $\Pi_P=(PM_{A_P},PM_{B_P})$ に対して，PM_{A_C}が PM_{A_N}, PM_{A_P}から，PM_{B_C}が PM_{B_N}, PM_{B_P}から上記の方法で合成されたプロトコル機械であるとする．文献[1]に示された条件が満たされており，かつΠ_N, Π_Pが安全であるならば，プロトコル$\Pi_C=(PM_{A_C},PM_{B_C})$が安全

であることが保証される[1].

4 検証法

2.1 のようにモデル化されたプロトコルにおいて検証すべき条件を表現するために, (1) プロトコル機械の状態が指定した状態集合に属するかどうかを表す式, (2) 通信路上のメッセージの系列が指定した正規集合に属するかどうかを表す式を原子式とする命題論理式を導入する.

初期合成状態から到達可能な任意の合成状態において, 論理式 Fが成り立つとき Fを**不変式**という. 論理式 F に対して, 次の条件を満たす論理式を $NEXT(F)$ とする.「合成状態 gs が, Fを満たすある合成状態から 1 回の遷移で到達可能であるときかつそのときのみ, gs は $NEXT(F)$ を満たす」. 初期合成状態が Fを満たし, かつ, $NEXT(F) \supset F$($\supset$は含意) が恒真であるならば, Fは不変式である. Fの原子式として上記 (1),(2) を考えているので, Fから $NEXT(F)$ は構成可能であり, また与えられた Fが恒真であるかも判定可能である. そして, 2.2 で述べたあらゆる安全でない状態が Fを満たさなければ, そのプロトコルは安全であると結論できる. この検証法に基づく検証システムが作成されている[3].

5 対象としたプロトコル

検証の対象として OSI セションプロトコル[2]の主要部であるカーネル, 全二重, 大同期, 小同期機能単位のコネクション確立, データ転送, コネクション解放フェーズを取り上げた. 簡単のため, トランスポートコネクションは常に確立されている状態であると仮定した.

OSI セションプロトコルは通信路の利用者切断サービスを含んでいる. この場合, 利用者切断サービス以外のすべてのサービスは本稿で言うところの通常動作とみなすことができ, 利用者切断サービスは優先サービスとみなすことができる.

実際, [2] に基づき, 全二重, 大同期, 小同期機能単位及び利用者切断サービス以外のカーネル機能単位を抽出したものをΠ_N, カーネル機能単位中の利用者切断サービスのみを抽出したものをΠ_Pとすると文献 [1] の条件を満たしている. さらにΠ_NとΠ_Pから合成したプロトコルΠ_Cは, 全二重, 大同期, 小同期, 及びカーネル機能単位を抽出したプロトコル仕様に一致する.

6 検証結果

4. で述べた検証法に従って UNIX ワークステーション (Solbourne Series 5/600, 2CPU 48MB) 上でプロトコルΠ_N, Π_P, Π_Cにおける安全性の検証作業を行なった.

表 1: 検証したプロトコルの規模と検証結果

プロトコル	Π_N		Π_P		Π_C	
プロトコル機械	A	B	A	B	A	B
状態数	24	24	4	4	32	32
イベント数	11	11	2	2	13	13
状態遷移数	28	28	5	5	55	53
不変式を記述する際に考えた合成状態集合数	22		11		104	
記述した不変式の原子式数	270		43		827	
システムが考慮した遷移の数	714		14		18058	
cpu 時間 (秒)	261.13		0.03		7977.33	
メモリ使用量	6MB		48kB		16MB	

3 つのプロトコルの規模と, 検証実行時に得られたデータを表 1 に記す.

Π_Pは非常に小規模なものであるが, Π_Cの状態遷移の数は, Π_Nの約 2 倍となっている. それにともなってΠ_Cの不変式の原子式の数, システムが考慮した遷移の数もΠ_Nに比べてそれぞれ約 3 倍, 約 25 倍となっている. さらに, 検証に要した cpu 時間が約 30 倍, メモリ使用量が 2 倍以上となった. Π_Pが複雑な場合は差がより顕著になると思われる.

また, Π_Cの不変式を記述する際に考慮した合成状態の数がΠ_Nの場合と比較して大きなものとなるため, Π_Cの不変式記述にはΠ_Nの場合と比べてかなり大きな手間を要した.

検証作業を通じて, 優先サービスを含むプロトコルにおけるサブプロトコル段階での検証の有効性が確認できた.

謝辞

日頃御討論頂く本学教養部藤井護教授並びに, 検証システムの利用について御助力頂いた本学大学院生白川理氏に感謝いたします.

参考文献

[1] 樋口, 関, 嵩: "優先サービスを含む通信プロトコルの可達性解析について", 信学技報, IN91-108(1991-09).

[2] ISO: "Basic Connection Oriented Session Protocol Specification", ISO 8327.

[3] 邵, 白川, 関, 藤井, 嵩: "順序機械によってモデル化された通信プロトコルの一検証法—OSI セションプロトコルを例にして—", 信学論 (D-I), vol.J74-D-I, no.12 pp.846-857(1991-12).