【 84 】

氏名	樋口昌宏
博士の専攻分野の名称	博士（工学）
学位記番号	第 11642 号
学位授与年月日	平成7年1月23日
学位授与の要件	学位規則第4条第2項該当
学位論文名	A Study on Verification Methods for Communication Protocols Modeled as Extended Communicating Finite－State Machines （拡張有限状態機械でモデル化された通信プロトコルの検証法に関する研究）
論文審査委員	（主査） 教授 藤井 護 （副査） 教授 都倉 信樹　教授 谷口 健一　教授 西川 清史 奈良先端科学技術大学院大学 助教授 関 浩之

論文内容の要旨

信頼性の高い通信システムの実現のため，プロトコル仕様の基本的性質の検証が重要である。検証すべき性質として安全性，生存性がある。安全性とは通信系がデッドロックなど望ましくない状態に決して陥らないという性質であり，生存性とは興味あるメッセージの送受信など所期の処理がいつかは実行されるという性質である。実用レベルの通信プロトコルはプロトコル機械が有限制御部の他に整数値などの値をとる変数を持つ拡張有限状態機械（以下，ECFSMと呼ぶ）でモデル化される場合が多い。しかし，モデルの複雑さのため，ECFSM モデル上での通信プロトコルの検証法に関する研究は従来ほとんど行なわれていなかった。

本論文では ECFSM モデルの通信プロトコルの安全性，生存性の一検証法を提案している。また，実用規模のプロトコルの検証を実際的な時間で完了できるようにするため，大規模プロトコルの検証を小規模プロトコル群の検証に帰着する一手法についても議論している。

第2章では，本論文で取り扱う ECFSM モデルのプロトコルの定義を与えている。

第3章では，ECFSM モデルのプロトコルに対する検証者の関与の下での安全性の検証法を提案している。提案している検証法の概略は以下の通りである。

(1) まず検証者がプロトコルⅡにおいて，初期状態から到達可能であると想定しているすべての状態で成立する条件を論理式 F で記述する。

(2) F が不変式である（初期状態から到達可能な任意の状態で成立する）ことを通信系の状態遷移系列に関する構造的帰納法により示す。さらに，F を満たす任意の状態が安全な状態であることを示すことによりⅡが安全であることを示す。帰納段階の証明では，2つの正規表現間の包含関係の判定，項書き換え系上の項の書き換え，整数線形計画問題の求解などの手続きを用いている。

4章では，3章の安全性の検証法に基づく ECFSM モデルのプロトコルの生存性の検証法を提案している。ここでは，生存性を「あらゆる到達可能状態から性質 Q を満たす状態へ到達可能である」という性質（Q－live性）として定式化している。提案している検証法では，以下の性質を満たす有限の縮退到達可能性グラフを構成し，そのグラフ上を探

索することにより Q－live 性の成立を示す。(i) 各頂点 v_i は状態集合 RS_i を表す，(ii)「RS_i に含まれる任意の状態から RS_j に含まれるある状態へ到達可能である」が成り立つときに限り v_i から v_j への辺が存在する。(ii) の性質の判定は，安全性の検証とほぼ同様の手続きにより行なっている。

3，4章それぞれにおいて，提案している検証法に基づく検証システムを試作し，2種類の一連番号を取り扱う例プロトコルの検証結果について述べている。

従来，大規模プロトコルの検証が可達集合の爆発的な巨大化により実際上不可能になるという問題は広く認識されている。5章ではこのような問題を解決するための一手法として，優先サービスを含むプロトコルを通常サービスを規定したプロトコルと優先サービスを規定したプロトコルの合成により定義する手法を提案している。ここで，優先サービスとは接続の強制切断など，緊急に処理されるべきサービスをいう。ここでは，優先サービスを規定したプロトコルの特徴付けを行ない，その通常サービスを規定したプロトコルとの合成を定義している。また，合成されたプロトコルが，合成前の各プロトコルの安全性などの諸性質を継承するための十分条件について議論している。提案された合成法に基づいて，優先サービスを含むプロトコルの検証を，優先サービスのみを規定したサブプロトコルと，通常サービスのみを規定したサブプロトコルそれぞれの検証，及び上記十分条件の検証により行なうことができる。提案した手法を用いることによる検証に要する時間の軽減の効果を計るための比較実験として，(i) 合成前の2つのサブプロトコルの安全性と上記十分条件の検証 (ii) 合成後のプロトコルの安全性の検証，を行ない，(i) の計算時間が (ii) の計算時間の約1／30という結果が得られた。

論文審査の結果の要旨

実用の通信プロトコルには，プロトコル機械が整数などの変数を持つ拡張有限状態機械 (ECFSM) として定義されるものが多い。しかし，従来，モデルの複雑さのため，ECFSM モデルのプロトコルを直接扱う検証法に関する研究はほとんど行なわれていなかった。

本論文では ECFSM モデルの通信プロトコルの一検証法を提案し，さらに，大規模プロトコルの検証を小規模プロトコル群の検証に帰着する一手法についても提案している。

3章では，通信系がデッドロックなどの安全でない状態に陥らないという性質（安全性）4章では，任意の到達可能な状態から一連の処理を完了した状態に到達可能であるなどの性質（生存性）の検証法を提案している。これらの検証法では，不変式記述のための4種類の原子式が導入され，構造的帰納法に基づく不変式の成立の証明手続き，不変式をもとに有限の縮退到達可能性グラフを構成，探索することにより生存性を示す手続きが与えられている。提案している検証法では，検証に用いる手続きの有限停止性，効率に配慮して，整数値に関する演算，各原子式の記述能力に制限をおいている。多くの実用の通信プロトコルでは整数値レジスタをタイマや一連番号の処理のために用いており，上記の制限のもとでそれらのプロトコルの検証を取り扱うことができることより，実用上十分有効な検証法と判断できる。

また，3，4章では，提案した検証法に基づいて開発した検証システムの概略と，OSI セションプロトコルから抽出した，整数値で表される一連番号を取り扱う例プロトコルの安全性，及び生存性の検証実験の結果についても述べており，提案している検証法の実現性，有効性が確認されている。

5章では，大規模プロトコルでは到達可能な状態数が非常に大きなものとなるため，その検証が実際上不可能になるという問題を解決するための一手法として，接続の強制切断などの緊急性を要する優先サービスを含むプロトコルを，通常サービスを規定したプロトコルと優先サービスを規定したプロトコルに分解して検証する手法を提案している。多くの大規模な実用のプロトコルが優先サービスとみなせる処理を含んでおり，提案されている検証手法の適用範囲は十分広いものと考えられる。比較実験として，OSI セションプロトコルの一部を抽出した，接続の強制切断を優先サービスとして持つプロトコルを例に，分解を用いた場合，分解を用いない場合，それぞれについての安全性の検証が行なわれ，分解を用いた場合の計算時間が用いない場合の計算時間の約1／30という結果が得られており，検証の効率化に大

きな効果があることも確認されている。

以上のように，本論文で提案された検証法を適用することにより，ECFSM モデルのプロトコルの検証が可能となり，通信システムの信頼性の向上に寄与するところ大であり，高く評価される。よって，本論文は，博士論文（工学）として価値あるものと認める。