OUKA
Osaka University Knowledge Archive

Title	Efficient Verification of Responsive Communication Protocols for Client-Server Systems
Author(s)	長野, 伸一
Citation	大阪大学, 1999, 博士論文
Version Type	
URL	https://hdl.handle.net/11094/41510
rights	
Note	著者からインターネット公開の許諾が得られていないため、論文の要旨のみを公開しています。全文のご利用をご希望の場合は、大阪大学の博士論文についてをご参照ください。

Osaka University Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

Osaka University

氏名	長野伸一（ながの しんいち）
博士の専攻分野の名称	博士（工学）
学位記番号	第 14716 号
学位授与年月日	平成11年3月25日
学位授与の要件	学位規則第4条第1項該当 基礎工学研究科情報数理系専攻
学位論文名	Efficient Verification of Responsive Communication Protocols for Client-Server Systems （クライアントサーバシステムのための通信プロトコルのリスポンシブネス性検証）
論文審査委員	（主査） 教授 菊野 亨 （副査） 教授 宮原 秀夫　教授 藤原 融

論文内容の要旨

実時間性と耐故障性の2つを満たす通信プロトコルを一般にリスポンシブプロトコルと呼ぶ。リスポンシブプロトコルの本質的な特徴は，システム内に故障が発生して異常状態に陥っても正常状態へ迅速に回復できることである。本論文は，リスポンシブプロトコルの検証手法の理論的提案とその有効性の実験的評価をまとめたものである。

従来，耐故障性と実時間性の2つの性質を共に検証できる統一的な手法はほとんど提案されていない。特に，物理時刻の取り扱いができなかったり，仮にできたとしても厳しい条件下であって必ずしも現実的ではなかった。また，通信プロトコルの検証は一般的にいわゆる状態爆発を引き起こし，その回避が本質的な問題となっていた。

本論文では，クライアントサーバシステム上で利用する通信プロトコルに対するリスポンシブネス性の検証法を新しく提案している。提案法はクライアントサーバシステムがもつ対称性に基づいて，等価なシステム状態を除くすべてのシステム状態を効率良く生成するので，前述の状態爆発を回避できる。また，実用性を考慮した極めて緩い条件下で実時間を導入している。そのため，生成されるシステム状態が現実のシステムの状況を厳密に表現しており，通信プロトコルの正確な検証が可能になる。更に，提案法では検証コスト（状態数，メモリ容量，検証時間）が非常に少なくてすむことを実験によって示している。

次に，通信プロトコルのリスポンシブネス性に反する設計誤りを検出する手法を提案している。提案法では，リスポンシブネス性に関して通信プロトコルが満たすべき条件を実時間論理の論理式ϕで与えて，ϕが偽となる異常状態を出力する。この異常状態は具体的な設計誤りを検出する手がかりとなる。また，提案法を用いると設計誤りの検出とその修正を非常に短い時間でかつ少ないメモリ容量で行えることを実験によって示している。

論文審査の結果の要旨

実時間性と耐故障性の2つの基本的性質を有する通信プロトコルを一般にリスポンシブプロトコルと呼ぶ。リスポンシブプロトコルの本質的な特徴は，故障発生したシステムが必ず正常状態へ迅速に回復できることである。本論文は，リスポンシブプロトコルの検証支援に関する技術開発についての理論的成果とその有効性の実験的評価をまとめたものである。本論文の主な成果は次の通りに要約される。

(1) リスポンシブプロトコル検証の基本技術として，システム状態を効率良く生成する手法を提案している。そのために従来法と比較して，極めて緩い条件下で実時間を考慮したシステムモデルを導入している。これにより，生成されるシステム状態が現実のシステムの状況を厳密に表現しており，通信プロトコルの正確な検証を可能にしている。

(2) 通信プロトコルの検証は一般にいわゆる状態爆発を引き起こし，その回避が本質的な問題となっていた。本論文では，対象をクライアントサーバモデルで記述されたプラント制御システムのための通信システムに限定し，その上で動くリスポンシブプロトコルの検証コスト（状態数，メモリ容量，検証時間）の削減について議論している。提案法はクライアントサーバモデルがもつ対称性に基づいて，等価なシステム状態を1つにまとめた状態を生成するので，状態爆発を回避できる。更に，ある企業で実際に開発中のプロトコルを用いた評価実験によって，提案法では検証コストが非常に少なくなることを示している。

(3) リスポンシブプロトコルの設計では，一般に故障発生について数多くの状況を想定し，各状況毎に回復処理を1つずつ決めなければならない。しかし，あらゆる状況を網羅することは難しく，想定もれや記述誤りが設計仕様に混入する可能性が高い。本論文では，実時間論理を用いてリスポンシブプロトコルの設計誤りを効率良く検出する手法も提案している。更に，設計誤りの検出とその修正が短時間で行えることを，(2)と同様の実験によって示している。

以上のように，本論文はリスポンシブプロトコルの検証に関して重要な成果を示しており，特に通信システムの検証支援技術の理論分野に貢献するところが大きい。よって本論文は学位論文として価値あるものと認める。