様式Ｃ－１９

科学研究費助成事業（科学研究費補助金）研究成果報告書

平成 24 年 6 月 6 日現在

機関番号：14401
研究種目：基盤研究(C)
研究期間：2009～2011
課題番号：21560462
研究課題名（和文）
セキュアな離散事象システム設計のためのスーパバイザ制御
研究課題名（英文）
Supervisory Control for Design of Secure Discrete Event Systems
研究代表者
高井　重昌（TAKAI SHIGEMASA）
大阪大学・大学院工学研究科・教授
研究者番号：60243177

研究成果の概要（和文）：離散事象システムのスーパバイザ制御理論を応用したセキュアなシステム設計の基礎となる理論的成果が得られた．秘匿性を保証するスーパバイザの設計アルゴリズムを開発し，ある条件のもとで，そのようなスーパバイザのモジュラ設計が可能であることを明らかにした．さらに，それらの成果をネットワーク化システム，リアルタイムシステムへ適用するために必要となる離散事象システムの分散制御，リアルタイム制御に関する成果も得られた．

研究成果の概要(英文)：Several theoretical results which form the base for design of secure systems using the supervisory control theory for discrete event systems have been obtained. An algorithm for synthesizing a secrecy-enforcing supervisor has been developed. It has been proved that, under a certain assumption, the modular synthesis of such a supervisor is possible. Further, in order to apply these results to networked systems and real-time systems, certain results on decentralized control and real-time control of discrete event systems have been derived.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
2009 年度	1,100,000	330,000	1,430,000
2010 年度	1,000,000	300,000	1,300,000
2011 年度	1,000,000	300,000	1,300,000
年度			
年度			
総　計	3,100,000	930,000	4,030,000

研究分野：工学
科研費の分科・細目：電気電子工学・制御工学
キーワード：システム理論，離散事象システム，セキュアシステム，スーパバイザ制御

１．研究開始当初の背景

個人情報を扱うような情報システムにおいて，その保持する個人情報が外部に漏れることを防ぐことは社会的責任として非常に重要である．また，企業など様々な組織においては，その機密情報を守る必要がある．このような背景から，セキュアなシステム設計に関する研究が様々な方面から盛んに行われている．コンピュータサイエンスの分野においては，対象システムの動作，および匿名性，不干渉性などの情報流の秘匿性に関する性質を形式的に記述し，それらの性質をモデル上で自動的に検証しようとする形式検証の研究が行われている．

もし検証結果から，例えば匿名性が保証されないことがわかった場合，それが保証されるようにシステムの動作を変更することが必要となる．しかし，コンピュータサイエンスにおける形式検証は，その結果から，どのようにシステムの動作を変更すればよいかの示唆を与えてくれる場合もあるが，システマチックな変更方法を教示するものではない．そのため，秘匿性が保証されるようにシステムの動作をシステマチックに変更する方法を開発することは重要な研究課題である．

２．研究の目的

本研究では，離散事象システムのスーパバイザ制御理論を応用した，セキュアなシステム設計に関する研究を行う．スーパバイザ制御は，与えられた制御仕様が満足されるように，可制御事象の生起を動的に制御することで対象システムの動作を制限する制御手法である．そこで，もし与えられたシステムにおいて秘匿性に関する性質が満足されない場合，その性質が満足されるようにシステムの動作を必要最小限に制限する最大許容スーパバイザをシステマチックに設計することで，セキュアなシステムを構築する．研究内容の詳細は以下の通りである．

(1) まず，秘匿性の概念をスーパバイザ制御の枠組みで定義し，その秘匿性が保証されるか否かを判定するアルゴリズムを開発する．

(2) もし秘匿性が保証されない場合は，スーパバイザ制御を用いて対象システムの動作を制限することにより，情報の秘匿性が保証されるようにする．そこでまず，秘匿性およびノンブロッキング性の両方を保証するような最大許容スーパバイザの存在性を明らかにする．そして，そのような最大許容スーパバイザの計算可能性についての理論的解析を行う．

(3) 物理的制約などにより，スーパバイザが事象の生起を完全には観測できない場合が考えられる．そこで，得られた設計アルゴリズムを拡張することで，部分観測スーパバイザの設計を可能にする．

３．研究の方法

本研究では，数学モデルに基づくシステム理論的アプローチを用いる．

秘匿性の概念をスーパバイザ制御の枠組みにおいて定義するため，対象システムおよび秘匿にしたいシステムの振舞いを有限オートマトンで記述する．そして，システムの各事象に対して，対応する出力シンボルが一意に存在し，外部の観測者はシステムで事象が生起する度に，その出力シンボルが観測できるとする．ただし，出力シンボルが空列となること，また，複数の事象が同一の出力シンボルを持つことを許す．よって，観測者は一般に，観測した出力シンボル列からシステムの動作，つまり生起した事象列を一意に特定することができない．このような状況の下で，有限オートマトンモデルおよび観測者の観測情報に基づき，秘匿性を定義する．そして，有限オートマトンモデルに基づき，秘匿性を検証するアルゴリズムを開発し，その計算量の理論的解析を行う．

つぎに，秘匿性を保証する最大許容スーパバイザの存在性を理論的に証明する．その上で，最大許容スーパバイザの設計問題に取り組む．通常のスーパバイザ制御においては，最大許容スーパバイザの計算は最大可制御部分言語の計算に帰着される．本研究では，秘匿性を保証するような最大可制御部分言語を計算する必要がある．そこで，そのような最大可制御部分言語の計算について考察する．最大許容スーパバイザが計算不可能である場合には，計算可能性を保証するための制約条件を新たに加え，必ずしも最大許容とはならないが，計算可能性が保証されるようなスーパバイザの計算アルゴリズムを開発する．そして，この計算アルゴリズムを部分観測スーパバイザの設計が可能となるように拡張する．

さらに，得られた成果をネットワーク化システム，リアルタイムシステムへ適用するために必要となる，離散事象システムの分散制御，リアルタイム制御に関する研究を行う．

また，離散事象システムにおける秘匿性の問題は，特定の事象列の生起の検出，予知に関する離散事象システムの診断問題と密接な関係がある．そこで，診断問題に関する研究を行い，得られた知見を秘匿性の問題解決に利用する．

なお，本研究を実施するために使用する主な設備はパーソナルコンピュータであり，スーパバイザの設計，シミュレーションなどに用いる．

４．研究成果

(1) 離散事象システムのスーパバイザ制御理論を応用したセキュアなシステム設計の基礎となる理論的成果が得られた．

① スーパバイザ制御理論の枠組みにおいて，情報流の秘匿性の概念を定義した．そして，有限オートマトンモデルに基づく秘匿性検証のためのアルゴリズムを開発し，その計算量の理論的解析を行った．

② 検証の結果，システムにおいて秘匿性が保証されないと判定された場合には，スーパ

バイザ制御により，システムの振舞いを制限することで，秘匿性を保証する．そこで，システムの動作の制限を最小にするという意味で最適な最大許容スーパバイザが存在することを証明した．さらに，最適性は保証されないが，有限ステップで計算可能なスーパバイザの設計アルゴリズムを開発した．

③ 本研究で定義した秘匿性の概念の特別な場合であるオパシティを保証するためのスーパバイザ制御について考察した．特に，システムにおける秘匿すべき動作が複数の言語の交わりで与えられる場合において，それぞれ言語ごとにオパシティを保証する最大許容スーパバイザを構成し，それらの合成により，すべての言語に関してオパシティを保証するような最大許容スーパバイザを得るモジュラ設計が可能であるための十分条件を導出した．このようなモジュラ設計法には，秘匿すべき動作の部分的な変更に対して，スーパバイザの再構成が容易である，などの利点がある．さらに，得られた十分条件のもとでは，最大許容スーパバイザは外部の観測者が観測できる事象だけを観測する部分観測スーパバイザとして構成できる．

①で述べた秘匿性の定義は，スーパバイザ制御において従来用いられていた定義の一般化となっている．さらに，秘匿性を保証するためのスーパバイザ制御の先行研究においては，システムの振舞いのノンブロッキング性が考慮されておらず，最大許容スーパバイザのモジュラ設計法についても考察されていなかった．②，③で述べた本研究の成果は，従来研究では未解決であったこれらの重要な課題を解決するものである．

(2) (1)で述べた成果をネットワーク化システム，リアルタイムシステムへ適用するために必要となる，離散事象システムの分散スーパバイザ制御，リアルタイムスーパバイザ制御に関する研究を行った．得られた主な成果は以下の通りである．

① 各サブシステムが独自の制御仕様を有する大規模離散事象システムを対象とした分散スーパバイザ制御について考察した．そのような大規模システムに対しては，サブシステムごとにローカルスーパバイザを構成する分散制御が有効である．そこで，分散制御により各サブシステムにおいて独自の制御仕様が満足されるための必要十分条件を導出した．さらに，その存在条件が満足される場合において，各ローカルスーパバイザの構成法を示した．

② 1 単位時間の経過を tick という事象の生起で表現するような，時間付き離散事象システムを対象としたリアルタイムスーパバイザ制御について考察した．リアルタイム制約を有する離散事象システムに対しては，スーパバイザはその生起を許容する事象の集合に加え，生起を強制する事象の集合を決定する必要がある．そこで，強制すべき事象を決定する方法を提案し，従来研究で得られていたスーパバイザが存在するための必要十分条件に比べ，簡単化された見通しのよい必要十分条件を導出した．

③ ②で述べた研究成果に基づき，時間付き離散事象システムの分散スーパバイザ制御について考察した．分散スーパバイザ制御においては，各ローカルスーパバイザの制御判断を統合する必要がある．そこで本研究では，複数のローカルスーパバイザの事象の強制に関する判断を AND ルール，OR ルールで統合する場合を考え，それぞれの場合について制御仕様が満足されるような分散スーパバイザが存在するための必要十分条件を導出した．さらに，導出した必要十分条件を判定するためのアルゴリズムを開発し，その計算量解析を行った．

離散事象システムの分散スーパバイザ制御に関する多くの研究では，制御仕様は全体システムに関して与えられており，各サブシステムにおいて，独自の制御仕様が満足されるためのスーパバイザ制御についてはこれまで考察されていなかった．①で述べた研究は，分散スーパバイザ制御に関する既存の研究結果を補完するものである．また，時間付き離散事象システムの分散スーパバイザ制御において，事象の強制に関する各ローカルスーパバイザの制御判断の統合は本研究で初めて考察されたものであり，③で述べた研究成果は，分散スーパバイザ制御に関する新たな知見を与えるものである．

(3) 離散事象システムにおける秘匿性の問題は，特定の事象列の生起の検出，予知に関する離散事象システムの診断問題と密接な関係がある．そこで，得られた知見を秘匿性の問題解決に利用することを目的に，離散事象システムの診断に関する研究を行い，以下の成果が得られた．

① 各ローカル診断器がシステムに関するローカルな観測情報に基づき診断を行う分散型診断により，特定の事象列の生起の予知が可能であるための必要十分条件を導出し，その条件を判定するためのアルゴリズムを提案した．そして，そのアルゴリズムの計算量解析を行った．さらに，各ローカル診断器によるオンライン診断アルゴリズムを提案した．

② 各ローカル診断器がローカルな観測情報を互いに通信しあうような分散型診断において，有限の通信遅れを陽に考慮したもとで，特定の事象列の生起の予知が可能であるための必要十分条件を導出し，その条件を判定するためのアルゴリズムを提案した．そして，そのアルゴリズムの計算量解析を行った．

③ モバイルシステムに見られるような，各事象に対応する出力記号の状態依存性，非決定性のもとで，特定の事象列の生起が分散型診断により検出できるための必要十分条件を導出し，その条件を判定するためのアルゴリズムを提案した．さらに，そのアルゴリズムの計算量解析を行った．

④ 離散事象システムの分散型診断において，各ローカル診断器が他のローカル診断器の判断を推論して診断を行う枠組みを提案した．そして，その枠組みのもとで，特定の事象列の生起の検出，予知が可能であるための必要十分条件を導出し，その条件を判定するためのアルゴリズムを提案した．そして，そのアルゴリズムの計算量解析を行った．

分散型診断による特定の事象列の生起の予知に関する研究はこれまでになく，①で述べた研究が最初であり，離散事象システムの分散型診断において新たな知見を与えるものである．さらに，②で述べた研究は，各ローカル診断器間での観測情報の通信を許した，①の研究の拡張となっている．また，③で述べた成果は，既存の分散型診断の研究結果をモバイルシステムへの応用を目指して拡張したものである．さらに，④で述べた成果は，従来の分散型診断の枠組みを特別な場合として含む，より一般的な枠組みを提案したものであり，現在，離散事象システムの分散型診断の最も一般的な枠組みとなっている．

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計 12 件）

① Shigemasa Takai, Ratnesh Kumar: Distributed failure prognosis of discrete event systems with bounded-delay communications, IEEE Transactions on Automatic Control, 査読有, Vol. 57, No. 5, 2012, pp. 1259-1265, DOI:10.1109/TAC.2011.2173419

② Shigemasa Takai, Toshimitsu Ushio: Verification of codiagnosability for discrete event systems modeled by Mealy automata with nondeterministic output functions, IEEE Transactions on Automatic Control, 査読有, Vol. 57, No. 3, 2012, pp. 798-804, DOI:10.1109/TAC.2012.2185881

③ Masashi Nomura, Shigemasa Takai: Decentralized supervisory control of timed discrete event systems, IEICE Transactions on Fundamentals, 査読有, Vol. E94-A, No. 12, 2011, pp. 2802-2809, DOI:10.1587/transfun.E94.A.2802

④ Shigemasa Takai, Yuta Watanabe: Modular synthesis of maximally permissive opacity-enforcing supervisors for discrete event systems, IEICE Transactions on Fundamentals, 査読有, Vol. E94-A, No. 3, 2011, pp. 1041-1044, DOI:10.1587/transfun.E94.A.1041

⑤ Shigemasa Takai, Ratnesh Kumar: Inference-based decentralized prognosis in discrete event systems, IEEE Transactions on Automatic Control, 査読有, Vol. 56, No. 1, 2011, pp. 165-171, DOI:10.1109/TAC.2010.2085590

⑥ Shigemasa Takai, Ratnesh Kumar: Synthesis of over-approximating inference-based decentralized supervisors for discrete event systems, IEEE Transactions on Automatic Control, 査読有, Vol. 55, No. 8, 2010, pp. 1881-1887, DOI:10.1109/TAC.2010.2048634

⑦ Shengbing Jiang, Ratnesh Kumar, Shigemasa Takai, Wenbin Qiu: Decentralized control of discrete event systems with multiple local specifications, IEEE Transactions on Automation Science and Engineering, 査読有, Vol. 7, No. 3, 2010, pp. 512-522, DOI:10.1109/TASE.2009.2025865

⑧ Shigemasa Takai, Ratnesh Kumar: Decentralized diagnosis for nonfailures of discrete event systems using inference-based ambiguity management, IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans, 査読有, Vol. 40, No. 2, 2010, pp. 406-412, DOI:10.1109/TSMCA.2009.2036939

⑨ Ratnesh Kumar, Shigemasa Takai: Decentralized prognosis of failures in

discrete event systems, IEEE Transactions on Automatic Control, 査読有, Vol. 55, No. 1, 2010, pp. 48-59, DOI:10.1109/TAC.2009.2034216

⑩ Ratnesh Kumar, Shigemasa Takai: Inference-based ambiguity management in decentralized decision-making: Decentralized diagnosis of discrete-event systems, IEEE Transactions on Automation Science and Engineering, 査読有, Vol. 6, No. 3, 2009, pp. 479-491, DOI:10.1109/TASE.2009.2021330

〔学会発表〕(計5件)

① Masashi Nomura: A new forcing mechanism for decentralized supervisory control of timed discrete event systems, The 26th International Technical Conference on Circuits/Systems, Computers and Communications, 2011年6月20日, Hyundai Hotel (Gyeongju, Korea)

② Shigemasa Takai: Robust failure diagnosis of partially observed discrete event systems, The 10th International Workshop on Discrete Event Systems, 2010年8月31日, Technische Universität Berlin (Berlin, Germany)

③ Shigemasa Takai: Decentralized diagnosis of discrete event systems modeled by Mealy automata with nondeterministic output functions, The 2010 American Control Conference, 2010年7月1日, Baltimore Marriot Waterfront (Baltimore, USA)

④ Shigemasa Takai: Distributed prognosis of discrete event systems under bounded-delay communications, The 48th IEEE Conference on Decision and Control, and the 28th Chinese Control Conference, 2009年12月16日, 上海国際会議センター(上海, 中国)

⑤ Shigemasa Takai: Verification and synthesis for secrecy in discrete-event systems, The 2009 American Control Conference, 2009年6月12日, Hyatt Regency St. Louis Riverfront (Saint Louis, USA)

〔その他〕
ホームページ等
http://is.eei.eng.osaka-u.ac.jp/takai/

６．研究組織
(1)研究代表者

高井　重昌 (TAKAI SHIGEMASA)
大阪大学・大学院工学研究科・教授
研究者番号：60243177

(2)研究分担者
(　　)

研究者番号：

(3)連携研究者
(　　)

研究者番号：