様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ６ 月　 ９ 日現在

機関番号：３２６６５
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ００１１１

研究課題名（和文）組み合わせテストを応用した組込みシステムの検証項目生成の研究

研究課題名（英文）A Research on property generation for embedded systems based on combination testing methodology

研究代表者
関澤　俊弦（Sekizawa, Toshifusa）

日本大学・工学部・准教授

研究者番号：１０５４９３１４

交付決定額（研究期間全体）：（直接経費）　　3,400,000円

研究成果の概要（和文）：本研究課題の目的は，センサー等で外部環境の情報を取得するサイバーフィジカルシステムに対して，情報システムの信頼性保証技術の一つであるモデル検査の適用により，システムの振舞いについて検証を行なうことである．この目的に対して，ロボティックス領域や，アドホックネットーワークにおける確率的な振舞いを含む系を具体的な対象として，対象物の位置を推定する自己位置推定アルゴリズムに基づく系にモデル検査を適用することにより，系の振舞いを保証できることを示した．また，系が望ましくない振舞いを示す際に，望ましい性質が成り立たない証拠である反例を応用することにより，系へのフィードバックする手法を示した．

研究成果の学術的意義や社会的意義
本研究は，組込みシステムの一つであるロボット制御やアドホックネットワーク環境において，ロボットやデバイスなどの移動体に加えて外部環境を含めて検証を行なうことにより，自己位置推定を可能とする系の構築手法を示した．自律移動やネットワーク領域において，自己位置推定は要素技術の一つである．本研究はGPS機能を持たない対象を想定しており，GPSなどに頼らずに位置推定を実現できる手法を示している．これは，信頼性が保証される情報システムの構築に寄与すると考える．

研究成果の概要（英文）：This research is a study of a method to ensure reliability of cyber physical systems that correct external information using sensors, by applying model checking technique which is one of reliability ensuring techniques for information systems. For this purpose, we set systems based on robotics and ad-hoc networks with uncertainty behaviors, as concrete targets. We applied model checking technique and property generation to systems based on self-localization algorithm, and showed reliability can be ensured by our proposed approach. As a result, it is possible to construct systems which show expected behaviors. Additionally, we showed a method to feed back to systems by applying analysis results of counter example that is an evidence that the expected property does not hold, when the systems exhibits undesired behaviors.

研究分野：ソフトウェア工学

キーワード：モデル検査　確率系　ロボティックス　アドホックネットワーク

様　式　C－１９、F－１９－１、Z－１９（共通）

１．研究開始当初の背景

本研究の研究開始時には，車載システムなどの組込み制御システムが社会に広く普及し，センサ等を用いて外部環境の情報を取得するサイバーフィジカルシステム (CPS: Cyber Physical System) の活用が広まりつつあった．CPS の普及と共に，その品質に対する保証の重要性も増してきていた．CPS では，センサ等により外部環境の情報を得るため，センサの読み取り誤差やノイズなどの外乱など様々な要因により，システムの振舞いには不確実さが生じる．CPS の研究開発にあたっては，不確実さを考慮に入れる手法が必要とされている．

形式手法の一つであるモデル検査は，情報システムの信頼性保証技術の一つであり，システムが仕様を満たすことを，状態空間の網羅的な探索により検証する手法である．ツールの整備が進んできたことから，モデル検査はその実用性の高さで多くの対象に適用されており，その使用が国際規格で推奨されるなどシステム開発への適用が広がりつつあった．モデル検査は，検証対象を表わすモデルと，仕様を表わす検査式を入力とする．検査式が成り立たない場合，モデル検査器によっては，成り立たない証拠である反例を出力する機能を備えている．モデル検査は成熟してきたと言われているが，検査式の構成や反例の活用，確率的な振舞いを示す系への適用手法など，解決するべき問題が残っている．

２．研究の目的

本研究は，組込み制御システムなどにおける不確実さを含む系の振舞いや仕様の信頼性の検証や，モデル検査における検査項目の生成，反例の活用を含めたモデルの再構築手法を目的とする．モデル検査は，対象を表わすモデルと対象系が満たすべき仕様を記述した論理式を入力として，網羅的な検証を行なう．本研究では，モデル検査において，検査項目が成り立たないときに，仕様が満たされない証拠である反例を活用する手法も目的とする．また，不確実さを含む対象は確率系として扱うことができるが，確率系のモデル検査では反例が生成されないことがある．このような系に対するモデル検査の適用手法も目的とする．

３．研究の方法

本研究では，センサ等を用いて外部環境の情報を参照して動作するロボットを具体的な対象とした．ここで，外部環境の情報を得る際に，センサやシステム外の要因に起因する測定誤差を考慮することにより，対象の系は不確実さをもつとした．ロボットの動作は，系において自己位置を推定するマルコフ位置推定アルゴリズムに基づくとした．マルコフ位置推定は，ロボティクス領域で用いられており，信念と呼ばれる確率分布を考えることで位置を推定するアルゴリズムである．位置の一様分布から，移動と観測を繰り返すことにより，位置の存在確率を求める．

（1）モデル化と検査項目の生成

壁やドアなどの測定可能な構造物を配置した地図上で動作する，マルコフ位置推定に基づくロボットの振舞いをモデル化の対象とする．マルコフ位置推定は連続系に対するアルゴリズムであるが，モデル検査は連続系の扱いには不向きなため，モデル化にあたっては，マルコフ位置推定を離散系に適用できるアルゴリズムとする．また，不確実さとしてセンサの誤検知を考え，外部環境の情報を取得する際に確率的に誤検知が発生するとする．この不確実さもモデル化に含める．これらの設定により，動作は非決定性で説明できる一方，確率的な要因も含むことになる．検査項目は対象系に依存するが，地図上の構造物の配置パターンによりロボットの動作が影響を受けることから，各配置パターンに対する期待される振舞いと，最終的に一意に位置を推定できる性質を生成する．図 1 に対象系のモデル化の例を示す．

（2）検証

方法（1）で構成したモデルと検査項目をモデル検査の入力として検証を行なう．反例の生成手法が十分に確立していないため，確率モデル検査では反例の取得が困難である．従って，確率を除去したモデルに対する検証を行なうことで反例を取得する．確率を除去することにより，検証可能な性質は限定されるが，到達可能性などの仕様が検証可能である．ここでは，確率を除去するためにモデルおよび検査項目を変換する．

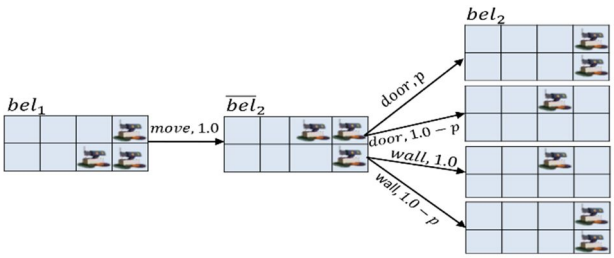

図 1: 対象系のモデル化

（3）対象系の拡張

本研究は，研究期間の途中で研究分担者の追加申請を行ない承認されている．これは，方法（1）および（2）の手法を，アドホックネットワークにおけるゲートウェイ配置問題にも応用可能であると考えたためである．ロボットの動作に関する検証では，検証対象はロボット自身であるが，ゲートウェイ配置問題ではゲートウェイからの信号到達数などを考慮したゲートウェイの再配置への適用となる．

４．研究成果

構造物を含む地図上でのマルコフ位置推定に基づくロボットの振舞いが検証可能であること

を示し，検証における問題点を明らかにするために，離散的な 2 次元系に対して検証を行なった．ここでは，対象系の拡張も見据えて，動作に不確実さを含むとした．これは，モデル化と構造物の配置による検査項目の生成に基づくモデル検査の適用可能性を探る取り組みである．結果として，地図のサイズに制限を設けるなど一定の制約元でマルコフ位置推定に基づくロボットの位置推定が検証可能であることを示した．具体的には，地図およびマルコフ位置推定アルゴリズムを離散化し，地図上に配置される構造物の取り得る値を二値に制限するなどの制約を設けてモデル化している．モデル検査の適用において問題となる状態数爆発問題に対応するために，地図に周期的境界条件を適用することにより同じパターンが繰り返される地図を表現し，状態空間の大きさを抑制する手法を用いた．予備的な検証の結果では，ロボットの振舞いは地図上の構造物の配置パターンにより位置推定の可否が変わることを確認した．これはモデル化の際に設けた制約に依存する要因も含まれていたため，構造物の配置を組合せ問題とみなして，各種の組み合わせに対して部分的な検証を行なった．これらの検証により，自己位置推定に対する検証が可能であることを示した．これらの検証では確率モデル検査器 PRISM を使用している．

自己位置推定へのモデル検査の適用が可能である結果を受け，自己位置推定ができない場合にロボットの振舞いを変えることにより，自己位置推定を可能とする手法に取り組んだ．具体的には，モデル検査の反例を活用することにより自己位置が推定できない理由を特定し，特定された理由に基づいて振舞いを変える．ここで，確率モデル検査器 PRISM は反例の生成機能を持たないため，確率を含むモデルから確率を除去したモデルへの変換を行ない，反例を生成可能なモデル検査器 SPIN で検証を行なう．図 2 に確率的振舞いの除去と検証の関連を示す．具体的には，1)確率的な振舞いを含む PRISM モデルを SPIN モデルに変換する，2)SPIN モデルに対する検証により反例を得る，3)反例の解析により自己位置推定ができない原因である構造物の配置パターンと動作の組み合わせを特定し，特定のパターンに対する動作を変更する，4)動作を変更したモデルを再構築し，自己位置が推定可能になるまで 2)と 3)を繰り返す，5)自己位置推定を可能とする動作を確率モデルに反映する．ここで，確率を除去することにより，確率的な振舞いの検証は検証できなくなるが，自己位置推定は到達可能性として表現できることから，確率を除去しても一定の性質を検証できることを示した．この取り組みは，ロボットの動作を変更の対象としているが，系を構成する因子や再帰的なモデル構成の手法であり，検証結果を対象系にフィードバックする手法の一つと考えられる．

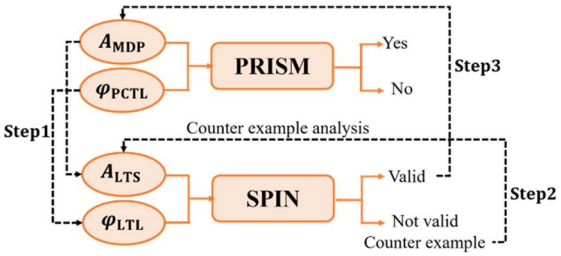

図 2: 確率的振舞いの除去と検証

これまでの取り組みでは，対象系の動作へのフィードバックを行なうことにより，仕様を満たしていた．対象系における構造物の配置パターンへのフィードバックも可能であるため，本研究の上記の研究成果の適用領域を拡張して，アドホックネットワークにおけるゲートウェイ配置問題に取り組んだ．研究代表者の専門領域はネットワークとは異なるため，この段階でネットワークを専門とする研究分担者 1 名に新たに参加していただき，ネットワーク領域における要件の確認や手法の適用可能性などを協力して取り組んでいる．この取り組みでは，GPS などの位置を特定する機能を持たないデバイスや屋内などの環境において，アドホックネットワーク上で，デバイスが位置推定を可能とするゲートウェイの配置手法を示すものである．具体的には，1)ゲートウェイの初期配置方法を定める．ここではネットワークの運用による制約として最低限の数のゲートウェイを配置する．配置方法としては均等配置などのポリシーを定める，2)ゲートウェイ配置とゲートウェイからの信号の受信数により自己位置推定が可能か否かをモデル検査により検証する．3)位置推定が可能でない場合，ゲートウェイを再配置する．再配置にあたっては，ゲートウェイの配置を変える方針であるルールに従って位置を変えることにより再構成する，4)再構成したゲートウェイ配置が自己位置推定を可能とするか否かの検証と，推定できない場合の再配置を繰り返す．この取り組みにより，ゲートウェイの配置問題に対して一つの解法を示した．図 3 にゲートウェイの再配置結果の例を示す．ネットワークに接続するモバイルデバイスは近接したゲートウェイを選択することにより省電力化を実現することや，ゲートウェイ配置に求められる要件を満たしつつ最小限のゲートウェイの配置の実現に繋がると考えられる．

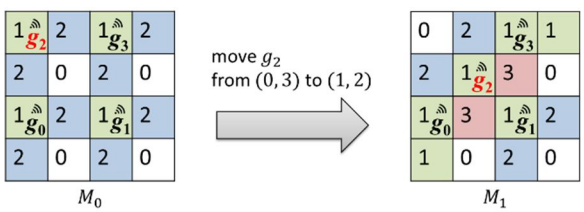

図 3: ゲートウェイの再配置

これらの取り組みは，「移動」と「観測」および「地図上の特徴」として抽象化が可能である．また，検査項目も地図を構成する構造物の配置パターンの組み合わせに基づいて部分的な検証を可能とする．自己位置の推定や要件を満たす地図の構築は，高度道路交通システムにおける物流の効率化や，車載機器との通信で用いられる狭域通信システムなど様々な応用が考えられる．また，本研究では不確実さの要因を定めていないが，GPS スプーフィングなどサイバーセキュリティにかかわる不確実さへの応用が考えられる．

５．主な発表論文等

〔雑誌論文〕　計1件（うち査読付論文　1件／うち国際共著　0件／うちオープンアクセス　0件）

１．著者名 Kozo Okano, Satoshi Harauchi, Toshifusa Sekizawa, Shinpei Ogata, and Shin Nakajima	４．巻 E102-D/ 8
２．論文標題 Consistency Checking between Java Equals and hashCode Methods Using Software Analysis Workbench	５．発行年 2019年
３．雑誌名 IEICE TRANSACTIONS on Information and Systems	６．最初と最後の頁 1498-1505
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018EDP7254	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

〔学会発表〕　計11件（うち招待講演　0件／うち国際学会　6件）

１．発表者名 Toshifusa Sekizawa, Qian Chen, and Taiju Mikoshi
２．発表標題 Recursive Gateway Allocation Combined with Self-localization and Model Checking in Mobile Ad-hoc Networks
３．学会等名 Tenth International Symposium on Information and Communication Technology（国際学会）
４．発表年 2019年

１．発表者名 Masashi Nakamura, Kozo Okano, Shinpei Ogata, and Toshifusa Sekizawa
２．発表標題 A review assistance system for class diagram with voice assistance based on NLP
３．学会等名 International Workshop on Informatics（国際学会）
４．発表年 2019年

１．発表者名 Kozo Okano, Kazuma Takahashi, Shinpei Ogata, and Toshifusa Sekizawa
２．発表標題 Analysis of Specification in Japanese Using Natural Language Processing
３．学会等名 Joint Conference on Knowledge-Based Software Engineering 2018（国際学会）
４．発表年 2018年

１．発表者名
Toshifusa Sekizawa, Taiju Mikoshi, Masataka Nagura, Ryo Watanabe, Qian Chen

２．発表標題
Probabilistic Position Estimation and Model Checking for Resource-Constrained IoT Devices

３．学会等名
The 8th International Workshop on Internet on Things: Privacy, Security and Trust（国際学会）

４．発表年
2018年

１．発表者名
Ryo Watanabe, and Toshifusa Sekizawa

２．発表標題
Counter Example Analysis of Robot Action Design for Self-localization Based on Model Checking using Probability Removed Model

３．学会等名
IEEE 4th International Conference on Computer and Communication Systems（国際学会）

４．発表年
2019年

１．発表者名
矢吹光，関澤俊弦

２．発表標題
ロボットの振る舞いの確率的な解空間からの解の選択手法の提案と協調解析の考察

３．学会等名
IPSJ 東北支部研究会

４．発表年
2019年

１．発表者名
渡邉亮，関澤俊弦

２．発表標題
確率除去モデルを用いたモデル検査に基づく自己位置推定の地図設計に対する反例解析

３．学会等名
IPSJ 東北支部研究会

４．発表年
2019年

１．発表者名
Ryo Watanabe, Kozo Okano, and Toshifusa Sekizawa

２．発表標題
Towards Verification of Robot Design for Self-localization

３．学会等名
13th International Haifa Verification Conference（国際学会）

４．発表年
2017年

１．発表者名
渡邊亮，岡野浩三 ，関澤俊弦

２．発表標題
自己位置推定を行なうロボット設計の検証に向けて

３．学会等名
IPSJ/SIGSE SES2017 ワークショップ

４．発表年
2017年

１．発表者名
矢吹光，関澤俊弦

２．発表標題
自己位置推定をするロボットの確率的な振舞いの協調解析に向けて

３．学会等名
JSSST FOSE2017

４．発表年
2017年

１．発表者名
渡邊亮，岡野浩三，関澤俊弦

２．発表標題
モデル検査を用いたロボット設計の検証

３．学会等名
JSSST FOSE2017

４．発表年
2017年

〔図書〕　計0件

〔産業財産権〕

〔その他〕

―

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考
研究分担者	岡野　浩三 (Okano Kozo) (70252632)	信州大学・学術研究院工学系・准教授 (13601)	
研究分担者	見越　大樹 (Mikoshi Taiju) (00634114)	日本大学・工学部・准教授 (32665)	