



HOKKAIDO UNIVERSITY

Title	Scenario Verification for Proximity-Based Federation of Smart Objects Using Model Checking [an abstract of dissertation and a summary of dissertation review]
Author(s)	蓑田, 玲緒奈
Degree Grantor	北海道大学
Degree Name	博士(情報科学)
Dissertation Number	甲第13081号
Issue Date	2018-03-22
Doc URL	https://hdl.handle.net/2115/70416
Rights(URL)	https://creativecommons.org/licenses/by-nc-sa/4.0/
Type	doctoral thesis
File Information	Reona_Minoda_abstract.pdf, 論文内容の要旨



学 位 論 文 内 容 の 要 旨

博士の専攻分野の名称 博士（情報科学） 氏名 蓑田 玲緒奈

学 位 論 文 題 名

Scenario Verification for Proximity-Based Federation of Smart Objects Using Model Checking (モデル検査によるスマートオブジェクトの近接連携シナリオの形式検証)

本論文では、生活の利便性向上を目的としたユビキタスコンピューティング (UC) におけるデバイス連携の信頼性を検証する形式手法を提案する。昨今、複数のデバイスを連携することで、様々な状況に応じて、状況に適したサービスをユーザーに提供するような UC は、センシング技術向上と低コスト化により、社会インフラとして実用化されつつある。例えば、外国人観光客に対して、入国から、滞在、出国に至るまでに必要なサービス提供のシナリオを定義し (以降では、UC シナリオと称する)、それらを統一化されたプラットフォームで提供する試みがある。一方で、こういった UC シナリオの形式的な記述を目的に、田中や Julia は、触媒反応ネットワークに基づくモデル (CRN) を用いたデバイス同士の連携方法を記述するモデルを提案したが、そのモデルによって記述された UC シナリオの正当性を検証する手法が確立されていなかった。これらの背景がある中で、UC を用いたサービスをインフラとして実用化するためには、UC シナリオの設計の妥当性の検証や信頼性の評価をするフレームワークが重要であり、本論文ではこの目的のために、1) デバイス連携により提供するサービスの信頼性検証、2) 大規模な UC シナリオに対応可能な形式手法への拡張、3) 信頼性とコストのトレードオフ関係の定量化、の 3 つのフレームワークを提案する。

1) デバイス連携により提供するサービスの信頼性検証

UC シナリオを状態遷移モデル上で扱うために、デバイス同士の連携方法を記述した CRN モデルに、ユーザーの移動トポロジをグラフで表現する要素を加えることで拡張した Context Catalytic Reaction Network (CCRN) という UC シナリオの記述モデルを提案する。ユーザーの位置情報とデバイス連携の組合せで定義した状態表現を用いることで、CCRN によって記述された UC シナリオを状態遷移モデルへ変換する手法も提案する。さらに、主に電子回路設計の分野で産業的に広く使われるモデル検査手法を本モデルに適用することで、デバイス連携の信頼性を形式手法により検証する枠組みを提案する。この手法により、UC の様々なサービスを設計する際に、設計上の欠陥を「ユーザーの移動経路によってはデバイス連携に問題が生じる」という反例として発見できる。

2) 大規模な UC シナリオに対応可能な形式手法への拡張

より大規模な UC シナリオを効率的に検証するために、記号モデル検査と呼ばれる手法を UC シナリオの信頼性検証に適用する方法を提案する。具体的には、記号モデル検査は状態遷移モデルにおける複数の遷移をまとめてコンパクトに表現することが可能であるが、これを用いて、1) の手法において扱うデバイス数の増大により発生していたデバイス連携の組合せ爆発に対処する手法を提案する。同一実験環境下において、1) の手法では計算機のメモリ不足により検証が難しかった規模の検証が可能になることを実験的に示す。

3) 信頼性とコストのトレードオフ関係の定量化

外乱によるデバイス同士の連携の失敗や、ユーザーの行動の振る舞いの不確実性を考慮するより現実的な問題設定を確率の概念によって表現する手法を提案する。デバイス同士の連携を阻害する外

乱とユーザーの行動の振る舞いの不確実性の2つは、1)の提案で扱う状態遷移モデルの遷移に確率的なふるまいを持たせることに対応する。そこで1)の提案で扱ったCCRNモデルに確率の概念を導入することで拡張し、この拡張されたモデル Probabilistic CCRN に対して確率的モデル検査を行うフレームワークを提案することで UC シナリオの信頼性を定量的に評価する。これにより、UC シナリオの満たすべき信頼性を一定以上にするような、デバイス同士の連携の信頼性を定量的に求めることができる。また、デバイス同士の連携の信頼性向上のためのコストと UC シナリオの信頼性のトレードオフを数値で示すことが可能になる。

上に挙げた3つの提案により、本論文では UC シナリオの設計の妥当性を形式検証するフレームワークを確立する。形式検証は、ある対象を実際に実装する前の段階である設計の段階で欠陥を発見できるが、UC シナリオのように社会インフラを担う対象は実装にコストがかかるため、欠陥がないかを設計段階で網羅的に検証することは重要である。本論文で提案しているフレームワークは、形式的なアプローチである UC シナリオの形式検証に加えて、外乱や不確定性を考慮した理想的ではない条件下での UC シナリオの信頼性を評価しているが、これは、理論的な貢献に加えて、UC シナリオが実際に実装される際の信頼性とコストのトレードオフの議論の実現という実用的な貢献につながるものである。このことから、本論文で提案するフレームワークは理論的と実用的の両面で有用性がある。