形式手法による短距離無線通信規格の検証に関する研究

高村 純平 (610054)

北陸先端科学技術大学院大学 情報科学研究科

2008 年 2 月 7 日

キーワード: 形式手法, 短距離無線通信規格, CafeOBJ, 検証.

1 研究背景と目的

近年，RFID(Radio Frequency IDentification) の技術を利用した FeliCa や，Mifare の普及により，RFID 技術が注目されている．NFC(Near Field Communication) は RFID 技術を用いて，ソニーと NXP(旧フィリップス) が共同で開発した無線規格で，2003 年 12 月に国際標準規格となった．NFC は Felica，Mifare 等と通信互換性があり，様々な分野での応用を期待されている．一方，ソフトウェア開発等の分野では，信頼性確保のために形式手法が注目されている．形式手法は，文法や意味を厳密な数学モデルや論理体系に基づいて仕様記述，検証を行う手法で，自然言語や図，表などの曖昧な表現をなくすことができる．これにより，仕様記述の段階でソフトウェアのミスが早期に発見でき，開発をスムーズに行うことができ，信頼性を向上させることができる．形式仕様記述言語としてはさまざまなものが存在する．ここでは，通信プロトコルなどのシステムの仕様記述や検証に用いられ，実際に成果を上げている CafeOBJ を用いる．

本研究では，NFC の仕様を形式手法，具体的には代数仕様記述言語 CafeOBJ を用いて，OTS/CafeOBJ 法により，記述・検証を行うことによって，NFC の信頼性を明らかにする．また，検証により問題が発見できれば，仕様の改善によって，その問題を解決する．これにより，NFC に基づいたシステムの安全性，信頼性を高めることができる．

2 本研究のアプローチ

CafeOBJ は代数仕様言語に分類される形式仕様言語であり，仕様を構成する等式を書換規則と解釈して実行することが出来る．等式の実行は仕様の意味を想定する等式論理に忠実であるので CafeOBJ システムを用いた対話的検証が可能である．ある状態における値を観測するための観測関数，状態を更新させるための遷移関数を用いた仕様記述及び検証の方法として，OTS/CafeOBJ 法がある．OTS/CafeOBJ 法とは，具体的には，観測

遷移機械 OTS を代数仕様言語 CafeOBJ によって記述し，観測遷移機械が所望の性質を満たすかどうかを CafeOBJ によって証明する方法である．観測遷移機械 OTS(Observation Transition System) は，観測関数，遷移関数を用いてシステムの振舞をモデル化したものである．OTS は観測関数の集合，初期状態の集合，遷移規則の集合により定義される．

本研究で仕様記述，検証の対象とした NFC は，2003 年 12 月に ISO/IEC IS 18092 として国際基準となった短距離無線通信規格で，自身の無線電波領域で，複数の Target からの応答を確認すると，SDD(Single Device Detection) アルゴリズムによって，複数の Target から 1 つの Target を選択する．選択後はデータ転送プロトコルにより，データの交換を行う．その後，選択した Target を解放コマンドによって解放する．

この NFC プロトコルを OTS/CafeOBJ 法を用いて抽象的に記述し，OTS/CafeOBJ 法により記述した仕様が，1 つの Target と通信しているかといった性質を CafeOBJ によって検証する．

3　まとめと今後の課題

本稿では，国際標準規格となった NFC の仕様を代数仕様記述言語 CafeOBJ を用いて，OTS/CafeOBJ 法により，形式化し，検証を行った．NFC プロトコルでは複数の Target からの反応を想定しており，いくつかの Target から SDD アルゴリズムにより 1 つの Target を選択する．そこで，複数の Target から 1 つの Target を選択し，その Target を解放するまで，その Target とのみ通信を行うという性質の検証を行った．NFC の仕様書の記述通りでは，1 つの Target とのみ通信を行うという性質の検証には不十分ではないかと考え，Target を一度選択したら，解放するまで sel コマンドを送らないことや，選択した Target を解放するまで SDD アルゴリズムを始めないといった条件を加えた結果，検証をスムーズに行うことができた．それらを条件に追加することは，NFC プロトコルに基づいたシステムを作成，理解する際の支援となりえる．

今後の課題としては，1 つの Target とのみ通信するという性質を満たすために，NFC の仕様に最低限どのような条件を加えれば，性質を満たすのかといった限界について解析を行っていく．また，今回の CafeOBJ の仕様は，NFC プロトコルをある程度抽象化しているので，その抽象度をさげ，より具体的な NFC の CafeOBJ 仕様を記述し，その CafeOBJ 仕様についても検証を行っていく．