氏　　名	GUO Xiaoyun		
学位の種類	博士(情報科学)		
学位記番号	博情第 413 号		
学位授与年月日	平成 31 年 3 月 22 日		
論文題目	Model Checking of In-vehicle Networking Systems		
論文審査委員	主査　青木　利晃	北陸先端科学技術大学院大学	教授
	丹　康雄	同	教授
	平石　邦彦	同	教授
	鈴木　正人	同	准教授
	岡野　浩三	信州大学	准教授

論文の内容の要旨

In-vehicle networking (IVN) systems consist of electronic components that are connected by buses and communicate through multiple protocols according to their requirements. Communications between these subsystems are getting more complicated as the requirements for safety, comfort, and entertainment. Different communication protocols have their special mechanisms to transmit messages on buses, which affect safety and timed property of the IVN system. In practice, intelligent vehicles need to exchange safety data between subsystems that use various protocols, such as the Controller Area Network (CAN) and FlexRay. Such systems are more likely to encounter delays and message loss during transmission, presenting serious safety issues. Moreover, IVN systems are extremely complicated because of their large number of nodes, multiple communication protocols, and diverse topologies. As a result, it is difficult to check properties of the system directly and accurately. Besides, safety-critical events occur with a probability in the IVN system, such as the probability of failures and the probability of emergency events happened during driving. These probabilistic events are crucial to estimate real-time and reliability of the IVN system.

In this work, we propose a framework based on UPPAAL model checker, for modeling and verifying communicative behaviors between multiple protocols in an IVN system. Due to the complicated of the IVN system, we present an appropriate abstraction with two stages for modeling IVN systems that utilize CAN and FlexRay during the design phase. The architecture of the IVN system is abstracted to reduce the number of nodes first, and then the composition of each protocol is abstracted to simplify states of systems based on protocol specifications. As there are numerous IVN system structures, a reusable framework is developed to build a design model for IVN systems with different topologies. In the framework, an IVN system model consists of protocol, interface, configuration, forwarder and environments modules. The environments and forwarder modules are changeable according to system design. The protocol, interface and configuration modules are fixed to construct various IVN systems.

Using this framework, we check IVN systems from qualitative verification and quantitative verification. Through the qualitative verification, the timed properties of communication are analyzed using the UPPAAL platform; we verify the reachability and response time of messages in the best case and worst case. Through the quantitative verification, the probability of message reachability during a time interval is given by application probability models in the SMC-UPPAAL; the probability density and probability distribution of response time is used to analyze the frequency for receiving messages. The two verifications complement each other. The qualitative verification is exhaustive, but the efficiency and capability is limited. The quantitative verification is more efficient, but the properties are satisfied with some degree of confidence.

The framework is evaluated through several aspects. First, we evaluate the validity of the abstraction. The framework is preservation for outside of the subsystem, however, the inside of subsystem cannot be preserved. We list properties from specifications, and the framework is validated by checking the communication behavior against the protocol specifications and some properties can be checked. But some properties cannot be checked because of the abstraction. Second, we demonstrate the applicability of the framework with three typical topologies. Third, we compare source code of three different systems in UPPAAL, the framework is reusable for different system with little change. Finally, we show the performance of the framework in qualitative verification and quantitative verification.

Keywords: Model Checking, Statistical Model Checking, UPPAAL, In-vehicle Network System, CAN and FlexRay.

論文審査の結果の要旨

本博士論文では，複数のプロトコルを用いて構成されている車載ネットワークシステムの振る舞いをモデル検査により検証する手法を提案している．近年の車載システムには，数多くの ECU(Electronic Control Unit)が使われており，それらはネットワークで接続され協調動作している．また，車載システム開発のオープン化の流れから，複数のサプライヤの部品が自動車に用いられるようになり，それらを接続するプロトコルが異なる状況が生じている．この場合，ゲートウェイを用いて部品を接続するが，それにより，車載ネットワークシステムは，複数の異なるプロトコルが混在するヘテロジニアスな構成となる．このようなリアルタイム性を有するデータリンク同士の接続を含むネットワークシステムの取り扱いは容易ではなく，その動作の分析が困難であるのが現状である．そこで，本博士論文では，モデル検査ツール UPPAAL を用いて，そのような車載ネットワークシステムの検証および分析する手法を提案している．

モデル検査ツールで車載ネットワークシステムを取り扱う場合，状態数を削減する必要

がある．本博士論文では，FlexRay と CAN のプロトコルを取り扱っているが，それらの動作仕様は 100 ページ以上にわたり，そのままの動作をモデル検査ツールで取り扱うことはできない．また，ネットワークノードの数も多く，車載ネットワークシステムの実際のトポロジをそのまま扱うこともできない．そこで，本博士論文では，プロトコル動作の抽象化とネットワークトポロジの抽象化の 2 段階の抽象化を提案している．また，提案した抽象化に基づいて，UPPAAL で車載ネットワークシステムを検証するための再利用可能な枠組みも開発している．作成した枠組みは，通常のモデル検査と統計的モデル検査で利用することが可能である．前者では，与えられた性質に対して真偽値を返すのみであるが，後者では，その性質が成立する確率を獲得することができ，さらに，より規模の大きいモデルを取り扱うことができる．単一のプロトコルに基づいてネットワークシステムをモデル検査で検証する研究は存在するが，複数のプロトコルを取り扱うものは無く，この点に新規性，独創性がある．

以上，本博士論文は，モデル検査を実践応用するための手法を提案しており，学術的にも工業的にも貢献するところが大きい．よって，博士(情報科学)の学位論文として十分に価値があるものと認めた．