Model Checking of FlexRay Communication Protocol

Xiaoyun Guo (1010230)

School of Information Science,
Japan Advanced Institute of Science and Technology

August 14, 2012

Keywords: Automotive Systems, FlexRay, Model Checking, UPPAAL.

Nowadays, the automotive systems mainly adopt electronic control units (ECUs) to realize X-by-wire technology. With the X-by-wire technology, the requirements or functionalities which was not able be realized mechanically before are now becoming possible. Generally, ECUs in an automotive system follow communication protocols to communicate with each other through one or multiple buses. Since communication protocols greatly affect the performance of an automotive system, protocols which can support high transmission rate and reliability are demanded. Recently, FlexRay communication protocol is considered as the de-facto standard of the automotive communication protocol. FlexRay communication protocol supports high transmission rate up to 10Mbs while still keeping the properties of reliability and fault-tolerance. These characteristics make FlexRay especially suitable for safety critical systems.

On the other hand, testing process of automotive systems is really time-consuming and complicated. In industry, devices implementing communication protocols should be prepared for testing applications implemented on ECUs. Connection between ECUs and protocol devices form a testing environment. Tests are conducted focusing on specific node or data transmission with support of data from previous tests. Since higher requirements result complex functionalities and therefore more ECUs are demanded, and the testing process becomes harder along with larger number of devices and high financial cost.

This thesis proposes a framework for verifying design model of automotive systems with FlexRay. The framework is based on UPPAAL, with a model checker of timed automata for modeling the time-related behavior. By using the framework for verifying the design models, developers could have better chances to find bugs at the design level with the support of model checking technology. This may lead to a reduction of cost of the system development while increasing the quality of applications.

Similar to the devices-based testing, the UPPAAL framework consists of a FlexRay model and an application model. The former one represents the FlexRay devices and the later represents the ECUs where applications are implemented. Since UPPAAL only provides primitive synchronization using channels, the FlexRay model and the application model have to be specially handled.

The FlexRay model is built upon the specification with three steps of abstraction:

- **Essential Component Selection:** The model design verification of applications only requires functionalities of sending and receiving frames to be presented in the FlexRay model. Therefore, only essential and necessary components which provide the communication functionalities are selected.
- **Functionality Reduction:** With components selected in first step, it is not necessary that the FlexRay model has the full behavior in sending and receiving frames. Behaviors such as adjustments for error control (i.e. fault tolerance feature) can be skipped.
- **State Space Reduction:** Due to the heaviness of the FlexRay model after step one and two, further abstraction is conducted in order to reduce the state space while preserving functionalities implemented.

The FlexRay model also provides parameters and interfaces for the communication and access of the application model. The application model only needs to follow these parameters and interfaces to cooperate with the FlexRay model as an automotive system design model.

To evaluate the framework, experiments are conducted as follows: (1) A testing application models with basic behaviors are introduced for examining the validity of the FlexRay model; (2)A simple application is established to verify the response time of the system which is tested by using observer model; (3)A simplified adaptive cruise control system is introduced to show the feasibility by using the framework on verifying the practical applications. The results of the experiments prove the validity of the FlexRay model and the feasibility of the framework, respectively. Timing properties are especially examined and experiences of improving the application model from checking results are learned.