Verification of railway interlocking systems

Keywords : Railway; Interlocking; Verification; Statistical model checking; Simulation.

Quentin Cappart, Christophe Limbrée, Pierre Schaus

Abstract* – *In the railway domain, an interlocking is the system ensuring a safe train traffic inside a station by controlling its active elements such as the switches or the signals. Modern interlockings are configured using particular data, called application data, reflecting the topology of the station and defining the actions that the interlocking can take. The safety of the train traffic relies thereby on application data correctness, errors inside them can cause safety issues such as derailments or collisions. However, the application data are nowadays prepared by tools that do not guarantee an intrinsic level of safety. Given the high level of safety required by such a system, verification of its data is a critical concern. We propose here a statistical model checking approach for verifying the application data correctness.

Until now, most of the research targeting the verification of the application data is based on model checking. First, the signaling principles and the application data are translated into a model. Secondly, the dangerous situations that the interlocking must avoid are translated into safety properties. Finally, a model checker tool unrolls the state space of the model and verifies that none of the reachable states violates the properties. The principle of verification is simple but suffers from the so-called state space explosion problem. In other words, the number of states is so big that its creation and exploration take exponential time. A different approach introduced by Cappart et al. [1] consists in performing the verification by a discrete event simulation. The idea is to simulate the behavior of an interlocking as described in its application data and to observe if any unwanted scenarios occur. Unlike model checking where all the states are considered, this approach only considers scenarios that can potentially happen in practice. However, this method does not provide enough guarantees that all the conflictual scenarios will be detected. We propose here an intermediate statistical model checking approach, offering both the advantages of model checking and simulation. Before performing the verification, we need to define what are exactly the situations that we want to avoid. An interlocking must ensure that it will cause no accident in the station. It is a safety requirement. It can be split into three properties:

- A track cannot have two trains on it at the same time in order to avoid collisions.
- A railway switch cannot move if there is a train on it otherwise it will derail.
- A railway switch must always be set on a position allowing trains to continue their path. Otherwise the trains will derail.

The data flow diagram presented on Figure 1 resumes our approach. All this process in entirely automated. Let us describe the different parts of this approach:

- **The translators:** they are used in order to build a model of an interlocking which can be verified thereafter. We designed two translators, one for the application data, describing the interlocking behaviour, and one for the track layout, reflecting the geographic topology of the station. Their output are then aggregated in order to construct the model.
- **The simulator:** it is used in order to simulate the interlocking model obtained from the translators. The key idea is to reproduce the interlocking behavior under a realistic train traffic. It gives as output a set of traces. Each of them represents the set of states reached by a particular simulation.
- **The statistical model checker:** it is used to verify that the model satisfies all the requirements stated. To do so, it performs several simulations, gets the resulting traces, analyses them and verifies that all of them contain no state violating the requirement. If there is at least one simulation that does not satisfy a requirement, we can deduce that the application data are incorrect.

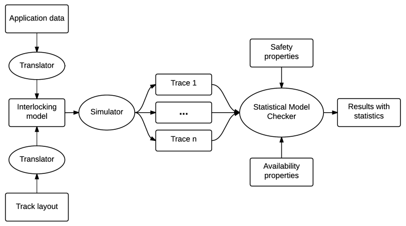

Figure 1: Steps of our approach.

The aim of statistical model checking is to approximate, in a controlled manner, the probability of satisfaction or violation of a property. To do so, two algorithms are used:

- **Monte Carlo:** the principle is to generate N random simulations and to compute how many of them satisfy the requirements. Furthermore, Chernoff bound can be used in order to determine the required number of simulations that must be performed to obtain a specific confidence interval. The simulation time can also be defined. In our experiments, we perform simulations of one day each.
- **Importance splitting:** it is used for increasing the probability of generating rare events (as collisions) in order ton speed up the errors detection by decreasing the number of simulations required to estimate the probability. It works by splitting the property that we want to verify into a sequence of subproperties easier to verify. Once a state satisfying a subproperty has been reached, it can be used as a new start for the next simulations.

In order to analyse the validity of our approach, we introduced several errors in the application data. All of them have been thoroughly detected with an execution less than three hours through 100 simulations of one day.

Automatic verification of interlocking systems is an active field of investigation in the railway domain. Up to now, most of the research dealing with this issue is based on model checking or on discrete event simulations. Howevever, both of these approaches have drawbacks. On this paper, we proposed an intermediate approach based on statistical model checking that overcomes both issues. Furthermore, experimental results confirm the validity of this method.

References

[1] Q. Cappart, C. Limbrée, P. Schaus, A. Legay “Verification by discrete event simulation of interlocking systems” in Proceedings of the 29th Annual European Simulation and Modelling Conference, EUROSIS (2015).