Formal and Experimental Verification of Robot Control Protocols for Smart Buildings

2310046 WU Jingting

With the increasing complexity of IoT systems, assuring the IoT system trustworthiness has become a critical work. Based on the IoT System Trustworthiness Levels (TALs) proposed by Beuran, this thesis reports about a case study to ensure that robot control protocols of a smart building meet high trustworthiness levels through formal and experimental verification.

The target smart building for this study has four subsystems, namely the robot subsystem, Building OS, the robot control platform subsystem, and the robot subsystem. The target protocol is implemented on the robot control platform subsystem, with the function to command a robot to move to another floor through the elevator.

Our formal verifications focus on model checking. We specified the basic version of the protocol for single robot control and the improved version for multi robots control in Maude, and successfully checked deadlock by using Maude's search command and checked safety and liveness properties by using Maude LTL Model Checker. All checked properties satisfy the requirements, which let us confirm the process correctness of the protocols.

Our experimental verifications focus on emulation and fuzzing, identifying unexpected problems. We developed an emulator for emulating the communication and action of the four subsystems. The emulator outputs communication and action logs, all of which can help us to diagnose problems when the system has any abnormal behaviors. Based on the emulator, we conducted fuzzing, an automatic test method by generating a large amount of random data. Our fuzzing involves mutating messages related to the robot control protocols in each subsystem, aiming to affect message transmission. In order to speed up the fuzzing, we applied some strategies. By applying our strategies, although the improvement of the three subsystems of robots, building OS and elevators is not obvious, the coverage of the fuzzing of 30 seeds of the robot control platform subsystem has increased from 36% to 94%. Based on the fuzzing results, we summarized 10 problems that had not been found in model checking and divided them into 6 categories according to Common Weakness Enumeration (CWE). Part of the problems comes from mistakes such as poor consideration in programming, and the other comes from abnormal situations such as data tampering. The discovery of these problems can be a supplement to the model checking.

To correct the problems, we modified the old model, got five new formal models according to the ten problems, and verified the properties again according to the requirements. At the same time, we conducted experimental

verification of the modified emulator again and observed the behaviors again to confirm that our solution is effective.

The results of our experiment not only show the effective but also show that the two methods have a certain complementarity. During the model checking, some operations were omitted in the system abstraction, while such operations are not omitted in the emulator, which is a good auxiliary supplement for the model checking; the characteristics of random mutation in the fuzzing are difficult to cover all paths, while the characteristics of all reachable paths traversal in the model checking prove the correctness of the paths.

On the other hand, state is used in emulating the operation of the system and devices, applied to both modeling in formal verification and emulator development in experimental verification. The problems located by one party can be easily located in the other party. Such convenience is reflected in later modification and re-verification. With this process of formal verification, experimental verification, analysis, modification, re-verification and re-analysis, we believe that our method is effective in high trustworthiness levels assurance.