Verification of Near Field Communication by Formal Method

Junpei Takamura (610054)

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

February 7, 2008

Keywords: Formal Method, Near Field Communication, CafeOBJ, Verification.

1 Introduction

Recently,Radio Frequency Identification(RFID) is paid to attention by the spread of FeliCa and Mifare. Near Field Communication(NFC) is short distance wireless communication standard that was developed by SONY and NXP. NFC became the international standard in December, 2003. NFC is communication compatible with FeliCa and Mifare, and is expected of the application in various fields. On the other hand, Formal Method is paid attention for reliability securing by software development. Formal Method is a technique for specification description and verifying the grammar or meaning based on strict mathematics model or logical system. It can eliminate a vague expression of the natural language, fugure, and the table, etc. As a result, the mistake of software can spot early at the state of the specification description, it is possible to develop smoothly, and reliability can be improved. There are various form in specification description language. I used CafeOBJ. Because CafeOBJ has actually achieved the result in the specification description and the verification of the communication protocol.

In this research, I elucidate reliability of NFC by description and verification using CafeOBJ. If the problem of the specification of NFC is found

by the verification, I propose a solution for it. As a result, safety and the reliability of the system based on NFC can be improved.

2 Approach

CafeOBJ is a formal specification language, and it can execute the equation by interpreting as the rewrite rule. Because the execution of the equation is correct to the equation logic, An interactive verification using CafeOBJ system is possible. The OTS/CafeOBJ is a method of the specification description and the verification that uses the observation function to observe the value and the transition function to update the state. OTS is modeling of the behavior of the system by using the observation function and the transition function. OTS is defined by the set of observation functions, the set of initial states, and the set of transition rules.

In the NFC protocol, if more than two Target responds, NFC selects one by using Single Device Detection algorithm. After selected, data is exchanged by the data transfer protocol. Then, selected Target is released by the release command.

I abstractly describe NFC by using the OTS/CafeOBJ, and verify the property which communicate with one Target in CafeOBJ.

3 Conclusion

In this research, I verified the specification of NFC by OTS/CafeOBJ. Specifically, I verified the property which communicate only one Target from selection of one Target to release of the Target. I thought that the verification of the property which communicate only one Target is insufficient in the description of specifications of NFC. So, if Initiator send select command once, initiator don't send select command until releasing the Target, initiator don't start SDD until releasing the Target. These conditions were added. These conditions enables me to verify the specification of NFC smoothly.

Future work of this research is to search a minimum condition and to describe the detailed specification of NFC.