Formalization anonymous protocol of based on OTS/CafeOBJ method

CHENG Jian (610058)

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

February 14, 2008

Keywords: anonymous protocol,I/O automaton, OTS, OTS/CafeOBJ, anonymous simulation.

This research is concerned with investigating how the OTS/CafeOBJ method can be used for modeling, specification and verification of anonymity property of distributed systems.

The issue of anonymity occurs in many real-life activities such as voting and donation, in which people may not want their identities to be disclosed. One would be reluctant to use a system unless it has been formally proved to satisfy anonymity property. However, the use of formal methods for analysis of anonymity property is still in its elementary stage and only a few studies exist in the literature.

Schneider et al. from London University proposed a formal definition of anonymity based on trace notations of CSP. Basic principle behind this definition, which is called principle of confusion, is that: an event that could have originated from one agent could equally have originated from any other (from a given set of agents). A CSP model checker FDR is then employed to analyze the satisfaction of finite-state systems to such anonymity. To analyze anonymity property of more general infinite-state systems, Kawabe et al. from NTT Communication Science Laboratories proposed the concept of trace anonymity based on trace notations of I/O automaton while keeping the basic principle of viewing anonymity used in Schneider's work. An inductive verification technique based on a notion of

anonymous simulation is then proposed. It is shown that the existence of an anonymous simulation leads to trace anonymity. The formal verification that an infinite-state system satisfies trace anonymity is carried out using Larch prover.

Our research on anonymity follows the definition of trace anonymity and its inductive proof technique proposed by Kawabe et al, but using Observational Transition Systems (OTSs) and CafeOBJ instead of I/O automaton and Larch prover. OTSs are a kind of transition systems that can be straightforwardly written in terms of equations, and CafeOBJ is an algebraic specification language underpinned with a term rewriting engine. This research starts from investigating the common and different features of I/O automaton and OTSs. It is found that there exist close correspondence between (1) state space, (2) the set of initial states, and (3) the set of actions of the two modeling methods. One difference between them is that: OTSs do not have the concepts of external and internal actions as I/O automaton do, but only has one set of transitions. Therefore, it is necessary to make revisions to OTS models to classify the set of transitions into external and internal ones, and thus to define the trace notion of OTSs. Our approach in this research is, more specifically, that: an infinite-state system to be analyzed is first modeled as an OTS, while trace anonymity property is formalized using trace notations of the OTS. The OTS is then specified using equations with the CafeOBJ specification language. At last, the satisfaction of the OTS to trace anonymity is verified by using CafeOBJ system as an interactive theorem prover.

In using the OTS/CafeOBJ method for anonymity analysis, the CafeOBJ specification has high readability in terms that the specification can be easily and straightforwardly understood. State transition of an OTS can be executed automatically with CafeOBJ system by treating equations in specification as left-to-right rewrite rules. Such state transitions have a natural correspondence with state chart diagrams, and one could easily be aware of the status of state transitions. The OTS/CafeOBJ method has a unique feature that: systems are modeled based on possible changes of observed values from outside of the systems, which provides high readability and makes the proof score based verification technique possible. In this research, we have revised the original definition of OTSs to define trace

notations, and consequentially to formalize trace anonymity. We have also made a small revision to the proof technique proposed by Kawabe et al to make the proof steps for trace anonymity more explicit. This research demonstrated that the proof score based verification technique could be used for anonymity analysis. This research is also a starting point for our further research on formal analysis of anonymity, and more broadly, formal analysis of privacy related properties of distributed systems.