Comparison of CafeOBJ and Coq by Formally Specifying and Verifying of STS protocol

Koutaro Hara (310088)

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

February 10, 2005

Keywords: Formal methods, Verification, CafeOBJ, Coq.

Protocol is a set of control the way data is sent between computers. Rapid prevalence and development of Computer Networks such as the Internet has brought about many studies for protocols. Especially, the more people have been interested in Network Security, the more stuides has been done to contrive secure protocols, called security protocols.

Security protocol is a protocol taken account of its secureness, and makes it possible for people to exchange confidential messages safely between computers. Now, many social systems such as traffic systems and financial systems use security protocols, and exchange many important data including personal and private one. If security protocols used in such kinds of systems were not secure, it would cause big social problems and losses. Therefore, security protocols need to be guranteed that they are really safe before they does be used. So, it has became very important to verify whether a security protocol is actually secure or not, and many people have studied and contrived the methods to verify security protocols.

Formal Method is famous for one method to analyze and verify security protocols effectively among these methods. For example, it was found with a formal method that NSPK protocol, which was contrived as one security protocol, has a defect which can not been found through some conventional tests by softwares and actual utilization. Formal method is the method which specifies a system mathematically and formally, and

verifies the formal specification, so the verification is strict and includes no contradiction. Threfore, it is thought formal methods are useful methods to make it clear that the system has prospected properties and thus the system is reliable for utilization. It brings that many formal methods to verify systems have been proposed and utilized, such as methods with algebraic specification languages, with proof assistants, with model checkers, with model logics of belief, and so on.

But, it looks like that there are few studies that compare different fomal methods and make their strong and weak points clear, although there are diffrent features between their ways to specify and verify based on their own theory and logic. It occures a problem that the verifiers may be at a loss which kind of formal methods to use in several situations. Our motivation is to show the differences between them and give a guide to help them decide which methods to select for their objectives.

We have performed a case study in this paper that the STS protocol, which is an authentication protocol(a kind of security protocol) based on the Diffie-Hellman key-exchange protocol, is analyzed whether it is secure and reliable just as one thought in order to compare different formal methods. Here, secureness of the protocol means that it can not happen for regular users, who send messages in accordance with rules of the protocol, to exchange keys with illegal intruders who don't comply with the rules but act as regular users and send fake messages. While, reliability of the protocol means that it is possible for regular users to exchage right keys each other certainly.

We use two different formal methods in the case study: The one is CafeOBJ and the other is Coq. CafeOBJ is an algebraic specification language/system mainly based on initial and hidden algebra, and it is used mainly to describe specification of a system. In algebraic specifiction method including CafeOBJ, systems are specified based on algebraic modeling, and the specifications are verified against requirements using algebraic techniques. While, Coq is a proof assistant based on the calculus of inductive constructions, and it is used mainly to prove theorems implying some properties. In Coq, formal development consists in a sequence of declarations and (Inductive)definitions, and Coq favors a style of reasoning, called Natural Deduction, which decompose reasoning into so called

introduction rules.

The following is the procedure to perform and describe the case study in this paper.

First of all, we model the behavior of the STS protocol mathematically including intruders who will do illegal conducts which they can do with all resources on the network. In the case study, we use Observation Transition System(OTS in short) to make the model of the protocol. In OTS, for the sake of making a model, we define relational values to the system and observe how the values are changed by actions which transfer state of the system. When it comes to modeling of the STS protocol in the case study, we define messages which have already been sent thorough the network as the relational value to the STS protocol, and we observe how the messages sent by regular users and intruders change the value and the resources which intruders can get and use.

Next, we describe the model made at the previous stage and we make two formal specifications. The one is described in CafeOBJ and the other is described in Coq. In order to make them, we define data types which need to model the protocol and describe transition rules each of which consists in conditions to transfer and the state after the transition with each formal languages.

Next, we describe the properties with each of CafeOBJ and Coq, which imply that the STS protocol is secure and reliable. In CafeOBJ, the properties are expressed as terms incuding CafeOBJ variables, and given their meanings by equations. In Coq, the properties are expressed as theorems incuding declarations of variables.

Finally, we verify with CafeOBJ that the specification made at the second stage has the properties described at the previous stage, and we do same thing with Coq. In CafeOBJ, the verification is proceeded by adding some rules(equations) as conditions and reducing terms with all rules to rewrite including them. While, in Coq, the verification is executed by a sequence of commands inputed by the verifier in order to deduce into goal. Conditions are automatically generated when they are needed.

In this paper, at last, we compare the two methods through the case study to specify and verify the STS protocol. Concretely speaking, we capture their features in view of the way to specify systems formally, for

example the way to define data types and to describe rules and properties, and the way to verify formal specifications, for exmaple the way to perform inductive proof and to describe proof scores and conditions in them, and so on.

As the result of these comparisons, we make the strong and weak points of the two methods clear: For example, in CafeOBJ, the specifications and the proof scores are easy to view, and it may be possible to finish easily verifying in brief time. While, in Coq, people can verify strictly without mistakes and proceed their proofs as they hoped. We also draw a conclusion about situations in which we should use CafeOBJ and Coq at the last of this paper.