504/E1

Formal verification of ez-reload SMS protocol using SPIN

M D V C Samasekera*
University of Colombo School of Computing, Colombo 07

The ez-reload is a Short Message Service (SMS) protocol offered by Dialog Telecom Ltd to reload the Keep In Touch (KIT) mobile package users. KIT is a pre-paid package, where the user has to subscribe before obtaining Dialog Telecom services. In the ez-reload system, Dialog Telecom has agents appointed island wide, from whom KIT subscribers can get their mobile phone re-loaded by simply paying the amount to reload. Once the payment is made, the agent will send a SMS containing the subscriber's mobile phone number and the amount paid to Dialog Telecom. Finally, Dialog Telecom will send a SMS to both the agent and the KIT subscriber confirming that the payment has been credited to the KIT subscribers account.

The research goal was to find out whether the ez-reload SMS protocol was reliable and if not propose modifications the ez-reload protocol. For this purpose it was checked whether money atomicity, goods atomicity and validated receipt properties were exhibited by the protocol. The model checking tool, Simple Promela Interpreter (SPIN) was used to model the ez-reload protocol. The behavior of the subscriber, agent and Dialog Telecom were modeled as Promela processes. The money atomicity, goods atomicity and validated receipt properties were modeled as Linear Temporal Logic (LTL) formulae. When SPIN tool was run in verification mode against LTL formulae it showed that the ez-reload protocol does not exhibit both money atomicity and goods atomicity properties under communication channel loss scenario. Additionally under normal operating conditions validated receipt property is also not exhibited.

Introducing a new SMS message for the subscriber, which gets a reference number for the transaction, eliminated the validated receipt property violation. This reference number is used by the parties to the transaction when sending SMS messages. Both money and goods atomicity property violations were eliminated by introducing another SMS message named BILL for the agent and the subscriber. When the BILL SMS is send to Dialog Telecom, it gives the last payment details for the subscriber. The said modifications were modeled and the SPIN tool was used to formally show that the modified ez-reload protocol has money atomicity, goods atomicity and validated receipt properties.

*virajsam@sltnet.lk Tel: 011-2712503