Verification of a Byzantine Agreement Protocol using Event-B

Roman Krenický and Mattias Ulbrich

Karlsruhe Institute of Technology
Institute for Theoretical Computer Science
D-76128 Karlsruhe, Germany
mattias.ulbrich@kit.edu

August 2, 2010

Abstract

Byzantine Agreement Protocols are used to distribute messages amongst communicating agents. They guarantee that even in the presence of a limited number of defect or malicious agents, eventually, all correctly working participants agree on one consensus message. The original problem statement and the first protocols were presented in [8] and [6]. Many protocol variations have been presented since.

Agreement protocols are of relevance today when in a safety-critical environment several components of a decentralised system need to share a common value (for instance the result of a self-test). If no central authority instance is present, the components have to follow an agreement protocol to come up with a consentaneous decision.

Byzantine agreement protocols are not too complex in their nature and can be described concisely. They are, on the other hand, also not trivial algorithms, and Lamport et al. admitted in [6]: "We know of no area in computer science or mathematics in which informal reasoning is more likely to lead to errors than in the study of this type of algorithm." They are therefore most appropriate for a formal examination. A protocol variation without secure signatures (called *oral messages*) has been formally verified in [7] using the higher order proof environment PVS.

We have formalised Byzantine agreement protocols which use secure signatures (called *written* or *signed messages*). The formalism chosen for our models is Event-B [1]. The description evolves over twelve steps of refinement each introducing a new aspect. The publicly available tool Rodin [2] has been used to deductively prove correctness, i.e., that an agreement is reached by the protocol.

The technical details, results and experiences of the case study have been published in [5].

References

[1] Jean-Raymond Abrial. *Modeling in Event-B*. Cambridge Univ. Press, 2010.

[2] Jean-Raymond Abrial, Michael Butler, Stefan Hallerstede, and Laurent Voisin. An open extensible tool environment for Event-B. In Zhiming Liu and Jifeng He, editors, *ICFEM 2006*, volume Lectur. Springer, June 2006.

[3] Christian Engel, Eric Jenn, Peter H. Schmitt, Rodrigo Coutinho, and Tobias Schoofs. Enhanced dispatchability of aircrafts using multi-static configurations. In *Embedded Real Time Software and Systems*, 2010.

[4] Stefan Hallerstede. Incremental system modelling in Event-B. In *FMCO 2008*, LNCS, pages 139–158. Springer-Verlag, 2008.

[5] Roman Krenický and Mattias Ulbrich. Deductive verification of a byzantine agreement protocol. Technical Report 2010-7, Karlsruhe Institute of Technology, Department of Computer Science, 2010.

[6] Leslie Lamport, Robert Shostak, and Marshall Pease. The byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982.

[7] Patrick Lincoln and John Rushby. A formally verified algorithm for interactive consistency under a hybrid fault model. In *Fault-Tolerant Computing Symposium, FTCS 23*, pages 402–411, Toulouse, France, June 1993. IEEE Computer Society.

[8] Marshall Pease, Robert Shostak, and Leslie Lamport. Reaching agreement in the presence of faults. *J. of the ACM*, 27(2):228–234, 1980.