Agreement Among Unacquainted Byzantine Generals*

Michael Okun

School of Computer Science, The Hebrew University of Jerusalem
mush@cs.huji.ac.il

Background. The Byzantine Agreement (BA) problem introduced by Pease, Shostak and Lamport in [1] is one of the central problems in distributed computing. It was extensively studied under various timing, topology, authentication and failure assumptions. In previous works it was assumed that the network topology is known to the processors in advance, i.e., every processor has an a priori knowledge of the true unique identifier of the processor to which it is connected by each of its communication channels (see Fig. 1a).

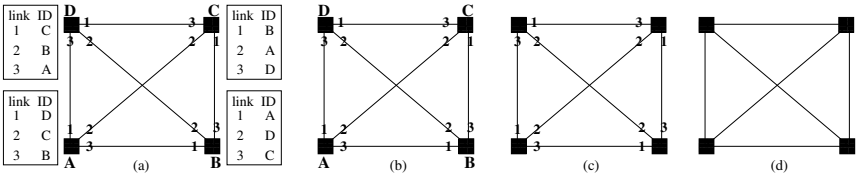

Fig. 1. A system with 4 processors: (a) the standard model, (b) without topology information, (c) anonymous model, (d) anonymous model without port awareness

This work deals with the BA problem when this assumption is relaxed. First, we consider the case in which each processor has a unique identifier, but the processors start without knowing the identifiers of the processors or the identifiers of the links between the processors (see Fig. 1b). In this case there are several reasonable models, all of which assume that each message carries an id of the sender. The models vary according to the ways in which a faulty processor may corrupt the id field in its messages. Specifically, we consider the following models:

($\mathcal{I}_1$) A message sent by any processor always includes its unique true id. In this case a faulty processor can prevent a correct processor p from directly learning about its id iff it sends no messages to p throughout the whole BA protocol.

($\mathcal{I}_2$) A faulty processor may send messages with different ids, not necessarily its own, however it cannot use an id belonging to a correct processor. This implies that "identity theft" is not allowed in this model.

* This research was supported by Israeli Council for Higher Education and by Sally Berg foundation.

P. Fraigniaud (Ed.): DISC 2005, LNCS 3724, pp. 499–500, 2005.

($\mathcal{I}_3$) A faulty processor may include any id in its messages, even that of correct processors, i.e., it is able to "fake" messages of correct processors.

In addition, we consider the case in which there are no identifiers at all (anonymous processors). Two types of anonymous networks are examined:

($\mathcal{A}_1$) The processors are port aware: each processor has an internal labeling of its communication channels, which allows it to distinguish between messages arriving via different channels (see Fig. 1c).

($\mathcal{A}_2$) The processors are port unaware: each processor receives all its messages through a single mailbox, and cannot associate a message with the link through which it was received (see Fig. 1d).

We note that the above five models form a strict hierarchy, in the sense that each model is the result of further relaxation of its predecessor.

Results. The BA problem has no deterministic solution in the $\mathcal{A}_2$ model even in the presence of a single faulty processor. This can be shown by a simple valency argument. On the other hand, Ben-Or's randomized algorithm can be used to achieve BA with probability 1 (whenever the number of faulty processors, f, is less than 1/3 of the total number of processors, n). These characteristics of $\mathcal{A}_2$ are similar to the asynchronous BA case.

For $\mathcal{A}_1$ we found an efficient BA algorithm that runs in at most $6f+1$ rounds, for $n > 3f$ [2]. It is based on the ideas of the Srikanth-Toueg (and similar) BA algorithms, though some non-trivial adaptations were required.

Finding the exact number of rounds required for achieving BA in the various models seems to be a much harder problem. The difficulty is that the Exponential Information Gathering algorithms (which are the only known algorithms for the standard BA that work in the optimal number of rounds), if at all, can be used only for $\mathcal{I}_1$.

In the $\mathcal{I}_2$ model BA can be achieved in $f + 1$ rounds. The proof of this (tight) upper bound is non-constructive, and is based on several new techniques [3]. Further model relaxations increase the number of rounds: in $\mathcal{I}_3$, even for $f = 1$, a relatively simple chain-argument shows that 3 rounds are required. However, it is still not clear if the additional round is also necessary for higher values of f.

Finding the exact number of rounds required for BA in the $\mathcal{A}_1$ model, or even proving a sufficiently tight upper bound is also an open problem.

References

[1] M. Pease, R. Shostak, L. Lamport, Reaching Agreement in the Presence of Faults, *J. ACM* 27(2) (1980) 228-234.

[2] M. Okun, A. Barak, On Anonymous Byzantine Agreement, Leibniz Center TR 2004-2, School of Computer Science, The Hebrew University, 2004, submitted for publication.

[3] M. Okun, On the Round Complexity of Byzantine Agreement Without Initial Set-Up, 2005, submitted for publication.