On the Number of Authenticated Rounds in Byzantine Agreement

Malte Borcherding

Institute of Computer Design and Fault Tolerance
University of Karlsruhe
76128 Karlsruhe
malte.borcherding@informatik.uni-karlsruhe.de

Abstract. Byzantine Agreement requires a set of nodes in a distributed system to agree on the message of a sender despite the presence of arbitrarily faulty nodes. Solutions for this problem are generally divided into two classes: authenticated protocols and non-authenticated protocols. In the former class, all messages are (digitally) signed and can be assigned to their respective signers, while in the latter no messages are signed.Authenticated protocols can tolerate an arbitrary number of faults, while non-authenticated protocols require more than two thirds of the nodes to be correct.

In this paper, we investigate the fault tolerance of protocols that require signatures in a certain number of communication rounds only. We show that a protocol that is to tolerate one half of the nodes as faulty needs only a few authenticated rounds (logarithmic in the number of nodes), while tolerating more faults requires about two authenticated rounds per additional faulty node.

Keywords: Byzantine Agreement, fault tolerance, distributed systems, authentication

1 Introduction

The problem of Byzantine Agreement (introduced in [LSP82]) arises when a set of nodes in a distributed system need to have a consistent view of messages uttered by one of them, despite the presence of arbitrarily faulty nodes. The problem is defined as follows: One of the nodes is distinguished as sender who attempts to transmit a value to the rest of the nodes. A protocol solving Byzantine Agreement must fulfill the following conditions:

- Each correct node eventually decides for a value.
- All correct nodes decide for the same value.
- If the sender is correct, all nodes decide for the value of the sender.

Protocols solving Byzantine Agreement are generally divided into two classes: authenticated protocols and non-authenticated protocols. In authenticated protocols, all messages are signed digitally in a way that the signatures cannot be
forged and a signed message can be unambiguously assigned to its signer. This mechanism allows a node to prove to others that it has received a certain message from a certain node. Authenticated protocols can tolerate an arbitrary number of faulty nodes. In non-authenticated protocols, no messages are signed. These protocols require more than two thirds of the participating nodes to be correct ([LSP82]).

While signatures allow for very fault-tolerant protocols, signing messages is a time-consuming action; typical durations for an RSA signature with a 512 bit key are 50 to 100 ms. Hence, it is useful to investigate the fault tolerance properties of authenticated protocols which require as few signatures as possible.

In this paper, we have a closer look at protocols where the nodes have to sign messages in certain communication rounds only. One implication of our results is that tolerating one half of the nodes as faulty requires a number of authenticated rounds logarithmic in the number of nodes, while tolerating more faults needs about two authenticated rounds per additional faulty node.

2 Preliminaries

2.1 System Model

Our world consists of $n$ nodes connected by a complete network. We assume that $t$ of the nodes may behave in an arbitrary manner, while $c = n - t$ behave correctly. The nodes operate at a known minimal speed, and messages are transmitted reliably in bounded time. The receiver of a message can identify its immediate sender, and we assume the existence of an authentic signature scheme such that a signature cannot be forged and each node knows whom a signature on a message belongs to.

During a protocol execution, the nodes communicate in successive rounds. In each round, a node may send messages to other nodes, receive the messages sent to it in the current round and perform some local computation. $m$ of the rounds ($s_1, \ldots, s_m$) are distinguished as authenticated rounds. In these rounds, all messages are to be signed.

2.2 The EIG Protocol

Our examinations are based on the Exponential Information Gathering (EIG) protocol which was introduced by Bar-Noy et al. [BNDDS87], based on the protocol in [LSP82]. In this protocol, the sender starts by sending its value to all other nodes. In the following $t$ rounds, each node forwards all messages it received in the previous round to the other nodes.

During protocol execution, each node maintains an EIG tree which contains the received information in a structured manner. Such a tree has $t+1$ levels, one level per communication round. The root has $n-1$ children, and in each of the

1 In [FL82, DS83] it is shown that $t+1$ rounds are necessary and sufficient to reach agreement with or without authentication.