Abstract

This paper presents a formal design for a novel group communication service targeted for wide-area networks (WANs). The service provides virtual synchrony semantics. Such semantics facilitate the design of fault-tolerant distributed applications. The presented design is more suitable for WANs than previously suggested ones. In particular, it features the first algorithm to achieve virtual synchrony semantics in a single communication round. The design also employs a scalable WAN-oriented architecture: it effectively decouples the main two components of virtually synchronous group communication—group membership and reliable group multicast. The design is carried out formally and rigorously. This paper includes formal specifications of both safety and liveness properties. The algorithm is formally modeled and assertionally verified.