

On the Security of Multi-Party Protocols in Distributed Systems

Danny Dolev
Avi Wigderson

Abstract

Security of protocols for network communication has received considerable attention in recent years. We concentrate on ensuring the security of cryptographic protocols in distributed systems.

In a distributed system, beyond eavesdropping, a saboteur may impersonate another user or alter messages being sent. A saboteur who is also a user may send conflicting messages or use other illegal messages in order to uncover secret information.

The problem we address, in its most general form, is “given a multi-party protocol which is provably secure when all the participants monitor every message being sent, can the protocol be modified to be secure in a distributed system?”

We use the Byzantine Agreement, Crusader Agreement, and other specific checks to improve protocols by making them secure in a general distributed network. We examine the trade-off between detection of faulty behavior and the number of messages exchanged.