Replacing Byzantine Participants

Researchers

Prof. Shlomi Dolev
shlomidolev@gmail.com

Amitay Shaer
shaera@post.bgu.ac.il

Prof. Roberto Baldoni (Cyber Security Czar of Italy)
baldoni@dis.uniroma1.it

Dr. Silvia Bonomi
bonomi@dis.uniroma1.it

Publications

S. Dolev, A. Shaer, R. Baldoni, and S. Bonomi, "Replacing Byzantine Participants," International Symposium on Cyber Security Cryptography and Machine Learning, 2017.

Goals

Detect two-faced malicious processes during distributed agreement, and kill and replace malicious participants while keeping the process time efficient.

Description

We suggest various ways for detection of Byzantine processes, i.e., processes which deviate from the protocol in an arbitrary way. Detection can be accomplished by comparing the (black boxed) result of the Byzantine consensus on each of the processes gossiped input, and then comparing these gossiped messages with the decision value of the consensus on the particular input.

We adopted a new approach to eliminating the Byzantine processes: Suppose several processes report another process as faulty, in this case, all the reporting processes will be killed unless enough reporting processes exist.

To address this issue, we suggest a protocol composed of fast and slow parts. At first, all processes are assumed to be correct and the protocol starts with the fast algorithm. As long as there is no indication of a Byzantine activity, the fast algorithm continues to work. The moment an indication of Byzantine activity has been discovered, the processes start to execute the slow algorithm and the two-faced processes are thus eliminated.