Byzantine Fault Tolerant Set Reconciliation

Degree programme : BSc in Computer Science | Specialisation : IT Security
Thesis advisor : Prof. Dr. Christian Grothoff
Expert : Han van der Kleij (SBB AG)

Set union is one of the most fundamental mathematical operations. Improving on prior work by Eppstein and Dold, this thesis presents a network protocol and implementation to efficiently compute the set union over a network.

Challenge:

When computing a set union, it is possible that the sets have a large overlap and that the actual difference between the sets is small. In these cases, it can be inefficient to simply transfer all elements to compute the set union. Eppstein proposed a protocol to reconcile two sets that required resources proportional to the set size difference.

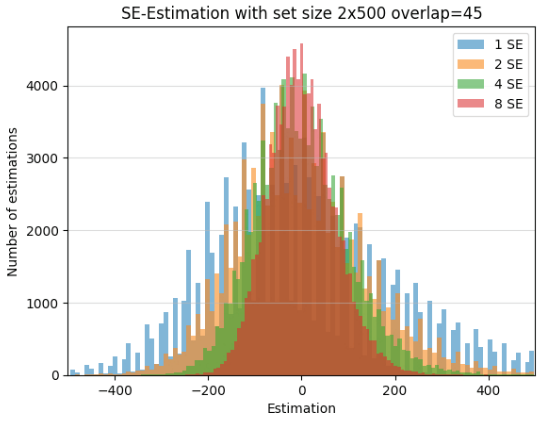
Objective:

The goal of the thesis is to review, improve and document the existing implementation by Dold of the „Byzantine Fault Tolerant Set Reconciliation“, which is a variant on Eppstein‘s original proposal used for key revocation in the GNU Name System. Other possible applications for the technology include e-voting systems, where a consensus must be established on the set of submitted ballots between the voting authorities.

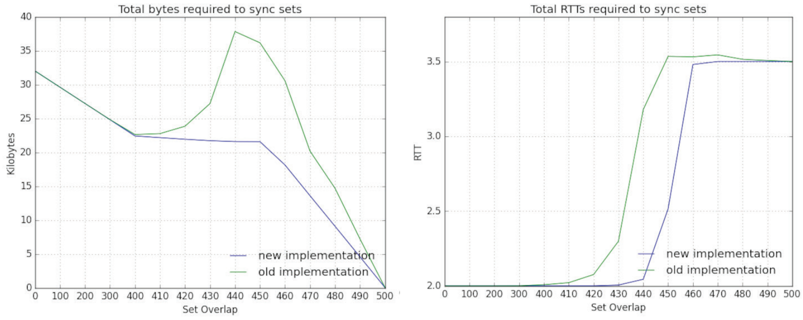
What has been achieved:

- The enhancements to the protocol done in this thesis have reduced the required bandwidth of matching sets with small differences by 30 to 42 percent.
- A number of improvements and optimizations of the code could be achieved. As an example, the Invertible Bloom Filters and Strata Estimators could be optimized.
- Several serious implementation bugs made the protocol unstable. The bugs have been identified and fixed (e.g. large sets were not supported).
- Through the exact analysis and documentation of the individual protocol phases and messages, various security improvements in the protocol could be realized.
- The complete binary level specification in form of an RFC can be found on the IETF Datatracker. If interested the link to the RFC can be found in the QR code below.

Elias Franz Summermatter
079 824 36 05
e.summermatter@seccom.ch



Precision of Strata Estimators



Link to the RFC

Measured performance gains