Trusted Execution Environments in Byzantine Tolerant Networks

TUDelft
Delft University of Technology

1. Background

- Consensus in Distributed Systems
- Byzantine Reliable Agreement
- Asynchronous n-connected Networks (Bracha-Dolev)[3]
- Trusted Execution Environment

2. Question

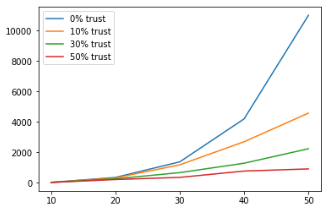
- How can protocols be modified to leverage the fact that some nodes have access to TEEs?
- What are the impact of these changes?
- Compare system models, which ones are realistic?

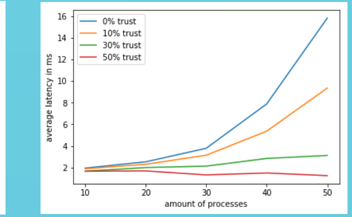
3. Method

- Simulate Networks using OMNET++ Network Simulator
- Transform nodes in trusted nodes that cannot be faulty
- Add trusted component to nodes that prevents equivocation

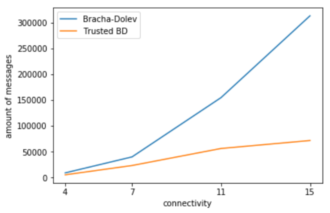
4. Results

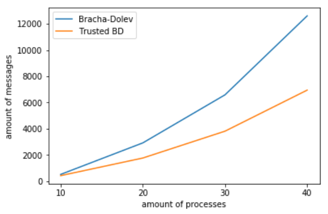
- Trusted nodes in the system improve the Dolev protocol significantly
- Average of 5 runs is shown, placement of trusted has high impact on number of messages sent and latency, both scale similarly





- Adding trusted component to prevent equivocation removes need for checking if everyone delivers same message
- Network kan tolerate up to N/2-1 faulty nodes instead of N/3-1
- A communication step in Bracha is cut out, each process only send one message to others





5. Conclusion

- Trusted nodes in the system decrease latency and throughput in messages by up to 92% with high levels of trust
- Trusted components lower upper bound of byzantine nodes and decrease Bracha's complexity by 50%
- Second model is a more realistic approach and shows improvements in amount of messages and latency

6. Future Work

- Research on placement and viability of trusted processes in network
- Implement trusted subsystem in real life TEEs
- Combine improvements with known topologies, authenticated processes or different protocols (CPA)

5. references

[3] Bonomi, Silvia and Decouchant, Jérémie and Farina, Giovanni and Rahli, Vincent and Tixeuil, Sébastien: Practical Byzantine Reliable Broadcast on Partially-Connected Networks, to appear.

Sebastien van Tiggele, s.l.vantiggele@student.tudelft.nl. Supervisor: Jérémie Decouchant. 01-07-2021 CSE3000