DECREASING MESSAGE COMPLEXITY IN BYZANTINE FAULT TOLERANT COMMUNICATION USING CONSISTENT BROADCAST

BACKGROUND

Communication in a distributed system is difficult

Byzantine generals problem: How can you achieve consensus when there could be adversarial nodes in a network?

Byzantine Fault Tolerant (**BFT**) protocols ensure consensus Bracha's and Dolev's works offer protocols that under certain conditions can achieve consensus.

Combined into Bracha-Dolev by Decouchant et al. [3] this protocol is applicable to any type of distributed network but it has a high message complexity.

Given the constraint that the sender can always be assumed to be reliable, there is an option that needs less messages to achieve consensus: Dolev with Authenticated Echo Broadcast (**AEB**) into BCB-Dolev. Part of the Consistent broadcast paradigm,

AEB eliminates the ready message type of Bracha entirely.

A new BCB-Dolev protocol first propagates a Dolev message through the network until it reaches a reliable node. That node then performs a BCB-Dolev broadcast to deliver the message through the network in two phases.

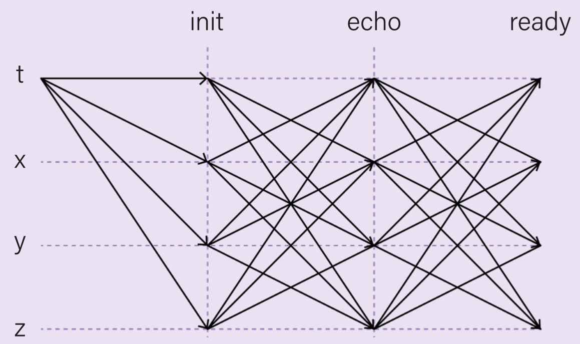

Figure 1: Bracha

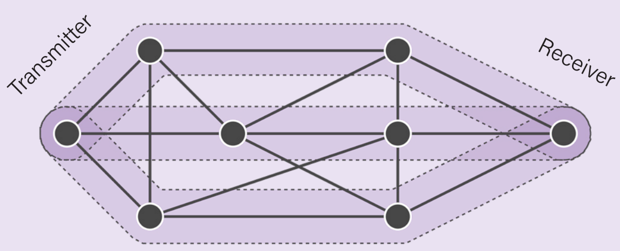

Figure 2: Dolev

Bracha's protocol [2]:

- Ensures agreement when a correct process delivers a messages if and only if every other correct process delivers a message.
- Works as a verification of a message
- Requires that f < n/3

Dolev's protocol [1]:

- Emulates direct connection between transmitter and sender by appending sender ID to the message and forwards it across disjoint paths
- Requires connectivity of 2f+1 where f is the amount of faulty nodes
- Requires that f < n/3

RESEARCH QUESTIONS

Is it possible to reduce the message complexity in Bracha-Dolev utilizing consistent broadcast given that the sender is always reliable?

Is this strategy valid and is it correct? Does it ensure consensus?

METHOD

Study the available options in the Consistent broadcast paradigm

Design and implement a new communication protocol: BCB-Dolev

Use the Salticidae network stack and Docker containers to simulate a real life network by using the containers as isolated processes

↓

Create an implementation of BCB-Dolev in C++

↓

Create two setups where the protocol to be used by an untrusted node is:

↓

1: Non-optimized Bracha-Dolev and BCB-Dolev

2: Fully optimized Bracha-Dolev and partially optimized BCB-Dolev

↓

Perform a static amount of broadcasts with a static amount of nodes in the network for varying connectivities and faulty nodes and compare the results

RESULTS

- 75 broadcasts
- Payload = 10 Bytes
- 31 nodes in the system

Non-optimized BCB-Dolev reduces the message complexity of non-optimized Bracha-Dolev by 65-75% across all connectivities and faulty nodes.

Partially optimized BCB-Dolev reduces the message complexity of optimized Bracha-Dolev by 25-45% but only when the amount of faulty nodes in the system is higher than 1.

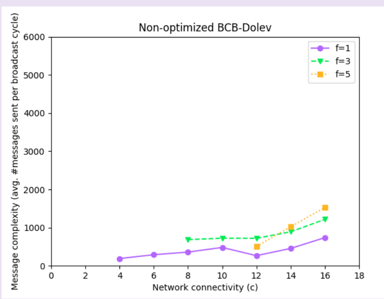

Figure 3: Message complexity non-optimized BCB-Dolev

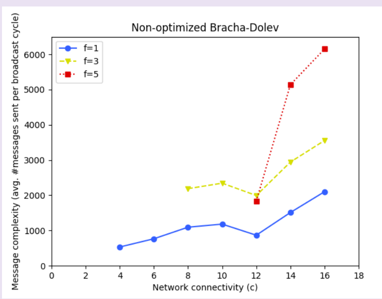

Figure 4: Message complexity non-optimized BRB-Dolev

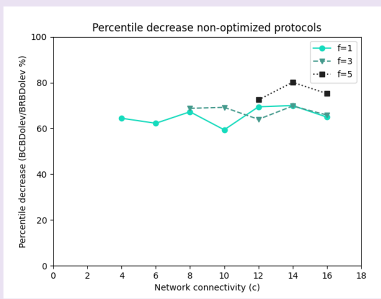

Figure 5: Percentile decrease of BCB-Dolev v.s. BRB-Dolev

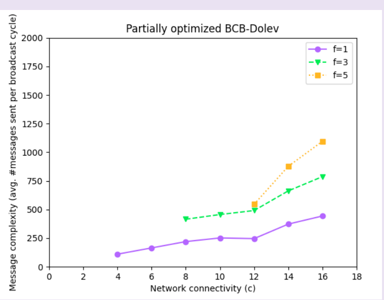

Figure 6: Message complexity optimized BCB-Dolev

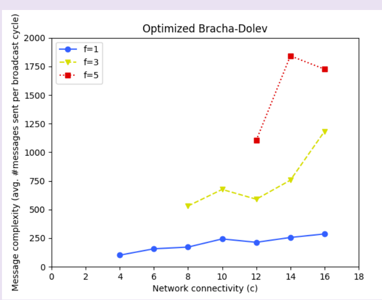

Figure 7: Message complexity optimized BRB-Dolev

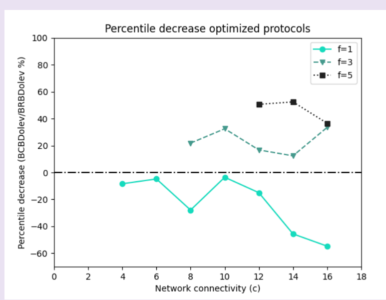

Figure 8: Percentile decrease of Opt BCB-Dolev v.s. Opt BRB-Dolev

CONCLUSIONS

- A fully functional and correct implementation of BCB-Dolev has been provided
- The partially optimized implementation has a lower message complexity compared to optimized Bracha-Dolev when the amount of faulty nodes is larger than $f=1$
- Future work can implement this protocol on real hardware and execute on real systems
- Further research into different applicable optimizations

REFERENCES

[1] D. Dolev. Unanimity in an unknown and unreliable environment. 22nd Annual Symposium on Foundations of Computer Science, pages 159–168, 1981.
[2] G. Bracha. Asynchronous byzantine agreement protocols. Information and Computation, 75(2):130–143, 1987
[3] Decouchant J. Farina G. Rahli V. Bonomi, S. and S. Tixeuil. Practical byzantine reliable broadcast on partially connected networks. Proceedings - International Conference on Distributed Computing Systems, pages 506–516, 2021.

Daan Prinsze (d.a.prinsze@student.tudelft.nl)
Supervisors: Dr. Jérémie Decouchant and Bart Cox