Approaching Message Optimal Byzantine Reliable Broadcast using Routing

Author
Dany Sluijk
D.Sluijk@student.tudelft.nl

Responsible Professor
Jérémie Dechouchant
J.Decouchant@tudelft.nl

Supervisor
Bart Cox
B.A.Cox@tudelft.nl

Background

In distributed systems there can be a need to broadcast a message to all nodes. In certain systems, nodes can behave differently and drop messages. These nodes are called faulty or byzantine.

Byzantine Reliable Broadcas (BRB): Guarantees that a broadcast will be delivered, even in the presence of byzantine nodes. Different protocols have different requirement. A protocol was introduced by Bracha [1], which required a fully connected network with a connectivity of `2f + 1`.

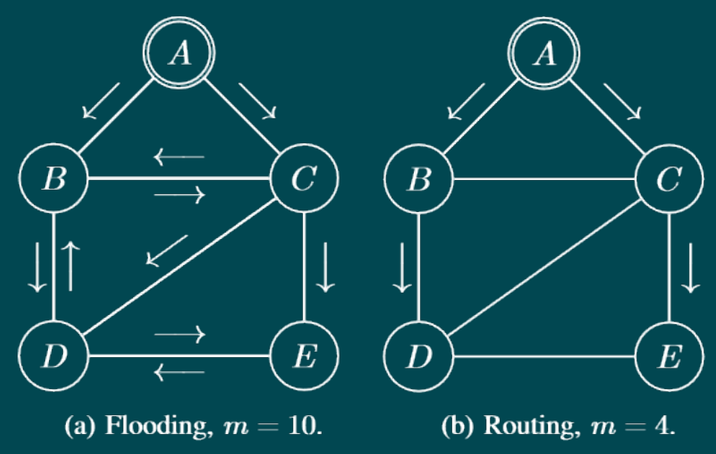
Reliable Communication (RC): Allows for the authentication and guaranteed delivery of messages without requiring signatures. This can be used to make a partially connected graph appear fully connected. RC was first introduced by Dolev [2].

Flooding with Signatures: Described last year by Klabér [3], this protocol utilized cryptographic signatures to reduce the amount of messages required to achieve BRB. This reduced the connectivity requirement to `f + 1`.

Research Question

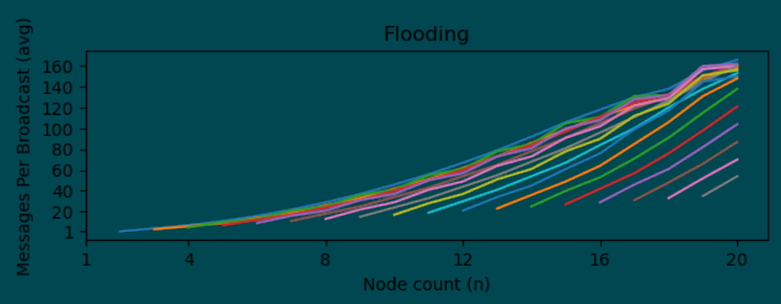
In the case where the network topology is known to processes, is it possible to further optimize performance?

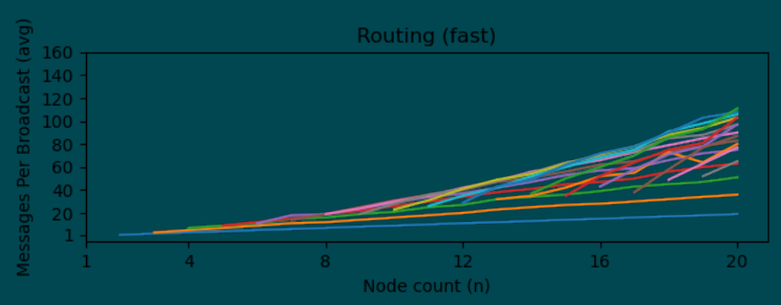
Example

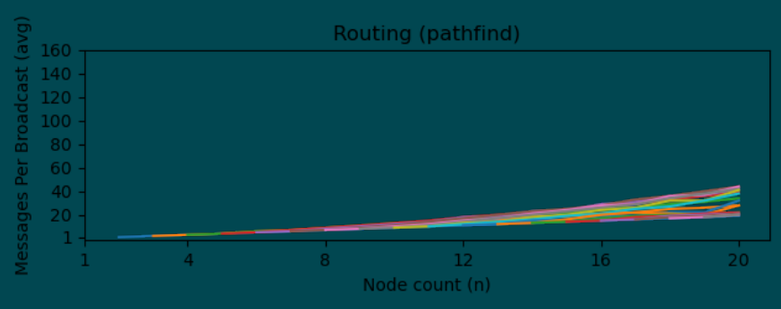


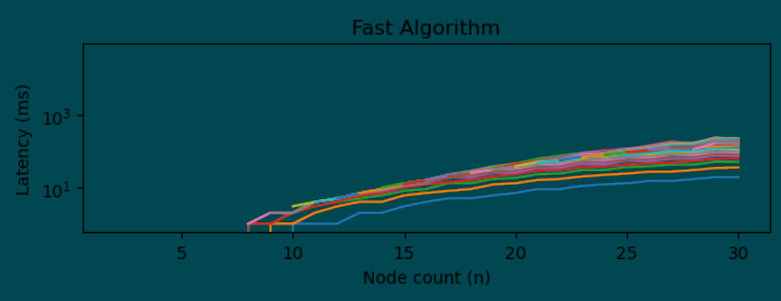
(a) Flooding, $m = 10$. (b) Routing, $m = 4$.

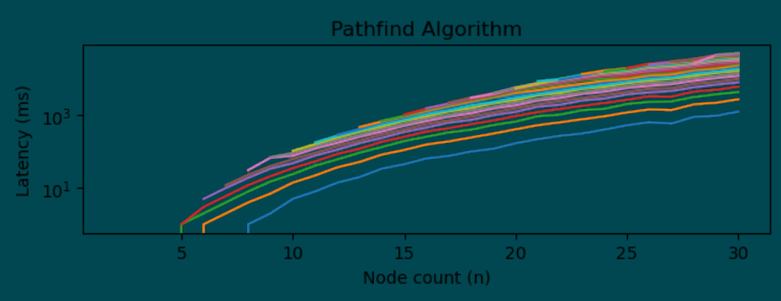
Results











Contributions

Routed Broadcast: By using the topology of the network, we observe that it's always possible to build a routing table to achieve a minimal message complexity. This while still upholding Byzantine Reliable Broadcast. It utilizes signatures to verify authenticity. Building these routes however, is a non-trivial excercise. This works especially well with highly connected graphs.

Route Building (Fast): Build a routing table by creating routes growing from the sending node. This quickly builds the routing table, but the routes are far from optimal as seen in the results.

Route Building (Pathfinding): Utilize pathfinding to find independent paths between pair of nodes, using existing routes whenever possible. This results in a routing table closer to optimal, but with a significant computational cost.

Conclusion

We have introduced a routed Dolev algorithm, which can theoretically enable BRB with an optimal message complexity. We also showed the need for a good route building algorithm. We introduced two approximation algorithms for this with an combined error rate of 0.0022. Future research in this might want to focus on creating a better route building algorithm, as this is currently the largest bottleneck.

[1] G. Bracha, "Asynchronous byzantine agreement protocols," Information and Computation, vol. 75, no. 2, pp. 130–143, 1987, ISSN: 0890-5401. DOI: https://doi.org/10.1016/0890-5401(87)90054-X
[2] D. Dolev, "Unanimity in an unknown and unreliable environment," pp. 159–168, 1981. DOI: 10.1109/SFCS.1981.53
[3] R. Klabér, "Byzantine reliable broadcast on partially connected networks with signatures," 2021. Available: https://resolver.tudelft.nl/uuid:c847d0e7-d85c-438e-97e6-ee917bb9f094

TU Delft Delft University of Technology