Using the message paths to optimize trust in the networks

Luka Dubravica (l.dubravica@student.tudelft.nl) - supervised by Dr. Jérémie Decouchant and Bart Cox

INTRODUCTION

Distributed systems require protocols that allow nodes to trust the messages in the network, since there are always malicious and malfunctioning nodes.

Bracha's algorithm - exchanges messages of three types (Initial, Echo, Ready) to ensure that all trustworthy processes agree on the certain values [1]

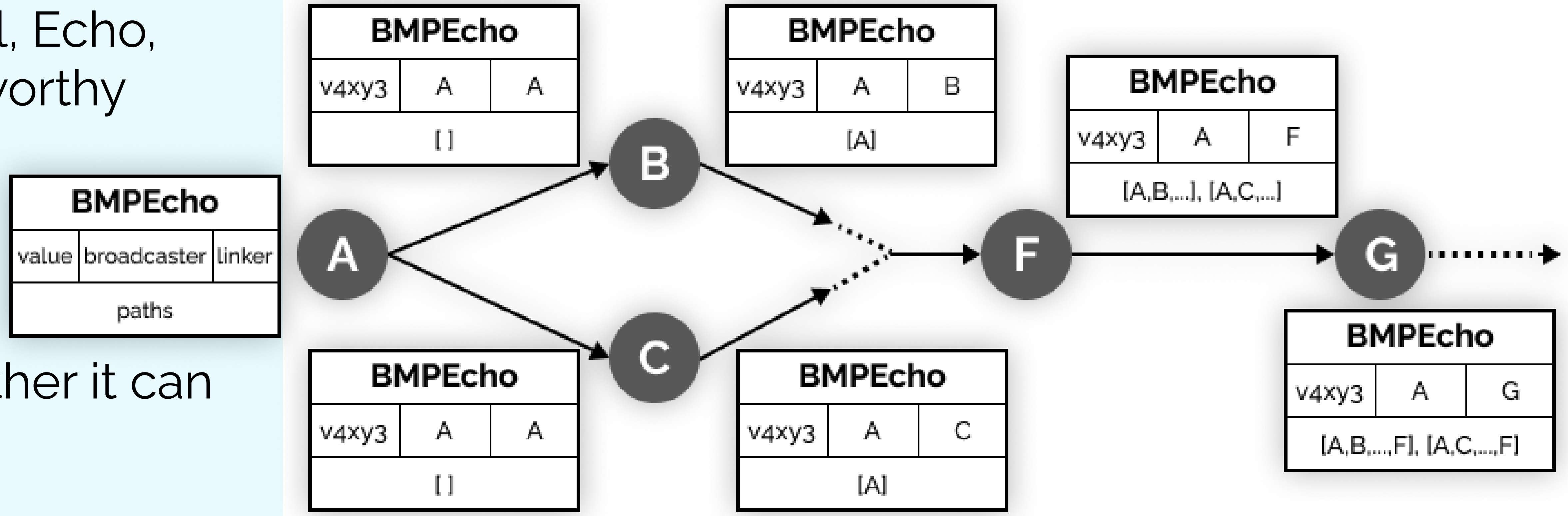
Dolev's algorithm - uses message paths to decide whether it can trust the message [2]

RESEARCH QUESTION

Is there an application for Bracha's algorithm implemented using message paths instead of message types?

METHOD & CONTRIBUTIONS

1. Construct the BMP algorithm, version of Bracha's that transmits a path that the message has crossed instead of the message type
2. Implement it in C++ for practical usages
3. Analyze its functionality and applicability



THE BMP ALGORITHM

Upon receiving a message

- Process received message paths
- Determine whether to accepts the value
- Determine whether to forward the message

OBSERVATIONS

- Handle lost messages in unstable networks
- Ability to trade latency for number of messages exchanged
- Single trusted message
- Deduce network trustworthiness
- Heavier messages

CONCLUSION

The BMP algorithm showed potential to outperform Bracha's algorithm in:

- networks with a low probability of transmitting a message
- networks where nodes have a system of trust.

Otherwise, Bracha's algorithm appears to be superior due to message size.

[1] Bracha, G., 1987. Asynchronous Byzantine agreement protocols. Information and Computation, 75(2), pp.130-143.
[2] Dolev, D., 1981, October. Unanimity in an unknown and unreliable environment. In 22nd Annual Symposium on Foundations of Computer Science (sfcs 1981) (pp. 159-168). IEEE.