Quantum Byzantine Agreement Protocol Under Noisy Conditions

Author

Prisha Meswani
p.m.meswani@student.tudelft.nl

Supervisor

Tim Coopmans

0 *How is the success probability of the quantum Byzantine agreement protocol affected by memory decoherence in a three-party network?*

1 ## Intro to Quantum

Unlike classical bits (0 or 1), qubits can exist in a *superposition* of both states.

General qubit state format: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$

Measurement *collapses* $|\psi\rangle$ to $|0\rangle$ or $|1\rangle$, with probabilities of $|\alpha|^2$ or $|\beta|^2$ respectively.

Qubits are manipulated by quantum gates, like the Pauli-Z gate, which flips the phase of $|1\rangle$:

$$|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle) \Longmapsto Z|+\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$$

Entanglement: A multi-qubit system where measuring one qubit instantly determines the states of the others.

2 **Byzantine Agreement Protocol**: Ensures multiple nodes in a network reach consensus on a value despite some nodes being faulty (i.e. communicates incorrectly).

The classical solution can tolerate < ⅓ faulty nodes; a quantum solution can tolerate < ½, a significant improvement.

All nodes decide on an output x_i and the protocol succeeds:
(a) If the sender is non-faulty and sends x_s all non-faulty receivers output x_s.
(b) If the sender is faulty, non-faulty receivers output the same value or abort.

3 ## *Quantum Byzantine Protocol Procedure*

1 3 nodes (S, R0, R1) share m copies of an entangled four-qubit state. In each copy, S holds the first two qubits, R0 the third, and R1 the fourth. The state is prepared on S and the appropriate qubits are distributed to R0 and R1 using **quantum teleportation**.

$$|\psi\rangle = \frac{1}{2\sqrt{3}}\left(2\,|0011\rangle - |0101\rangle - |0110\rangle - |1010\rangle - |1001\rangle + 2\,|1100\rangle\right)$$

2 S sends the bit *x* to R0 and R1, measures both its qubits in all m states, and shares a check set to R0 and R1 indicating which states had both bits equal to *x*.
3 R0 and R1 measure their qubits, confirming all measurement outcomes of qubits in the check set are opposite to x and the set size exceeds threshold T. If these conditions are met, they accept x; otherwise, they abort
4 R0 sends its output value and received check set to R1.
5 If R1's output ≠ R0's, it checks that R0's set size ⩾ T and that its measurements oppose R0's output for a sufficient fraction of R0's check set; if so, R1 accepts R0's value.

Faultiness *is incorporated as follows*

A Faulty Sender (S): S manipulates the bit and check sets sent to R0 and R1 in Step **2**, by trying to make R0 accept 0 and R1 accept 1 as the sent value.

B Faulty Receiver (R0): R0 manipulates the data sent in Step **4**, by sending the bit 1 - x and altering the check set accordingly.

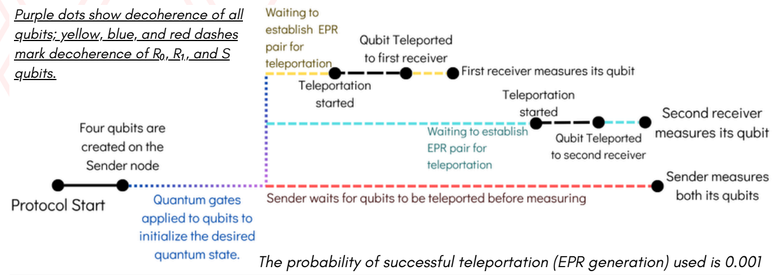
Related literature

Guba et al., Resource analysis for quantum-aided Byzantine agreement with the four-qubit singlet state. Quantum, 8:1324, April 2024

4 ## *Memory Decoherence*

- In Step **2**, the quantum teleportation process is probabilistic and may take multiple attempts, introducing some latency.
- Quantum memory cannot preserve their states indefinitely; they **decohere** over time. **Decoherence** is the deviation from a qubit's initial state.
- 2 Types of Decoherence for qubits: **T1** and **T2**.
  - **T1** is modeled by amplitude damping ($|1\rangle$ decays to $|0\rangle$, causing bitflips), **T2** by dephasing (application of a Pauli-Z gate).

Decoherence Timeline of the Protocol's Qubits

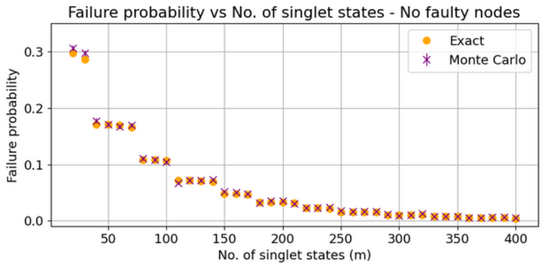


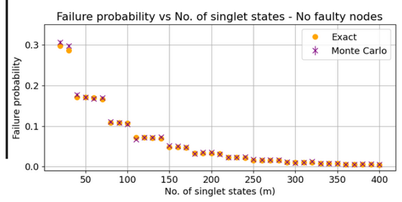
The probability of successful teleportation (EPR generation) used is 0.001

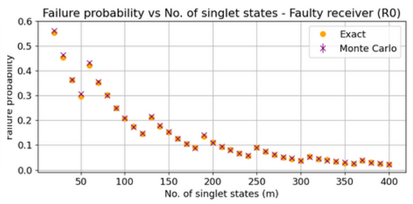
5 ## *Methodology & Experimental Setup*

- The protocol was simulated in Python using SquidASM. Three fault scenarios were tested: no faults, S faulty, and R0 faulty.
- Simulations include: Noiseless failure rate vs. m, Failure rate vs. T_2, Failure rate vs. T_1 and T_2 combined. Monte Carlo simulations were used to estimate failure probabilities.

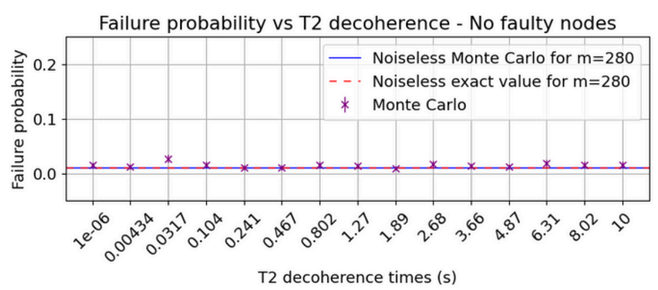
6 ## *Noiseless simulation results*

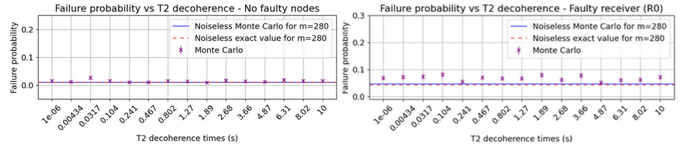


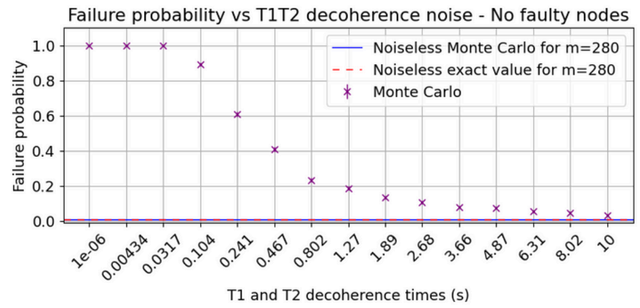


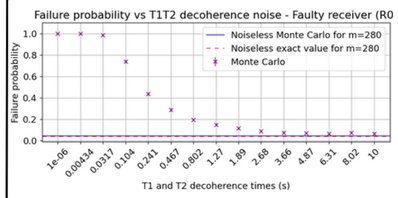


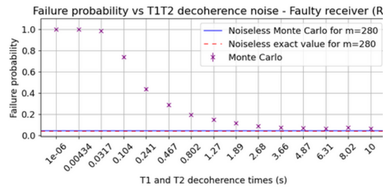
7 ## *Simulation Results - Noisy Simulations*











8 ## *Limitations*

Sequential teleportation increases decoherence due to SquidASM's nitrogen vacancy model allowing only one teleportation attempt per node pair at a time. The protocol achieves Weak Broadcast but cannot identify faulty nodes. Failure rate calculations may be overly pessimistic by treating cases where faulty nodes do not have enough measurement outcomes to form a false check set as failures.

Future Work

Test protocol under decoherence in non-Z bases to assess T_2 effects. Add a noise-tolerant threshold to the Check Phase for better T_1 resilience, and optimize it to prevent aiding faulty senders.

9 ## *Conclusion*

T_2 decoherence has minimal impact due to Z-basis measurements that ignore phase. In contrast, shorter T_1 times result in higher failure rates. However, as T_1 times get longer, the failure probabilities approach the noiseless value.

The realistic nitrogen vacancy estimate for T_1 = 10 hrs, which is 3600 times greater the 10s upper bound used in simulations. Since 10s already approaches noiseless failure rates, 10 hrs would perform similarly or better.