Bachelor’s Research Project

Evaluating the Impact of Gate Errors on a Quantum-Aided Byzantine Agreement Protocol

Jerzy Ksawery Wierzbicki
Supervisor: Tim Coopmans

EEMCS, Delft University of Technology, The Netherlands

A Thesis Submitted to EEMCS Faculty Delft University of Technology,
In Partial Fulfilment of the Requirements
For the Bachelor of Computer Science and Engineering
June 22, 2025

Name of the student: Jerzy Ksawery Wierzbicki
Final project course: CSE3000 Research Project
Thesis committee: Tim Coopmans, Arie van Deursen

Abstract

The Byzantine agreement problem in computer science focuses on honest parties trying to achieve consensus in a network with malicious actors. The performance of a quantum-aided Byzantine agreement protocol was evaluated under more realistic noise conditions, with a particular focus on gate-level errors. Since quantum systems are affected by various forms of noise, understanding the impact of quantum noise is crucial for assessing the practical viability and robustness of such protocols. Our results indicate a gate error probability threshold of 0.001%, below which the protocol maintains a failure probability of less than 5%. However, only a single source of noise was considered, with the depolarizing probabilities for single- and two-qubit gates assumed to be equal. This noise level closely matches the currently achievable error rate for single-qubit gates, but is over an order of magnitude lower than that for two-qubit gates on quantum network hardware. Consequently, our findings suggest that the protocol, in its current form, requires further research before it can be deployed on existing quantum devices. Moreover, the results strongly indicate that two-qubit gate errors are the primary bottleneck. These results highlight the significant impact of quantum noise on distributed quantum protocols and underscore the need for either improved quantum hardware or enhanced fault-tolerant protocol designs.

1 Introduction

Reaching agreement among parties in distributed systems in the presence of faulty or malicious nodes is arguably the most fundamental problem in distributed computing, as described by Civit et al. [1]. Faulty, malicious and byzantine nodes are nodes that do not adhere to the consensus protocol, or try to exploit the loopholes. Known as the *Byzantine Agreement* problem [2], it is particularly relevant for applications such as blockchain, distributed databases, and critical infrastructure systems. In classical computing, various protocols, that aim to solve this problem, have been developed, but they usually require high communication overhead or assumptions that may not hold in real world distributed systems.

1.1 Related Work

Quantum communication offers a new approach to tackle this issue. By making use of properties of superposition and entanglement, it is possible for honest parties to detect inconsistencies introduced by malicious or faulty nodes, thus offering higher resilience while still achieving reasonable computational complexity. One such approach was originally proposed by Adán Cabello [3], who introduced a quantum-aided weak broadcast protocol based on a four-qubit entangled singlet state. In short, the broadcast functionality is achieved if data is distributed consistently among correctly functioning components, whereas weak broadcast allows for an 'abort' option at the receivers if the sender is an adversary [4, 5]. Guba et al. [4] later extended this idea [3] by introducing a parameter-dependent version of this protocol, allowing for systematic analysis and optimization. The protocol however succeeds only with a certain probability. The authors quantified the failure probability under ideal conditions and also provided noise analysis on hardware primarily focused on quantum computing, rather than quantum networks. The nitrogen-vacancy (NV) center in diamond has recently emerged as one of the leading candidates for these technologies [6]. Recently, Bartling et al. [7] achieved gate fidelities of approximately 99.94% for single-qubit gates and 99.93(5)% for two-qubit gates within the two-qubit space of an NV center system. In a more specific configuration, where only the nitrogen-spin qubit was actively used and the other qubit was idle, they demonstrated a significantly higher gate fidelity of 99.999(1)%. Practical implementation of this protocol [4] must still take into account hardware noise, such as measurement, qubit decoherence and gate errors for designated components.

1.2 Problem Statement

Understanding how hardware imperfections affect the success probability of the protocol remains a question. This question is important, because real world quantum hardware is noisy, and understanding impact of the noise is necessary for assessing the practicality of this quantum-aided consensus protocol [4].

1.3 Research Question

This work aims to address the following question:

> What is the maximum probability of gate error for the protocol to ensure the failure probability does not exceed 5%?

Gate errors are a subset of hardware noises. Quantum gate errors refer to inaccuracies that occur when performing quantum logic operations (gates) on qubits. The value of 5% as a threshold was chosen based on previous work of Section 4.3 of Ref. [4] where the same value was used for their experiments, and changing this value would result in a need for re-doing their research and analysis. This value however was chosen arbitrarily.

1.4 Main Contributions

This research makes three main contributions toward evaluating the practicality of a quantum-aided Byzantine Agreement protocol. First, it focuses specifically on gate errors, a significant source of quantum hardware noise, and analyzes their impact on the protocol's failure probability. Second, it systematically evaluates the protocol under varying levels of gate noise. Finally, the research presents quantitative findings that show to what extent is the protocol resistant to the gate errors.

1.5 Paper Organization

The paper is structured in a following way. Chapter 2 contains a description of the research methodology and provides the necessary background information. Chapter 3 presents the noise model used to assess the robustness of a protocol presented in Ref. [4]. In Chapter 4 the experimental setup and results are outlined. Reflection on the ethical aspects of my research can be found in Chapter 5. In Chapter 6 results are discussed. Chapter 7 presents the conclusion and discusses potential future work.

2 Methodology and Background

This chapter describes the methodology used to evaluate the failure probability of the protocol proposed by Guba et al. [4]. The chapter provides background on the specification and implementation of the protocol, explains noise modeling, and justifies the use of simulation in SquidASM [8] as a tool to assess the probability of failure in various fault scenarios.

2.1 Background

For understanding the functioning of the protocol and experiments that were conducted in this paper, necessary background about quantum information and protocol is presented in the following two subsections.

2.1.1 Quantum Information Background

A n-qubit quantum state is a complex vector of 2^n dimensions. The quantum states are typically denoted using Dirac notation as $|0\rangle$ and $|1\rangle$, which form an orthonormal basis for a two-dimensional Hilbert space. In mathematics, a Hilbert space is a real or complex inner product space that is also a complete metric space with respect to the metric induced by the inner product. An arbitrary single-qubit state can be written as $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$, where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. Gates that are performed on such a state are 2^nx2^n unitary matrices. The entangled state can not be described without the state of the other qubits. Finally quantum teleportation is a process by which the quantum information can be transmitted from one location to another, with the help of EPR pairs and classical communication. Further details about EPR pairs and quantum teleportation can be found in Sections 1.3.6 and 1.3.7 of Nielsen and Chuang [9], respectively. For any other background information related to quantum computation and quantum information, the reader is also referred to this source.

2.1.2 Protocol's Background

The quantum-aided 'weak-broadcast' protocol presented by Guba et al. [4], that addresses the Byzantine agreement problem, is designed for a network of three nodes, one sender and two receivers, and can tolerate up to one faulty node, thus achieving a resilience of $t < n/2$, which improves upon the classical bound $t < n/3$ found in protocols such as Pease et al. [10], where n is the number of components in the distributed system, and t is the maximum number of components exhibiting Byzantine fault. The protocol relies on the preparation and distribution of a specific four-qubit entangled state repeated multiple times, with the total number of repetitions denoted by $m \in \mathbb{Z}^+$.

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

The qubits from this state are distributed among the three nodes. The sender holding first two qubits, receiver R_0 holds the third qubit, and receiver R_1 holds the fourth. The Weak Broadcast protocol presented in [4] has two real-valued parameters: $0 < \mu < \frac{1}{3}$ and $\frac{1}{2} < \lambda < 1$. The protocol consists of four main phases: *Invocation*, *Check*, *Cross-calling*, and *Cross-check.*

Invocation Phase The sender S transmits a classical bit x_S to receivers R_0 and R_1, who record the received bits x_0 and x_1, respectively. Simultaneously, S measures its share of the entangled qubits and constructs a *check set* σ_S containing the indices where the measurement outcomes match the sent bit x_S. This set σ_S is then communicated to both receivers.

Check Phase Each receiver R_j measures all qubits in its check set σ_j and verifies two conditions:

- **Consistency Condition**: All measurement results differ from x_j.
- **Length Condition**: The size of the check set satisfies

  $$|\sigma_j| \geq T \equiv \lceil \mu \cdot m \rceil,$$

  where $0 < \mu < \frac{1}{3}$ and m is the total number of singlet states.

If both conditions hold, R_0 sets its output as $y_0 = x_0$, while R_1 sets an intermediate value $\tilde{y}_1 = x_1$. If either condition is violated, they abort the protocol by setting $y_0 =\perp$ for R_0 and $\tilde{y}_1 =\perp$ for R_1.

Cross-calling Phase Receiver R_0 sends its output value y_0 and the check set σ_0 it received from the sender S to receiver R_1. Receiver R_1 receives these as y_{01} and ρ_{01}, respectively.

Cross-check Phase Receiver R_1 evaluates the following three conditions. If **all** hold, it outputs the value received from R_0, that is,

$$y_1 = y_{01},$$

otherwise it outputs its intermediate value

$$y_1 = \tilde{y}_1.$$

The conditions are:

(i) **Confusion Condition**:

$$y_{01} \neq \tilde{y}_1, \quad \text{and} \quad y_{01} \neq \perp, \quad \tilde{y}_1 \neq \perp .$$

(ii) **Length Condition**:

$$|\rho_{01}| \geq T \equiv \lceil \mu \cdot m \rceil,$$

similarly to the Length Condition of the Check Phase above

(iii) **Consistency Condition**: Let N_{opp} denote the number of indices in ρ_{01} where R_1 measures the bit opposite to y_{01}. Then,

$$N_{\text{opp}} \geq \lambda T + |\rho_{01}| - T,$$

where the tolerance parameter satisfies $\frac{1}{2} < \lambda < 1$.

Note that this Consistency Condition is less stringent than the one in the earlier Check Phase.

The four phases of the protocol cooperate toward secure and fault-tolerant agreement despite adversaries. The invocation phase provides receivers with the sender's data bit and a check set for later validation. The check phase enables each receiver to confirm the sender's message using local measurements. Omitting this step would allow a malicious sender to distribute inconsistent data undetected and receiving nodes would not be able to abort. However, disagreement may still occur if the sender misleads only one receiver. In the cross-calling phase, node R_0 forwards its information to node R_1, and the cross-check phase allows R_1 to resolve potential disagreements, but only on his side. All these phases however do not guarantee the protocol to work correctly. Example of malicious strategies, that lead to failure, can be found in Appendix B of Ref. [4].

Note that, based on functionality of the protocol, the R_1 node does not communicate with any of the other nodes thus has no influence on the values they agree on, and this scenario can be omitted. Therefore three scenarios of byzantine fault will be evaluated: no faulty nodes, faulty sender and faulty receiver R_0.

To ensure a failure probability below 5%, Guba et al. [4] used Monte Carlo simulations ($N = 10{,}000$ trials) and determined a minimal number of entangled resources $m = 280$ in a noise-free, single-Byzantine setting.

Gate errors may occur during the preparation of the entangled state (1), potentially resulting in the generation of an incorrect quantum state. Such deviations can compromise the protocol's correctness, leading to failure in satisfying the phase-specific conditions.

2.2 Method

To recreate the results, in noise free conditions, and evaluate the protocol under noisy environment, the exact same protocol functionality was implemented with the use of SquidASM [8], a simulator based on NetSquid [11] that can execute applications written using NetQASM [12]. The correctness of implementation of the protocol was tested by comparing the obtained results, in our noise free conditions, to the one mentioned in Figure 4 of Ref. [4]. The strategies for byzantine nodes in byzantine scenarios were implemented as described in Appendix B of Ref. [4]. The failure was assessed adhering to the Table 2 in Appendix B of [4].

Simulation in SquidASM is an effective way of assessing the effect of noise and comparing it to the analytical approach used in the paper, because it allows controlled manipulation of noise parameters, such as gate error rates, while preserving the protocol's core logic. This enables empirical estimation of failure probabilities under varying environmental conditions, such as different probabilities of different noise sources.

To determine the maximum tolerable gate error rate that keeps the protocol's failure probability below or equal to 5% in all scenarios, a noise factor was incorporated into simulation and varied using SquidASM [8]. Specifically, the impact of introducing gate errors was analyzed. Number of four-qubit states, used to verify correctness of received information, was kept constant at $m = 300$. This value was chosen to provide a safety margin above the critical cut-off value of $m = 280$, and because prior results, such as Figure 5 in Ref. [4], showed that it performs reliably across all tested combinations of other varying parameters. The value could be chosen to be larger, however, according to the noise analysis in Section 4.5 of Ref. [4], this would not necessarily result in increased resilience.

3 Noise Model

This chapter presents the new approach of assessing the protocol's robustness by simulating hardware noise. The chapter also reasons why the approach is applicable and why is it an improvement.

Pauli errors are fundamental concept in quantum error correction. They refer to a specific set of errors that can affect a single qubit in a quantum system, represented by the Pauli matrices. A Pauli channel models the effect of noise by applying a Pauli operator I,X,Y or Z at random, according to a probability distribution. A Pauli channel assumes that:

- With probability p_I, no error occurs.
- With probability p_X, a bit-flip occurs.
- With probability p_Y, a bit and phase flip occurs.
- With probability p_Z, a phase-flip occurs.

The sum of these probabilities must equal 1:

$$p_I + p_X + p_Y + p_Z = 1$$

More specifically the following case of a depolarizing channel, where probabilities for every Pauli error are equal, will be studied:

$$p_X = p_Y = p_Z$$

This means a gate error occurs with some total probability p, and when it does, one of the three Pauli errors is chosen uniformly at random. For example, if $p = 0.01$, then each of X, Y, and Z is applied with probability 0.0033, and with probability 0.99 no error occurs.

Quantum devices today are characterized by non-negligible gate error rates. Modeling these imperfections using a well-understood noise model, such as depolarizing channels, enables simulations to more accurately reflect the real-world conditions under which the protocol would operate. In our simulation the error probabilities for single- and two-qubit gates were set equal to each other. This choice was made to simplify the protocol's robustness analysis.

Importantly, the noise model is implemented in a way that does not alter the logical flow or decision-making processes of the protocol. This ensures that any observed degradation in performance is related solely to gate errors, not to modifications in protocol behavior.

In summary, this approach is applicable and is an improvement over the studies conducted in Ref. [4] because it provides a more realistic, controlled experiment for understanding how the protocol behaves under non-ideal conditions, a step toward deploying quantum consensus protocols in real-world systems.

4 Experimental Setup and Results

This chapter describes the experimental environment and presents the results of the simulation of the noisy protocol, to enable reproducibility by the readers. It outlines the setup that was used, including SquidASM and python versions, and analyzes the impact of varying noise levels on the protocol failure probability.

To be able to reproduce the experiment, we present the setup that was used. The protocol was implemented in Python version 3.12.7, and additionally the 0.13.4 version of SquidASM [8] was used. Figure 1 represents circuit proposed by Guba et al. [4] that was used to prepare a quantum state into the desired one (1). In addition, the Sender node prepared the state (1), and distributed it via quantum teleportation. The parameters were set as follows: $\mu = 0.272$ and $\lambda = 0.94$.

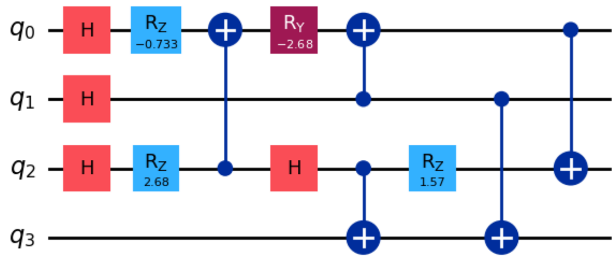


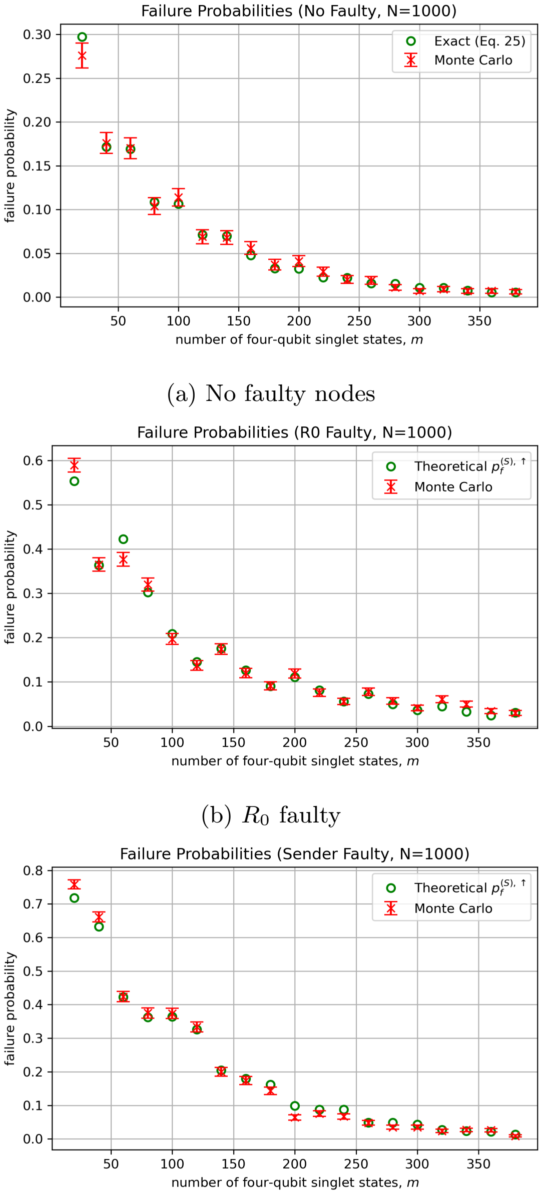
Figure 1: Circuit taken from Figure 6 in the paper by Guba et al. [4]. This circuit prepares quantum state mentioned in Eq. (1). The decimal fractions present in the circuit map to -0.73304, 2.67908 and 1.5708.

4.1 Simulation in a Noise-Free Environment

First the noise-free case was simulated. The same as in Ref. [4], Monte Carlo simulation was used, however with smaller number of random events, meaning $N = 1000$, and with bigger difference in singlet states between each simulation, m was incremented by 20. This choice was motivated by the need to balance computational efficiency with sufficient statistical confidence. With $N = 1000$ samples and error bars included, the results still clearly reveal meaningful trends in the results. The results, across all cases, from the experiment closely matched the expected or theoretical upper bounds for failure probabilities reported in Figure 4 of Ref. [4] and can be found in Figure 2. The expected and theoretical upper bounds were calculated based on equations (25), (27) and (35) of Ref. [4]. In nearly all instances, observed values did not deviate more than standard mean error. Only a few minor exceptions were noted. The general trend of decreasing failure probability with increasing number of four-qubit singlet states was obtained.

4.2 Simulation Results with Gate Errors

For the simulation with gate errors, Monte Carlo simulation was used as well, and single-qubit gate depolarizing probability was kept equal to the two-qubit one. The experiment resulted in plots with varying gate error rate against the failure probability. The results can be found in Figure 3. For two scenarios, one with no faulty nodes that can be found in Figure 3a and one with the receiving node being faulty (R_0), Figure 3b, we can notice a trend that the increased probability of gate error increases the probability of failure of the protocol. For this two scenarios and $m = 300$ the cut off for the failure probability to be kept below 5% is 0.001% as it is the first value for which measured failure probability exceeded the threshold. However, in the R_0 faulty scenario, the threshold initially lies within the range of the standard mean error, and the measured failure probability only truly exceeds the 5% threshold when the gate depolarizing probability reaches 0.004%. In a situation where the sending node behaves maliciously, the measured failure probability first exceeds 5% at a gate depolarizing probability of 0.004%. However, the standard mean error suggests that this threshold could be surpassed at a lower value. After surpassing the threshold the



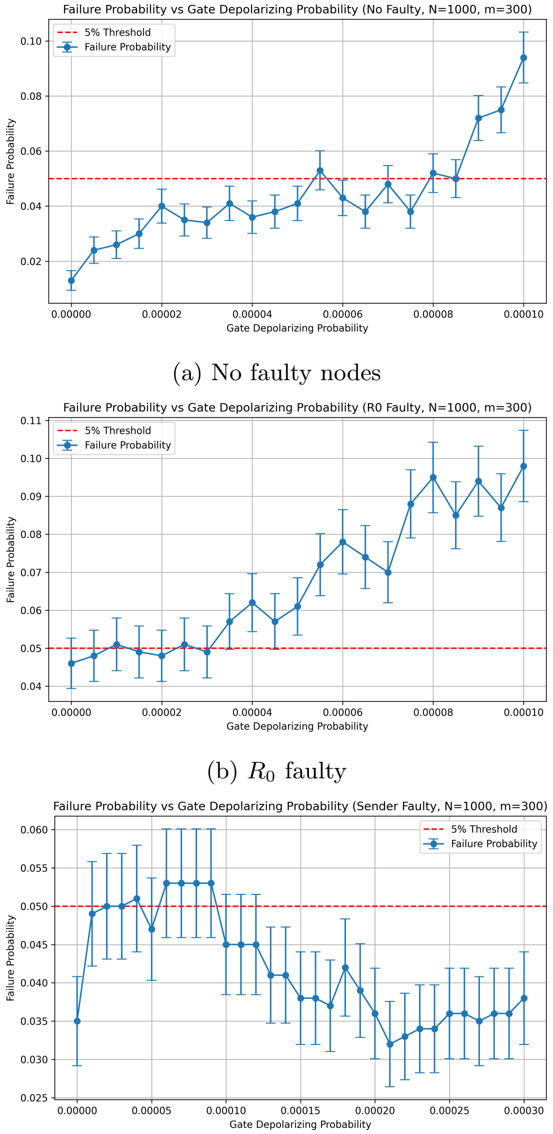
(a) No faulty nodes

(b) R_0 faulty

(c) Sender faulty

Figure 2: Comparison of failure probabilities under different faulty node configurations. On the horizontal axis the number of four-qubit singlet states and on the vertical axis the failure probability can be found. Monte Carlo simulation with $N = 1000$ random samples was used to obtain this data. The green circles indicate theoretical failure probabilities, or their upper bounds, and red crosses with bars indicate achieved failure probability with standard mean error.

failure probability starts to decrease with an increase in gate error rate. For all scenarios, the gate depolarizing probability found to keep the protocol's failure probability below the desired cut-off is 0.001%. However, this value remains uncertain, as many measurements below it include it within their standard mean error range.



(a) No faulty nodes

(b) R_0 faulty

(c) Sender faulty

Figure 3: Comparison of failure probabilities under different faulty node configurations. On the horizontal axis the gate error rate and on the vertical axis the failure probability can be found. Monte Carlo simulation with $N = 1000$ random samples was used to obtain this data. The blue dots with bars indicate measured failure probability with standard mean error, for respective gate error rate.

5 Responsible Research

This section reflects on the ethical and responsible aspects of research. It focuses on reproducibility, transparency and potential implications and responsibilities associated with advancements in quantum consensus protocols.

5.1 Reproducibility

To ensure reproducibility, all simulations were implemented using quantum computing framework, namely SquidASM [8]. This tool is publicly accessible, supporting replicable experimentation. The quantum circuit used in our simulations was constructed based on the circuit proposed by Figure 6 in Ref. [4], ensuring consistency with prior work. The noise models were clearly documented and implemented, making it possible for other researchers to validate or extend our results.

5.2 Data Integrity and Transparency

We adhered to principles of data integrity by treating all simulation outcomes equally, regardless of whether they aligned with expected behavior. No results were excluded or selectively reported to support any hypothesis. This approach ensures a more comprehensive understanding of system performance under varying conditions and preserves analytical transparency. The simulation parameters were clearly documented and presented as a proof of that.

5.3 Ethical Considerations

Quantum technology can have various military applications, as studied in Michal Krelina's work [13]. Contributing to research on the Byzantine agreement protocol directly supports advancements in quantum networks. Such protocols can enable secure and reliable communication in adversarial settings, which may have both civilian and military implications. The former can be benefited by criminal organizations which could exploit quantum protocols to ensure the integrity of their communications, taking advantage of features like tamper detection and manipulation resistance, making their operations harder to trace or disrupt. The latter is especially dangerous since it could accelerate the development of quantum warfare which could destabilize global security, provoke arms races, and influence current international conflicts.

5.4 Positive Societal Impact

Quantum Byzantine agreement protocols could significantly improve the reliability and security of critical infrastructure systems such as financial networks, electric grids, and air traffic control. By enabling fault-tolerant consensus even in the presence of compromised or malfunctioning nodes, these protocols could help ensure uninterrupted service and prevent failures in systems where trust and accuracy are vital for public safety.

6 Discussion

This section analyzes the effects of noise on the failure probability of the protocol, by finding the maximum level of noise for the protocol to keep the failure probability below 5%. It reflects on what has been concluded and gives a further explanation of the results.

6.1 Interpretation of Findings

In the absence of noise, the protocol achieved a failure probability well below 5% for m=300, confirming its robustness under ideal conditions. In Figure 2, we reproduce the experiment from Ref. [4] in Figure 4. In the faulty sender and faulty receiver (R_0) scenarios, the observed failure probabilities align well with their theoretical upper bounds. This likely results from the fact that the strategies followed by the nodes are designed to maximize the failure probability in these adversarial settings. When the noise was introduced into the simulation, we observed a clear increase in the probability of failure. Specifically, the simulations showed that when the gate depolarizing probability exceeded 0.001%, the measured failure probability surpassed the 5% threshold in at least one of the cases studied. The observed trend for two scenarios, no faulty nodes and one of the receivers being faulty (R_0), indicates that with higher probability of a Pauli gate error the failure probability increases. Based on our analysis it mainly comes from the *Consistency Condition* in *Check Phase* where all measured outcomes have to differ from the received bit from the sender. Even a small gate error can cause the state to deviate from the ideal form given in (1), thereby violating the assumptions required for the protocol to function correctly. Therefore, if the nodes abort the protocol it is counted as a failure according to Table 2 in Appendix B of Ref. [4]. In the case of a faulty sender, the trend is less clear. According to Table 2 in Appendix B of Ref. [4], an aborted protocol run is counted as successful. This means that if the *Consistency Condition* fails and the protocol is aborted, it is not counted as a failure. As a result, higher gate depolarizing probabilities may lead to more frequent abortions, which in turn can reduce the measured failure probability.

6.2 Implications for Real-World Implementation

While our simulations identified a specific noise threshold below which the protocol maintains an acceptable failure probability, it is important to compare these findings with current technological capabilities. The identified cut-off of 0.001% closely matches the currently achievable single-qubit error rate of 0.001(1)% reported for a specific scenario in Ref. [7], but is over an order of magnitude lower than the 0.07(5)% typical for two-qubit gates. If the specific scenario is not applicable to our case, the single-qubit error rate would likely be over an order of magnitude higher than the achieved threshold however, this requires further investigation. The currently achievable values for gate errors were based on gate fidelities reported in Ref. [7], using the relation Gate Error Rate $\approx 1 - F_{\text{avg}}$, which allows direct estimation of the error rate from experimentally measured average fidelities. In our simulation, the error rates for single- and two-qubit gates were assumed to be equal. This suggests that the higher noise level of two-qubit gates may be a critical bottleneck for practical implementation, particularly for the circuit shown in Figure 1, where two-qubit gates make up 5 out of the 13 total gates.

Moreover, our study focused solely on gate noise, isolating it from other sources of error such as measurement errors or decoherence. In practice, all of these factors contribute to the overall noise affecting a quantum system, and their combined effect could further increase the failure probability of the protocol.

Therefore, although the protocol shows potential under ideal or low-noise conditions, its practical implementation remains challenging with current hardware. These results highlight the critical need for robust error mitigation [14] or correction techniques, as well as improvements in hardware quality, before this protocol can be considered viable in real-world quantum systems.

7 Conclusions and Future Work

This section concludes the study by revisiting the main research question, *How is the failure probability of the protocol affected by hardware noise?* and highlights key findings. It also recommends directions for potential future research.

The specific question refined the main question to: *What is the maximum probability of gate error for the protocol to ensure the failure probability does not exceed 5%?*

Our main findings indicate that a gate depolarizing probability of 0.001%, when nodes use $m = 300$ four-qubit states to verify information, is sufficient to maintain the protocol's failure probability below or equal to 5%, even in the various Byzantine attack scenarios. Simulations showed that without any noise, the protocol consistently achieved high success rates. After introducing gate errors through simulation, a threshold was found beyond which the failure rate exceeded acceptable levels.

However, there are several open issues that need further investigation. This study only considered gate errors, which represent just one class of noise. Other realistic noise types, such as measurement errors and qubit decoherence were not included in our simulations. Additionally, while we fixed $m = 300$, determining the minimum value of m that ensures a failure probability below 5% under realistic noise conditions remains an open problem. We have also fixed the single-qubit depolarizing probability to be equal to a two-qubit one. How they individually contribute to the success probability of the protocol needs further research.

For future work, we recommend the following directions:

- **Extend the noise model** to include and combine additional noise types.
- **Investigate error detection and mitigation**, including whether such noise can be identified and corrected in real time.
- **Parameter optimization**, especially determining the smallest number of distributed four-qubit states for a given error rate that keeps the failure probability within acceptable bounds.
- **Protocol improvement**, the protocol is very intolerant to errors, we suggest exploring ways to loosen some of the strict conditions, such as *Consistency Condition.*
- **Varying gate error probabilities**, to analyze the individual impact of single-qubit and two-qubit gate errors on protocol performance. Studying their separate contributions could help identify which operations are the main bottlenecks and guide targeted hardware improvements or protocol adaptations.
- **Larger Simulation**: Our results exhibit a wide range of standard mean errors. Running simulations with more random samples could help narrow this range and identify the threshold with greater certainty.

Overall, while this paper establishes a foundational understanding of the protocol's tolerance to gate errors, a complete assessment of its robustness under realistic hardware conditions will require further research.

8 Code and Data

The code and data utilized in this study are publicly accessible via my personal GitHub repository [15]. Readers interested in replicating or extending our work are encouraged to explore the materials provided.

References

[1] Pierre Civit et al. *All Byzantine Agreement Problems are Expensive.* 2023. arXiv: `2311.08060 [cs.DC]`. URL: `https://arxiv.org/abs/2311.08060`.

[2] Leslie Lamport, Robert Shostak, and Marshall Pease. "The Byzantine Generals Problem". In: *ACM Trans. Program. Lang. Syst.* 4.3 (July 1982), pp. 382–401. ISSN: 0164-0925. DOI: `10.1145/357172.357176`. URL: `https://doi.org/10.1145/357172.357176`.

[3] Adán Cabello. "Solving the liar detection problem using the four-qubit singlet state". In: *Phys. Rev. A* 68 (1 July 2003), p. 012304. DOI: `10.1103/PhysRevA.68.012304`. URL: `https://link.aps.org/doi/10.1103/PhysRevA.68.012304`.

[4] Zoltán Guba et al. "Resource analysis for quantum-aided Byzantine agreement with the four-qubit singlet state". In: *Quantum* 8 (Apr. 2024), p. 1324. ISSN: 2521-327X. DOI: `10.22331/q-2024-04-30-1324`. URL: `https://doi.org/10.22331/q-2024-04-30-1324`.

[5] Matthias Fitzi. "Generalized communication and security models in Byzantine agreement". PhD thesis. TU, 2003.

[6] Lilian Childress and Ronald Hanson. "Diamond NV centers for quantum computing and quantum networks". In: *MRS Bulletin* 38.2 (Feb. 2013), pp. 134–138. ISSN: 1938-1425. DOI: `10.1557/mrs.2013.20`. URL: `https://doi.org/10.1557/mrs.2013.20`.

[7] H.P. Bartling et al. "Universal high-fidelity quantum gates for spin qubits in diamond". In: *Phys. Rev. Appl.* 23 (3 Mar. 2025), p. 034052. DOI: `10.1103/PhysRevApplied.23.034052`. URL: `https://link.aps.org/doi/10.1103/PhysRevApplied.23.034052`.

[8] SquidASM Developers. *SquidASM Documentation.* URL: `https://squidasm.readthedocs.io`.

[9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge: Cambridge University Press, 2010. ISBN: 9781107002173.

[10] M. Pease, R. Shostak, and L. Lamport. "Reaching Agreement in the Presence of Faults". In: *J. ACM* 27.2 (Apr. 1980), pp. 228–234. ISSN: 0004-5411. DOI: `10.1145/322186.322188`. URL: `https://doi.org/10.1145/322186.322188`.

[11] Tim Coopmans et al. "NetSquid, a NETwork Simulator for QUantum Information using Discrete events". In: *Communications Physics* 4.1 (July 2021). ISSN: 2399-3650. DOI: `10.1038/s42005-021-00647-8`. URL: `http://dx.doi.org/10.1038/s42005-021-00647-8`.

[12] Axel Dahlberg et al. *NetQASM: Low-level quantum instruction set architecture for quantum networks.* `https://github.com/QuTech-Delft/netqasm`. 2021.

[13] Michal Krelina. "Quantum technology for military applications". In: *EPJ Quantum Technology* 8.1 (Nov. 2021). ISSN: 2196-0763. DOI: `10.1140/epjqt/s40507-021-00113-y`. URL: `http://dx.doi.org/10.1140/epjqt/s40507-021-00113-y`.

[14] Zhenyu Cai et al. “Quantum error mitigation”. In: *Reviews of Modern Physics* 95.4 (Dec. 2023). ISSN: 1539-0756. DOI: `10.1103/revmodphys.95.045005`. URL: `http://dx.doi.org/10.1103/RevModPhys.95.045005`.

[15] Jerzy Wierzbicki. *Code and data for the research project*. 2025. URL: `https://github.com/jrzwrz/research_project`.