A Committee Based Optimal Asynchronous Byzantine Agreement Protocol W.P. 1

Nasit S Sony and Xianzhong Ding

A COMMITTEE BASED OPTIMAL ASYNCHRONOUS BYZANTINE AGREEMENT PROTOCOL W.P. 1

Nasit S Sony
University of California, Merced
CA 95340, USA
nsony@ucmerced.edu

Xianzhong Ding
Lawrence Berkeley National Laboratory
CA 94720, USA
dingxianzhong@lbl.gov

ABSTRACT

Multi-valued Byzantine agreement (MVBA) protocols are essential for atomic broadcast and fault-tolerant state machine replication in asynchronous networks. Despite advances, challenges persist in optimizing these protocols for communication and computation efficiency. This paper presents a committee-based MVBA protocol (cMVBA), a novel approach that achieves agreement without extra communication rounds by analyzing message patterns in asynchronous networks with probability 1. Unlike traditional MVBA, which requires all n parties (where $n = 3f + 1$, with f as the maximum number of faulty parties), cMVBA leverages a committee-based selection where a subset of $f + 1$ parties—ensuring at least one honest party—can efficiently achieve agreement. Integrating the asynchronous binary Byzantine agreement protocol, cMVBA uses verifiable proofs from these parties to finalize the agreement. The protocol is resilient to up to $\lfloor n/3 \rfloor$ Byzantine failures, with an expected runtime of $O(1)$, message complexity of $O(n^2)$, and communication complexity of $O((l + \lambda)n^2)$, where l is the input bit length and λ the security parameter.

Keywords Blockchain, Distributed Systems, Byzantine Agreement, System Security

1 Introduction

Byzantine Agreement (BA) protocols are essential for agreement in decentralized infrastructures, particularly in blockchain and other distributed applications. These protocols ensure agreement even with malicious actors, a necessity highlighted by the success of applications like Bitcoin [7] and similar decentralized systems [3]. However, existing asynchronous BA protocols face high communication costs and require time parameters to guarantee liveness, which limits their practical efficiency. The FLP impossibility result [6] further demonstrates that deterministic BA protocols cannot achieve guaranteed agreement in asynchronous networks, creating a need for efficient alternatives [5].

Traditional Multi-Valued Byzantine Agreement (MVBA) protocols like Cachin's [4] achieve agreement over large inputs but are constrained by high communication complexity, typically $O(n^3)$, making them impractical for large-scale systems. Approaches like VABA [5] and Dumbo-MVBA [12] improve efficiency with view-based methods and erasure coding, but at the expense of additional communication rounds. Signature-free solutions, such as Mostefaoui et al.'s protocol [1], further reduce overhead by relaxing validity conditions, yet achieving strong validity in asynchronous settings remains challenging.

We propose a Multi-Valued Byzantine Agreement (cMVBA) protocol to address these limitations. Our approach introduces a committee-based structure that dynamically selects a subset of $f + 1$ parties, ensuring at least one honest party in each instance. This design reduces message complexity by integrating the Asynchronous Binary Byzantine Agreement (ABBA) protocol, which reaches agreement with probability 1 without extra communication rounds. The cMVBA protocol achieves optimal performance with runtime $O(1)$, message complexity $O(n^2)$, and communication complexity $O((l + \lambda)n^2)$, where l is the input bit length and λ the security parameter.

Contributions:

- Introduce a committee selection protocol with at least one honest party, enhancing resilience against Byzantine failures.
- Propose cMVBA, reducing communication complexity from $O(n^3)$ to $O((l+\lambda)n^2)$ by selectively broadcasting proposals.
- Integrate ABBA to achieve reliable agreement on a proposal by a committee member.
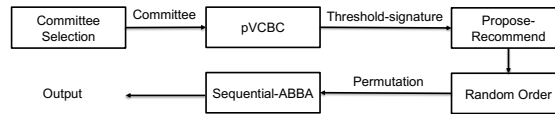- Provide theoretical analysis showing the effectiveness and the correctness of the protocol.

Figure 1: An overview of the proposed protocol framework.

2 Design of cMVBA

2.1 Overview

The cMVBA protocol achieves multi-valued Byzantine agreement by tolerating up to $f < \frac{n}{3}$ Byzantine faults, with an expected communication complexity of $O(ln^2 + \lambda n^2)$ and a constant asynchronous round count. The protocol is divided into five key sub-protocols: Committee Selection (CS), Prioritized Verifiable Consistent Broadcast (pVCBC), Propose-Recommend, Random Order, and Sequential-ABBA. Figure 1 illustrates the protocol's framework.

2.2 Committee Selection (CS)

CS optimizes Byzantine agreement efficiency by selecting a subset of $f + 1$ parties, based on party ID and protocol instance, to broadcast proposals rather than requiring all n parties. This subset selection ensures that at least one honest party participates and is dynamically determined via a cryptographic coin-tossing scheme inspired by FasterDumbo [2]. This randomness reduces risks of adversarial influence, prevents starvation, and mitigates Denial-of-Service attacks, ensuring fair participation across parties.

2.3 Prioritized Verifiable Consistent Broadcast

After committee selection, each member provides a verifiable proof of their proposal, confirming it has been sent to at least $f + 1$ honest parties. This proof, a threshold signature, ensures consistency by verifying that the proposal has been disseminated accurately. A modified version of the traditional VCBC protocol, called pVCBC, is used here to limit broadcast only to committee members, improving efficiency.

2.4 Propose-Recommend

In cMVBA, the Propose-Recommend step replaces the classic commit step to enhance efficiency. Here, only the committee members propose requests, attaching threshold signatures as verifiable proofs. The recommend phase collects these proofs, reaching agreement once $n - f$ recommendation messages are gathered. This streamlined process avoids the need for an n-length proof array, reducing complexity.

2.5 Random Order

This step generates a random permutation of the selected committee members to define proposal order, maintaining fairness and preventing adversaries from manipulating message delivery order. By randomizing order, cMVBA reduces the risk of increased asynchronous rounds and enhances protocol security.

2.6 Sequential-ABBA

The final phase in the cMVBA protocol is the Sequential-ABBA protocol, which is responsible for reaching an agreement on one of the proposals submitted by the selected parties. Building on the random order generated in the previous step, the Sequential-ABBA protocol runs an agreement loop that systematically evaluates each selected party's proposal. The input to this protocol consists of the permutation list generated in the Random Order step and the list of

recommendations obtained from the Propose-Recommend step. The output is the final proposal agreed upon by the parties.

3 Security Analysis of the Proposed Protocol

The correctness of the proposed protocol is critical to ensure that it adheres to the standard MVBA outcomes. Our goal is to prove that reducing the number of broadcasts does not compromise the protocol's reliability. The output of a party's request depends on the output of an ABBA instance within our protocol's agreement loop, typically resulting in a value of *1*. For the ABBA protocol to output *1*, at least one honest party must input *1*. We substantiate our protocol's integrity by demonstrating that at least $2f + 1$ parties receive a verifiable proof of a party's proposal, thus ensuring the necessary input for the ABBA instance. Here we provide the lemmas and theorem to prove the effectiveness and correctness of the protocol inspired from [9, 8, 11, 10].

Lemma 3.1. *At least one party's proposal reaches $2f + 1$ parties.*

Since the selected parties can be byzantine and the adversary can schedule the message delivery to delay the agreement, we have considered the following scenarios:

1. Among $\langle f + 1 \rangle$ selected parties, f parties are non-responsive.
2. Selected $\langle f + 1 \rangle$ parties are responsive, but other f non-selected parties are non-responsive.
3. Every party is responsive, including the selected $\langle f + 1 \rangle$ parties.
4. Selected $t \leq \langle f + 1 \rangle$ parties are responsive, and total m parties are responsive, where $\langle 2f + 1 \rangle \leq m \leq n$.

This lemma ensures that if $2f + 1$ parties receive a verifiable proof, at least one honest party will input *1* to the ABBA instance, ensuring the protocol reaches an agreement on *1*.

Lemma 3.2. *Without any permutation, the adversary can cause at most $f + 1$ iterations of the agreement loop in the Sequential-ABBA protocol.*

Lemma 3.3. *Let $\overline{A} \subseteq \{1, 2, ..., f + 1\}$ be the set of selected parties for which at least $f + 1$ honest parties receive the verifiable proof, and let Π be a random permutation of the $f + 1$ selected parties. Then, except with negligible probability:*

- *For every party $p \in \overline{A}$, the ABBA protocol on $ID|p$ will decide 1.*

- *$|\overline{A}| \geq 1$.*

- *There exists a constant $\beta > 1$ such that for all $t \geq 1$, $Pr[\Pi[1] \notin \overline{A} \wedge \Pi[2] \notin \overline{A} \wedge ... \wedge \Pi[t] \notin \overline{A}] \leq \beta^{-t}$.*

Theorem 3.4. *Given a protocol for biased binary Byzantine agreement and a protocol for verifiable consistent broadcast, the Prioritized-MVBA protocol provides multi-valued validated Byzantine agreement for $n > 3f$ and invokes a constant expected number of binary Byzantine agreement protocols.*

4 Conclusion

This paper introduced cMVBA, a novel MVBA protocol that minimizes communication complexity via a committee-based approach and ABBA integration. By dynamically selecting $f + 1$ parties to broadcast, cMVBA maintains resilience and efficiency, achieving optimal message complexity of $O(n^2)$ and expected constant asynchronous rounds. The introduction of the pVCBC protocol to reduce the number of broadcasts further enhances the effectiveness of the protocol, making cMVBA ideal for large-scale decentralized applications. Future work will explore adaptive scalability, protocol optimizations, and empirical validations to enhance robustness in diverse settings.

References

[1] Achour Mostefaoui, and Michel Raynal. Signature-free asynchronous byzantine systems: from multivalued to binary binary consensus with $t < n/3, O(n^3)$ messages, and constant time. In *Acta informatica* , volume 54, 2017.

[2] Bingyong Guo, Zhenliang Lu, Qiang Tang, Jing Xu and Zhenfeng Zhang. Dumbo: Faster asynchronous bft protocols. In *Proceedings of the ACM Conference on Computer and Communications Security*, page 803–818, 2020. URL: `"https://doi.org/10.1145/3372297.3417262"`.

[3] Christian Cachin and Marko Vukolic. Blockchain consensus protocols in the wild (keynote talk). In *Andréa W. Richa, editor, 31st International Symposium on Distributed Computing, DISC 2017*, Vienna, Austria, October 16-20 2017.

[4] Christian Cachin, Klaus Kursawe, Anna Lysyanskaya, and Reto Strobl. Asynchronous verifiable secret sharing and proactive cryptosystems. In *In Proc. ACM CCS*, page 88–97, 2002.

[5] Ittai Abraham, Dahlia Malkhi, and Alexander Spiegelman. Asymptotically optimal validated asynchronous byzantine agreement. In *PODC*, 2019.

[6] Michael J. Fischer, Nancy A. Lynch, and Michael S. Paterson. Impossibility of distributed consensus with one faulty process.32(2):. In *ACM*, page 374–382. ACM, April 1985.

[7] Satoshi Nakamoto. A peer-to-peer electronic cash system, 2008. URL: `http://bitcon.org/bitcoin.pdf`.

[8] Nasit S Sony, Xianzhong Ding, and Mukesh Singhal. Optimizing Communication in Byzantine Agreement Protocols with Slim-HBBFT. In *Euro-Par*, 2024. URL: `"https://easychair.org/publications/preprint/Zs8Mw/open"`.

[9] Nasit S Sony, Xianzhong Ding, and Mukesh Singhal. Prioritized-MVBA: A New Approach to Design an Optimal Asynchronous Byzantine Agreement Protocol. In *arXiv preprint*, June 2024. URL: `"arXivpreprintarXiv:2406.03739"`.

[10] Nasit S Sony. An Approach to Optimizing the VABA Protocol Using κ-size Committee. *arXiv preprint arXiv:2412.03789*, 2024.

[11] Nasit S Sony, Xianzhong Ding, and Mukesh Singhal. Slim-ABC: An Optimized Atomic Broadcast Protocol. *arXiv preprint arXiv:2410.04268*, 2024.

[12] Yuan Lu, Zhenliang Lu, Qiang Tang and Guiling Wang. Dumbo-MVBA: Optimal Multi-Valued Validated Asynchronous Byzantine Agreement, Revisited. In *Proceedings of the 39th Symposium on Principles of Distributed Computing*, July 2020.