

Byzantine Agreement with Faulty Majority using Bounded Broadcast

Jeffrey Considine, Leonid A. Levin*, David Metcalf
Boston University[†]

Abstract

Byzantine Agreement introduced in [Pease, Shostak, Lamport, 80] is a widely used building block of reliable distributed protocols. It simulates broadcast despite the presence of faulty parties within the network, traditionally using only private unicast links. Under such conditions, Byzantine Agreement requires more than $2/3$ of the parties to be honest. [Fitzi, Maurer, 00], constructed a Byzantine Agreement protocol for any honest majority based on an additional primitive allowing transmission to any two parties simultaneously. They proposed a problem of generalizing these results to wider channels and fewer honest parties. We prove that a $2k$ party channel is necessary and sufficient for implementing broadcast when honest parties are in $1/k$ minority.

1 Introduction

Broadcast primitives play a special role in multiplayer game theory as an integral component in the fault-tolerant implementation of game protocols. Given an honest majority, broadcast and private channels are sufficient to simulate any multi-party computation [Rabin, Ben-Or, 89], based on [Goldreich, Micali, Wigderson, 87], and [Ben-Or, Goldwasser,

Wigderson, 88]. With additional primitives, such as private and oblivious transfer channels, even a majority of faulty parties can be tolerated [Beaver, Goldwasser, 89], [Goldwasser, Levin, 90].

Since broadcast involves an unbounded number of participants, a reliable hardware solution was perceived as too strong an assumption. Byzantine Agreement protocols simulate broadcast on networks with faulty parties. Given only private channels, Byzantine Agreement is possible if and only if faulty parties are in a $< 1/3$ minority ([Pease, Shostak, Lamport, 80]). For this reason, protocols tolerant to more faults generally assume broadcast as a primitive.

Various hardware assumptions and communication goals were studied in the literature. For instance, [Angluin 80], [Goldreich, Goldwasser, Linial 91], [Franklin, Yung 95] and other papers studied problems of private communication on an incomplete broadcast network. [Franklin, Wright 98] showed that such a network with p disjoint paths from sender to receiver could tolerate $< p/2$ faulty parties. [Wang, Desmedt 01] showed that $< p$ faulty parties could be handled with probabilistic reliability.

The broadcast primitive is rather special in that, unlike other common primitives, it involves an unlimited number of parties. It is thus natural to explore the power of a limited version of broadcast, with a constant number of recipients. Assuming any honest majority, [Fitzi, Maurer, 00] used a 3-party broadcast primitive to simulate full broadcast. They

*Supported by NSF grants CCR 9820934, 0311411

[†]Leonid A. Levin (e-mail: Lnd@bu.edu), Computer Sci. dept., 111 Cummington St., Boston, MA 02215.
Last revised: August 9, 2013

asked what fraction of honest parties would be required given wider broadcast primitives. This is especially interesting in view of results (e.g. [3, 11]) that convert arbitrary protocols into equivalent ones with added tolerance to any faulty majorities, assuming the availability of broadcasts and two-party primitives, such as oblivious transfer and private channels. We show below that a $2k$ -party channel is necessary and sufficient to implement broadcast when honest parties are in a $1/k$ minority.

2 Definitions and Results

Definition 1 *A protocol is an algorithm used in rounds by several communicating parties. Each party starts with an input appended with its and other parties' identities. We assume reliable channels for all pairs of parties. That is, at each round parties can select messages and recipients who receive the message and the sender's identity as input for the next round. We refer to inputs, messages, and outputs as communications. Besides parties, the interaction is affected by the Adversary who can select the initial inputs of all parties, choose (possibly with restrictions) a subset of faulty parties and replace their communications by data of its choice.*

Definition 2 *A size k channel or k -channel is a primitive for authenticated reliable communication among k parties. To use it, (to k -send) one party, the sender, selects $k - 1$ recipients, and a message m . Each recipient gets m , as well as the identities of the sender and the other recipients.*

Definition 3 *Byzantine agreement is a broadcast simulating protocol. The party's value is its output for a recipient or input for the sender. The protocol succeeds if the values of non-faulty (honest) parties are all identical.*

Notation 1 *We will denote n, h the numbers of all and of honest parties respectively and call their ratio $r = n/h$ resilience. Its Byzantine number $\text{Byz}(r)$ is the minimal channel size that assures the Byzantine agreement.*

$\text{Byz}(r)$ could vary with n , but this dependence turns out inessential.

Theorem 1 $\text{Byz}(r) = 2r$ for integer r .

In other words, a $2k$ -channel is necessary and sufficient for implementing broadcast when honest parties are in $1/k$ minority. The theorem follows from these two Lemmas:

Lemma 1 $\text{Byz}(r) \geq \lfloor 2r \rfloor$.

Lemma 2 $\text{Byz}(r) \leq 2\lceil r \rceil$.

We give two constructions for the proof of Lemma 2. One is based on induction and gives the channel size indicated. The alternative construction is more transparent and efficient but gives a twice larger bound.

3 Tools

3.1 Broadcast and Consensus

In a traditional consensus model, each party starts with an input value. After running a consensus protocol, all honest parties output values which agree with each other and with an input of at least one honest party. With honest majority, consensus is easily shown to be equivalent to broadcast. To achieve consensus, each party broadcasts its value to the others who then output the majority value. To broadcast, the caster sends its input to all parties who then run a consensus protocol on the values received.

This equivalence fails when majority is faulty. The Adversary gives inputs 0 and 1 to equal number of parties. They all run the

protocol faithfully. The Adversary defeats the consensus by keeping honest some parties with different outputs or declaring faulty all parties whose inputs match the uniform output.

We generalize the consensus model, by assuming each party to have not just one input and output values but rather a *distribution*, *i.e.*, a value for each $(k-1)$ -set (*i.e.*, $(k-1)$ -node set) he belongs to. All honest members of a $(k-1)$ -set get the same input value for it. All output values of honest parties must agree with each other and with at least one input of an honest party. This model can simulate broadcast after the sender *distributes* his input, *i.e.*, k -sends it to all $(k-1)$ -sets.

3.2 Trust Graphs

As a tool in visualizing and analyzing relationships between parties, we use *trust graphs* linking pairs of parties that may be both honest. Such a graph is generated either by a single party or a group based on transmissions received by the entire group (or agreed upon by a group including all honest players). Edges connect parties that report consistently inputs received by both. A *pruning* is then conducted as follows. The h honest parties must form a clique; edges not in cliques can be removed. Since cliques are hard to detect, we remove instead (until none left) edges (a, b) that do not belong to any *bi-star* *i.e.*, an h -node star with two centers a, b (adjacent to all its nodes). Two “sender nodes” S_0, S_1 are then added and connected to all players who report uniform inputs 0 and 1 respectively.

Trust graphs are a useful tool for choosing an agreement value and placing bounds on the broadcast size it requires. All honest parties must be adjacent in the graph. If they know a unique sender node any of them may have paths to in their respective graphs, honest parties may immediately output its value.

Any path connecting S_0 to S_1 must have at least k parties. Otherwise there would be one k -send that all of these parties received; since parties connected to S_m claim this k -send was m , there must be some disagreement along this path. Each edge between parties belongs to an h -node bi-star. These bi-stars are disjoint for odd edges of any shortest path: otherwise they would yield a shorter path. So, $h\lfloor k/2 \rfloor$ or more nodes (besides S_m) are needed.

4 Proofs

4.1 Proof of Lemma 1

For $k < \lfloor 2r \rfloor$, the parties can be arranged into a $(k+1)$ -node *ring* with at least h parties in any two adjacent nodes. The sender’s node is denoted S . The Adversary picks two adjacent nodes and corrupts all parties in the other nodes.

All parties faithfully execute the protocol P with the exception that faulty parties may pretend to receive different messages in the same transmission from S . Each transmission from S misses all parties in at least one other node. The leftmost such node splits the ring into two parts: L and R . One of the parts has no honest parties who are all in adjacent nodes. Parties in S run two copies of P each: S_0 and S_1 . The sender’s S_0 gets input 0, his S_1 gets 1. Each transmission from S comes to L (including S_0) and R (including S_1) as if generated by S_0 and S_1 , respectively. If S is honest its *real* messages are those received by the other honest node.

With these restrictions each party can compute the claimed results of any transmission regardless of which other parties are honest. So, they need not actually communicate as prescribed by P , and can produce their outputs at the start. Then, either the nodes adjacent to S have the same outputs (one of

which conflicts with the respective side of the sender) or some two adjacent nodes have conflicting outputs. The Adversary defeats the protocol by keeping the conflicting nodes honest. ■

4.2 Proof of Lemma 2

Assume n is the minimal number of parties for which any Byzantine protocol with h honest parties can be disrupted. The sender starts by distributing its input. Then each party i distributes the content M_i of all messages it received, and all parties except the sender try to achieve an agreement about M_i . They succeed if the sender is faulty, since n is minimal; otherwise their results may conflict.

The parties who received the same message consistently from the sender output that message. This will include all honest parties if the sender is honest. The remaining parties form identical trust graphs. If S_0, S_1 are in different connected components, each party outputs the value of S_m it has a chain to or 0 if there is none. As explained in Section 3.2, the chain connecting S_0 to S_1 requires $h\lfloor k/2 \rfloor$ connecting nodes. This implies $k < 2\lceil r \rceil$. ■

4.3 A Faster Protocol

King’s Consensus. [Berman, Garay, Perry 89] define *king’s consensus* protocols from which broadcast is easily derived. [Fitzi, Maurer 2000] implemented king’s consensus in two rounds of 3-send. We use a similar idea. A *king’s consensus* protocol is a variation of Byzantine Agreement where one party is designated as a king. Honest outputs must agree with at least one honest input and, if the king is honest, with each other. To broadcast, the sender first sends its message to each receiver. Then, king’s consensus is repeated with each party in turn used as a king and outputs of each round used as inputs to the next one.

Moderated Consensus. We use a modification of king’s consensus adopted to our “distributional” consensus model of Section 3.1 and call it *moderated consensus*. Each party maintains a value for each $(k-1)$ -set it belongs to; the values of honest parties for the same set are always identical. Honest outputs must agree with at least one honest input and, if the moderator is honest, with each other. The consensus is achieved by running n rounds of moderated consensus with all (or any $n + 1 - h$) parties serving as a moderator, in turn.

4.3.1 2-Round Moderated Consensus

The combined size of messages grows by a factor n^c with each round of c -party broadcast. We treat c as a constant, thus, any constant number of rounds preserves polynomial complexity of the protocol. Let $k = 2\lfloor r \rfloor$. Moderated consensus can be implemented in two rounds of $2k$ -send as follows.

First, each receiver distributes the value for each of its $(k-1)$ -sets to each $(2k-1)$ -set including the moderator. In the second round, the moderator distributes copies of all messages received. Each party then generates an output for each $(k-1)$ -set G it belongs to. It considers only messages sent to the entire G preventing discrepancy between its honest members. A trust graph is built using values x for the message distributed by each party p determined as follows: x is used if p sends it consistently in all $(2k-1)$ -sends that include either G or, as reported by moderator, another $(k-1)$ -set; otherwise p is disconnected from the graph. G then outputs 1 if any its member has a path to S_1 ; otherwise it outputs 0.

Like in Section 2, the graph is too small to connect S_0 to S_1 . This assures agreement with honest moderator. If all honest parties start with the same value m for all their $(k-1)$ -sets, then at least $h-1$ of them, includ-

ing the sender node S_m , form a clique. This assures that each honest output agrees with at least one honest input.

References

- [1] *Proceedings of the Annual ACM Symposium on Theory of Computing.*
- [2] D. Angluin. Local and Global Properties in Networks of Processors. [STOC], 1980. pp. 82-93.
- [3] D. Beaver, S. Goldwasser. Multi Party Fault Tolerant Computation with Faulty Majority Based on Oblivious Transfer. *Proceedings of the Annual IEEE Symposium on Foundations of Computer Science*, 1989, pp. 468-473.
- [4] M. Ben-Or, S. Goldwasser, A. Wigderson. Completeness Theorems for Non-cryptographic Fault-tolerant Distributed Computation. [STOC], 1988, pp. 1-10.
- [5] M. Fischer, N. Lynch, M. Merritt. Easy Impossibility Proofs for Distributed Consensus Problems. *ACM Symposium on Distributed Computing*, 1985, pp. 59-70.
- [6] Matthias Fitzi, Ueli Maurer. From Partial Consistency to Global Broadcast. [STOC], 2000, pp. 494-503.
- [7] M. Franklin, R. Wright. Secure Communication in Minimal Connectivity Models. *Advances in Cryptology (Eurocrypt)*, 1998, pp. 346-360.
- [8] M. Franklin, M. Yung. Secure Hypographs: Privacy from Partial Broadcast. [STOC], 1995, pp. 36-44.
- [9] O. Goldreich, S. Goldwasser, N. Linial. Fault-tolerant Computation in the Full Information Model. *SIAM J. Computing*, 27(2), 1998, pp. 506-544.
- [10] O. Goldreich, S. Micali, A. Wigderson. How to Play Any Mental Game, or A Completeness Theorem for Protocols with Honest Majority. [STOC], 1987, pp. 218-229.
- [11] Shafi Goldwasser, Leonid A. Levin. Fair Computation of General Functions in Presence of Immoral Majority. *Annual CRYPTO Conference (IEEE/LACR)*, Santa Barbara, August 1990 (Proceedings 1991).
- [12] Danny Dolev, Michael J. Fischer, Rob Fowler, Nancy A. Lynch, and H. Raymond Strong. An efficient algorithm for Byzantine agreement without authentication. *Information and Control*, 52(3):257-274, 1982.
- [13] M. Pease, R. Shostak, L. Lamport. Reaching agreement in the presence of faults. *J. Comput. Mach.* 27:121-169, 1980.
- [14] T. Rabin, M. Ben-Or. Verifiable Secret Sharing and Multi-party Protocols with Honest Majority. [STOC], 1989, pp. 73-85.
- [15] Y. Wang, Y. Desmedt. Secure Communication in Multicast Channels: The Answer to Franklin and Wright's Question. *Advances in Cryptology (Eurocrypt)*, 1999, pp. 446-458.