On the Power of Imperfect Broadcast

Matthias Fitzi*, Stefan Wolf†, Jürg Wullschleger†
*Department of Computer Science
University of Århus, Denmark
fitzi@daimi.au.dk.
†Computer Science Department
ETH Zürich, Switzerland
{wolf, wjuerg}@inf.ethz.ch.

***Abstract*— A fundamental result in information-theoretic fault-tolerant distributed computing is that unconditionally secure broadcast (or Byzantine agreement) among three players is impossible if one player is misbehaving. In particular, imperfect broadcast with failure probability ε is achievable if and only if $\varepsilon \geq \frac{3-\sqrt{5}}{2}$.**

In this paper, we examine to what extent the failure probability of imperfect broadcast can be reduced. As a main result, we show that, among three players, broadcast with failure probability ε can be turned into broadcast with negligible failure probability if and only if $\varepsilon < 1/3$. This result is finally extended to the more general case of n players and any number of misbehaving players.

I. Introduction

A fundamental problem in fault-tolerant distributed computing is to achieve consistency of the involved parties' views, even if some of the parties (also called players) deviate from the protocol in an arbitrary manner. A core primitive for achieving global consistency is broadcast, i.e., a mechanism or protocol allowing one player, the sender, to send a value consistently to all other players such that, even in case of malicious behavior by the sender and/or some of the other players, all honest players receive the same value. The seminal result of Lamport, Shostak, and Pease [LSP82] is that broadcast can be implemented if and only if less than a third of all the players misbehave.

A. Model

We assume a set P of n players that are connected via a complete synchronous network of pairwise authenticated channels, i.e., channels that guarantee the authenticity of the sender. Whether the channels additionally guarantee privacy against a potential eavesdropper does not matter for our results. Synchronicity means that all players share common, synchronized clock cycles and that messages being sent during a clock cycle are guaranteed to have arrived at the beginning of the next cycle.

The resilience of a protocol is characterized by the number t of players that may deviate from the protocol. We refer to such a player as being *corrupted* whereas a non-corrupted player is called *correct*. It helps to imagine a central adversary who can corrupt up to t players and make them cheat in an arbitrary, coordinated manner.

In this paper, we make the distinction between a rushing and a non-rushing adversary. The natural assumption is that the adversary is *rushing*. A rushing adversary is given the power, during each communication cycle, to first collect all messages addressed to corrupted players — and exploit this information in order to decide on what the corrupted players send during the same cycle. In [GY89], this model is called the *sequential model*.

A less natural assumption is a *non-rushing* adversary. A non-rushing adversary cannot base the messages to be sent during a particular cycle on the messages the corrupted players receive during the same cycle. In [GY89], this model is called the *simultaneous model*.

B. Broadcast

Definition 1 (ε-BC): A protocol among n players $P = \{p_1, \ldots, p_n\}$ where player p_s (the *sender*) holds an input value $x_s \in \mathcal{D}$ (from a finite domain $\mathcal{D}$) and every player p_i finally decides on an output value $y_i \in \mathcal{D}$ achieves *ε-broadcast (ε-BC)* if it satisfies the following conditions with probability at least $1 - \varepsilon$:

- Consistency: All correct players p_i compute the same output, $y_i = y$.
- Validity: If p_s is correct then every correct p_i computes $y_i = x_s$. ◇

Typically, broadcast protocols are required to involve a negligible error probability $\varepsilon > 0$ or even required to be perfect ($\varepsilon = 0$). For this case, it was shown that broadcast is achievable if and only if $t < n/3$ [LSP82]. In particular, this implies that broadcast among three players with negligible error probability is impossible. The minimal error probability that is still achievable in this case was given in [KY84] (simultaneous model) and [GY89] (sequential model).

Proposition 1: [KY84] In the simultaneous model, ε-BC among three players is achievable if and only if $\varepsilon \geq 1/3$.

Proposition 2: [GY89] In the sequential model, ε-BC among three players is achievable if and only if $\varepsilon \geq (3 - \sqrt{5})/2 \approx 0.38$.

C. Contribution

In this paper, we demonstrate the somewhat counterintuitive fact that μ-BC with sufficiently small μ can be amplified to ε-BC with arbitrarily small error probability $\varepsilon > 0$. In particular, we show that this is possible if and only if $\mu < 1/3$. For the general case of n players and any number of corrupted players, we finally show that μ-BC with $\mu < 1/n$ allows for ε-BC with arbitrarily small ε.

II. Results

Lemma 1: In the sequential (or even simultaneous) model, among three players, μ-BC with $\mu \geq 1/3$ cannot be amplified to ε-BC with $\varepsilon < 1/3$.

Proof: The lemma directly follows from Proposition 1. ■

In order to prove the achievability part, we use the result in [FM00] that weak broadcast (or crusader agreement) [Dol82] is sufficient to achieve broadcast among three players.

Definition 2 (ε-WBC): A protocol where the sender holds input $x_s \in \mathcal{D}$ and every player p_i finally decides on $y_i \in \mathcal{D} \cup \{\perp\}$ achieves *ε-weak-broadcast (ε-WBC)* if it satisfies the following conditions with probability at least $1 - \varepsilon$:

- Consistency: If any correct player p_i computes $y_i \neq \perp$ then every correct player p_j computes $y_j \in \{y_i, \perp\}$.
- Validity: If p_s is correct then every correct p_i computes $y_i = x_s$. ◇

Theorem 1: In the sequential model, among three players, μ-BC with $\mu < 1/3$ allows for ε-BC with arbitrarily small $\varepsilon > 0$. In particular, this can be achieved from $O(k \cdot \delta^{-2})$ invocations of μ-BC where k is the security parameter ($\varepsilon < 2^{-k}$) and $\delta = 1/3 - \mu$.

Proof: In [FM00], it was shown that one invocation of weak broadcast among three players can be turned into broadcast without introducing any additional error probability. It is thus sufficient to show how to achieve ε-WBC.

The sender sends his input message $x_s \in \{0, 1\}$ m times (for large enough m) using μ-BC. Each recipient R_i decides on $y_i = b$ if he received bit $b \in \{0, 1\}$ at least $2m/3$ times, and on $y_i = \perp$, otherwise.

Let X_i ($i = 1, \ldots, m$) be the m independent binary random variables such that $X_i = 1$ exactly if the i-th invocation of μ-BC failed; and let $\delta = 1/3 - \mu$.

If the sender is correct then the probability that the protocol fails can be estimated by Chernoff Bound

$$\text{Prob}_{err} \leq \text{Prob}\left(\sum_{i=1}^{m} X_i \geq m/3 = (\mu + \delta)m\right) \leq e^{-\frac{\delta^2}{3\mu}m} .$$

If the sender is corrupted then, in order to make the protocol fail, he must achieve that both recipients disagree on the outcome of at least m invocations of μ-BC. Thus, the probability that the protocol fails with a corrupted sender can be estimated by the same Chernoff bound as above.

Choosing $m \geq \frac{3\mu \ln(\varepsilon^{-1})}{\delta^2} = O(k\delta^{-2})$ thus guarantees an error probability of at most $\text{Prob}_{err} \leq \varepsilon$. ■

More generally than in the three-player case, it can be shown that, among any number n of players, μ-BC for sufficiently small μ allows for ε-BC with arbitrarily small ε.

Theorem 2: In the sequential model, among n players where any number of players can be corrupted, μ-BC with $\mu < 1/n$ allows for ε-BC with arbitrarily small $\varepsilon > 0$. In particular, this can be achieved from $O(n^2 k \cdot \delta^{-2})$ invocations of μ-BC where k is the security parameter ($\varepsilon < 2^{-k}$) and $\delta = 1/n - \mu$.

Proof: In [CFF$^+$05] it was shown that, among n players, n-proxcast (a generalization of weak broadcast with multiple intermediary values $\perp$) is sufficient in order to achieve broadcast. Furthermore, n-proxcast can be achieved from μ-BC ($\mu < 1/n$) in a similar way as, among three players, weak broadcast from μ-BC ($\mu < 1/3$). The theorem now follows from the analysis in [CFF$^+$05]. ■

III. Acknowledgments

The work by Matthias Fitzi was supported by the European project SECOQC.

References

[CFF+05] Jeffrey Considine, Matthias Fitzi, Matthew Franklin, Leonid A. Levin, Ueli Maurer, and David Metcalf. Byzantine agreement given partial broadcast. *Journal of Cryptology*, 18(3), 2005.

[Dol82] Danny Dolev. The Byzantine generals strike again. *Journal of Algorithms*, 3(1):14–30, 1982.

[FM00] Matthias Fitzi and Ueli Maurer. From partial consistency to global broadcast. In *Proceedings of the 32nd Annual ACM Symposium on Theory of Computing (STOC '00)*, pages 494–503, 2000.

[GY89] Ronald L. Graham and Andrew C. Yao. On the improbability of reaching Byzantine agreements. In *Proceedings of the 21st Annual ACM Symposium on Theory of Computing (STOC '89)*, pages 467–478, 1989.

[KY84] Anna Karlin and Andrew C. Yao. Probabilistic lower bounds for Byzantine agreement and clock synchronization. Manuscript, 1984.

[LSP82] Leslie Lamport, Robert Shostak, and Marshall Pease. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems*, 4(3):382–401, July 1982.