Distributed Computing Meets Game Theory

Fault Tolerance and Implementation with Cheap Talk

Joseph Y. Halpern
Cornell University, Ithaca, NY, USA

Abstract

Traditionally, work in distributed computing has divided the agents into "good guys" and "bad guys". The good guys follow the protocol; the bad guys do everything in their power to make sure it does not work. By way of contrast, game theory has focused on "rational" agents, who try to maximize their utilities. Here I try to combine these viewpoints. Specifically, following the work of Abraham et al. [2], I consider (k,t)-*robust* protocols/strategies, which tolerate coalitions of rational players of size up to k and up to t malicious players. I focus in particular on the problem that economists have called implementing a mediator. That is, can the players in the system, just talking among themselves (using what economists call "cheap talk") simulate the effects of the mediator (see, e.g., [3, 4, 5, 6, 8, 10, 11]). In computer science, this essentially amounts to multiparty computation [7, 9, 12]. Ideas from cryptography and distributed computing allow us to prove results on how many agents are required to implement a (k,t)-robust mediator just using cheap talk. These results subsume (and, in some cases, correct) results from the game theory literature.

The results of Abraham et al. [2] were proved for what are called *synchronous systems* in the distributed computing community; this is also the case for all the results in the economics literature cited above. In synchronous systems, communication proceeds in atomic rounds, and all messages sent during round r are received by round $r+1$. But many systems in the real world are *asynchronous*. In an asynchronous setting, there are no rounds; messages sent by the players may take arbitrarily long to get to their recipients. Markets and the internet are best viewed as asynchronous. Blockchain implementations assume *partial synchrony*, where there is an upper bound on how long messages take to arrive. The partial synchronous setting already shows some of the difficulty of moving away from synchrony: An agent i can wait to take its action until it receives a message from j (on which its action can depend). This cannot happen in a synchronous setting. Abraham, Dolev, Geffner, abnd Halpern [1] extend the results on implementing mediators to the asynchronous setting.

2012 ACM Subject Classification Theory of computation → Algorithmic game theory and mechanism design

Keywords and phrases robust equilibrium, implementing mediators, asynchronous systems

Digital Object Identifier 10.4230/OASIcs.Tokenomics.2021.1

Category Invited Talk

Related Versions The talk described by this paper is based on two papers: "Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation", by Ittai Abraham, Danny Dolev, Rica Gonen, and Joseph Y. Halpern, which appeared in the *Proceedings of the 25th Annual ACM Symposium on Principles of Distributed Computing*, pp. 53–62, 2006, and "Implementing mediators with asynchronous cheap talk", by Ittai Abraham, Danny Dolev, Ivan Geffner, Joseph Y. Halpern, which appeared in *Proceedings of the 38th Annual ACM Symposium on Principles of Distributed Computing*, pp. 501–510, 2019.
Full Version: `https://arxiv.org/abs/1806.01214`

Funding Halpern's work was supported in part by NSF grants IIS-1703846 and IIS-0911036, ARO grant W911NF-17-1-0592, MURI (MultiUniversity Research Initiative) under grant W911NF-19-1-0217, and a grant from Open Philanthropy.

3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics 2021).
Editors: Vincent Gramoli, Hanna Halaburda, and Rafael Pass; Article No. 1; pp. 1:1–1:2
OpenAccess Series in Informatics
Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

References

1 I. Abraham, D. Dolev, I. Geffner, and J. Y. Halpern. Implementing mediators with asynchronous cheap talk. In *Proc. 38th ACM Symposium on Principles of Distributed Computing*, pages 501–510, 2019.

2 I. Abraham, D. Dolev, R. Gonen, and J. Y. Halpern. Distributed computing meets game theory: robust mechanisms for rational secret sharing and multiparty computation. In *Proc. 25th ACM Symposium on Principles of Distributed Computing*, pages 53–62, 2006.

3 I. Barany. Fair distribution protocols or how the players replace fortune. *Mathematics of Operations Research*, 17(2):327–340, 1992.

4 E. Ben-Porath. Cheap talk in games with incomplete information. *Journal of Economic Theory*, 108(1):45–71, 2003.

5 F. Forges. Universal mechanisms. *Econometrica*, 58(6):1341–64, 1990.

6 D. Gerardi. Unmediated communication in games with complete and incomplete information. *Journal of Economic Theory*, 114:104–131, 2004.

7 O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game. In *Proc. 19th ACM Symposium on Theory of Computing*, pages 218–229, 1987.

8 Y. Heller. A minority-proof cheap-talk protocol. Unpublished manuscript, 2005.

9 A. Shamir, R. L. Rivest, and L. Adelman. Mental poker. In D. A. Klarner, editor, *The Mathematical Gardner*, pages 37–43. Prindle, Weber, and Schmidt, Boston, MA, 1981.

10 A. Urbano and J. E. Vila. Computational complexity and communication: coordination in two-player games. *Econometrica*, 70(5):1893–1927, 2002.

11 A. Urbano and J. E. Vila. Computationally restricted unmediated talk under incomplete information. *Economic Theory*, 23(2):283–320, 2004.

12 A. Yao. Protocols for secure computation (extended abstract). In *Proc. 23rd IEEE Symp. Foundations of Computer Science*, pages 160–164, 1982.