Inria

WIDE Team

# PhD Topic: REDA
# Reliable Distribution in Adversarial environments

**Supervision:** Davide Frey and Achour Mostefaoui (WIDE Team, Inria Rennes)

**Context:** Distributed algorithms lie at the core of a variety of modern information systems like social networks [1], collaborative platforms [2, 3, 4], blockchain [5, 6, 7, 8], identity management systems [9, 10, 11], or decentralized machine learning [12, 13, 14]. Maintaining their ability to operate in the presence of adversarial behaviors, therefore, plays a paramount role in modern systems.

Traditionally, research in distributed algorithms has modeled such adversarial behavior with Byzantine processes [15, 16]: participants that may deviate arbitrarily from their prescribed algorithm, for instance by omitting, corrupting, or sending spurious messages. But adversarial behavior, be it malicious or simply resulting from actual failures, may also affect communication. This is typically modelled through a notion of Message Adversary (MA). Initially introduced by Santoro and Widmayer [17], the MA fault model has since then been used in many subsequent works [18, 19, 20, 21, 22, 23, 24, 25].

Almost all research combining Byzantine and Message adversaries considers, however, a synchronous model [26], which represents an oversimplification with respect to real systems. Only a few instances address a hybrid Byzantine/MA adversary in an asynchronous network [27, 28, 29]. But contrary to the oversimpification of the synchronous setting, an asynchronous model often results in overpessimistic assumptions. This has led to the development of partial synchrony [30] and even to models [31] where each link in the communication graph may provide different synchrony guarantees.

Similarly, the very notion of message adversary as studied by most research work [18, 19, 20, 21, 22, 23, 24, 25, 27, 28, 29] considers an overly aggressive model in which the communication graph can continuously change, almost in an arbitrary manner. But luckily, failures or even adversarial behavior tend to have a more limited disruptive power. For this reason, some authors [32, 24] have considered weakenings of the message-adversary model: for example, by considering a network that stabilizes over time.

**Goals:** This PhD thesis aims to explore more realistic adversarial models for distributed algorithms that better match the challenges of real systems. We plan to consider mainly the problem of reliable broadcast, which we have already studied under the classical message-adversary model [29, 28]. But depending on the interest of the PhD candidate, we may also consider Consensus or other problems in the message-passing domain. This will involve a number of research directions:

— Explore novel relaxations of the message-adversary model, for example, by introducing the notion of invulnerable links and nodes, which may, for example, model protected communication channels or computing devices equipped with trusted-execution environments.

— Consider the whole spectrum of models between synchrony and asynchrony, including partial synchrony and the newly introduced notion of granular synchrony [31]. In particular, we envision

combining it with a similar but novel notion of a granular message adversary, where different links exhibit different levels of vulnerability with respect to the adversary.

— Go beyond the notion of a deterministic message adversary and associate each link with a probability of disruption. This would better model existing systems and may result in making some impossible problems, like consensus, solvable in the probabilistic setting.

The selected candidate will be able to leverage the expertise of the WIDE team, and in particular of Davide Frey, Francois Taiani, on the notion of message adversary [29, 28], and that of Achour Mostefaoui on Byzantine Fault Tolerance and asynchronous distributed algorithms [33].

## REFERENCES


[1] Marin Bertier, Davide Frey, Rachid Guerraoui, Anne-Marie Kermarrec, and Vincent Leroy. The gossple anonymous social network. In Indranil Gupta and Cecilia Mascolo, editors, *Middleware 2010*, pages 191–211, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[2] Brice Nédelec, Pascal Molli, and Achour Mostéfaoui. A scalable sequence encoding for collaborative editing. *Concurrency and Computation: Practice and Experience*, 33(8):e4108, 2021. e4108 cpe.4108.

[3] Brice Nédelec, Pascal Molli, Achour Mostefaoui, and Emmanuel Desmontils. Lseq: an adaptive structure for sequences in distributed collaborative editing. In *Proceedings of the 2013 ACM Symposium on Document Engineering*, DocEng '13, page 37–46, New York, NY, USA, 2013. Association for Computing Machinery.

[4] Hoai Le Nguyen and Claudia-Lavinia Ignat. Time-position characterization of conflicts: A case study of collaborative editing. In Alexander Nolte, Claudio Alvarez, Reiko Hishiyama, Irene-Angelica Chounta, María Jesús Rodríguez-Triana, and Tomoo Inoue, editors, *Collaboration Technologies and Social Computing*, pages 65–80, Cham, 2020. Springer International Publishing.

[5] Victor Luchangco. Theory meets practice in the algorand blockchain (invited talk). Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2023.

[6] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. Algorand: Scaling byzantine agreements for cryptocurrencies. In *Proceedings of the 26th Symposium on Operating Systems Principles*, SOSP '17, pages 51–68, New York, NY, USA, 2017. ACM.

[7] J. Sousa, A. Bessani, and M. Vukolic. A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform. In *2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 51–58, June 2018.

[8] Emmanuelle Anceaume, Davide Frey, and Arthur Rauch. Sharding in permissionless systems in presence of an adaptive adversary. In Armando Castañeda, Constantin Enea, and Nirupam Gupta, editors, *Networked Systems - 12th International Conference, NETYS 2024, Rabat, Morocco, May 29-31, 2024, Proceedings*, volume 14783 of *Lecture Notes in Computer Science*, pages 1–31. Springer, 2024.

[9] Mathieu Gestin. *Privacy-preserving and fully distributed identity management systems*. Theses, Université de Rennes, December 2024.

[10] The Sovrin foundation. Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust. Technical report, January 2018.

[11] Jolocom white paper v2.1, A Decentralized, Open Soure Solution For Digital Identity and Access Management. Technical report, December 2019.

[12] Martijn de Vos, Sadegh Farhadkhani, Rachid Guerraoui, Anne-Marie Kermarrec, Rafael Pires, and Rishi Sharma. Epidemic learning: Boosting decentralized learning with randomized

communication. In *37th Annual Conference on Neural Information Processing Systems (NeurIPS '23)*, 2023.

[13] Sayan Biswas, Davide Frey, Romaric Gaudel, Anne-Marie Kermarrec, Dimitri Lerévérend, Rafael Pires, Rishi Sharma, and François Taïani. Low-Cost Privacy-Preserving Decentralized Learning. In *Proceedings on Privacy Enhancing Technologies Symposium*, volume 2025, pages 451–474, Washinghton DC, United States, July 2025. 24 pages, accepted at Pets 2025.

[14] Róbert Ormándi, István Hegedűs, and Márk Jelasity. Gossip learning with linear models on fully distributed data. *Concurrency and Computation: Practice and Experience*, 25(4):556–571, 2013.

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

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

[17] Nicola Santoro and Peter Widmayer. Time is not a healer. In *STACS 89*, pages 304–313, Berlin, Heidelberg, 1989. Springer Berlin Heidelberg.

[18] Yehuda Afek and Eli Gafni. Asynchrony from synchrony. In *Proc. 14th Int'l Conference on Distributed Computing and Networking (ICDCN'13)*, volume 7730 of *Lecture Notes in Computer Science*, pages 225–239. Springer, 2013.

[19] Bernadette Charron-Bost and André Schiper. The heard-of model: Computing in distributed systems with benign faults. *Distributed Comput.*, 22(1):49–71, 2009.

[20] Michel Raynal and Julien Stainer. Synchrony weakened by message adversaries vs asynchrony restricted by failure detectors. In *Proc. 32th ACM Symposium on Principles of Distributed Computing (PODC'13)*, pages 166–175. ACM, 2013.

[21] Nicola Santoro and Peter Widmayer. Agreement in synchronous networks with ubiquitous faults. *Theor. Comput. Sci.*, 384(2-3):232–249, 2007.

[22] Lewis Tseng, Qinzi Zhang, Saptaparni Kumar, and Yifan Zhang. Exact consensus under global asymmetric Byzantine links. In *Proc. 40th IEEE International Conference on Distributed Computing Systems (ICDCS'20)*, pages 721–731. IEEE, 2020.

[23] Étienne Coulouma, Emmanuel Godard, and Joseph Peters. A characterization of oblivious message adversaries for which consensus is solvable. *Theoretical Computer Science*, 584:80–90, 2015. Special Issue on Structural Information and Communication Complexity.

[24] Manfred Schwarz, Kyrill Winkler, and Ulrich Schmid. Fast consensus under eventually stabilizing message adversaries. In *Proceedings of the 17th International Conference on Distributed Computing and Networking*, ICDCN '16, New York, NY, USA, 2016. Association for Computing Machinery.

[25] Ami Paz, Hugo Rincon Galeana, Stefan Schmid, Ulrich Schmid, and Kyrill Winkler. The Time Complexity of Consensus Under Oblivious Message Adversaries. *Algorithmica*, 86(6):1830–1861, 2024.

[26] Martin Biely, Ulrich Schmid, and Bettina Weiss. Synchronous consensus under hybrid process and link failures. *Theor. Comput. Sci.*, 412(40):5602–5630, 2011.

[27] Ulrich Schmid and Christof Fetzer. Randomized asynchronous consensus with imperfect communications. In *22nd Symposium on Reliable Distributed Systems (SRDS 2003)*, pages 361–370. IEEE, 2003.

[28] Timothé Albouy, Davide Frey, Michel Raynal, and François Taïani. Asynchronous byzantine reliable broadcast with a message adversary. *Theor. Comput. Sci.*, 978(C), November 2023.

[29] Timothé Albouy, Davide Frey, Ran Gelles, Carmit Hazay, Michel Raynal, Elad Michael Schiller, François Taïani, and Vassilis Zikas. Near-optimal communication byzantine reliable broadcast under a message adversary. In *OPODIS*, volume 324 of *LIPIcs*, pages 14:1–14:29. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2024.

[30] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. Consensus in the presence of partial synchrony. *J. ACM*, 35(2):288–323, April 1988.

[31] Neil Giridharan, Ittai Abraham, Natacha Crooks, Kartik Nayak, and Ling Ren. Granular Synchrony. In Dan Alistarh, editor, *38th International Symposium on Distributed Computing (DISC 2024)*, volume 319 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 30:1–30:22, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[32] Martin Biely, Peter Robinson, and Ulrich Schmid. Agreement in directed dynamic networks. In *Proceedings of the 19th International Conference on Structural Information and Communication Complexity*, SIROCCO'12, page 73–84, Berlin, Heidelberg, 2012. Springer-Verlag.

[33] Kowalski Vincent, Mostéfaoui Achour, and Perrin Matthieu. An optimal byzantine scd-broadcast protocol. In *2024 19th European Dependable Computing Conference (EDCC)*, pages 139–146, 2024.