MSc Research Internship – Stage M2 2019-2010 : Scalable Byzantine Reliable Broadcast

1 Supervision

Advisers	François Taiani, `francois.tainai@irisa.fr`, 02 99 84 75 04
	George Giakkoupis, `george.giakkoupis@inria.fr`
	Davide Frey, `davide.frey@inria.fr`
	Michel Raynal, `michel.raynal@irisa.fr`
Lab	Centre Inria Rennes, IRISA (UMR 6074)
Team	WIDE (The World Is DistributEd)
	Équipes-Projet Inria / Département D1 IRISA

2 Context

The rise of blockchain-based crytocurrencies and smart-contract technology such as Bitcoin [5, 8] or Ethereum have brought a renewed and growing interest in Byzantine fault tolerant (BFT) protocols and primitives [6]. Such protocols are designed to deliver provable guarantees even when a substantial proportion of their participants (e.g. up to $\frac{1}{3}$) behave maliciously, which makes them particularly attractive when constructing trust-less peer-to-peer systems.

Originally centered on Byzantine consensus, these efforts have since then expanded to revisit weaker (and hence more efficient) Byzantine primitives, such as snapshot memory [2] and Byzantine reliable broadcast [1, 4].

Traditional Byzantine protocols unfortunately often suffer from a high message complexity (e.g. in $O(n^2)$ or worse), which makes them difficult to apply in large-scale systems. Recent proposals have therefore started to explore how stochastic techniques from epidemic protocols can be used to boost the scalability of BFT systems, while retaining most of their Byzantine resilience [3, 7].

In this project, we are particularly interested in the work recently presented in [3]. This work takes an existing Byzantine reliable broadcast protocol that relies on well-chosen intersecting *quorums* to negate the malicious influence of Byzantine nodes, and replaces these quorums by probabilistic sampling operations of the system, relying on a Random Peer Sampling (RPS) mechanism for this step.

3 Objective

The goal of this research internship is to explore how the strategy used in [3] can be applied to other Byzantine protocols, by focusing in particular on the Byzantine reliable broadcast algorithm proposed in [4], which presents a different trade-off between Byzantine resilience and efficiency.

4 Tasks

- The first task will consists in formalizing the properties the (Probabilistic) Byzantine Reliable Broadcast should obey by adapting the standard deterministic properties of the deterministic version of the protocol.
- In a second step, we will design a probabilistic version of the Raynal and Imbs algorithms, striving for simplicity and conciseness.
- Finally, the internship will seek to prove using tools from discrete probability, random graph theory, and discrete stochastic processes that the proposed algorithm fulfills the above properties.
- If time permits, we might consider other Byzantine broadcast algorithms, with richer properties, and possibly envisage generic approach to transform deterministic distributed algorithms in a scalable probabilistic version.

5 Candidate Profile

In this internship, the student is expected to provide formal proofs, which will involve the analysis of discrete stochastic processes, so the student should have a good background in discrete probability. Some background on algorithms would be appreciated, along with some basic programming skills in order to implement simple simulation experiments.

References

[1] Gabriel Bracha. Asynchronous byzantine agreement protocols. *Inf. Comput.*, 75(2):130–143, 1987.

[2] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovič, and Dragos-Adrian Seredinschi. The consensus number of a cryptocurrency. In *PODC'19*, pages 307–316. ACM Press, 2019.

[3] Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovič, and Dragos-Adrian Seredinschi. Scalable byzantine reliable broadcast. In *33rd International Symposium on Distributed Computing (DISC'19)*, 2019.

[4] Damien Imbs and Michel Raynal. Trading off t-resilience for efficiency in asynchronous byzantine reliable broadcast. *Parallel Processing Letters*, 26(04):1650017, 2016.

[5] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system, 2008.

[6] Michel Raynal. *Fault-Tolerant Message-Passing Distributed Systems.* Springer International Publishing, 2018.

[7] Team Rocket. Snowflake to Avalanche: A Novel Metastable Consensus Protocol Family for Cryptocurrencies, May 2018.

[8] Gavin Wood. Ethereum: A secure decentralised generalised transaction ledger, 2014. http://bitcoinaffiliatelist.com/wp-content/uploads/ethereum.pdf (accessed April 3rd, 2018).