{tag} {/tag}

International Journal of Computer Applications

Volume 43 - Number 22

Year of Publication: 2012

Authors:

Nazreen Banu

Samia Souissi

Taisuke Izumi

10.5120/6400-8878

{bibtex}pxc3878878.bib{/bibtex}

Abstract

We study the problem of Byzantine agreement in synchronous systems where malicious agents can move from one process to another and try to corrupt them. This model is known as mobile Byzantine faults. In a previous result [10], Garay has shown that n > 6t (n is the total number of processes, and t is the number of mobile faults) is sufficient to solve this problem even in the presence of strong agents. These agents can move at full speed (in the sense that each agent can take a movement in every round) and can make corrupted processes forget that they run the algorithm (as a result, after recovery a process must learn the current state of computation including the code from other processes). Many following results [3] have improved the above result but with some additional assumptions such as a corrupted process must recover and learn the current state of computation before another process can fail instead of it. The question, whether the result of Garay can be improved without any additional assumption, remains open. In this paper, we answer this question by providing an algorithm MBA that works with n > 4t.

References

- M. Biely and M. Hulte: "Consensus When All Processes may be Byzantine for Some Time", In Proc. 11th International Sympo- sium on Stabilization, Safety, and Security of Distributed Systems (SSS '09), vol. 5873, pp. 120–132, 2009.
- A. N Bessani and P. Sousa and M. Correia and N. F. Neves and P. Verissimo: "The CRUTIAL way of critical infrastructure protection", IEEE Security and Privacy, vol. 6(6), pp. 44-51, 2008.
- H. Buhrman, J. A. Garay and J. Hoepman: "Optimal Resiliency Against Mobile Faults", In Proc. 25th International Symposium on Fault-Tolerant Computing (FTCS'95), 1995.
- C. Cachin and K. Kursawe and F. Petzold and V. Shoup: "Secure and efficient asynchronous broadcast protocols (extended abstract)", Kilian, J. , editor, Advances in Cryptology: CRYPTO 2001, vol. 2139 of LNCS, pp. 524-541, 2001.
- M. Castro and B. Liskov: "Practical Byzantine fault tolerance and proactive recovery", ACM Transactions on Computer Systems, vol. 20(4), pp. 398-461, 2002. CMS07,
- T. Chandra and S. Toueg: "Unreliable failure detectors for reliable distributed systems", Journal of the ACM, vol. 43(2), pp. 225-267, 1996.
- B. G. Chun and P. Maniatis and S. Shenker and J. Kubiatowicz: "Attested append-only memory: making adversaries stick to their word", In Proc. of the 21st ACM Symposium on Operating Systems Principles, pp. 189- 204, 2007. 6 REFERENCES International Journal of Computer Applications (0975 - 8887) Volume 43- No. 21, April 2011
- M. Correia and N. F. Neves and P. Verissimo: "From consensus to atomic broadcast: Time-free Byzantine-resistant protocols without signatures", "Computer Jour- nal, vol. 41(1), pp. 82-96, 2006.
- V. Hadzilacos and S. Toueg: "A modular approach to fault-tolerant broadcasts and related problems", Technical Report TR94- 1425, Cornell University, Department of Computer Science, 1994.
- J. A. Garay: "Reaching (and Maintaining) Agreement in the Presence of Mobile Faults", In Proc. 8th International Workshop on Dis- tributed Algorithms, LNCS. No. 857, pp. 253– 264, 1994.
- R. Guerraoui and A. Schiper: "The generic consensus service", IEEE Transactions on Software Engineering, vol. 27(1),pp. 29-41, 2001.
- Kepphart and White: "Directed graph epidemiological models of computer viruses", IEEE symposium on Security and Privacy, 1991.
- L. Lamport and R. E. Shostak and M. C. Pease: "The Byzantine Generals Problem", ACM Transactions on Programming Lan- guages and Systems (TOPLAS), vol. 4(3), pp. 382–401, 1982.
- R. Ostrovsky and M. Yung: "How to withstand mobile attacks" In Proc. of tenth an- nual ACM symposium on Principles of dis- tributed computing(PODC'91), 1991.
- R. Reischuk: "A new solution for Byzantine generals problem", Information and Control, vol. 64, 1985.
- N. Santoro and P. Widmayer: "Time is not a healer", In Proc. 6th Annual Sympo- sium on Theor. Aspects of Computer Sci- ence(STACS89), LNCS. No. 349, pp. 304-313, 1989.

- U. Schmid, B. Weiss and I. Keidar: "Impossibility Results and Lower Bounds for Consensus under Link Failures", SIAM Journal on Computing", vol. 38, pp. 1912–1951, 2009.
- F. B. Schneider: "Implementing faul-tolerant services using the state machine approach: A tutorial", ACM Computing Surveys, vol. 22(4), pp. 299-319, 1990.
- P. Thambidurai and You-Keun Park: "Interactive Consistency with Multiple Failure Modes", In Proc. Reliable Distributed Sys- tems, pp. 93–100, 1988.
- G. S. Veronese and M. Correia and A. N. Bessani and L. C. Lung: "Highly-resilient services for critical infrastructures", In Proc. of the Embedded Systems and Communica- tions Security Workshop, 2009.
- J. Yin and J. Martin and A. Venkataramani and L. Alvisi and M. Dahlin: "Separating agreement from execution for Byzantine fault-tolerant services", In Proc. of the 19th ACM Symposium on Operating Sys- tems Principles, pp. 253-267, 2003.

Index Terms

Computer Science

Keywords

Synchronous Systems Agreement(consensus) Problem Mobile Byzantine Adversary