DECENTRALIZED STORAGE SYSTEM WITH VERIFICATION

(KISS)

Ivan Luchev, 724727

MY GROUP

DECENTRALIZED STORAGE SYSTEM WITH VERIFICATION

March 2023

Advisor: Niels Olof Bouvin

AARHUS
UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

1 RELATED WORK

The aim in this project is to build resilience against malicious peers, and not invent a new decentralized storage system. Comparison between performance between decentralized storage systems has been done before [4] & [1]. The results are that Pastry is the best performer for networks with under 1000 peers, but the paper also suggests that Kademlia would probably outperform Pastry for larger networks. The results in the 2 papers differ somewhat from the results in [3], which suggests that theoretically Chord should outperform Kademlia, but the paper does not do in-depth evaluation of networks with high churn rate like [4]. Since we want to build a network to withstand disruptions, we build this project on top of Kademlia. This means that in terms of performance of the storage operations, the system in this project will perform the same as Kademlia.

We can compare the approach in this project and the ARA proposal [2]. Both KISS and ARA rely on auditing to detect malicious peers or degradation of the network. Peers in ARA share information about what data they are storing and check each other. This is based on a list of interested peers (peers that interacted recently with a given peer). An issue with this approach would be if a subnet is composed entirely of malicious peers. Then a peer that has only malicious peers can freely adjust its credit score. Another problem would be generation of fake requests in order to increase the score of malicious peers, that store data for these requests. Peers in the KISS network are not as "smart" and do not have such responsibility. Instead, the audit is performed by an outside entity. This entity might be another decentralized network or a centralized authority. This delegates the complexity of keeping the network in check and shifts the problem elsewhere. KISS doesn't suffer from malicious subnets, because the Verifiers are rotated and are not necessarily peers that have recently interacted with a given peer. Also, since answering requests doesn't contribute to a peer's reputation there is no reason to flood the network with fake requests. It doesn't mean that a DoS attack against the network is impossible, but it will not affect the reputation/trust of the peers. A strategy to prevent a DoS attack can be deployed separately from the reputation system, and it can work independently without taking into account what is the underlying network.

AN APPENDIX

BIBLIOGRAPHY

[1] Mohammad Asyraff Mohamad Ariff, Suraya Mohamad, and Ahmad Roshidi Amran. "A review of recent advancement in Kademlia and Chord algorithm." In: *5th International Conference on Green Design and Manufacture (IConGDM 2019)*. Vol. 2129. American Institute of Physics Conference Series. July 2019, 020131, p. 020131. DOI: 10.1063/1.5118139.

[2] MyungJoo Ham and Gul Agha. "ARA: a robust audit to prevent free-riding in P2P networks." In: *Fifth IEEE International Conference on Peer-to-Peer Computing (P2P'05)*. 2005, pp. 125–132. DOI: 10.1109/P2P.2005.2.

[3] Lacine KABRE and Telesphore Tiendrebeogo. "Comparative Study of can, Pastry, Kademlia and Chord DHTS." In: *International Journal of Peer to Peer Networks* 12 (Aug. 2021), pp. 1–22. DOI: 10.5121/ijp2p.2021.12301.

[4] Rafiza Ruslan, Ayu Zailani, Hidayah Zukri, Nur Khairani Kamarudin, Shamsul Jamel Elias, and R.Badlishah Ahmad. "Routing performance of structured overlay in Distributed Hash Tables (DHT) for P2P." In: *Bulletin of Electrical Engineering and Informatics* 8 (Mar. 2019). DOI: 10.11591/eei.v8i2.1449.