Improving the Anonymity of Layer-Two Blockchains Adding Random Hops

Paolo Arash Kazemi Koohbanani (a.kazemikoohbanani@student.tudelft.nl)
Supervisors: Stefanie Roos and Satwik Prabhu Kumble

1. Background

- The Lightning Network is a layer-two solution on top of the Bitcoin blockchain.
- It uses source routing, the sender of the payment determines the hops a transaction will go through.
- Hash Time Locked Contracts are used to enforce payment expiration.

2. Motivation

- The Lightning Network enables users to send payments to each other by routing them through a network of nodes.
- Different lightning implementations (LND, c-lightning, Eclair) use little to no randomness when deciding the payment route.
- It is possible as an adversary hop in a transaction path to de-anonymize the sender or receiver [1].
- Onion routing style encryption is not enough to guarantee anonymity.

[1] S. P. Kumble, D. Epema, and S. Roos, "How lightning's routing diminishes its anonymity," in Proceedings of the 16th International Conference on Availability, Reliability and Security, pp. 1–10, 2021.

3. Research Question

- Can the anonymity in Lightning be improved by changing its routing protocol to add random hops?
- What is the cost of improving anonymity?

4. Method

- Simulation framework written in Python[2].
- The Lightning Network snapshot is taken from lnchannels[3].
- Anonymity and efficiency metrics are used to evaluate the modification.
- The modification takes a computed short path and randomly adds an extra hop between nodes.
- A minimum of 2 hops added on any given path, unless there is a direct channel between the sender and receiver.
- Two attack strategies analysed considering the adversary is aware of the modification.
- First strategy checks whether suboptimal paths could have been generated by the modification.
- Second strategy tries to exhaustively search for all possible sources that can match a destination.

[2] https://github.com/paolokazemi/Lightning-Network-Anonymity
[3] https://ln.fiatjaf.com/

5. Results

- The success of an attack finding the sender and receiver dropped to 53%.
- 1% of the attacks singularly de-anonymized both the source and destination.
- The average hop count increases by 2.16.
- The average fee increases 4.77 times.

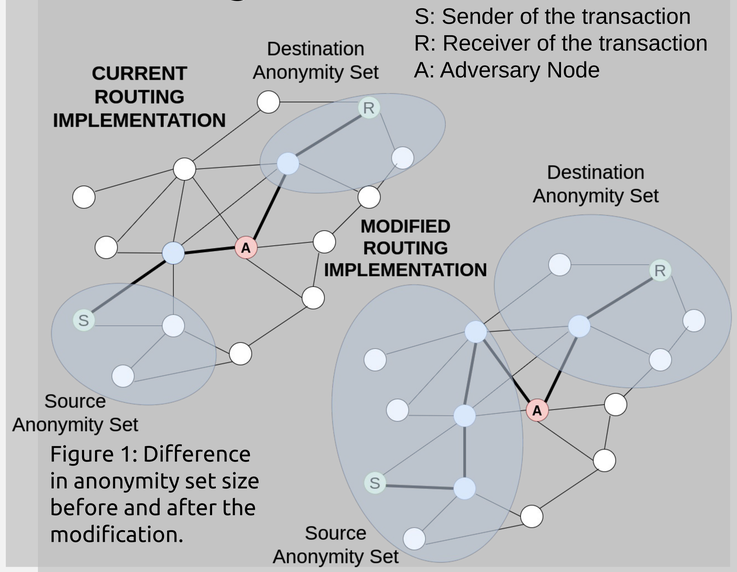

Figure 1: Difference in anonymity set size before and after the modification.

6. Conclusion and Future Work

- Introduced randomness increases anonymity.
- Simulate concurrent payments.
- Analyse increase in fee costs and ways to reduce it.