Expose for bachelor thesis

Vulnerability Assessment and Enhancement of Current Rebalancing Approaches in Lightning Network

Introduction

Cryptocurrencies make financial transactions possible without the intervention of central authorities. However, the speed of Bitcoin transactions is relatively low compared to deployed payment services such as Visa [4]. This delay occurs because of the Bitcoin network's limited ability to process large numbers of transactions in small intervals of time. One potential solution to this problem is payment channel networks (PCN) operating over blockchains. The most researched example of such networks is the Lightning Network (LN) protocol, the most famous implementations of which are Lnd[1] and C-Lightning[2].

With the recent increasing popularity of cryptocurrencies, the security of financial asset transfers of this kind is becoming increasingly important. Security analysis and possible exploits involving LNs have already been investigated in [2], [3], [8], [9]. Investigated attacks take advantage of the Lightning protocol's features, such as gossip and probing mechanism, source-based onion routing, and attracting routes technique.

Closely related to network security are the problems of imbalance, rebalancing, and route topology. Although routing has been classified as an unsophisticated challenge in the primary source about LNs [6], optimization mechanisms related to the organization of off-chain networks are being actively studied. The development community has created Rebalance plugin[3] and Lndmanage[4] among other approaches to provide an effective balancing mechanism for C-Lightning and Lnd accordingly.

[1] https://github.com/lightningnetwork/lnd
[2] https://github.com/ElementsProject/lightning
[3] https://github.com/lightningd/plugins/tree/master/rebalance
[4] https://github.com/bitromortac/lndmanage

Problem Definition

It can be seen that routing in Lightning's network can lead to security breaches and be exploited maliciously. For instance, in [2] the authors described achieving a DoS attack, which uses the routing mechanism to attract and hijack transactions using a small number of channels owned by the attacker. When performing a probing attack, the hacker has the opportunity to find out the maximum amount that can be transmitted in a given direction through the target channel and launching a timing attack provide an opportunity for an attacker to analyse the data for determining the distance to the destination [3]. Jona Haris and Aviv Zohar have also demonstrated that by inducing a large number of channel closures, an attacker can influence transaction fees and even steal some funds [8]. By reaching the maximum number of unresolved requests, the attacker can also neutralise channels for several days [9].

In my thesis, I would like to focus more on the improvement of security and effectiveness for a concept called rebalancing. This term describes the actions taken by a node to rebalance the balances of the channels between the participants and improve their liquidity. PCNs representing Layer 2 operate only by executing a funding transaction and closing transaction on the blockchain, which itself is Layer 1 [1]. The rest of the transactions are performed off-chain and without broadcasting to the blockchain. In funding, transaction participants declare the number of locked funds, which is called the balance. Due to HTLC, there are intermediary nodes in the LN through which funds can be transferred without opening a direct payment channel with each peer. The main obstacle for such nodes is that they have to fund their channels in advance. In the aftermath of continuous routing, such nodes can come to a state of imbalance.

To cope with such a scenario, there are several strategies, which are mainly implemented in a variety of plugins. The main methods of rebalancing include Loop Out, circular routes or waiting for routed payments that flow in the opposite direction [13]. In addition, this problem is also often solved by the owners of the nodes of the influence on the transaction fees. In the scientific community, I would like to distinguish two main suggested mechanisms for rebalancing: Revive [11] and Hide&Seek [12].

In my thesis, I would like to explore already existent rebalancing techniques and evaluate them via particular parameters. Using simulations, I will provide information that currently used rebalancing algorithms outperform the method described in [12]. Estimate performance of the method described in [12] against currently used rebalancing solutions.

Proposed Solution

All previously proposed protocols existing for Lightning do not show perfect performance and provide room for improvement. The authors of "HIDE & SEEK: Privacy-Preserving Rebalancing on Payment Channel Networks" have clearly demonstrated that their proposed method can be implemented both securely and globally optimal and ultimately maximises the total amount of money rebalanced [12]. I consider the evaluation of this algorithm against the other methods to be crucial and can be very beneficial for the scientific environment. With the help of certain simulations, I will demonstrate why this algorithm would be preferable to the current rebalancing mechanisms implemented today. Besides, I will investigate how this mechanism could be fully or partially implemented in C-Lightning. I will also consider the scenario if there are trampoline nodes in the network when running this algorithm.

Tools

To begin with, I plan to set up a *lightning node* (implementation of *C-Lightning and Lnd*) locally on the computer to familiarise myself with how it works and the different control options. For a bitcoin node, I will use *Bitcoin Core Daemon*. For algorithm evaluation, I will use metrics such as reachability, payment success, amount of transactions and amount of successful transactions, expected payment success ratio, maximum flow, average payment time. Based on the data obtained with these metrics, I will conclude how well this algorithm will rebalance and how good it will be in terms of privacy.

Schedule

Starting from the registration of my bachelor thesis, I plan my time as follows:

- Week 1-4 “Research phase & Comparison used in Lightning”
    - Define scopes for bachelor thesis
    - Deep dive into current rebalancing approaches
- Week 4-9 “Setup phase”
    - Simulation set up
    - Analysis development
    - Plots and stats creation
    - Setup algorithm local (or on testnet)
- Week 9-13 “Main phase”
    - Results assessment and evaluation
- Week 13-17 “Final phase”
    - Writing of the text
    - Finalization of the thesis

Sources

1. Dotan, Maya, Yvonne-Anne Pignolet, Stefan Schmid, Saar Tochner, and Aviv Zohar. "Survey on Blockchain Networking: Context, State-of-the-Art, Challenges." Proc. ACM Computing Surveys (CSUR) (2021).
2. Tochner, Saar, Aviv Zohar, and Stefan Schmid. "Route Hijacking and DoS in Off-Chain Networks." In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, pp. 228-240. 2020.
3. Nisslmueller, Utz, Klaus-Tycho Foerster, Stefan Schmid, and Christian Decker. "Toward active and passive confidentiality attacks on cryptocurrency off-chain networks." arXiv preprint arXiv:2003.00003 (2020).
4. Trillo, Manny. "Stress test prepares visanet for the most wonderful time of the year." URl: http://www. visa. com/blogarchives/us/2013/10/10/stress-testprepares-visanet-for-the-most-wonderfultime-of-the-year/index. html (2013).
5. Nakamoto, Satoshi. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019.
6. Poon, Joseph, and Thaddeus Dryja. "The bitcoin lightning network: Scalable off-chain instant payments." (2016).
7. Pickhardt, Rene, and Mariusz Nowostawski. "Imbalance measure and proactive channel rebalancing algorithm for the Lightning Network." In 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), pp. 1-5. IEEE, 2020.
8. Harris, Jona, and Aviv Zohar. "Flood & loot: a systemic attack on the lightning network." In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, pp. 202-213. 2020.
9. Mizrahi, Ayelet, and Aviv Zohar. "Congestion attacks in payment channel networks." arXiv preprint arXiv:2002.06564 (2020).
10. Sebastian Reca. Rebalancing in the lightning network: Analysis and implications. http://diyhpl.us/wiki/transcripts/scalingbitcoin/ tokyo-2018/rebalancing-lightning/. Accessed: 2021-05-21.
11. Khalil, Rami, and Arthur Gervais. "Revive: Rebalancing off-blockchain payment networks." In Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 439-453. 2017.
12. Avarikioti, Zeta, Krzysztof Pietrzak, Iosif Salem, Stefan Schmid, Samarth Tiwari, and Michelle Yeo. "HIDE & SEEK: Privacy-Preserving Rebalancing on Payment Channel Networks." arXiv preprint arXiv:2110.08848 (2021).
13. https://github.com/lnbook/lnbook/blob/ec806916edd6f4d1b2f9da2fef08684f80acb671/05_node_operations.asciidoc