Improving anonymity of the Lightning Network
using Suboptiomal Routes

Author: Mihai Plotean (m.plotean@student.tudelft.nl) Professor: S. Roos Supervisor: S. Prabhu Kumble

TUDelft

BACKGROUND

Bitcoin scalability issue:

Bitcoin	Visa
7 transactions/sec	47.000 transactions/sec

Solution: Lightning Network (LN) [1]

- A second layer on top of bitcoin
- Two users open a channel and lock an amount as collateral
- A direct channel with the receiver is not necessary - the payment can be routed via multiple intermediaries

Because of Lightning's determenistic payment routing protocol, an adversary node that acts as intermediary in a transaction can uniquely identify the sender or the receiver in 70 % of cases [2]. This puts the anonymity of users under question.

METHOD

- Study existing routing protocols in Lightning
- Choose metrics to evaluate performance and anonymity
- Design a new non-determenistic routing protocol that chooses suboptimal routes
- Simulate the routing protocol
- Create an attack on the protocol by an adversary that is aware of the protocol modification
- Evaluate perfomance and anonymity of the protocol

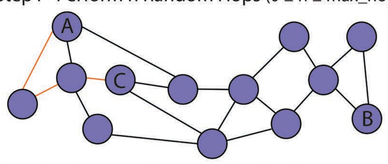
OBJECTIVES

- How can the anonymity of the Lightning Network be improved using sub-optimal routes?
- What kinds of routing protocols are used in Lightning?
- How to analyze the anonymity and performance of the created protocol?

RESULTS

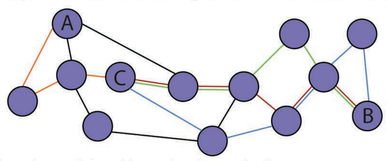
New Routing Protocol

Step I - Perform n Random Hops ($0 \leq n \leq max\_hops$)



A - sender, B - recipient, C - the node after 3 random hops

Step II - Choose randomy one of the k Best Paths



A random path from blue, red and green is chosen

- Attack executed on two graphs
- Graphs are randomly generated
- 200 nodes, 800 egdes
- 10 adversaries, 300 transactions

Metric	$max\_hops = 0$ $k = 1$	$max\_hops = 3$ $k = 5$	$max\_hops = 7$ $k = 10$
R_{att}	0.87	0.91	0.95
$Sings$	0.06	0.005	0.00
$Sing_R$	0.60	0.32	0.23
$Sing_{both}$	0.26	0.002	0.00
$Avg_{\|R\|}$	2.03	9.2	9.64
$Avg_{\|S\|}$	20.5	19.1	17.7
Avg_{hops}	3.93	5.28	6.55
Avg_{fee}	1.26	1.96	2.65

Table 1. Attack and efficiency metrics based on a random graph

Metric	$max\_hops = 0$ $k = 1$	$max\_hops = 3$ $k = 5$	$max\_hops = 7$ $k = 10$
Avg_{hops}	3.27	5.24	6.78
Avg_{fee}	1.41	2.18	3.26

Table 2. Efficiency metrics based on a snapshot of Lightning

Impact of the parameter from each step

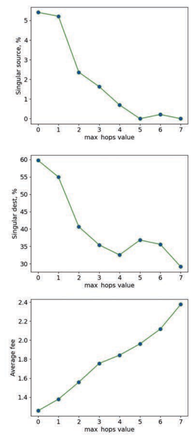


Figure 1. Metrics as a function of max_hops. We keep k = 1 fixed.

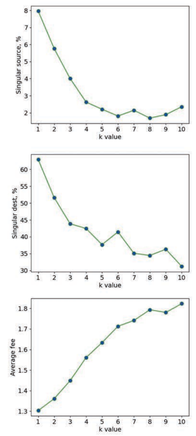


Figure 2. Metrics as a function of k. We keep max_hops = 0 fixed.

CONCLUSION

- Number of anononymity sets with a singular destination descreased by a factor of 2-3.
- Number of anononymity sets with a singular destination descreased by a factor of 2 to 12, depending on the graph.
- Number of anononymity sets with both a singular souce and destination is close to zero.
- Fees increased by 107%-110% for third parameter pair.

- The results should be valided on the Lightning Network.
- Other types of graphs could be considered.
- Optimal parameters for max_hops and k need to be found.

[1] J. Poon and T. Dryja. The Bitcoin Lightning Network: Scalable off-chain instant payments. 2016. Available at: https://lightning.network/lightning-network-paper.pdf
[2] 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'. 2021.