IMPROVING ANONYMITY ON THE LIGHTNING NETWORK

Simulating Multiple Path Segment Routing

TU Delft

1 Background

- Lightning Network (LN) is a second-layer solution for Bitcoin
- Promises increased scalability and improved privacy
- However, a recent study showed LN routing is weak to anonymity-compromising attacks [1]
- The current routing protocol is partially deterministic, allowing attackers to determine the sender and the recipient of a transaction

LN needs a more sophisticated routing protocol!

2 Research question

How can we simulate the usage of a new Lightning routing protocol using multiple path segments, and what are the anonymity benefits and efficiency costs?

Contact info:
Joran Heemskerk (j.s.heemskerk@student.tudelft.nl)
Supervisors:
Stephanie Roos (s.roos@tudelft.nl)
Satwik Prabhu Kumble (s.prabhu@tudelft.nl)

3 Method

- Construct metrics to evaluate the performance of routing protocols
- Design modified LN protocol using path segment routing
- Design counterattack for modified routing protocol
- Simulate LN using simulation framework [2] and estimate performance of the proposed protocol

4 Design

- Novel routing protocol, inspired by the Next-Generation Internet's 'Dovetail Protocol'[3]
- Split path generation in halves that connect on a 'dovetail' node
- Generate full path by appending the two separate paths

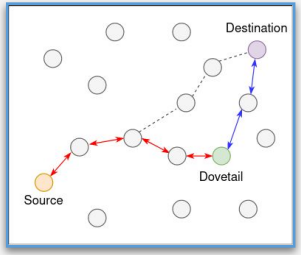

Figure 1: Visualising multiple path segment routing

- Counterattack by splitting attack into 3 types:
- Path 1 attack: find sender and dovetail
- Path 2 attack: find dovetail and recipient
- Center attack: find sender and recipient

[1] S. P., Kumble, D. Epema and S. Roos. How lightning's routing diminishes its anonymity. 2021
[2] https://github.com/jsheemskerk/Attacking-Lightning-s-anonymity
[3] Jody Sankey and Matthew Wright. Dovetail: Stronger anonymity in next-generation internet routing. 2014

5 Results

	Barabasi-Albert		Erdos-Renyi	
	Old	New	Old	New
$Success$	92.51%	83.12%	82.43%	70.14%
AVG_{fee}	1.08	2.33	2.62	4.63
AVG_{hops}	3.40	5.74	5.62	9.01

Table 1: Anonymity metrics for Barabasi-Albert and Erdos-Renyi graphs

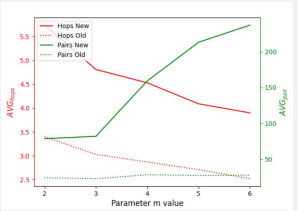

Figure 2: Effect of varying graph density

Barabasi-Albert	Old	Path 1	Center	Path 2	New
Transactions attacked	85.01%	-	-	-	92.0%
Number of attacks	1313	1000	177	851	2028
Correct pair present	98.02%	99.2%	95.48%	99.18%	98.87%
Avg number of pairs	24.04	73.25	368.32	24.59	78.58
Avg number of senders	20.63	17.84	44.01	21.51	21.66
Avg number of recipients	1.81	17.94	8.19	1.63	10.24
Singular sender	13.02%	10.8%	0.0%	0.0%	5.32%
Singular recipient	63.21%	4.3%	15.25%	67.92%	31.95%

Table 2: Cost efficiency metrics for Barabasi-Albert graph

Erdos-Renyi	Old	Path 1	Center	Path 2	New
Transactions attacked	77.03%	-	-	-	82.98%
Number of attacks	1967	1263	200	1159	2622
Correct pair present	73.51%	82.66%	64.5%	81.88%	80.93%
Avg number of pairs	23.23	135.05	46.67	25.74	79.99
Avg number of senders	18.63	14.83	21.95	21.23	18.20
Avg number of recipients	1.18	15.03	1.725	1.24	7.92
Singular sender	1.98%	3.17%	0.0%	0.17%	1.60%
Singular recipient	49.26%	0.95%	21.0%	57.03%	27.26%

Table 3: Cost efficiency metrics for Erdos-Renyi graph

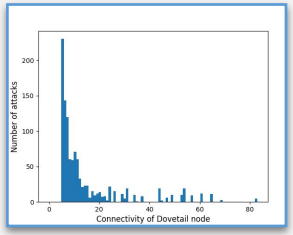

Figure 3: Effect of Dovetail node connectivity

6 Conclusions & Further research

- Anonymity improvement: source/destination pairs amount tripled
- Efficiency cost: doubling of average fee + 60% increase in hop count
- Further research: investigate semi-source routing & dovetail node choice heuristic