Improving the Anonymity of the Lightning Network Using Random Hops with Partial Route Computation

Rick de Boer (r.e.j.deboer@student.tudelft.nl)
Supervised by Satwik Prabhu Kumble and Stefanie Roos

Background

- The Lightning Network (LN) is Bitcoin's second-layer solution
- LN promises better scalability, instant payments and low transaction costs
- However, it's vulnerable to deanonymization attacks [1]
- This can be resolved by adding randomness to payment routing

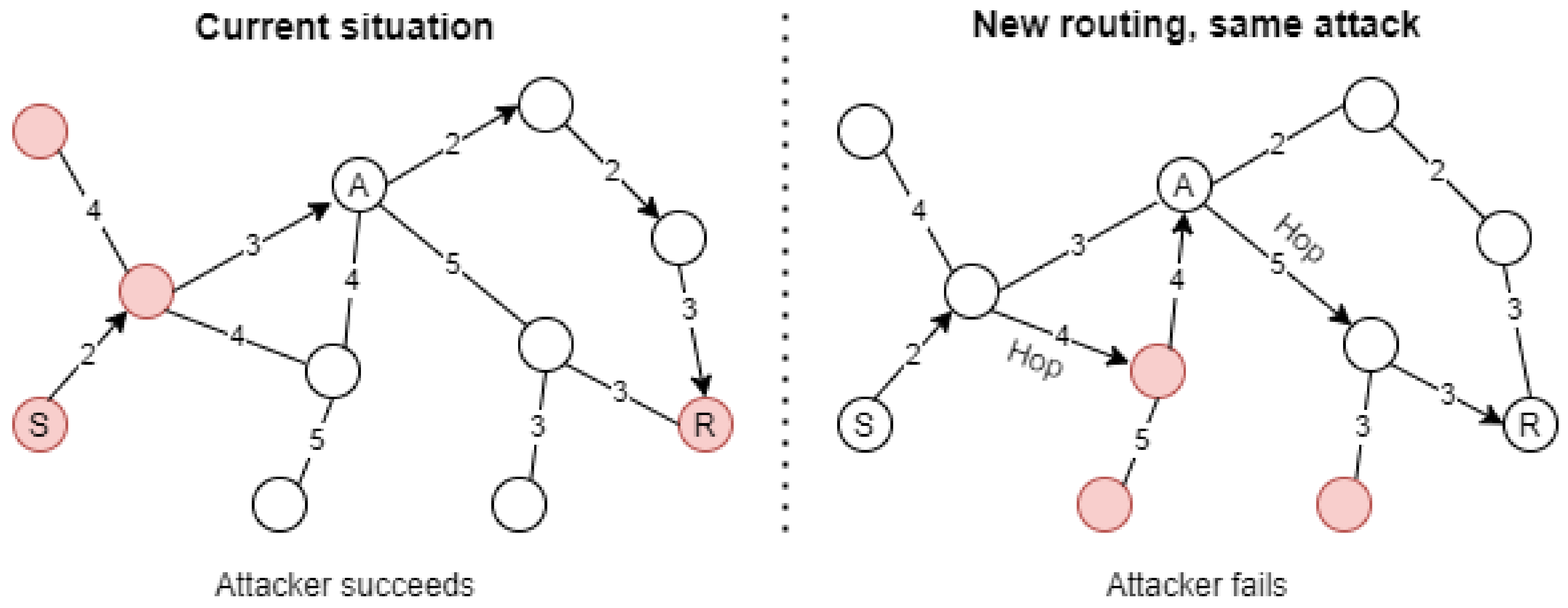
Questions

- Will we still have LN's high performance after adding random hops?
- Is the new protocol sufficiently resillient to deanonymization attacks?

Methodology

- Define metrics which are able to measure anonymity and performance
- Design a new routing protocol with increased anonymity
- Simulate both protocols by extending the provided framework [2]
- Compare and evaluate the results

Design



● Anonymity set

Edge weights represent cost function results
S = sender, R = receiver, A = adversary

- Paths are computed starting from the receiver
- During path computation, suboptimal nodes are randomly picked
- We resume path computation from the suboptimal node
- The chance of hopping depends on the degree of the current node, adding additional randomness

[1]: S. P. Kumble, D. Epema, and S. Roos, "How Lightning's Routing Diminishes its Anonymity." private communication, 2021
[2]: https://github.com/SatwikPrabhu/Attacking-Lightning-s-anonymity

Results

Anonymity results			
Metric	Old routing	New routing	New attack
Transactions attacked	38.35%	66.94%	66.94%
Pairs found	99.0%	8.38%	54.64%
Average source anonymity set size	298.36	8.12	1135.30
Average destination anonymity set size	51.90	55.41	131.63
Singular source	42.46%	3.51%	0.0%
Singular destination	57.82%	22.97%	22.84%
Source false positives	0.0%	83.19%	24.48%
Destination false positives	1.40%	68.65%	61.35%

Table 1: Anonymity results, gained by simulating 1000 transactions on the LN snapshot

Performance results		
Metric	Old routing	New routing
Average hopcount	2.43	11.95
Average fee (fee / amount)	5.38%	6.52%
Average delay	95.27	106.12
Transaction failures	8.73%	11.45%

Table 2: Performance results, gained by simulating 5000 transactions on the LN snapshot

Evaluation

- The randomness forces attackers to be more inclusive, increasing the size of anonymity sets
- This increased anonymity causes a slight hit in performance
- Recipients are still uniquely identified in some cases