chaincode

Hackathon Project: PathMaker

Repository: New Project
Groups: Multiple
Topics: Lightning, Privacy, Graph Theory

Overview

The lightning specification has recently merged the blinded paths proposal, which improves receiver privacy by replacing the recipient's public key in invoices with a "blinded path" that obscures the receiver's identity. Receiving nodes need to carefully select their blinded path to manage the tradeoff between privacy and reliability: providing more diverse blinded paths makes it easier to successfully make a payment, but it also reveals more information to a deanonymizing adversary. There are a number decisions a recipient can make in blinded path selection:

- Number of paths: how many blinded paths to the destination to provide.
- Path length: the number of hops (and fake "dummy" hops) in each blinded path.
- Introduction node(s): the cleartext node included in the blinded path, and whether to select multiple distinct nodes.
- Fee/cltv aggregation: how much to aggregate (/round up) fees in the blinded path to hide the actual channel policies from an adversary.
- Channel liquidity: size of the channels selected compared to the payment size (greater ratio, greater reliability).

Project

Write a "pathmaker" project that accepts a recipient public key and lightning graph and creates a blinded path(s) for the recipient to receive a specified payment amount. As part of this task, you must design a user-friendly metric that captures the tradeoff between privacy and reliability, and use it to determine how to select paths.

Input format:

- Graph (json): a json description of the public graph.
- Amount (uint64): payment amount expressed in millisatoshis.
- Recipient (string): hex encoded public key of the receiving node.

Output a key/value list of possible recipients:

- A json representation of the blinded path(s) to use for the recipient

```
{
  "introduction_node": "pubkey",
  "blinded_nodes": [“pubkey1”, “pubkey2”],
  "fee_base_msat": uint64,
```

```
  "fee_proportional_millionths": uint64,
  "htlc_minimum_msat": uint64,
  "cltv_expiry_delta": uint32,
  "max_cltv_expiry": uint32,
}
```

Example

An example of an expensive privacy/reliability metric that you could use for this project is the anonymity set of the blinded path. This value represents the number of nodes that could feasibly be recipients for the blinded payment:

- They are within len(blinded hops) of the introduction node.
- The fee/cltv policy to reach is node is < aggregate reported by the blinded path

A trivial example of this metric is that a value of 1 would mean that the blinded path simply selects the recipient as the introduction node and has no dummy hops - it is the only node that could possibly be receiving this payment.

Feel free to use this metric, or produce one of your own!