Universiti Kebangsaan Malaysia
National University of Malaysia

Improvements of the Balance Discovery Attack on Lightning Network Payment Channels

VISUAL INFORMATICS

What is Lightning?

Bitcoin is designed to only handle 3 to 7 transactions per second, worldwide. This is way too few to make Bitcoin a viable alternative for a centralized global payment network. Payment Channel Networks are a technique on top of Bitcoin to make it more scalable. Lightning Network [3] is the first of such networks that has been put into practice. Lightning Network has the potential to handle enough transaction to rival payment networks like VISA.

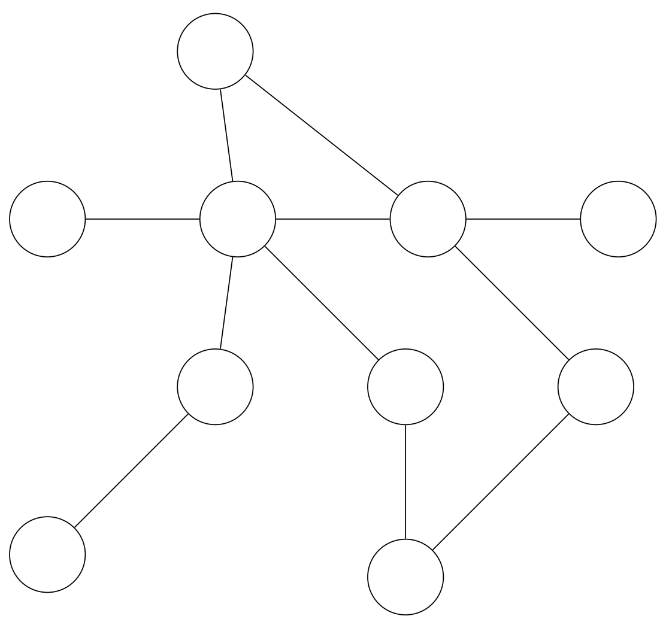


Figure 1: Lightning Network as a Graph with edges being channels and vertices being Lightning Nodes

Lightning and Privacy

For our analysis of Privacy in the context of Lighting we used the following threat model [2]

- Balance security: Users don't run the risk of losing coins.
- Serializability: Executions of a PCN are serializable as understood in concurrency control of transaction processing.
- (Off-path) Value Privacy: Malicious participants in the network cannot learn information about payments they aren't part of.
- (On-path) Relationship Anonymity: Intermediaries cannot determine the sender and the receiver of a transaction better than just by guessing.

Our research focusses on Value Privacy.

Balance Discovery Attack

In the basic Balance Discovery Attack[1], M opens up a channel with A, and tries to route fake/unknown payments to B. If the balance between A and B allows for the payment, B returns an error stating the payment is unknown. If the balance doesn't allow for the payment, A returns an error stating insufficient balance. Using a simple binary search algorithm, the exact balance is disclosed.

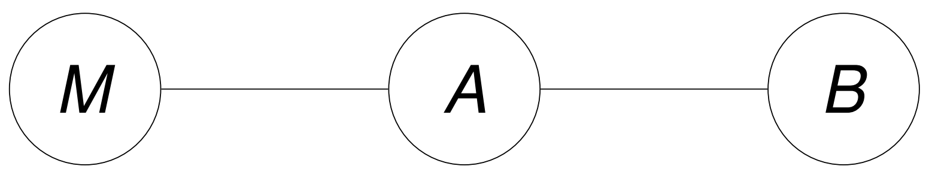


Figure 2: Basic Balance Discovery Attack with M probing the balance between A and B

This attack makes it possible to trace payments by monitoring balances over time. Value Privacy is threatened because of this.

Two-way probing

The basic attack has an upper bound of *BTC* 0.0429. Our improved attack (See fig. 3) raises that upper bound to *BTC* 0.0859

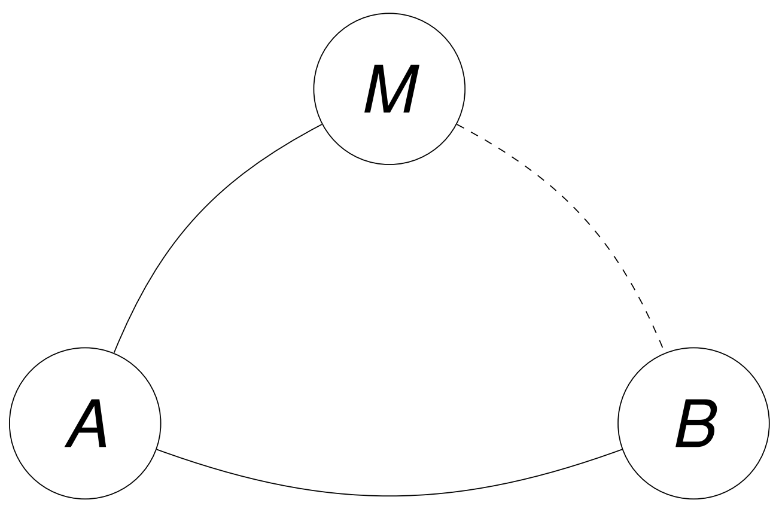


Figure 3: Basic scenario with an optional second channel for two-way probing

Results: Improved algorithm

The Two-way Probing raises the percentage of channels that can have their balances disclosed from 89.1% to 94.3%

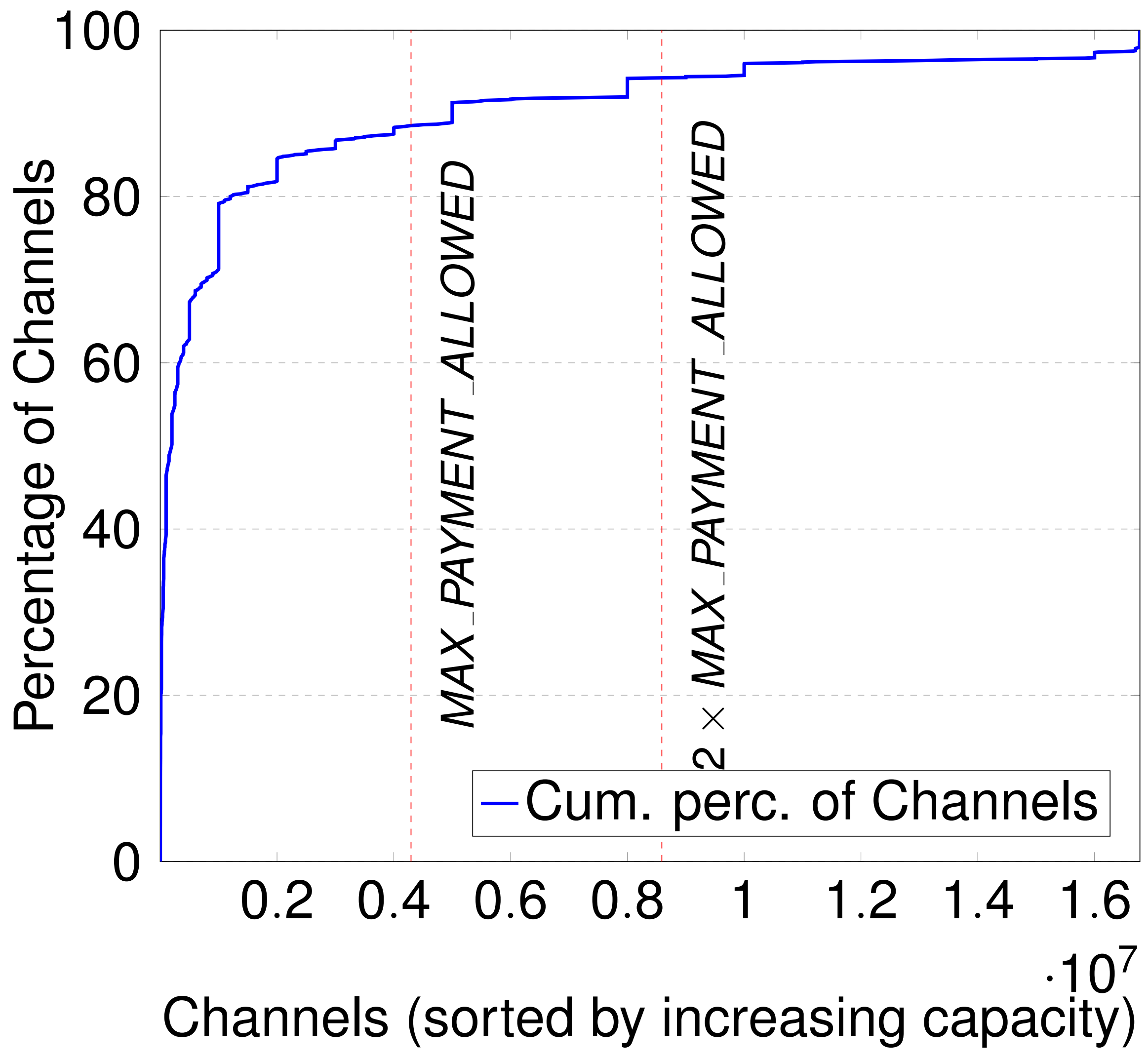


Figure 4: Basic attack compared to two-way probing

Results: Software differences

There are three main software implementations of the Lightning specifications that together have a share of over 99% of the network. (See fig. 5)

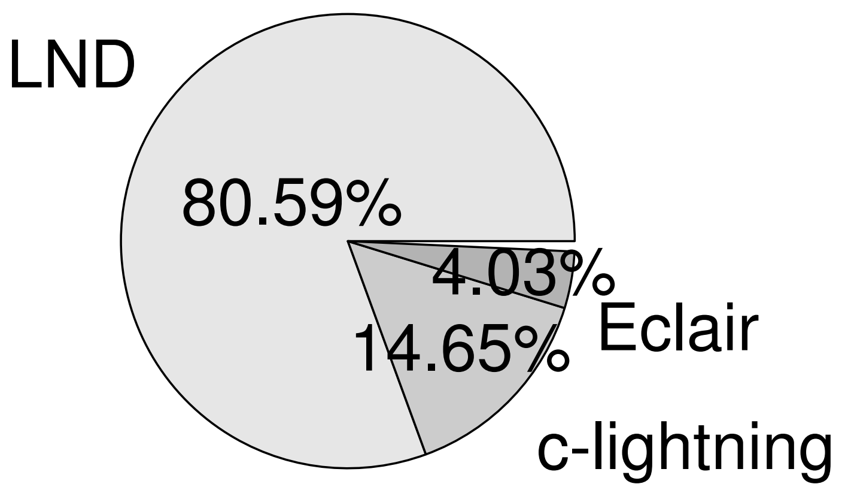


Figure 5: Network share of three main clients

This research also found differences between the three main clients that can be exploited in two ways.

- Uncover channel balances with no upper bound in channels with LND software on both nodes.
- Shutdown channels with LND software on one node and c-lightning software on the other.

The former increases the percentage of channels that can have their balances disclosed to 98.4%. The latter affects 2.7% of all channels.

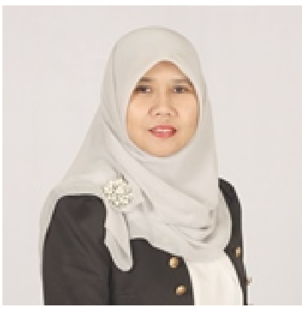
References

[1] J. Herrera-Joancomartí, G. Navarro-Arribas, A. Ranchal-Pedrosa, C. Pérez-Solà, and J. Garcia-Alfaro.
On the Difficulty of Hiding the Balance of Lightning Network Channels.
pages 602–612, 2019.

[2] G. Malavolta, P. Moreno-Sanchez, A. Kate, M. Maffei, and S. Ravi.
Concurrency and Privacy with Payment-Channel Networks.
In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security - CCS '17*, pages 455–471, New York, New York, USA, 2017. ACM Press.

[3] J. Poon and T. Dryja.
The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.
jan 2016.

Drs. Gijs van Dam
Institute of Visual Informatics
p95677@siswa.ukm.edu.my
+601-7283 4642



Dr. Rabiah Abdul Kadir
Institute of Visual Informatics
rabiahivi@ukm.edu.my
+603-8921 7167

Dr. Puteri Nor Ellyza Nohuddin
Institute of Visual Informatics
puteri.ivi@ukm.edu.my
+603-8921 7168

Prof. Dato' Dr. Halimah Badioze Zaman
Institute of Visual Informatics
halimahivi@ukm.edu.my
+603-8921 6079