Congestion Attacks in Payment Channel Networks

Ayelet Mizrahi

Payment channel networks are a second layer off-chain solution to the scalability problems of blockchains. Such payment channel networks allow both a higher number of transactions and faster transaction resolution. These properties, that are in stark contrast to the blockchain's slow transaction throughput and slow confirmation times make payment channel networks one of the leading approaches to increase the adoption of cryptocurrencies and may even allow low-fee micropayments in these systems.

The Lightning Network that runs on top of Bitcoin is the most widely used payment channel network, having more than 10k nodes and 35k channels and holds a total capacity of around 860 BTC (~8,500,000 USD).

We will present an accessible, low-cost attack on the Lightning Network, in which the attacker paralyzes multiple payment channels for several days. The attack is based on overloading channels with requests that are kept unresolved until their expiration time. Reaching the maximum allowed unresolved requests (HTLCs) locks the channel for new payments. The attack is in fact inherent to the way off-chain networks are constructed, since limits on the number of unresolved payments are derived from limits on the blockchain. We will consider two main versions of the attack: one in which the attacker attempts to block as many high liquidity channels as possible, and one in which it tries to isolate individual nodes from the network. We will present the evaluation of the costs of both attacks and will compare how changes in the Lightning Network have affected the cost of attack. Specifically, we will consider how recent changes to default parameters in each of the main Lightning implementations contribute to the attack. As we evaluate the attacks, we will also look at statistics on parameters in the Lightning Network which are of independent interest and compare the various implementations of Lightning nodes. Finally, we will suggest mitigation techniques that make the attack much harder to carry out.