Quantitative Analysis of Lightning Network Privacy

Sergei Tikhomirov (University of Luxembourg),
Pedro Moreno-Sanchez (TU Wien), Matteo Maffei (TU Wien)

Full paper: https://eprint.iacr.org/2020/303

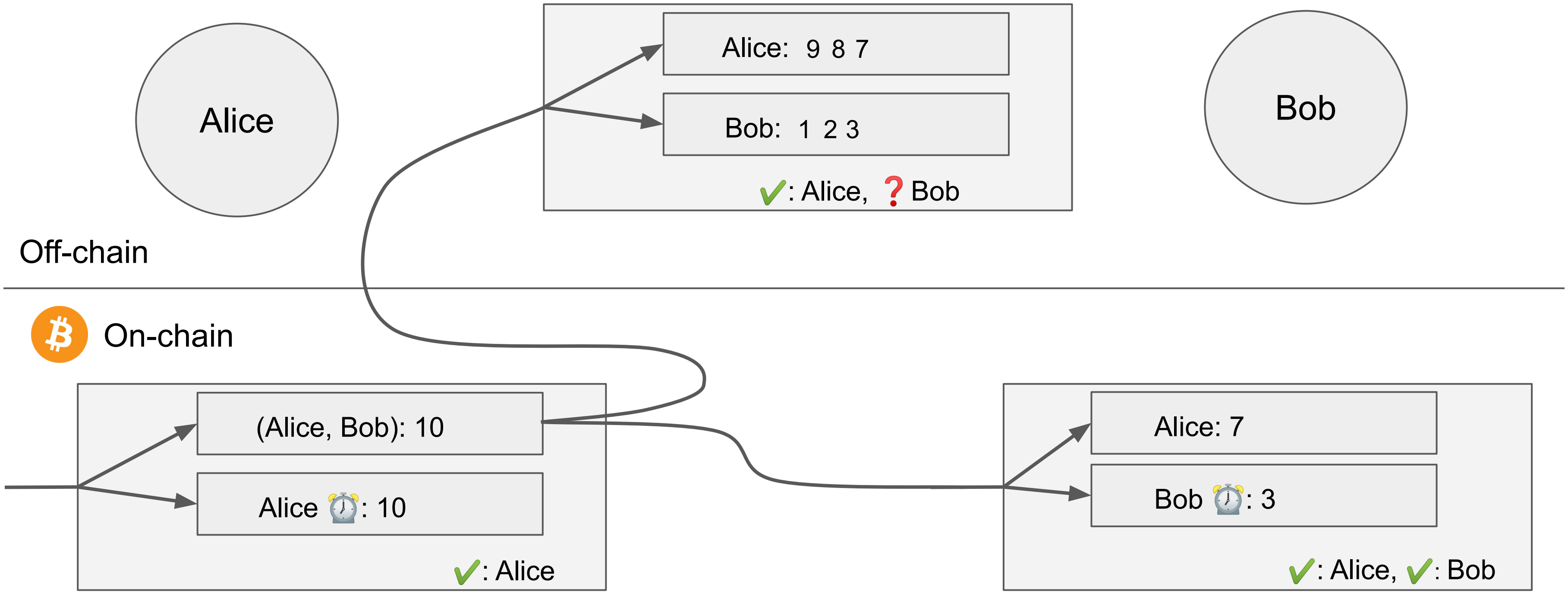
Why Lightning?

- Bitcoin scales poorly (~3 tx / sec): all nodes validate all transactions
- Two approaches: on-chain (sharding) and off-chain (Lightning)

We focus on the Lightning Network – a payment channel network for Bitcoin:

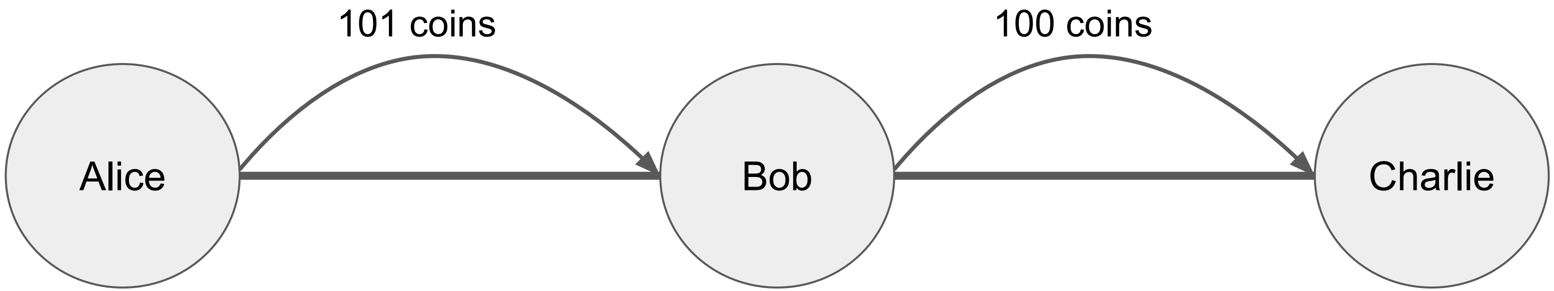
- Backwards compatible
- Deployed and used in practice (1000 BTC in 30k+ channels)
- New security and privacy challenges

Payment channel example



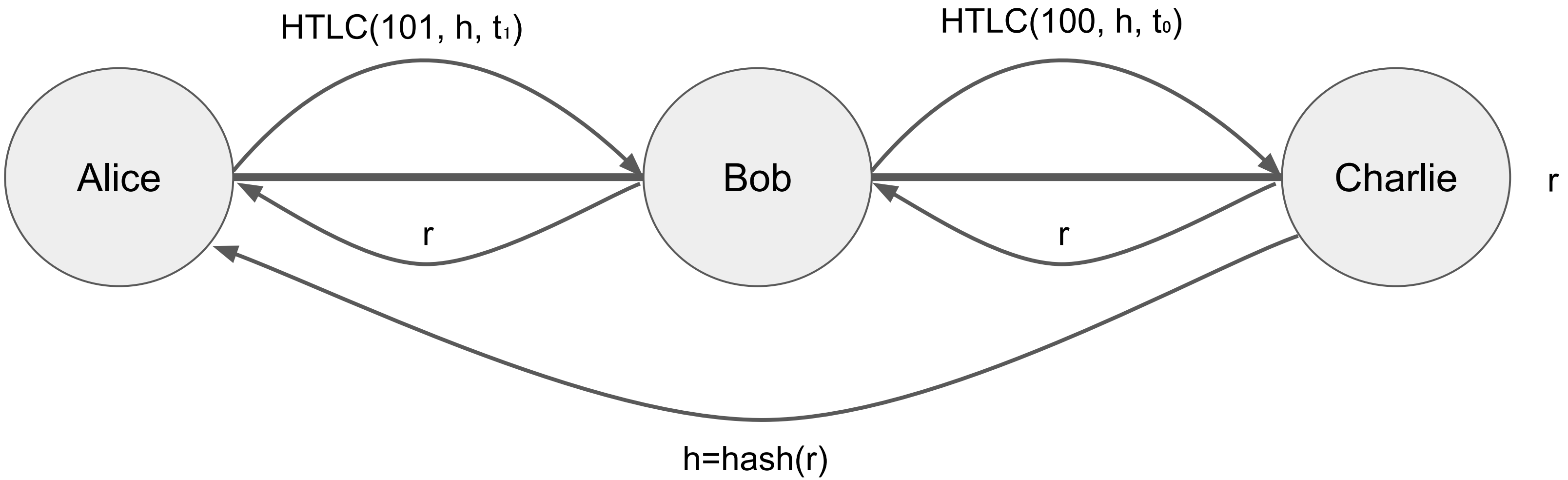
Payment channel network

- Expensive to open channels between every two users (fees, confirmations)
- Solution: a network of payment channels
- Must ensure atomicity in multi-hop payments



Lightning Network architecture

- LN ensures atomicity with hash time-locked contracts (HTLCs)
- Coins go to Bob if he shows a hash preimage before time t, otherwise to Alice



Our contributions

LN offers security (HTLC) and privacy (off-chain), but attacks have been reported.

We all want LN to be secure and private, but what exactly does that mean?

In this work, we:

- quantify the effect of three previously described attacks*
- analyze a limitation on payment concurrency
- describe a new DoS attack vector

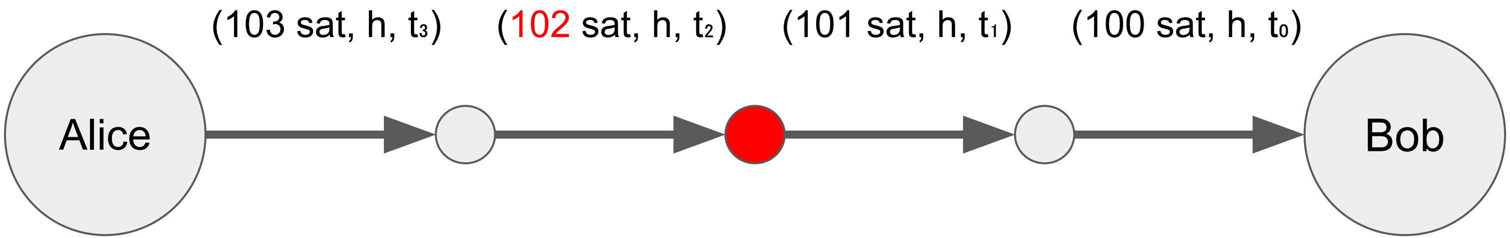
* Malavolta et al. Concurrency and privacy with payment-channel networks. CCS, 2017.
Malavolta et al. Anonymous multi-hop locks for blockchain scalability and interoperability. NDSS, 2019.

Value privacy

Attacker learns how much is being transacted.

Trivial for on-path adversaries: amounts are in plaintext.

Sufficient condition: 1 attacker's node on the path.

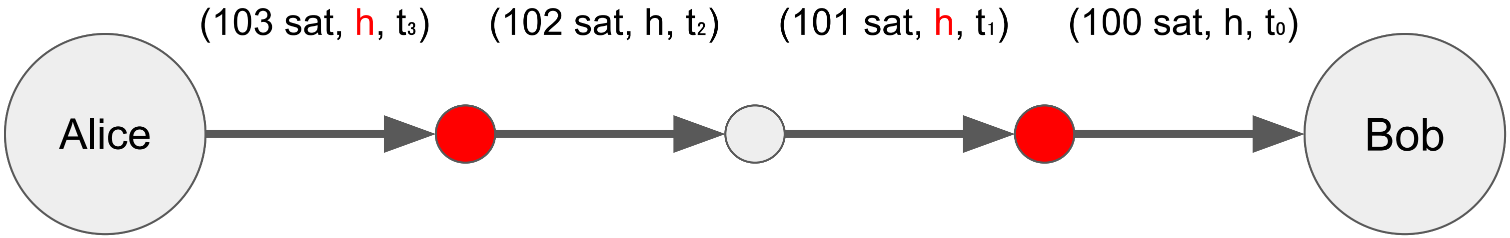


Relationship anonymity

Attacker learns who pays whom (with probability much better than random guess)

Payments are linked by the same hash value.

Sufficient condition: 2 attacker's nodes on the path.

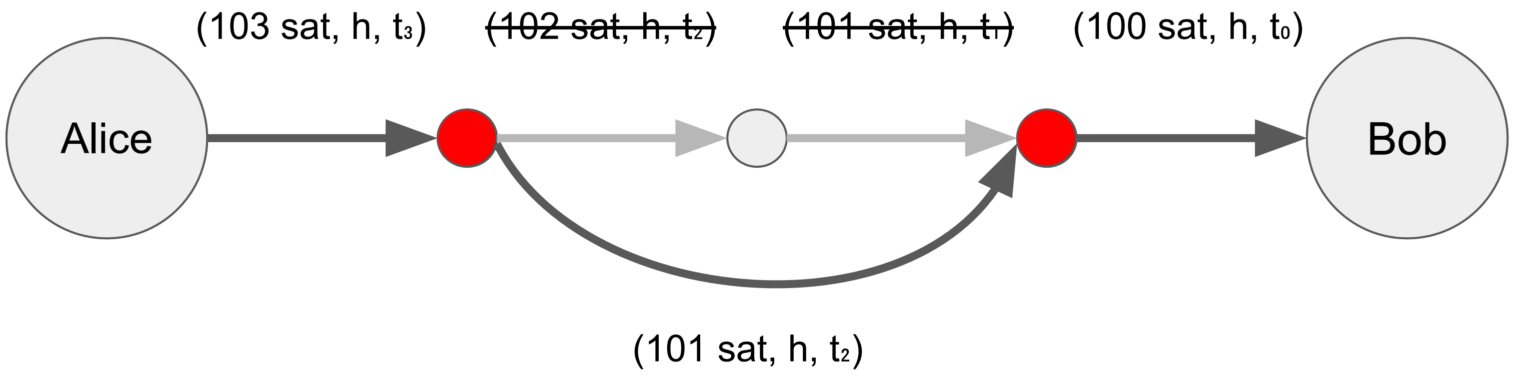


Wormhole attack

Attacker "shortcuts" a payment, taking fee from the honest node.

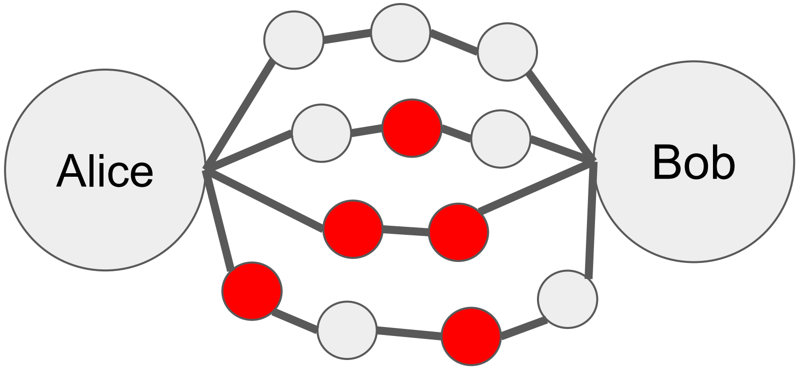
Damage for the honest node: a) no fees, b) capital locked until timeout expires.

Sufficient condition: 2 attacker's nodes on the path with honest nodes in between.



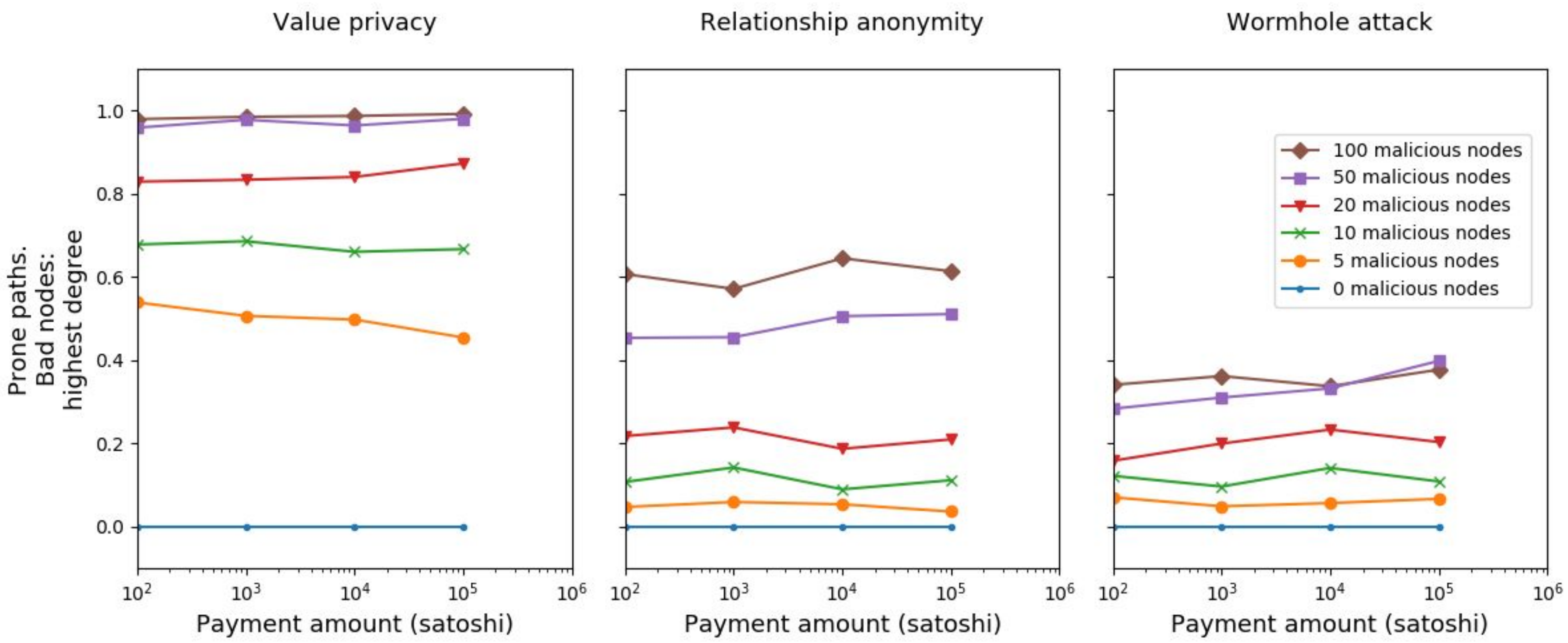
Experiment outline

- Assume that a certain subset of nodes is compromised
- Find all suitable paths between random sender and receiver
- Calculate the share of paths vulnerable to a given attack
- Average the result across many random runs



	VP	RA	WA
Path 1	Safe	Safe	Safe
Path 2	Prone	Safe	Safe
Path 3	Prone	Prone	Safe
Path 4	Prone	Prone	Prone
Prone	75%	50%	25%

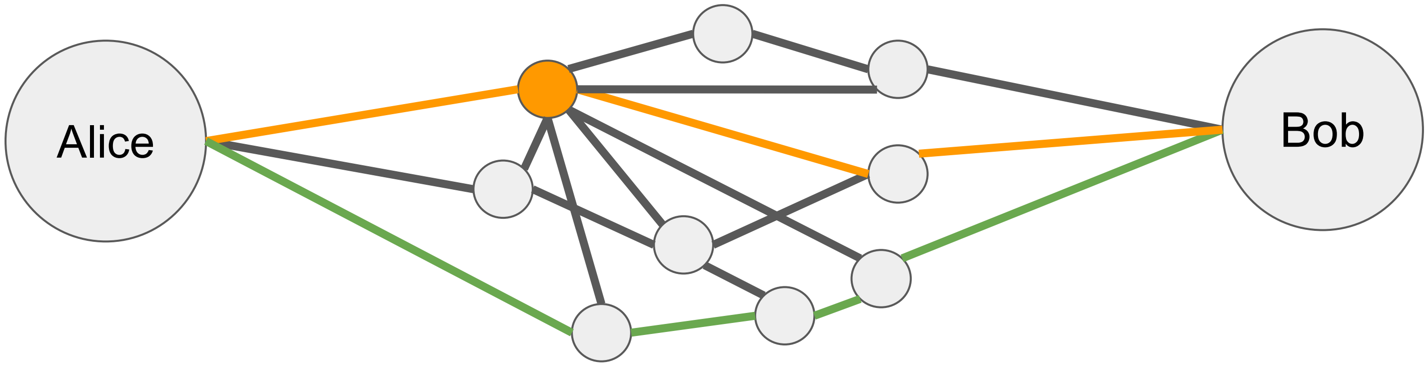
Results: highest degree nodes compromised



Countermeasures

A trade-off between connectivity and privacy:

- Routing via large nodes: dangerous if they are compromised
- Routing via small nodes: less liquidity and uptime



HTLC limit

How many concurrent payments can LN handle?

- One channel may hold multiple concurrent HTLCs
- Channel parties must be able to dispute malicious closures on-chain
- Dispute transactions include all in-flight (unresolved) HTLCs
- Bitcoin transactions must be < 100 KB
- Consequently, a channel supports at most 966 HTLCs (*HTLC limit*)

Example of HTLC depletion

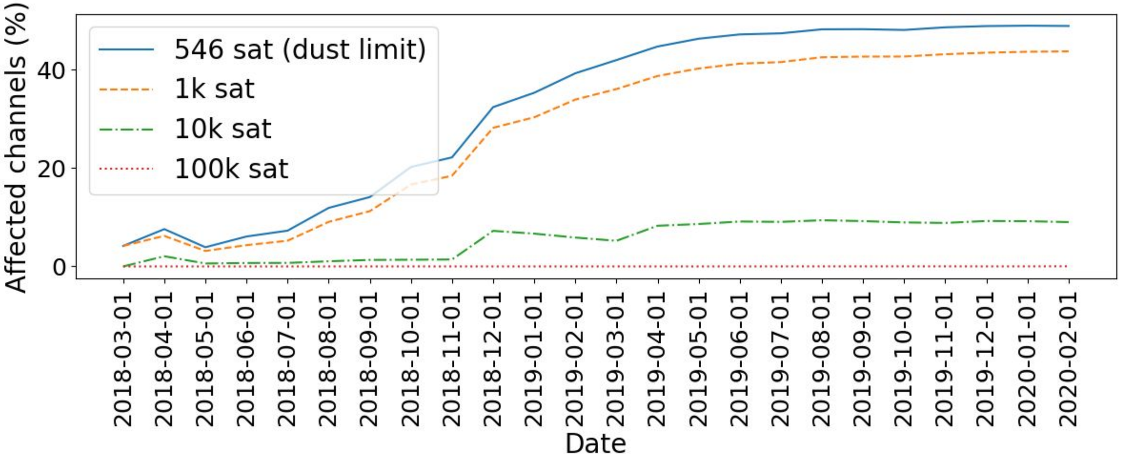
Consider a channel with capacity of 1M sat. No HTLCs can be added, though capacity is not depleted.

	Unresolved HTLCs
1	HTLC (to Alice, 1000 sat, 0xdf86...)
2	HTLC (to Bob, 1000 sat, 0x0a1f...)
…	…
966	HTLC (to Alice, 1000 sat, 0x6f26...)
Total value of HTLCs (sat)	966k < 1M
Number of HTLCs	966

Up to 50% of channels affected

Two limiting factors: capacity and HTLC limit. Depends on the amount:

- 0 – 546 sat (dust limit): no HTLC created
- 546 – **2700 sat** (0.3 USD): HTLC limit is more important
- >2700 sat: capacity is more important



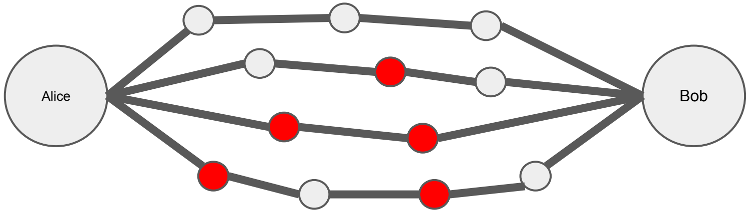
DoS by exceeding the HTLC limit

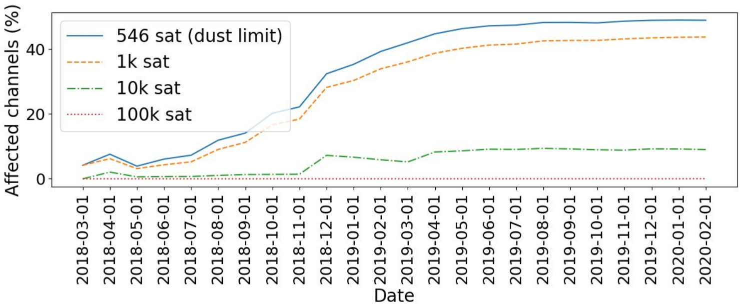
- An attacker blocks a channel by sending 966 near-dust payments
- Does not require as many coins as in the victim channel
- Can block a channel with 966*546 = 527k sat (~60 USD)

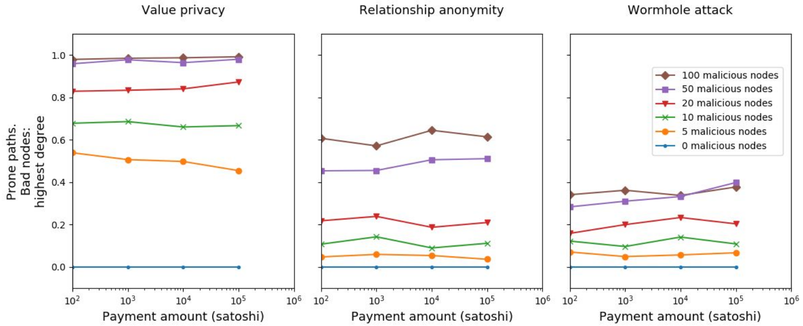
Channel capacity (sat)	Attacker’s capital for DoS	
	Capacity-based	HTLC-based
100k	100k	527k
1M	1M	527k
10M	10M	527k

Conclusion

- Privacy attacks are possible with only a few “important” nodes compromised
- Limited throughput for micropayments
- A new DoS vector







Full paper: https://eprint.iacr.org/2020/303