Mitigating Sybil Attacks on the I2P Network Using Blockchain

RP #97, Kotaiba Alachkar & Dirk Gaastra

Supervisor: Vincent Van Mieghem, Deloitte

3 July, 2018

MSc Security and Network Engineering
University of Amsterdam

Introduction

I2P - Invisible Internet Project

Anonymous Communication Network (ACN), similar to TOR, but with a few differences.

- Fully peer-to-peer
- No exit nodes
  - Internal communication only
- Designed for slightly different purposes (e.g. filesharing)
- Garlic routing
- Unidirectional tunnels

Network Topology

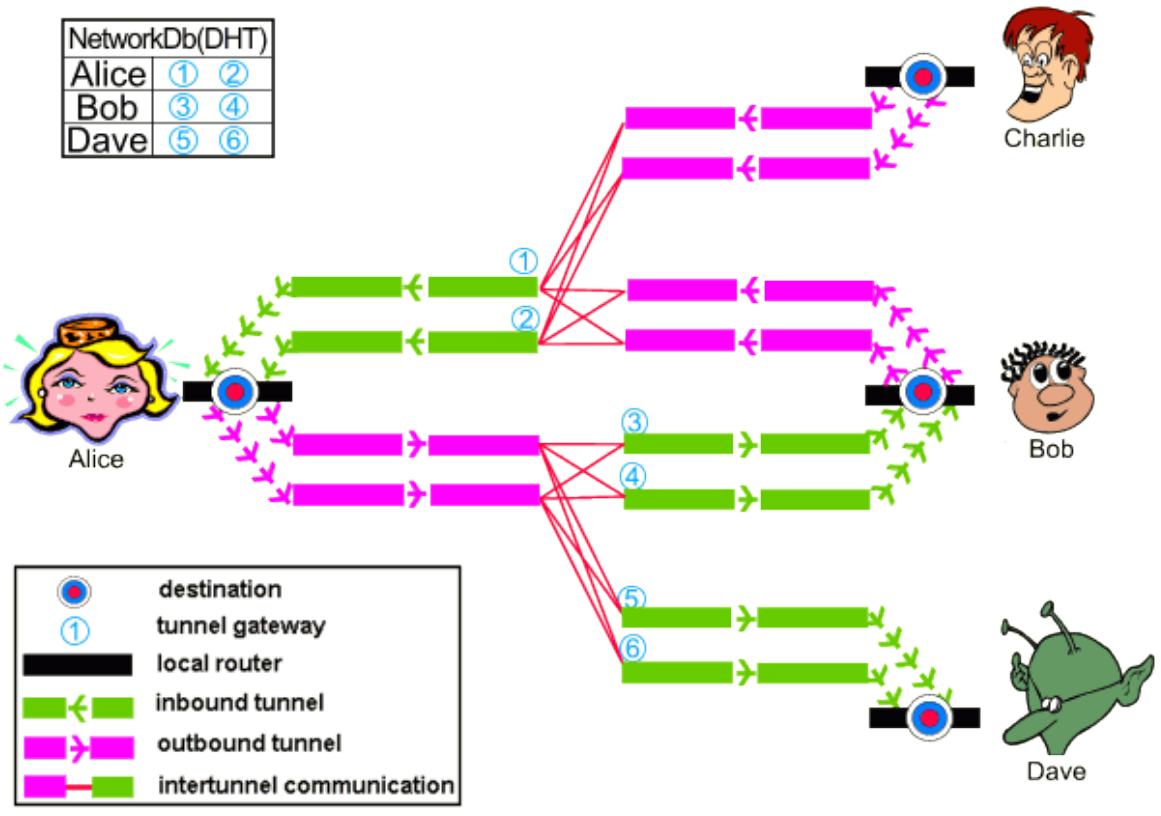

Figure 1: I2P network topology example [1]

[1] https://geti2p.net/_static/images/net.png

netDb - Network DataBase

- Used for looking up resources: **RouterInfos** and **LeaseSets**
- Distributed across so-called *FloodFill routers*
  - Automatically selected based on performance (e.g. bandwidth)
  - Or manually enabled
- Each FF router is responsible for a part of the network
  - Based on Kademlia-style metric to determine closeness
  - Hash of **RouterIdentity** + current date
  - Changes every day at midnight (UTC)
  - aka "keyspace rotation"

I2P - User-base

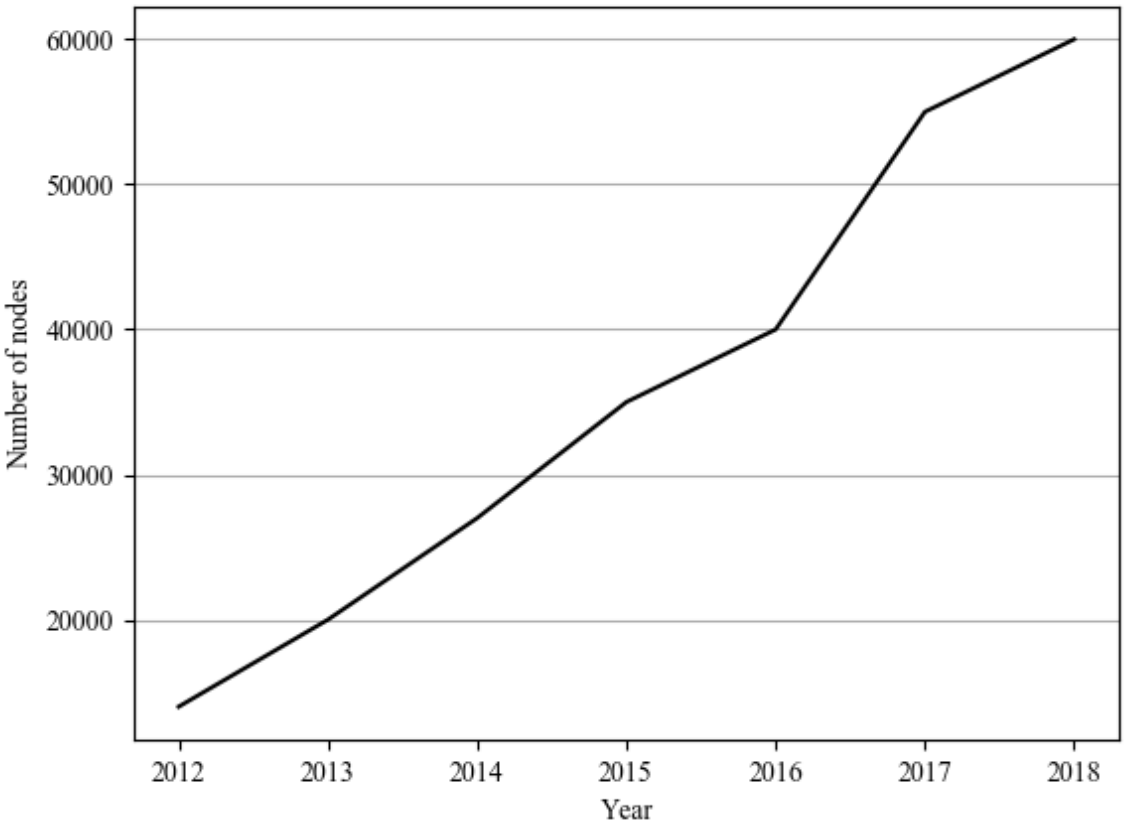

Figure 2: Rough estimation of the average number of I2P nodes

Sybil Attack

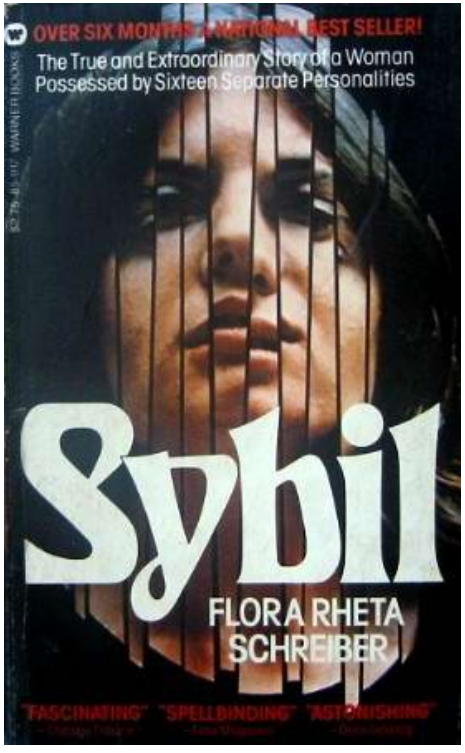

Figure 3: Sybil by F. R. Schreiber [2]

"A case study of a woman diagnosed with dissociative identity disorder [3]"

[2] http://whenfallsthecoliseum.com/wp-content/uploads/sybil.jpg
[3] https://en.wikipedia.org/wiki/Sybil_(Schreiber_book)

Sybil Attacks

Create a large number of pseudonymous identities in order to cripple the peer-to-peer system

Its impact depends on:

- how cheaply identities can be generated
- accept inputs from untrusted entities
- whether all entities treated identically

Sybil Attack on I2P

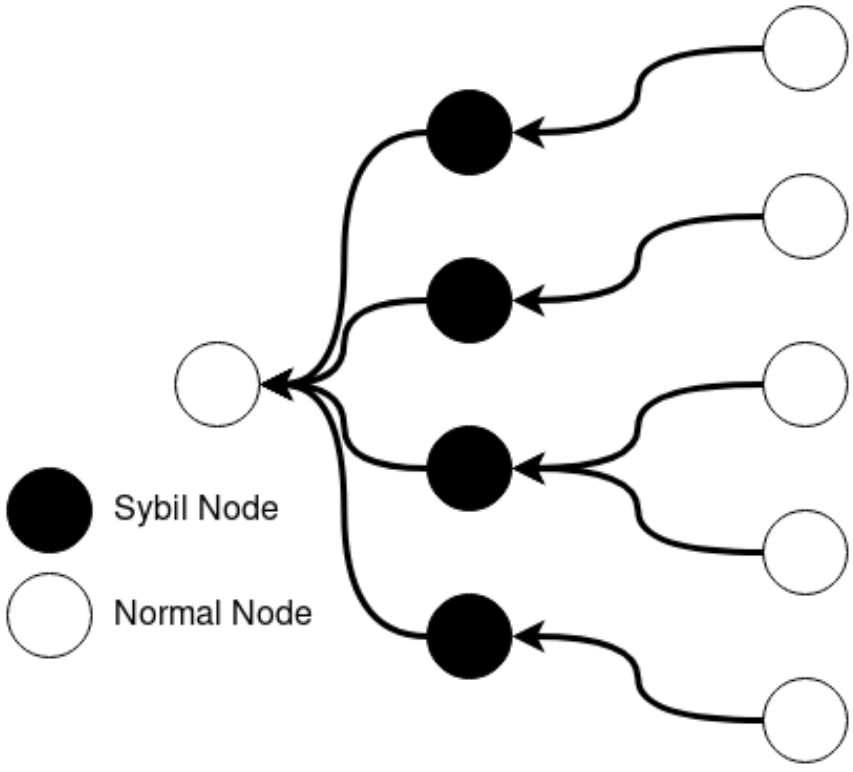

Figure 4: Partial keyspace Sybil attack example

Attack is very feasible, even with limited resources [1]

Research Question

How can a Sybil attack on the I2P network be made infeasible?

Methodology

Methodology

- Evaluate existing mitigation state on the network
- Examine proposed solutions from previous research
- Construct our own solution

Evaluation

Current State

- Router election
  - Enough resources required to be considered
  - Currently, becoming FF router is not hard
- Keyspace rotation
  - Router ID hashed with date to determine closeness
  - Possible to precompute identities
- Blacklist
  - Block known bad IPs
  - Centralized (blogs, forums, etc.)
  - `Quis custodiet ipsos custodes?`

Previous Research

Previous Research: PoW

Proof-of-Work (PoW) suggested by I2P contributors [2]

- Using HashCash [4]
- Finish PoW before creating router
- However,
  - Difficulty of PoW hard to determine
  - Trivial for a reasonably powerful attacker

[4] http://www.hashcash.org/

Previous Research: Reputation

Age-based reputation suggested by Egger et al. [1]

- The longer a router is active, the higher the reputation
- Bootstrapping issue
  - New router has no age information on peers

Our Contribution

Goal

- Make it harder to create successful Sybil nodes
- Create tamper-proof platform
  - Traceability
  - Evaluate FF routers
- Offer both preventative, proactive, and retroactive solutions

Criteria

Our solution should be:

- Distributed
- Public
- Permissionless
- Anonymous
- Open-source

Distributed ledger technologies - why blockchain

Distributed ledger - decentralized database which is synced and consented upon by all participants of the network

	Blockchain	Tangle	Hashgraph
Data structure	Blockchain	DAG	DAG
Ledger type	Public	Public	Private
Permissioned	No	No	Yes
Anonymous	Yes	Yes	No
Consensus	PoW, PoS	PoW	GaG, VV
Efficiency	Low	High	High
Central Authority	No	Yes	No
Copyright	Open-source	Open-source	Proprietary

Figure 5: DLTs comparison summary

Distributed ledger technologies - why blockchain

Distributed ledger - decentralized database which is synced and consented upon by all participants of the network

	Blockchain	Tangle	Hashgraph
Data structure	Blockchain	DAG	DAG
Ledger type	Public	Public	Private
Permissioned	No	No	Yes
Anonymous	Yes	Yes	No
Consensus	PoW, PoS	PoW	GaG, VV
Efficiency	Low	High	High
Central Authority	No	Yes	No
Copyright	Open-source	Open-source	Proprietary

Figure 6: DLTs comparison summary

Implementation

General Concept

- Keeping track of FF routers
  - Verify age
  - Determine trustworthiness of FF router
- Use blockchain randomness for closeness metric

Implementation

- Proof-of-Work vs Proof-of-Stake
  - PoW: High computation power required to add block
  - PoS: nodes with more coins have a higher chance to add a block
- Incentive for miners
  - Reputation
- Nodes should make decisions individually
  - Who to trust?
  - Who not to trust?

Proof-of-Stake

- Miner chosen based on their wealth
  - Wealthier miners have a higher stake and are more likely to be trustworthy
- No expensive hardware required
  - Virtually all nodes are able to join
- More decentralized than PoW
  - In PoW, miners tend to pool together

Individual Decisions

Being able to make decision about trustworthiness of a router is important...

- Be as decentralized as possible
- Nodes can come up with own criteria
  - Strict criteria for the paranoid
  - Loose criteria for performance-minded

Transaction types

MinerTransaction	Reward for the miner
EnrollmentTransaction	Enrollment as miner
RouterUp	Announcement of new FF router
RouterDown	FF router no longer responsive

Table 1: Blockchain transactions [3]

General Structure

- First block should have all FF routers
- Subsequent blocks update that list
- Traverse chain to get router age

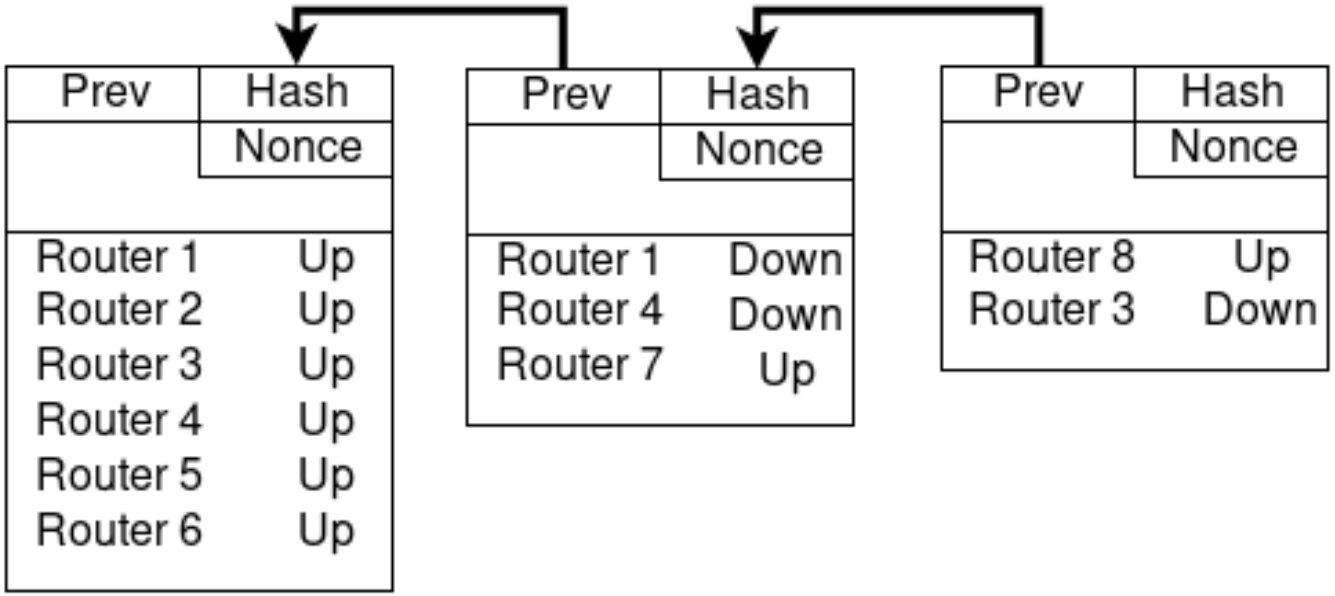

Figure 7: Overview of blockchain

Positive Externalities

More advantages to blockchain...

- Bootstrapping issue solved
- Nonce provides non-deterministic hash for router closeness
- Retroactively and proactively verify attacks
  - Check certain criteria
  - Individually verify attack likelihood

Conclusion

Conclusion

A Sybil attack can be made less feasible by using blockchain

- The age and reputation of Floodfill routers can be identified
- Routers are able to build up reputation
  - FF routers need reputation before they can join
- The Kademlia closeness metric can be made non-deterministic

Future Work

Future Work

- Study privacy implications
- Implementational details
  - Exact Proof-of-Stake algorithm used
- Analysis of the network's performance with blockchain
- Practical analysis of other technologies
- Explore other solutions blockchain could provide to I2P
  - Replace netDb
  - Provide payment platform

Q&A

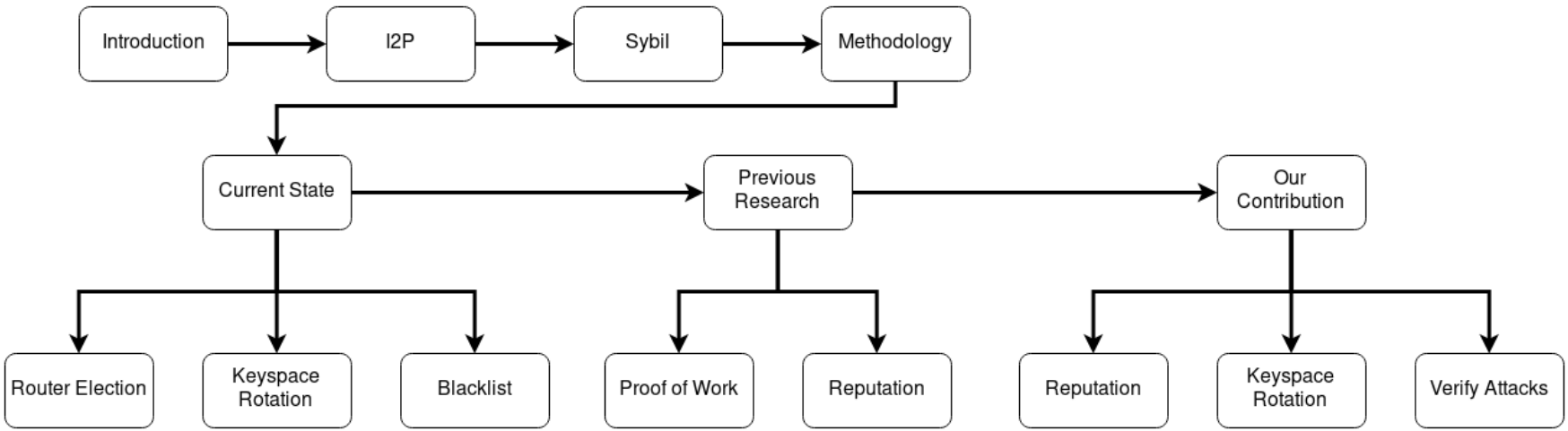

Figure 8: Presentation Overview

References


Christoph Egger, Johannes Schlumberger, Christopher Kruegel, and Giovanni Vigna.
Practical attacks against the i2p network.
In *International Workshop on Recent Advances in Intrusion Detection*, pages 432–451. Springer, 2013.


I2p's threat model, 2010.
https://geti2p.net/en/docs/how/threat-model.


Neo white paper, Nov 2016.
http://docs.neo.org/en-us/.

Miner Incentive

- Altruistic nodes
  - Could work for I2P. However...
  - Blockchain reliability should not lean on this
- Monetary
  - Advantage: currency for users
  - Disadvantage: complicated blockchain construction
- Reputation
  - Two birds, one stone
  - Incentive and measure of trustworthiness