Trying to De-Anonymize I2P Network Participants

Thesis

- Title
  - De-anonymization of participants of the I2P-based trading network for digital assets ("DIVA.EXCHANGE")
- Students
  - Brian Boss & Marco Purtschert
- Initiator
  - Konrad Bächler (DIVA.EXCHANGE)

Depth of this Presentation

- Simplified
  - Trade-off between profound and understandability
- Main scope of research
- Focus on I2Pd (C++ Implementation)

Problem

- A service stores the B32-address of its participants.
- Storage is public available.
- Is it possible to infer the IP address from the B32-address?

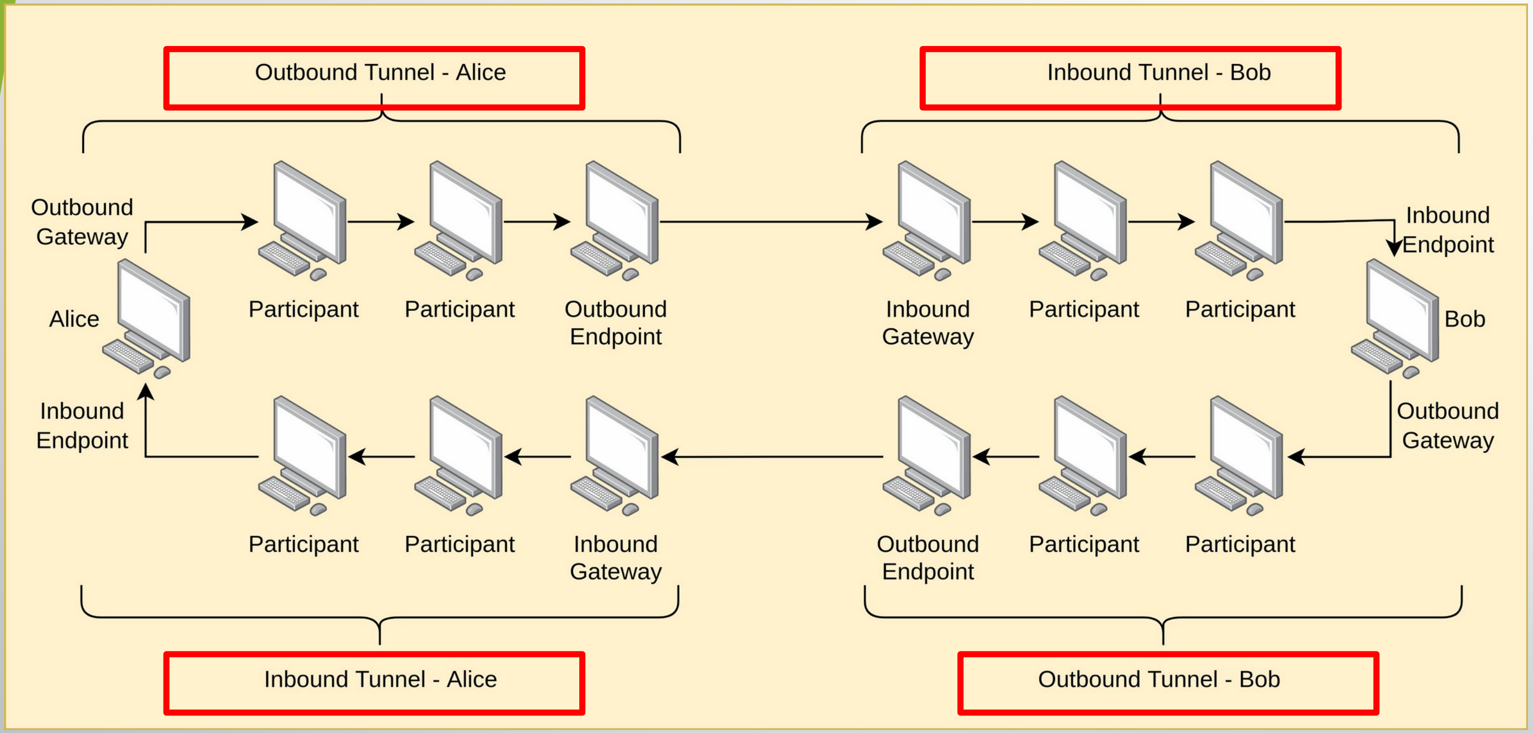
What is I2P

- Invisible Internet Project
- Decentralized & distributed P2P Overlay Network
- Multiple Implementations (Java & C++)
- Provides Security Anonymisation
  - Communication
  - Source & Destination

What is I2P not

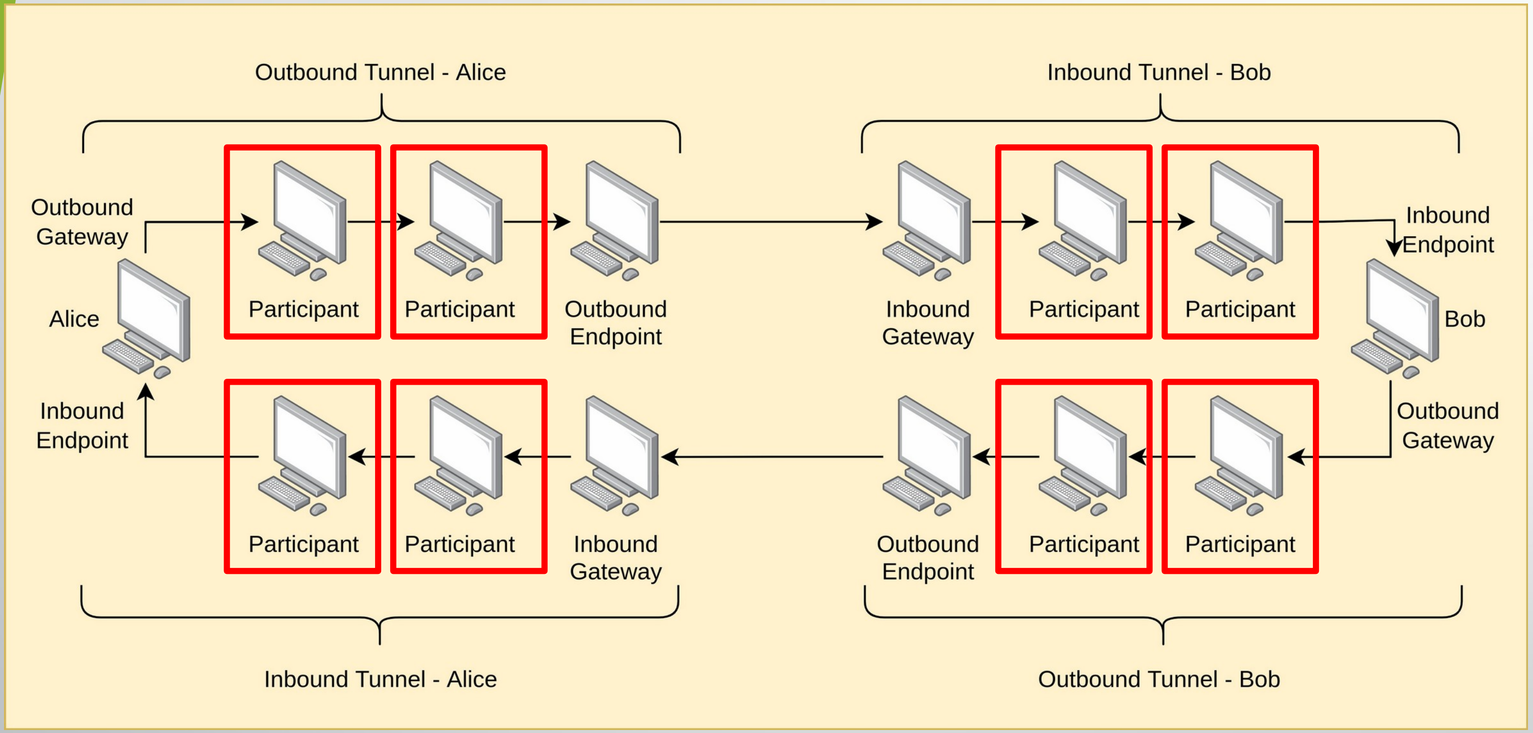
- Disguise that you are a participant of the I2P network
- Completely decentralized & distributed
  - 13 Reseed Server for bootstrapping

What are I2P Tunnels



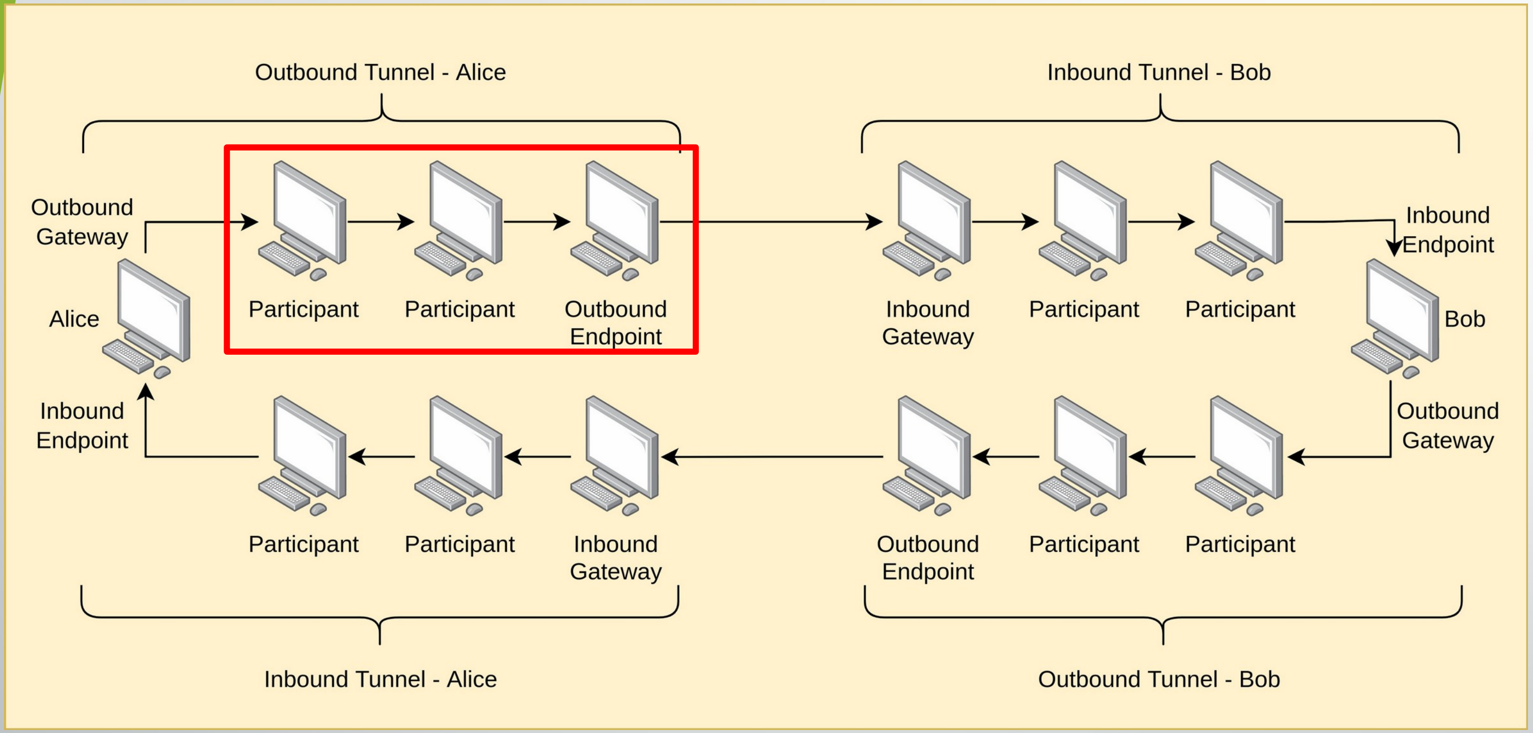
- Unidirectional Tunnels

What are I2P Tunnels



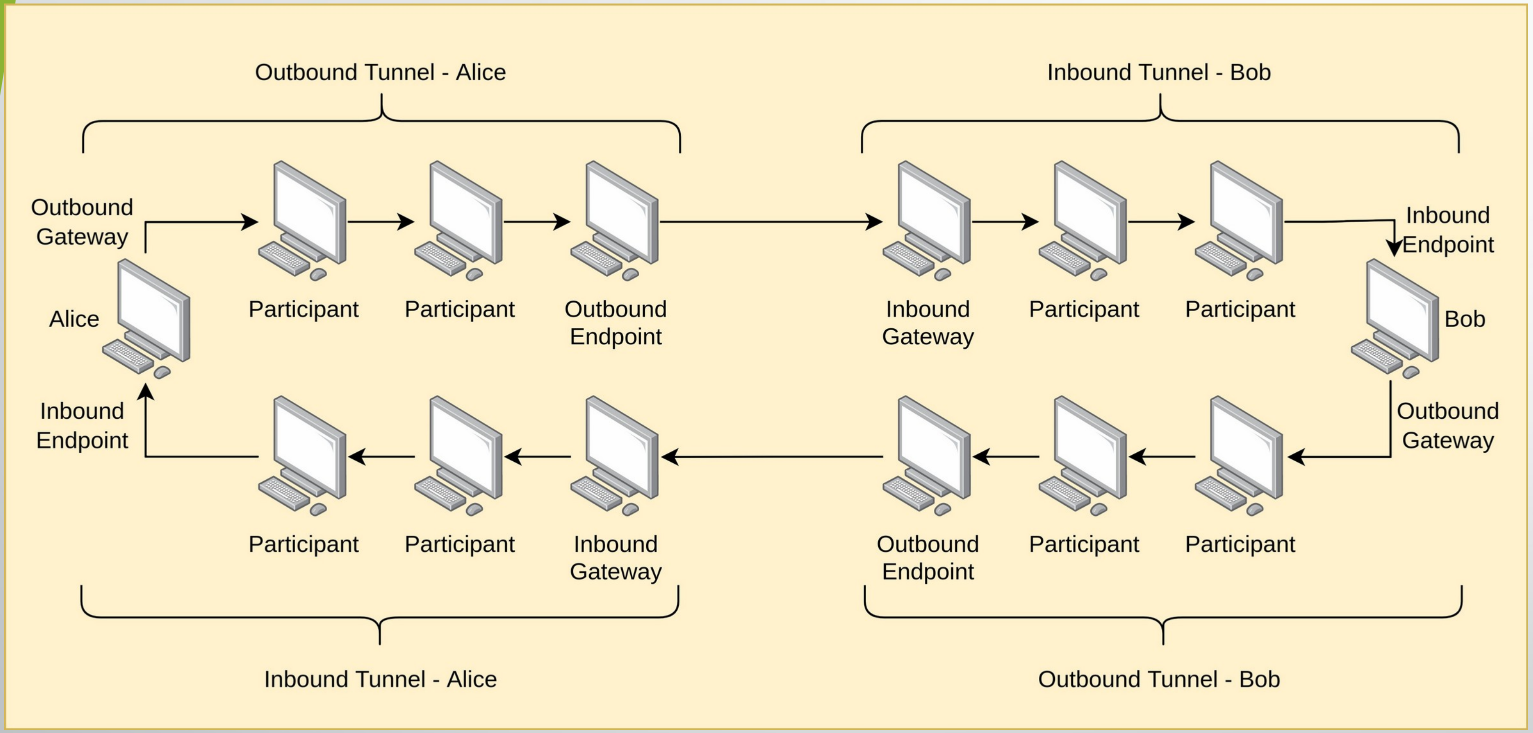
- Participants not knowing their position

What are I2P Tunnels



- Default Length
  - 2-3 Hops
- Default Amount
  - 2 IN & OUT

What are I2P Tunnels

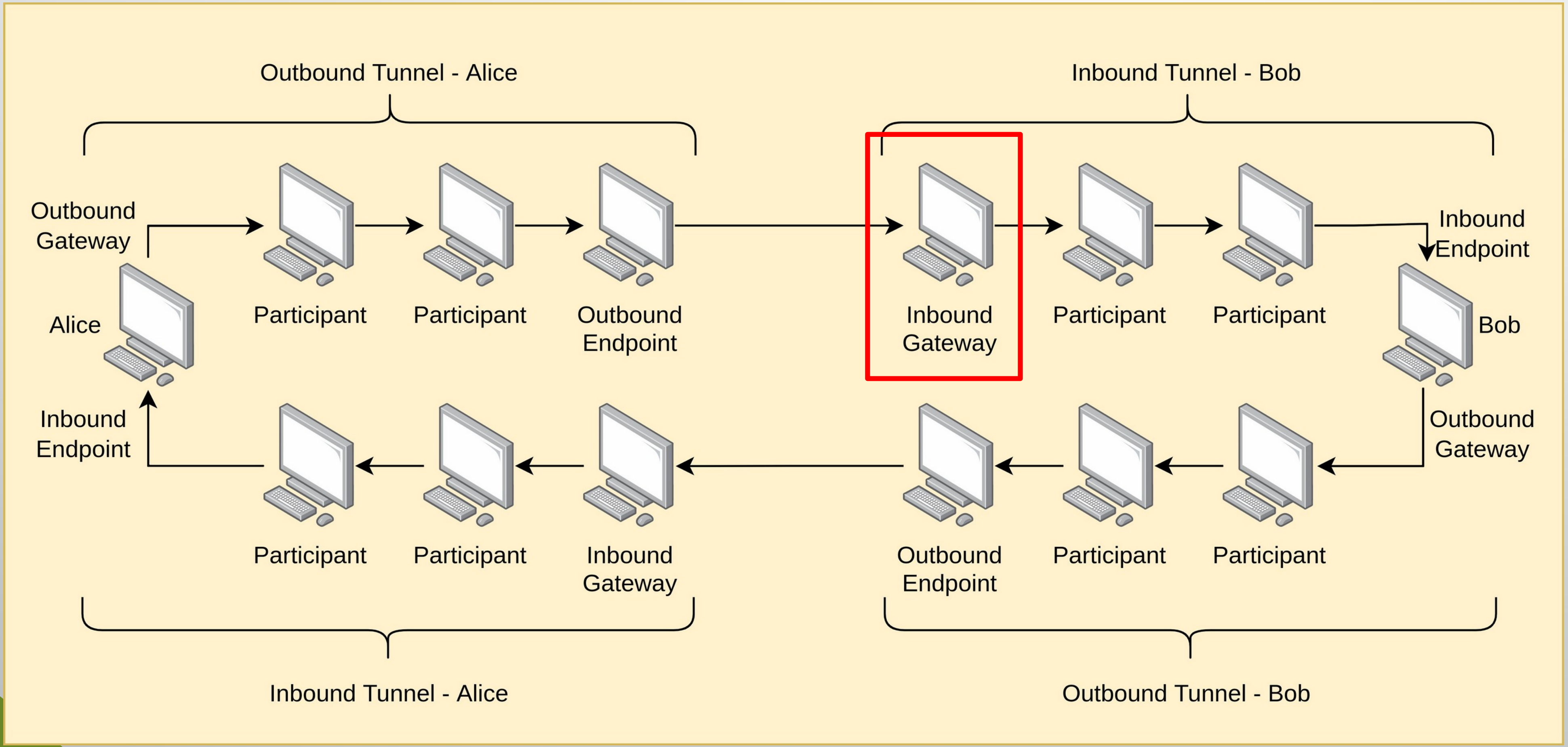


- Tunnel Renewal
  - 10 Minutes

What is I2P NetDB

- Distributed Network Database
  - DHT (distributed hash table)
  - Kademlia
- RouterInfo
  - Contact information for individual routers
  - IP Addresses of Individual Routers
- LeaseSet
  - Contact information for Services inside I2P
  - B32-Address
  - IP Addresses & Tunnel IDs of IN-Gateways

What are I2P Tunnels



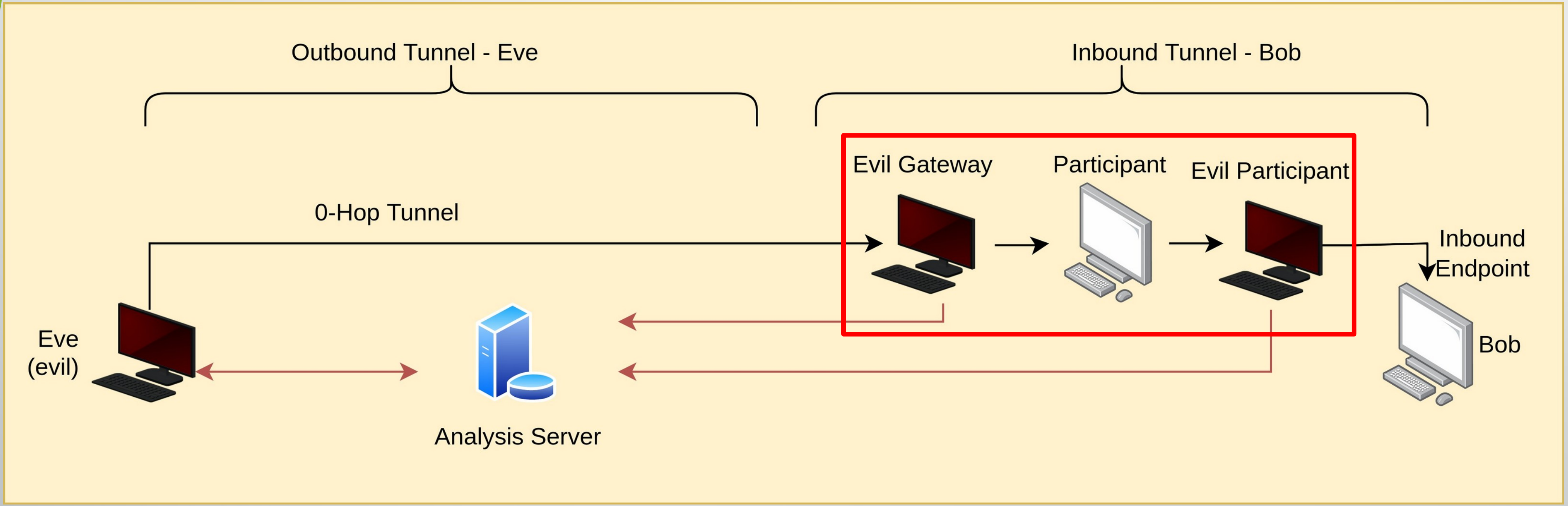
Attacks

- Analysed multiple P2P-attacks
  - No malware injection involved
- All attacks were covered theoretically
  - Starting to build a test-net for attack simulation
- Main scope of research
  - Tunnel takeover (sybil & intersection attack)

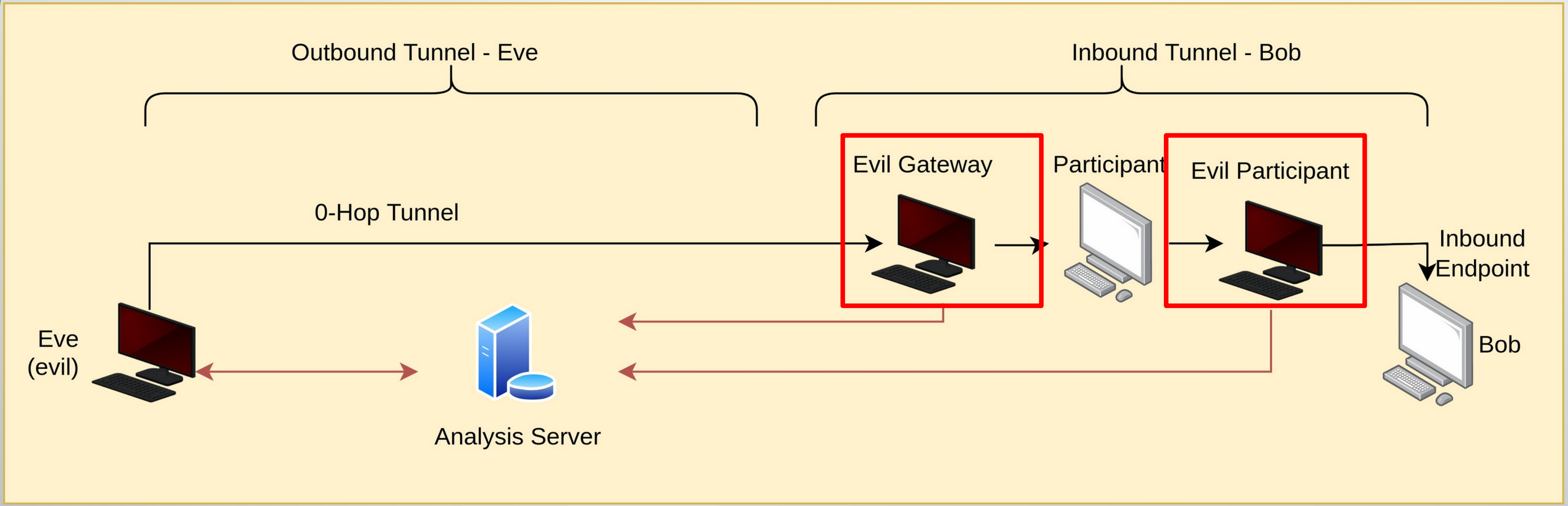
In a nutshell

- It’s about mass-attacking a Network
- Attack is based on statistical probability
  - No 100% guarantee, but repeating the attack will increase probability

Tunnel Takeover

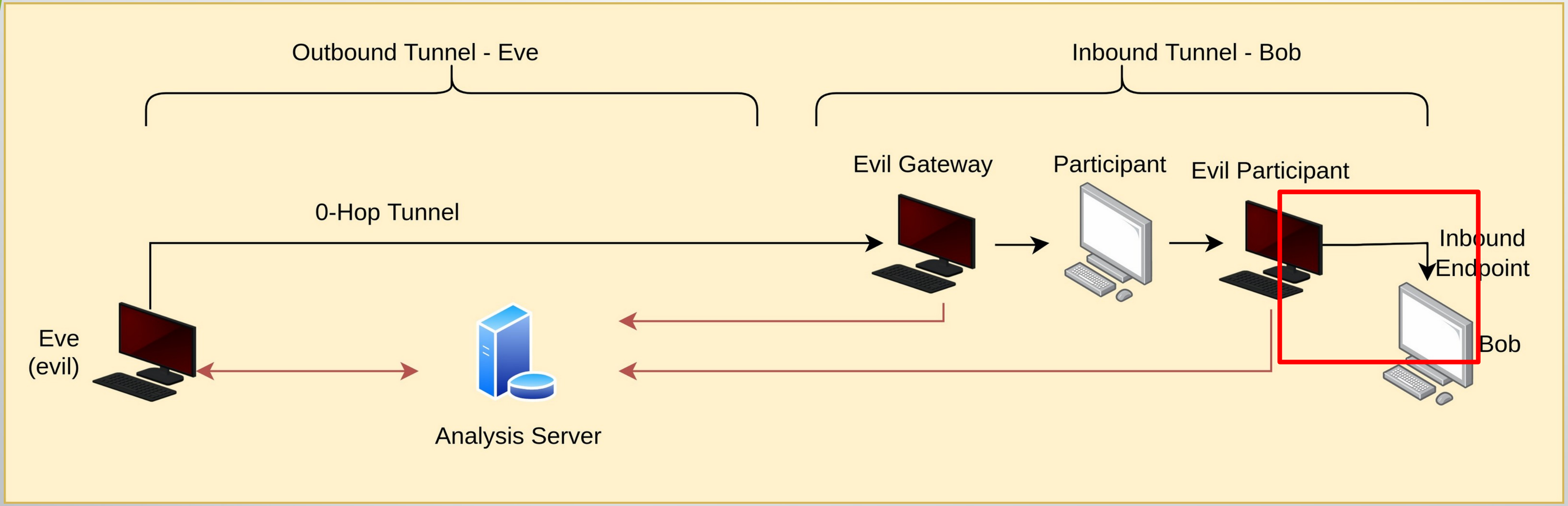


Tunnel Takeover



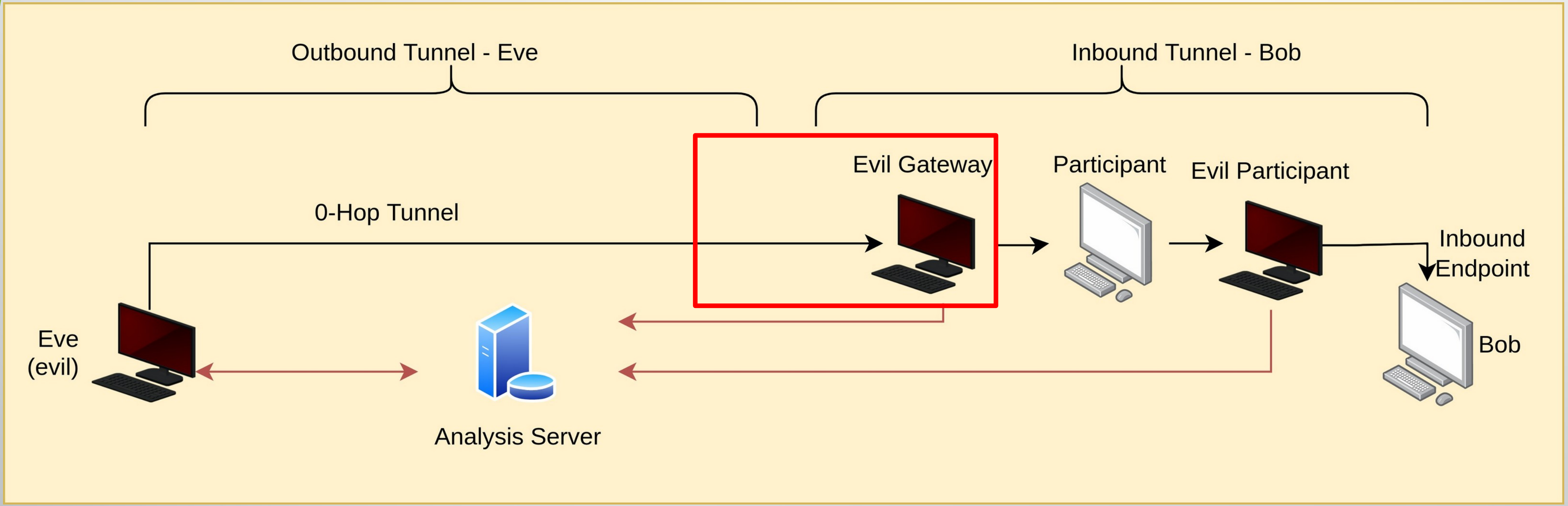
- Main Idea: two colluding routers

Tunnel Takeover



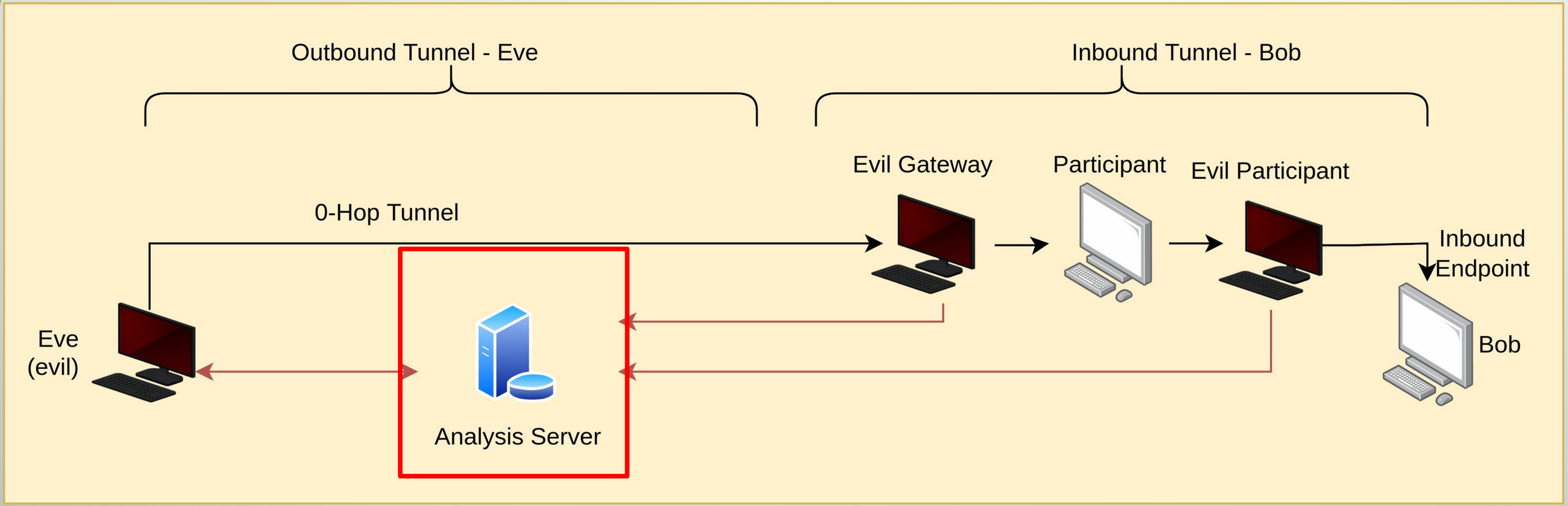
- Evil participant knows RouterInfo of Bob

Tunnel Takeover



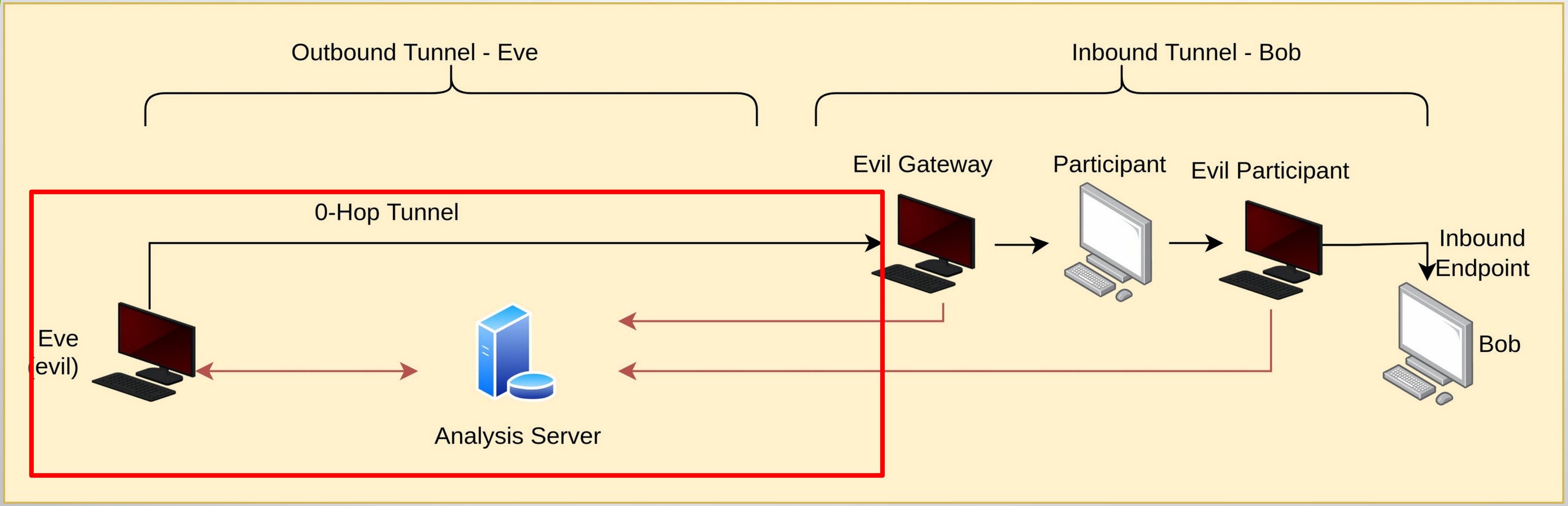
- Evil Gateway knows his IP-Address & Tunnel ID

Tunnel Takeover



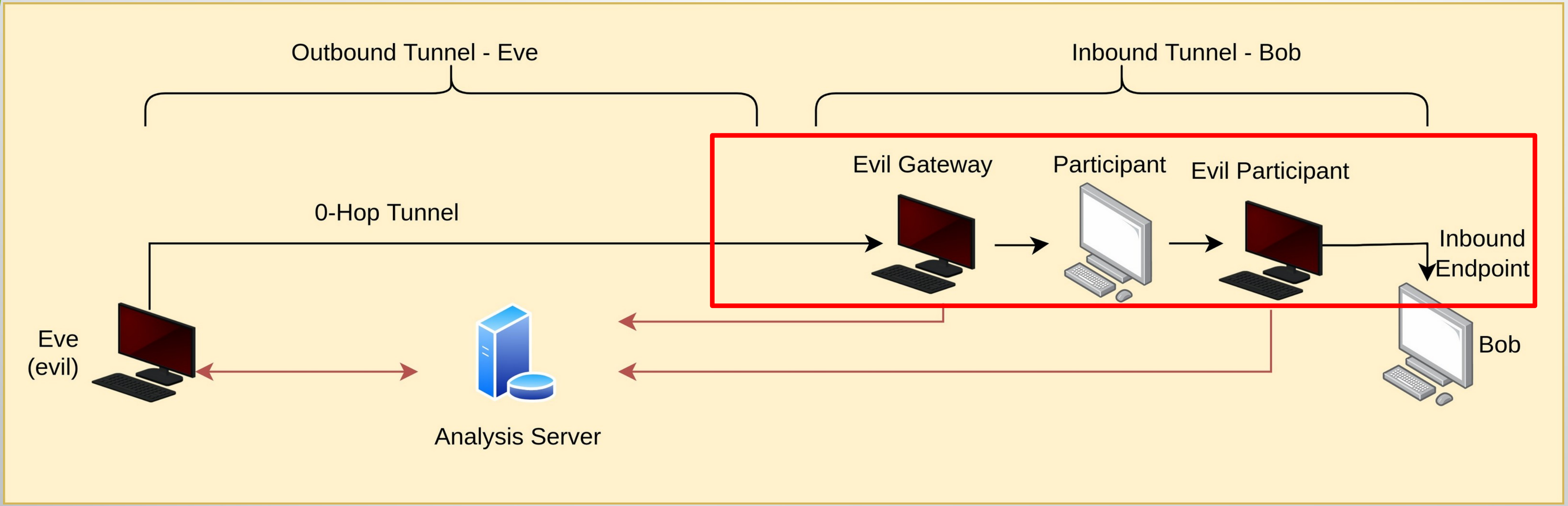
- With enough Information, Analyse Server can recreate Tunnel

Tunnel Takeover



- (Revers-Lookup) of LeaseSet

Tunnel Takeover



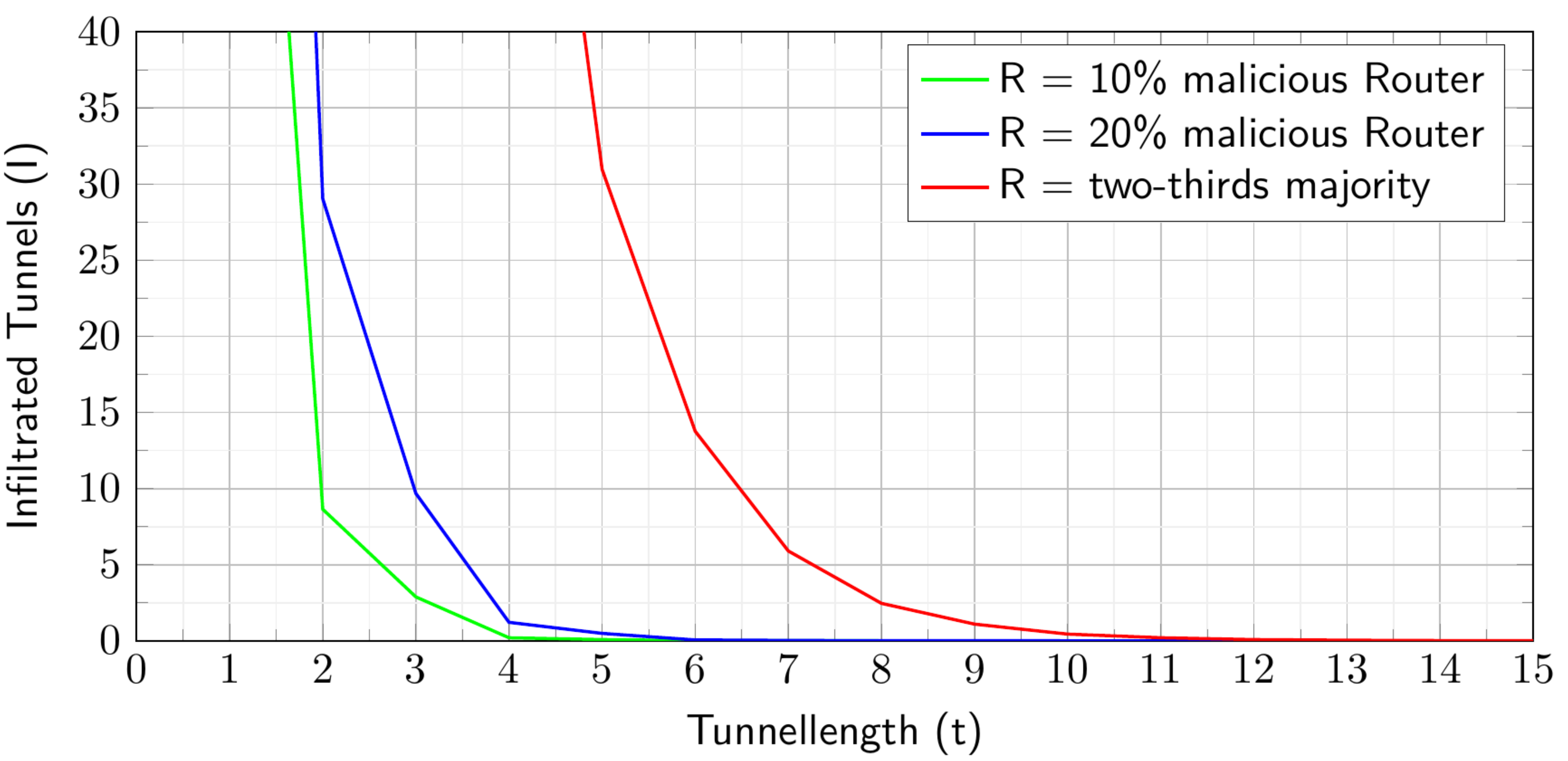
- LeaseSet-->Tunnel-->Routerinfo --> Deanonymisation

Mathematical Simulation

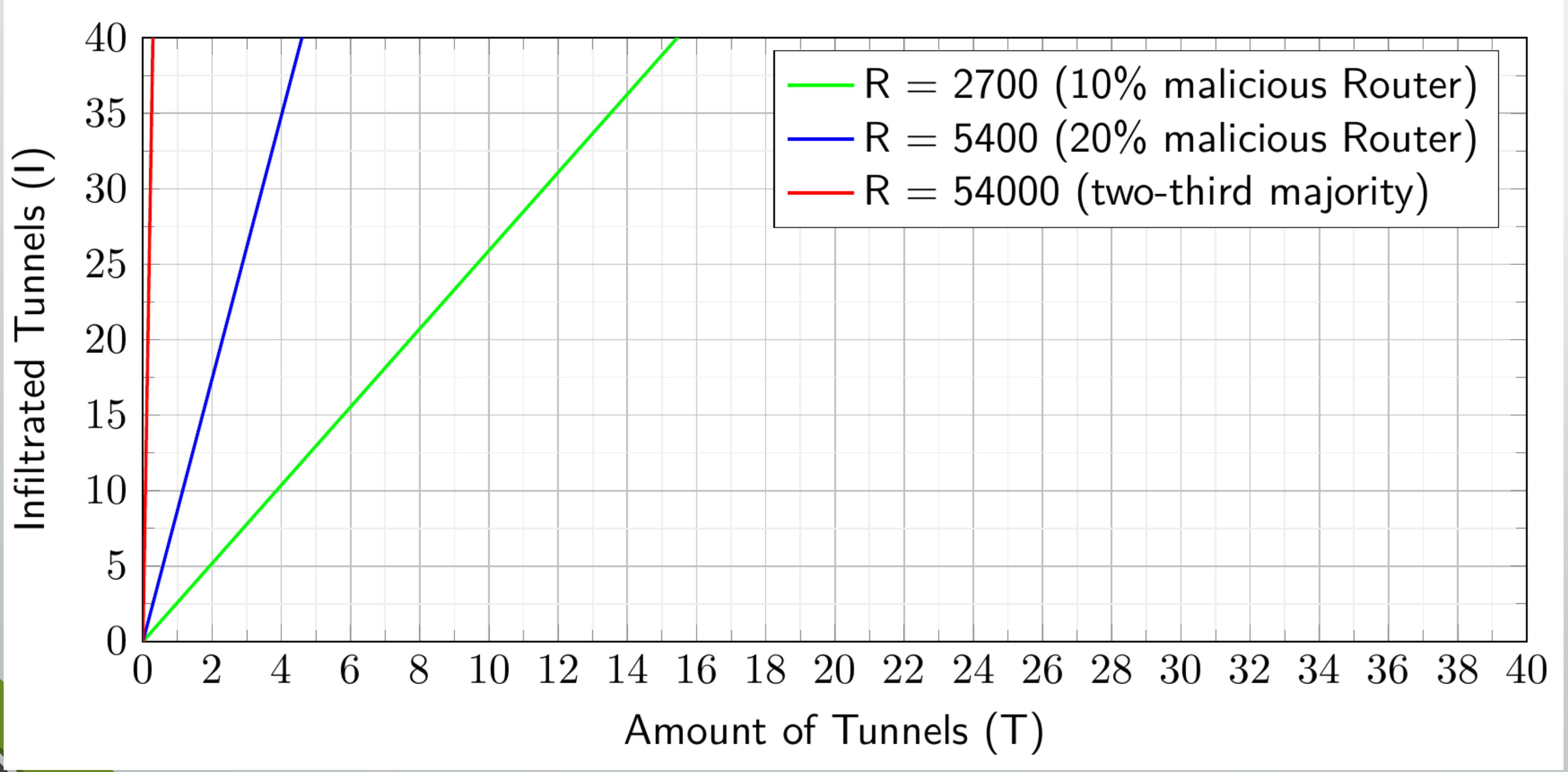
- To estimate the behaviour of various parameters, we have established the following formula.

$$I \approx \left(\frac{R}{N+R} \cdot p \right)^{h} \cdot \frac{a}{\frac{t!}{h! \cdot (t-h)!}} \cdot T \cdot r \cdot d$$

Influence of tunnel length

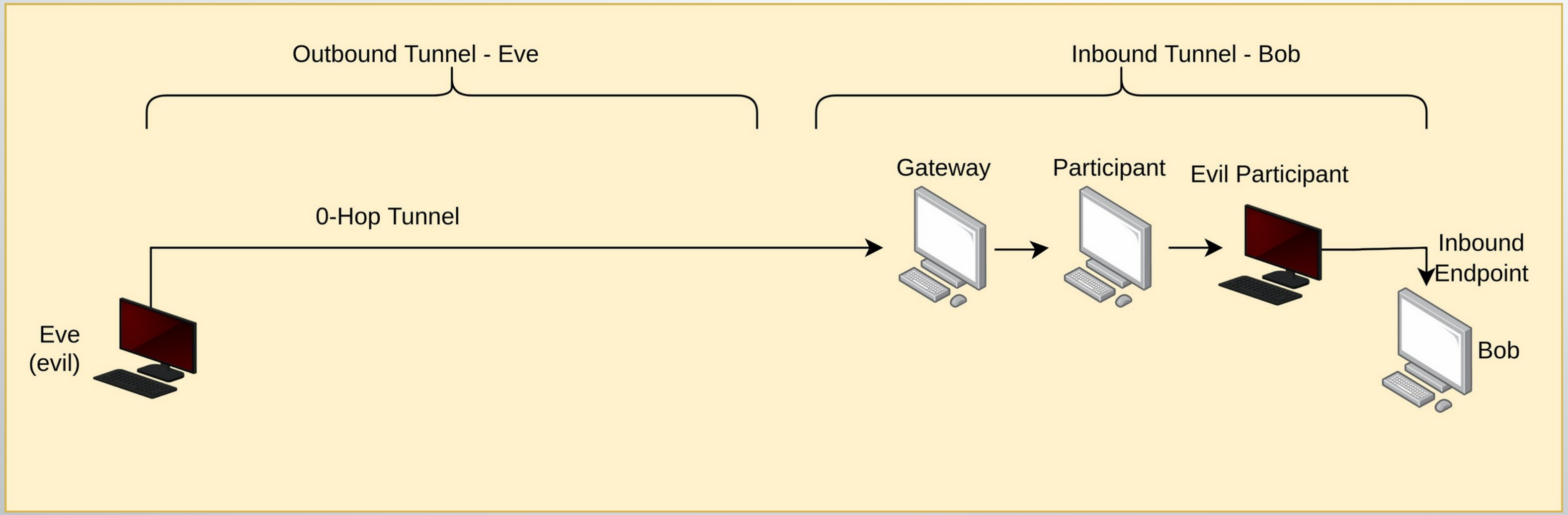


Influence of tunnel Amount



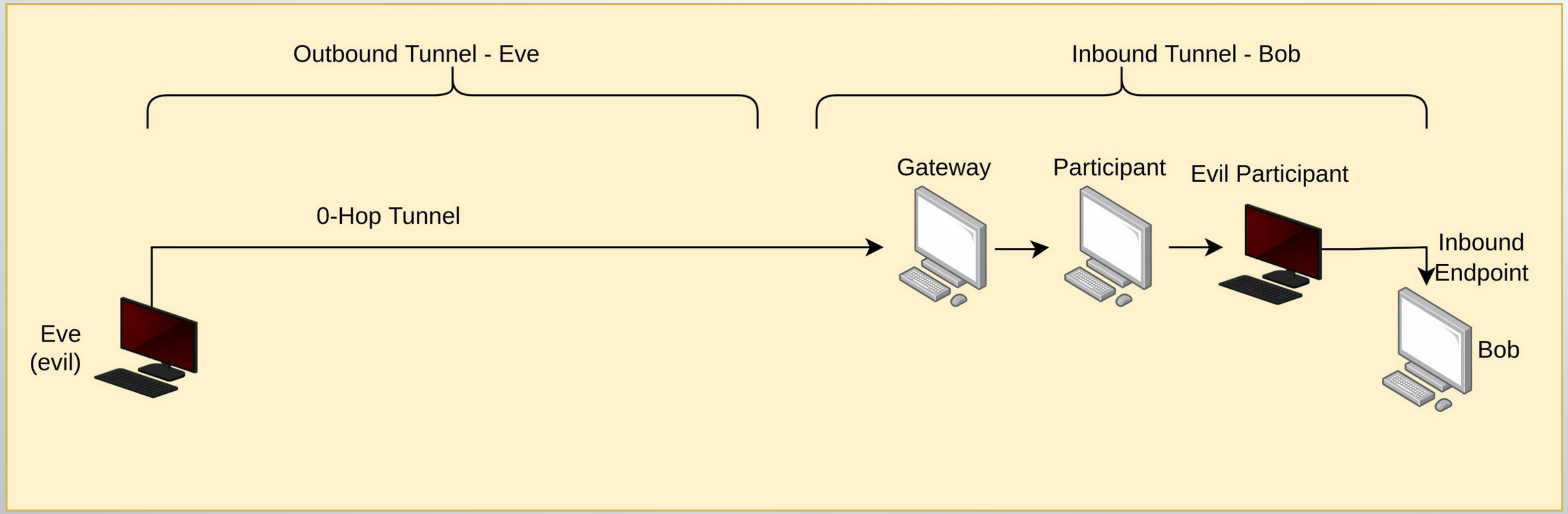
Alternative: Tunnel Takeover & DDoS

- Especially useful, if B32-Address already is known



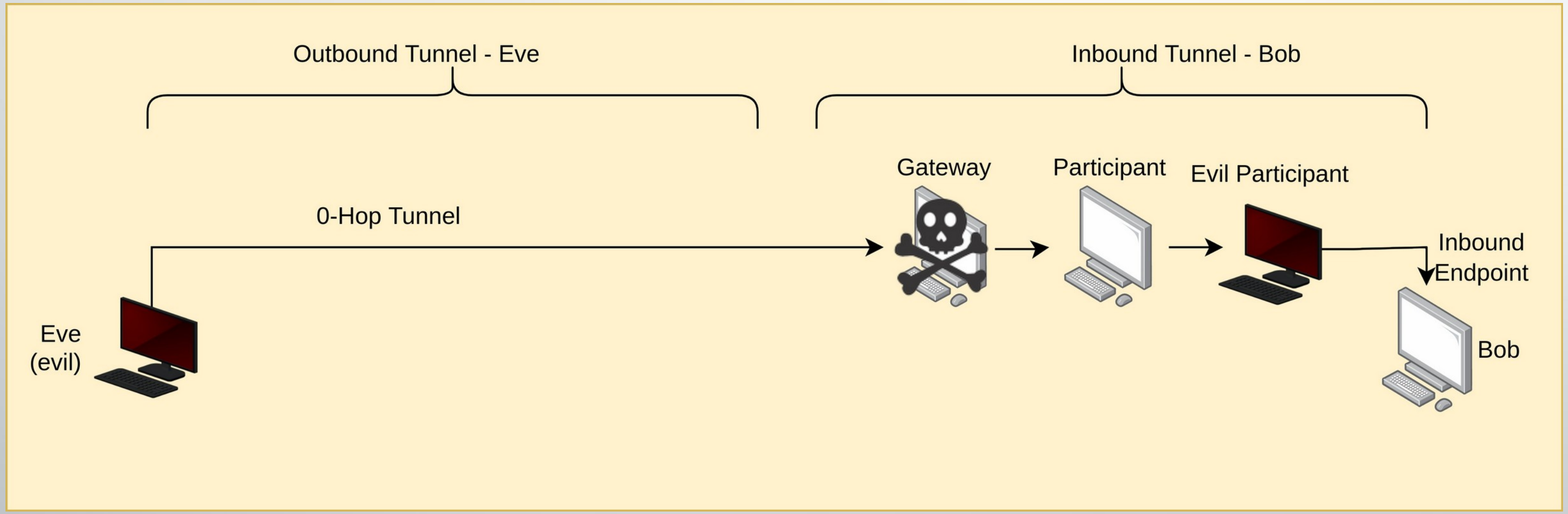
Alternative: Tunnel Takeover & DDoS

- Identify Inbound-gateway



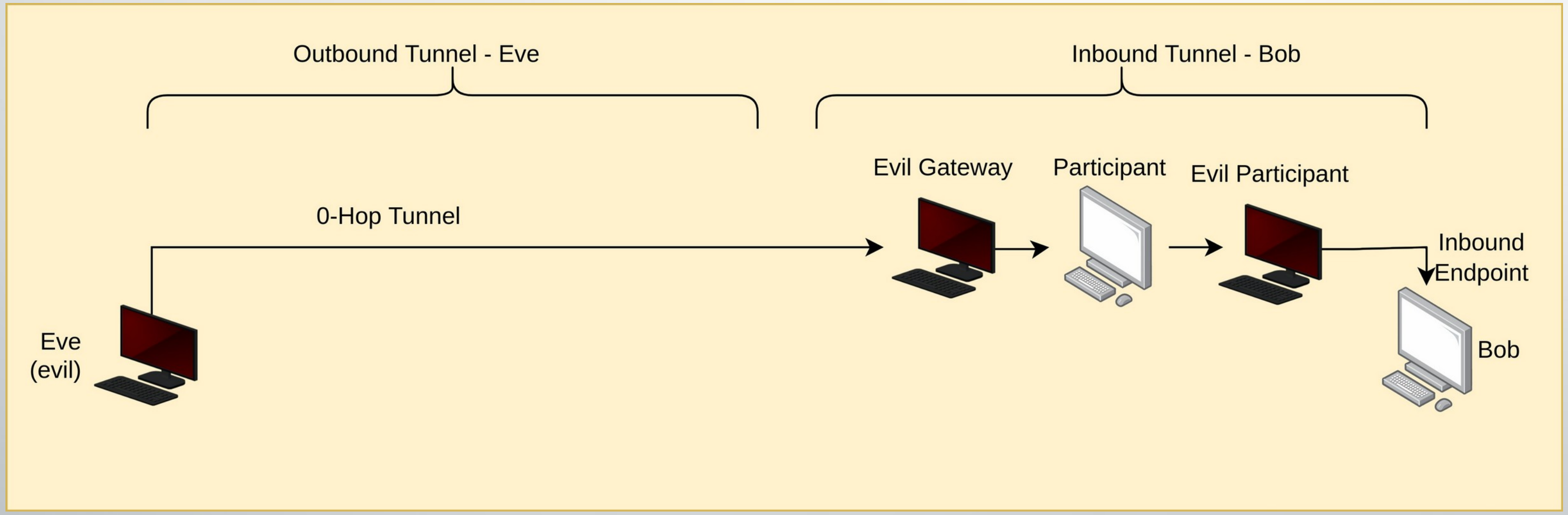
Alternative: Tunnel Takeover & DDoS

- DDoS Inbound-gateway



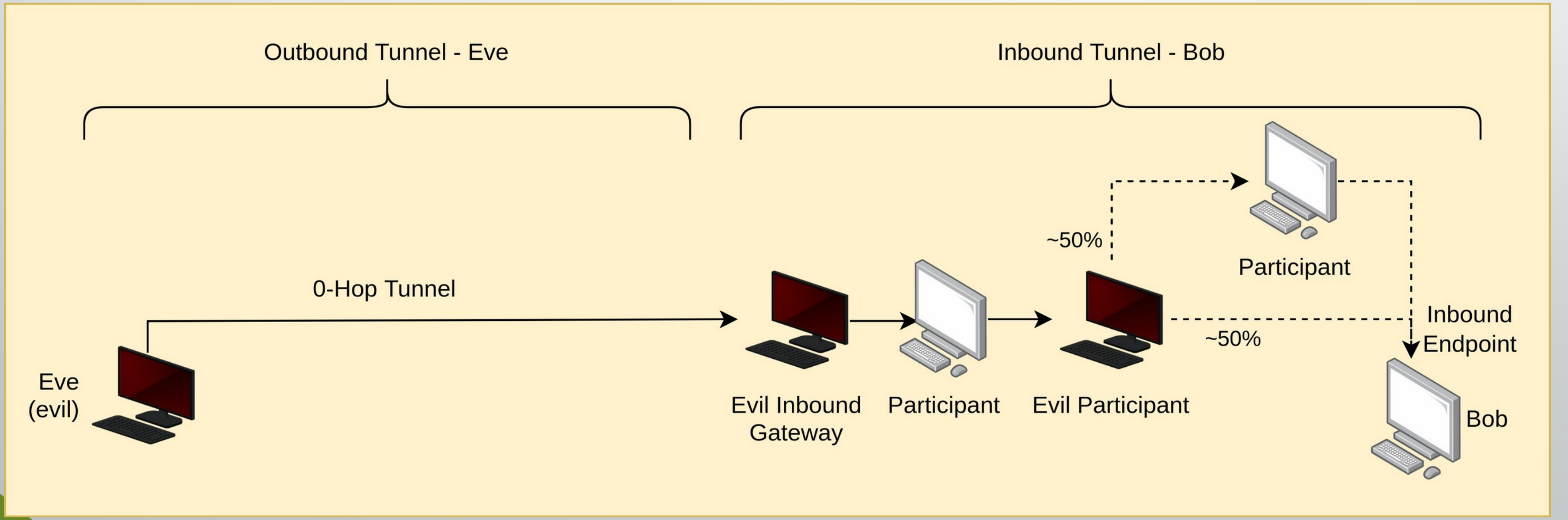
Alternative: Tunnel Takeover & DDoS

- Repeat until done



Tunnel Takeover - Mitigation

- Longer Tunnels
- Less Tunnels
- Variable Tunnel lengths



Conclusion

- Resistant against «common» Attacks
  - Various mitigations.
- De-anonymization within the I2P cannot be ruled out
  - Two colluding routers inside a tunnel
  - Traffic analysis on ISP / state-level-actor
- More research needed