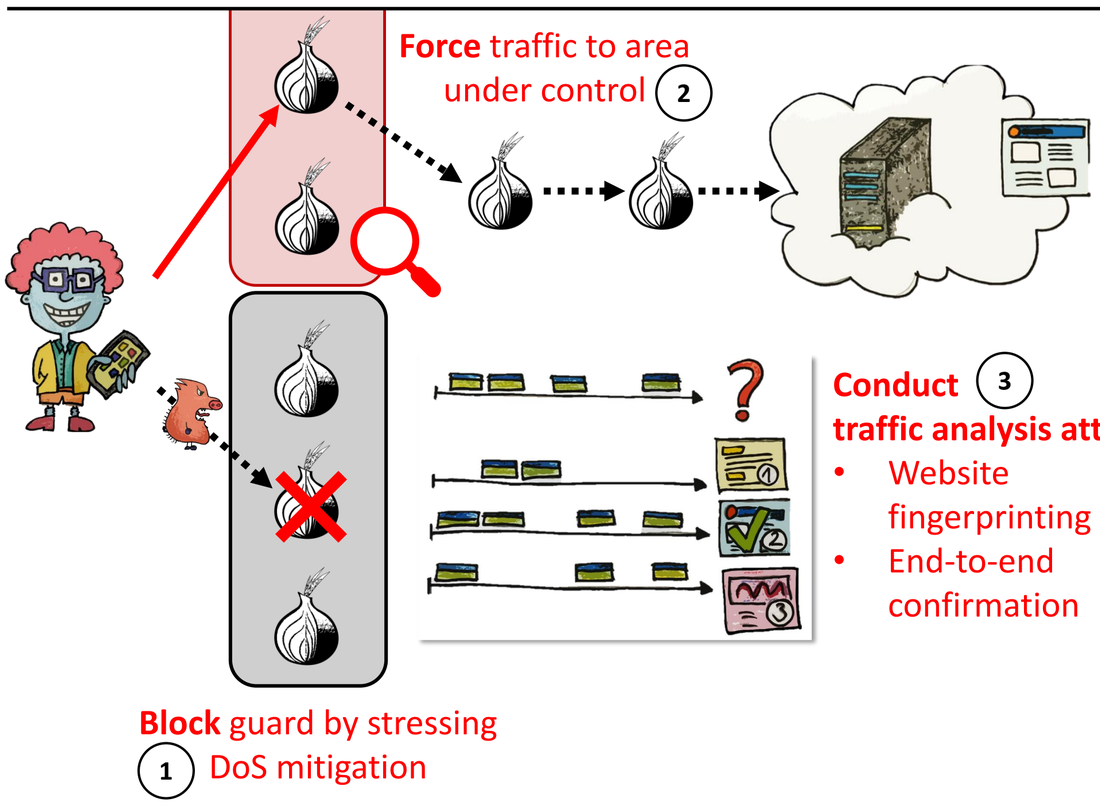
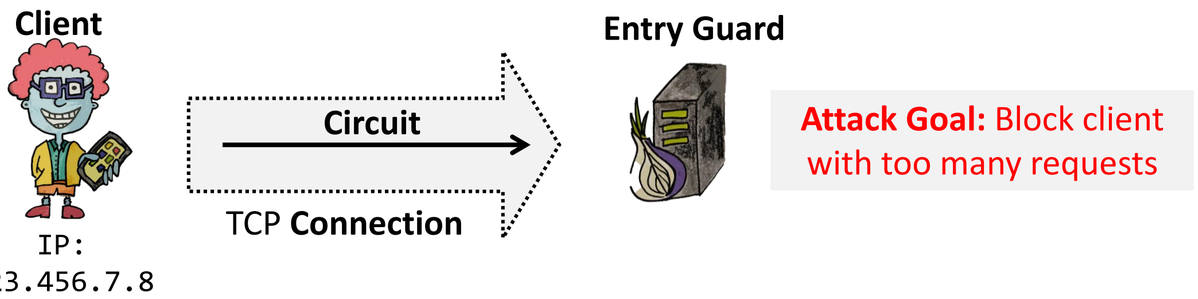
# Application-Layer Routing Attacks on Tor

**Katharina Kohls,** Ruhr University Bochum

## 1. Routing and Traffic Analysis Attacks




## 2. Denial of Service Mitigation in Tor

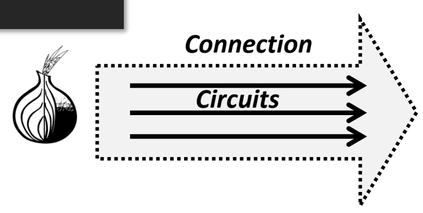



```
DoSConnectionMaxConcurrent
```

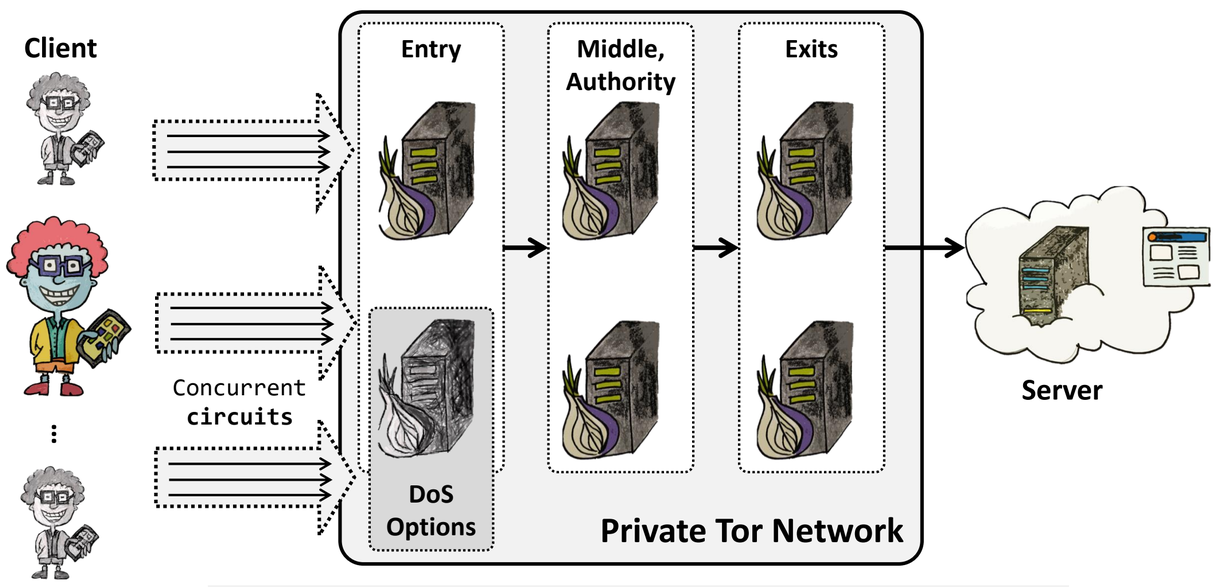
Too many ***connections*** from IP address


```
DoSCircuitCreationMinConnections
DoSCircuitCreationRate
DoSCircuitCreationBurst
```

Too many ***circuits*** from client




## 3. Preliminary Experiments: Stressing Features



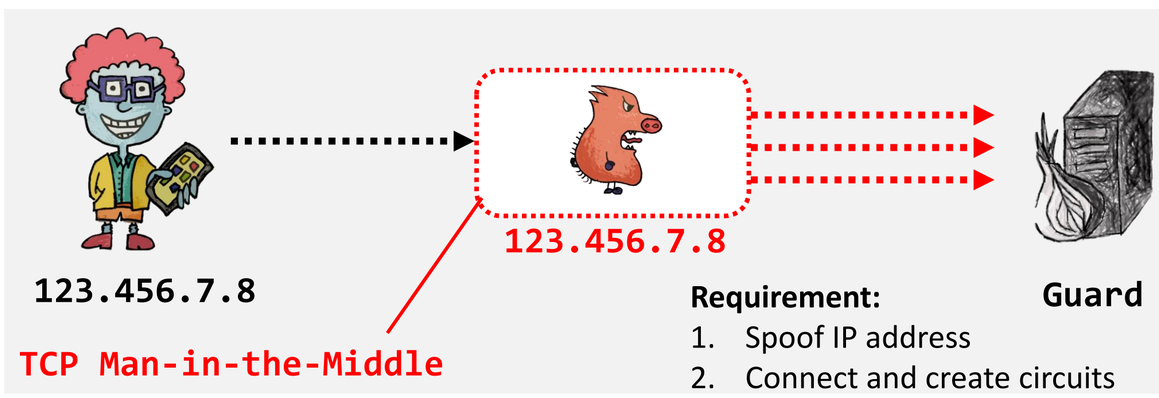

**Experiments Goal:**
**Stress mitigation options and record behavior**

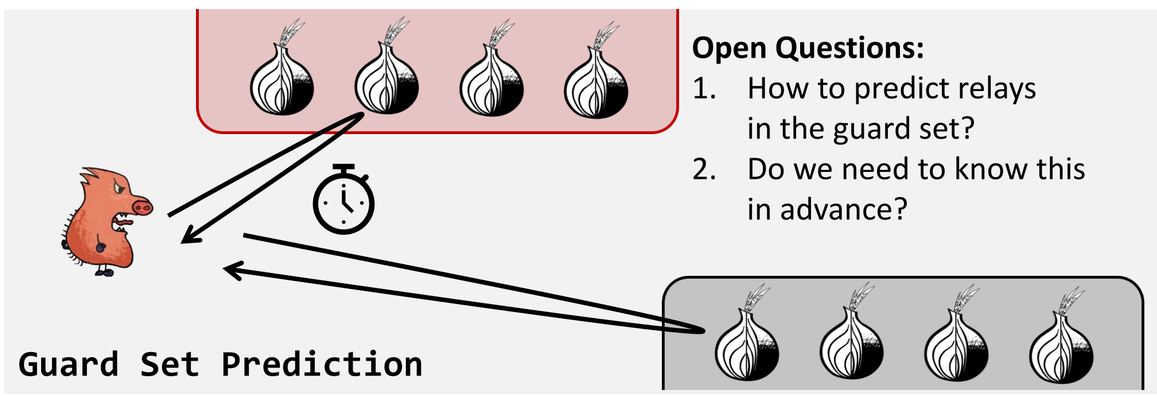
## 4. Results

**Logging the mitigation effects:**
`notice.log`
`info.log`

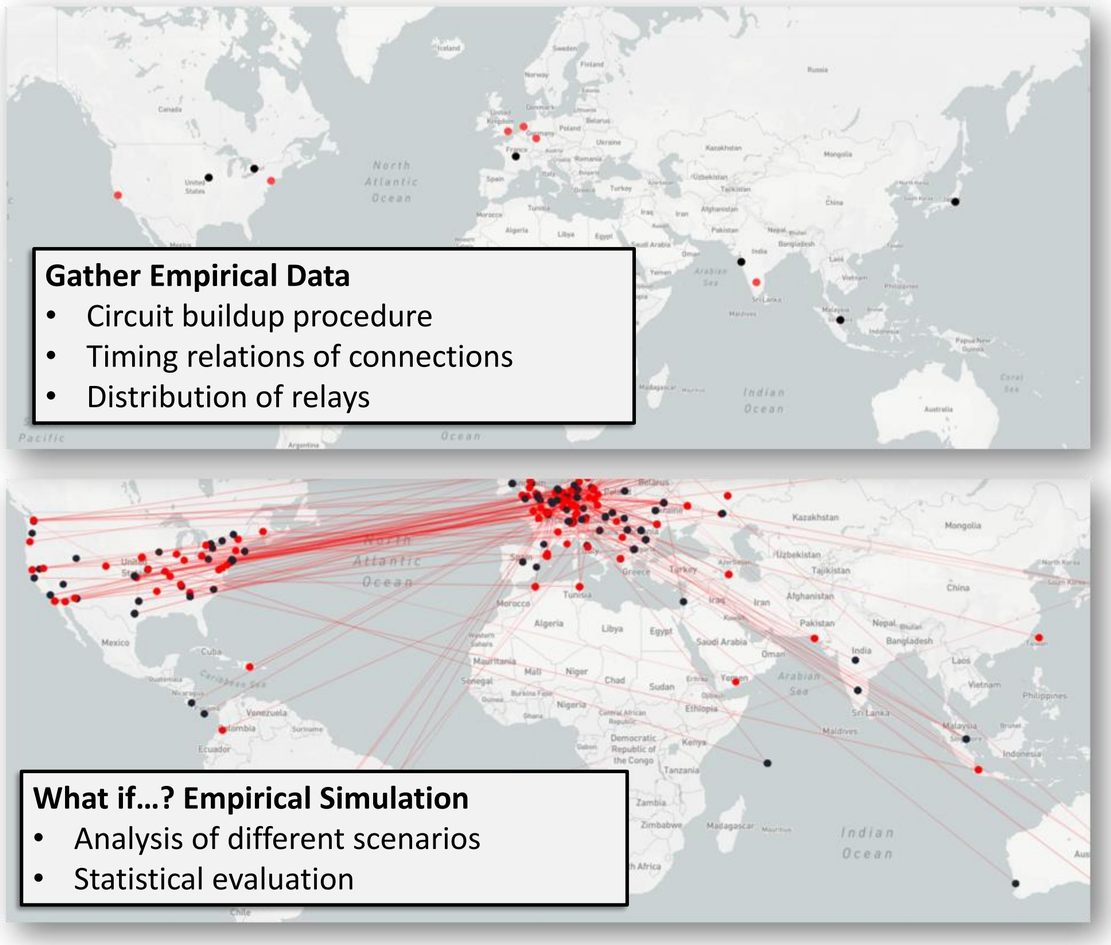
```
DoS mitigation since startup: 0
circuits killed with too many cells.
5535 circuits rejected, 2 marked
addresses. 3390 connections closed.
```

## 5. Attacker Model




## 6. Next Steps




## 7. Summary

**Attack Concept:**
1. Conduct routing attacks on the application layer
2. Empower traffic analysis attacks

**Current Status:**
1. Verify behavior of DoS mitigation features
2. Simulate and analyze impact

**Katharina Kohls**
katharina.kohls@rub.de
Ruhr University Bochum

**Christina Pöpper**
christina.poepper@nyu.edu
New York University Abu Dhabi