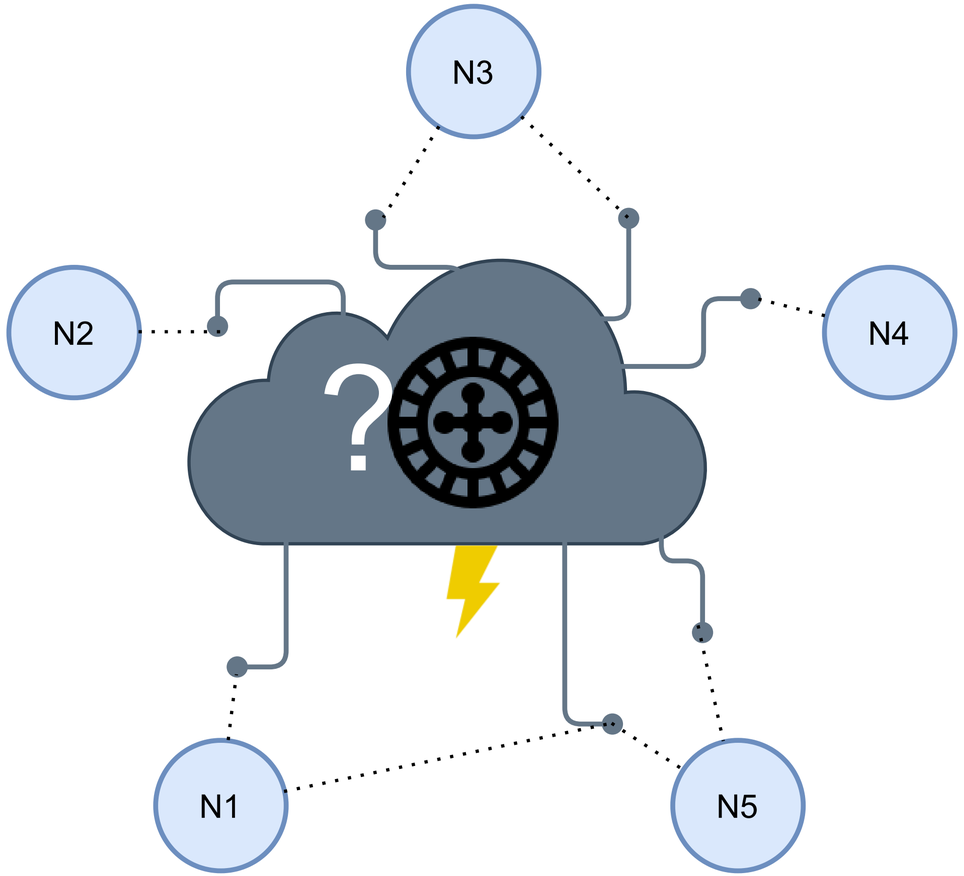
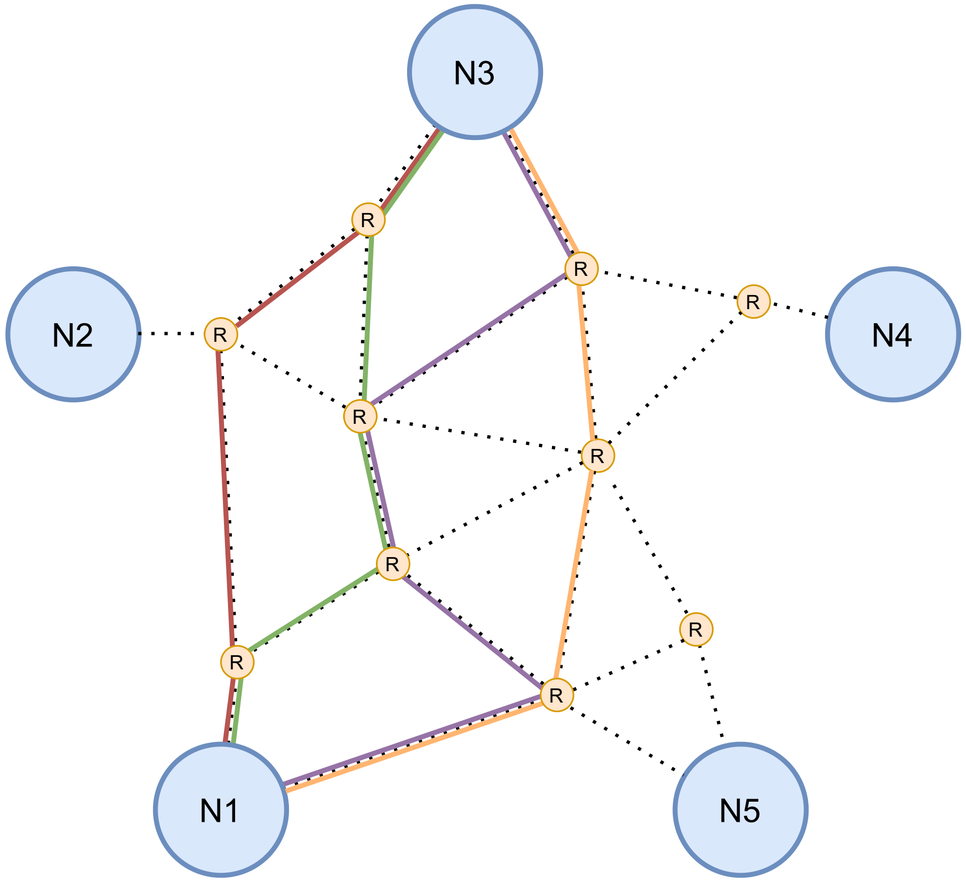
Distributed Applications
Challenges

- Threats for validator / consensus nodes:
  - DDoS
  - Outages
  - Routing hijacks
- Goal: Network performance and availability
- Challenges
  - Nodes run by different entities connected via Internet
  - Leased lines / private WAN solutions very costly and inflexible



Distributed Applications
SCION Properties

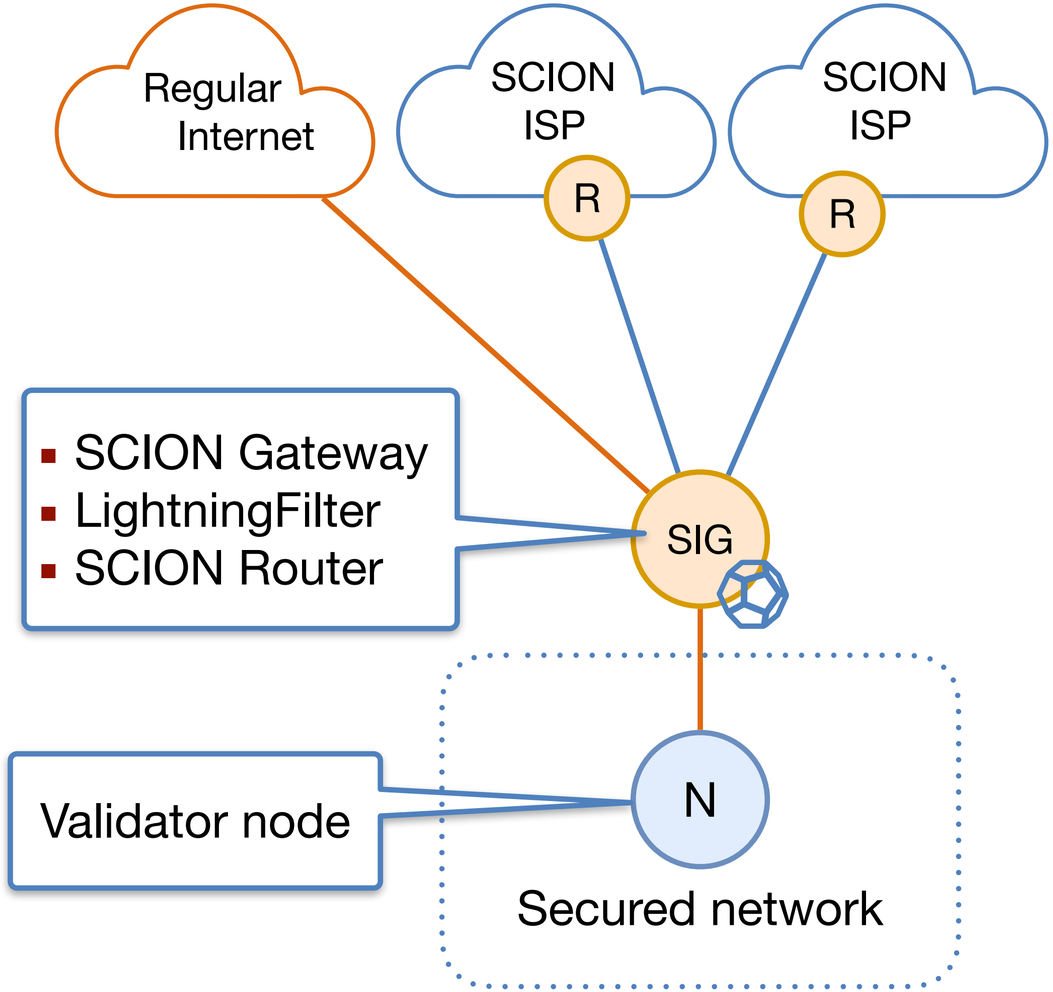
- High availability, secure against DDoS and routing attacks
- Fast failover & multipath
- High efficiency through path optimization
- Works in distributed scenarios
- Fault-independent from today's Internet
- With SIG (next slide) no change to application required



How to connect to SCION

SCION IP Gateway

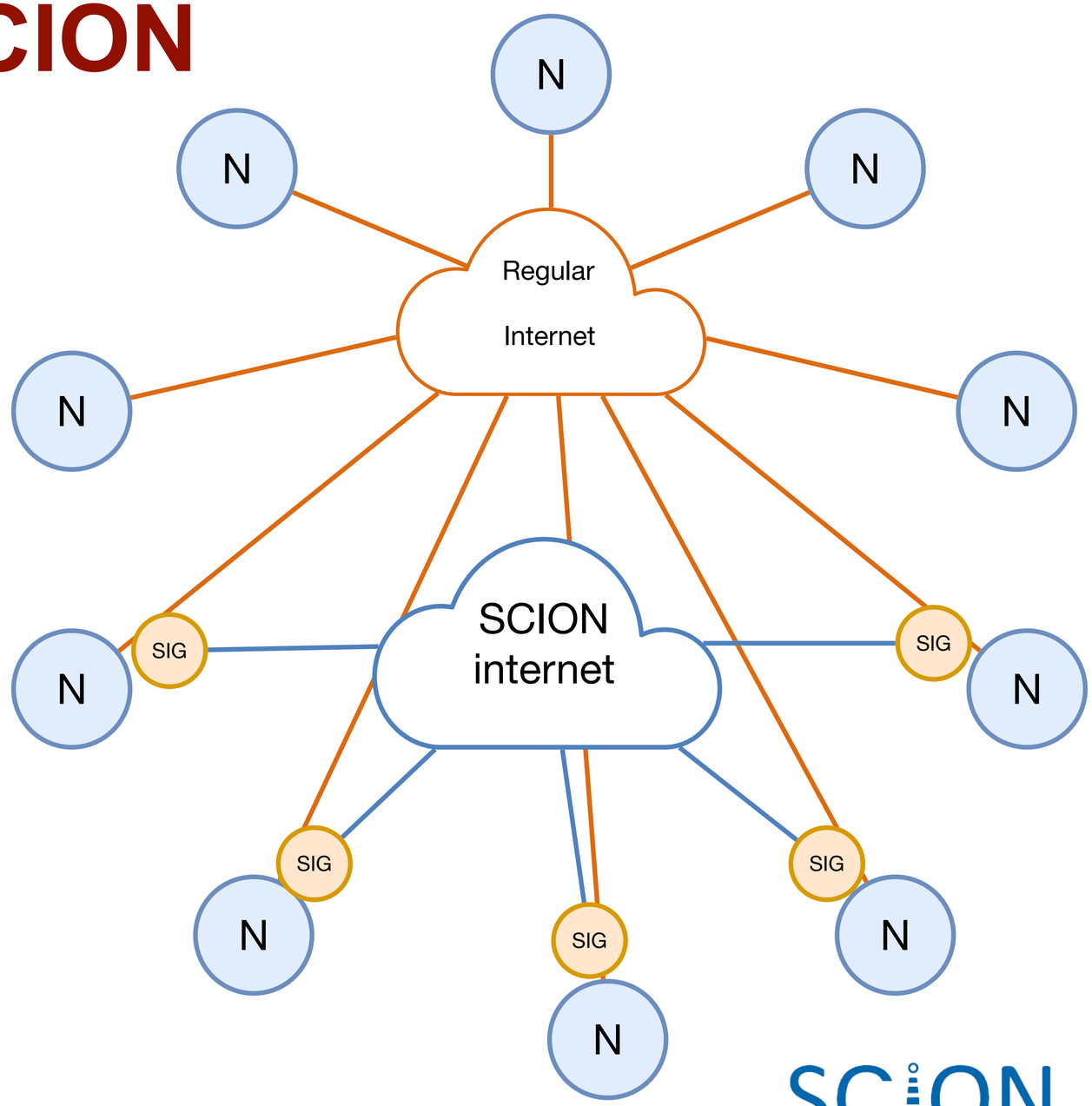
- SCION IP Gateway (SIG) enables seamless integration of SCION capabilities in end-domain networks
- No upgrades of end hosts or applications needed
- Validator node can communicate over SCION and IP to other nodes



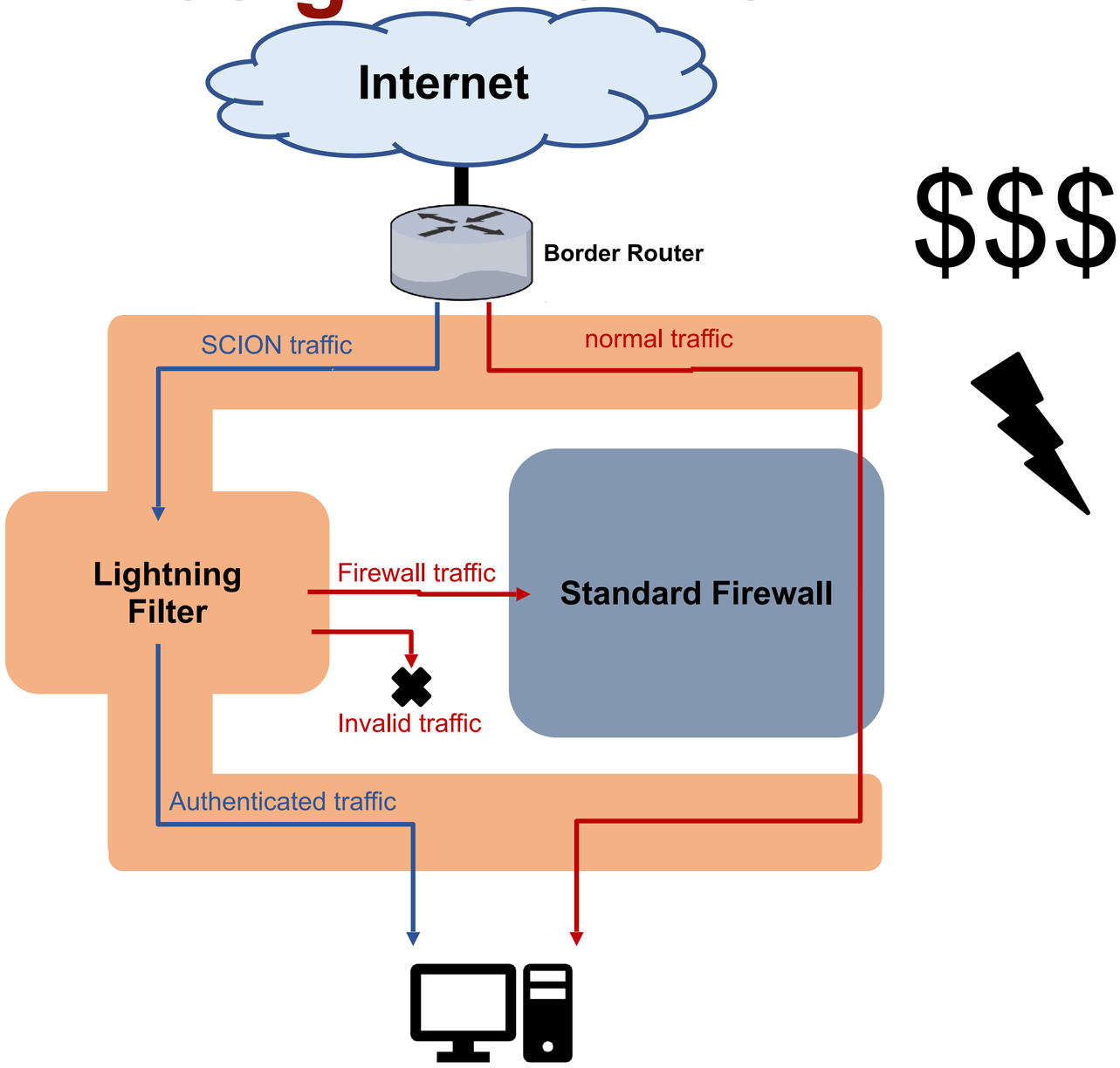
How to connect to SCION
Deployment Model

- Nodes communicate over IP & SCION
- Communication between SCION nodes with strong guarantees
  - Packet authentication
  - DDoS resilience
  - Internet fault-independence

- No upgrades of end hosts or applications needed

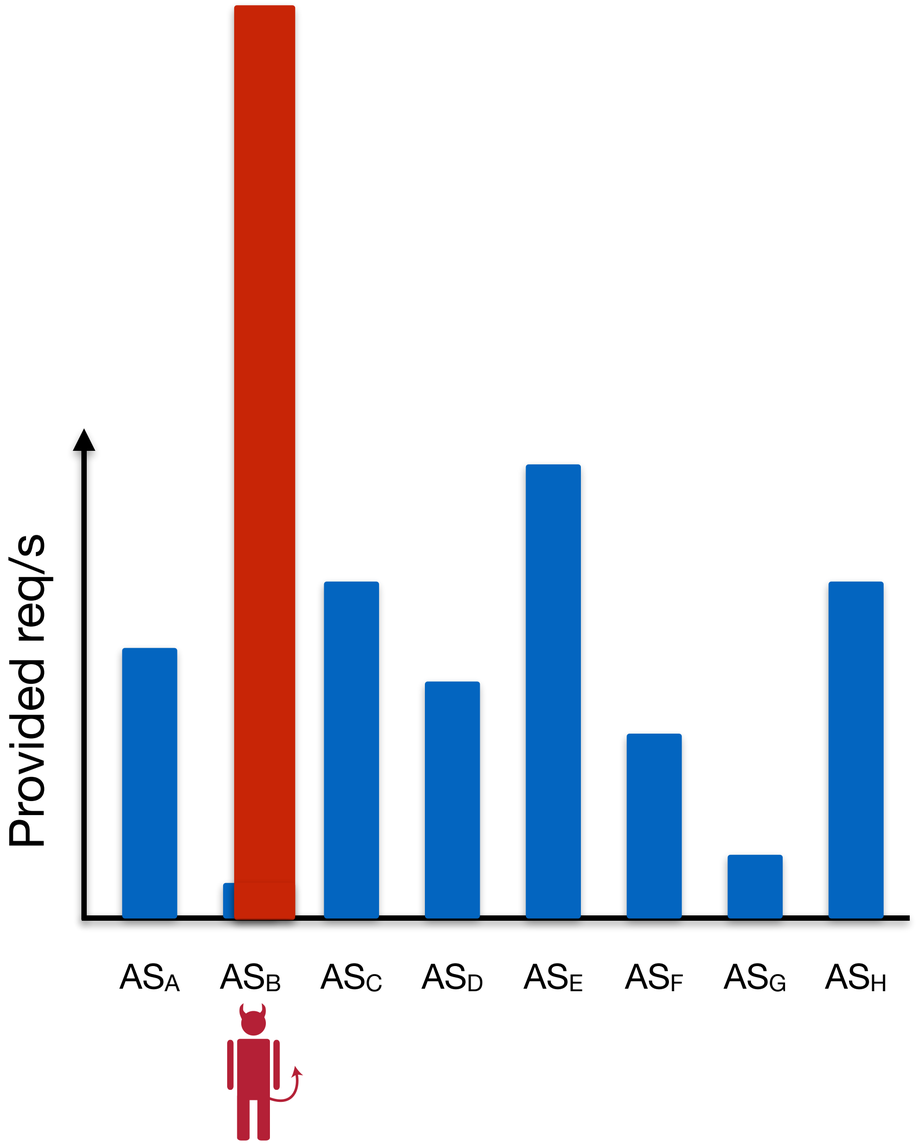


Lightning Filter: Design Overview



Lightning Filter: History-based Filtering

- Filtering service that is deployed upstream of protected end server
- Performs:
  - Packet authentication (DRKey)
    → authentic source AS
  - Duplicate suppression (using Bloom Filter)
    → no duplicates
  - Per-AS history collection (using Cuckoo hash table)
  - History-based resource allocation and filtering during DoS
    → fair resource allocation based on previous usage
- Result: collateral damage only for hosts within attacker-controlled AS



ETH zürich

SCION