Enhancing ICMP/ICMPv6 Error Message Authentication Using Challenge-Confirm Mechanism

Presenter: Yuxiang Yang, Ao Wang
INTAREA

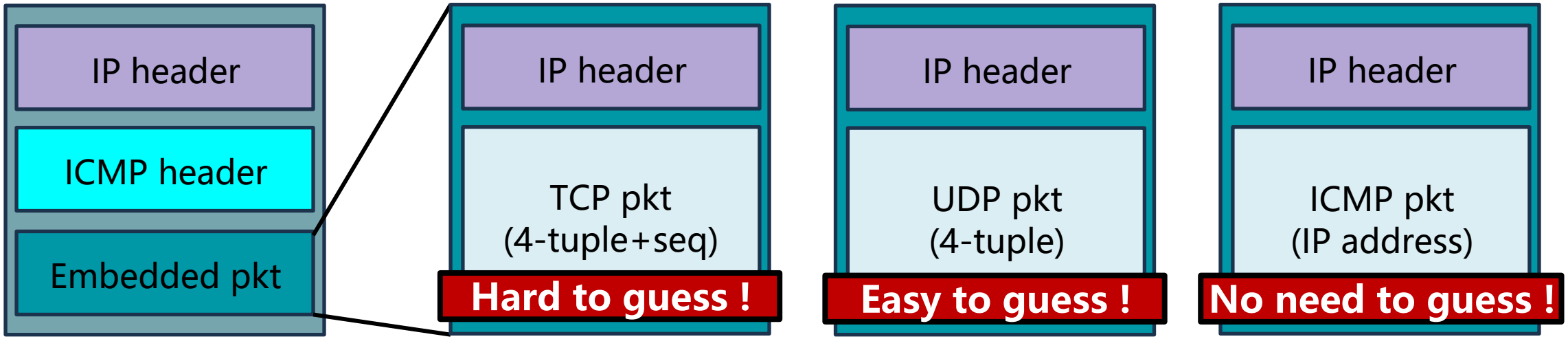
IETF 123, July 2025, Madrid

Goal

Problem

Current ICMP/ICMPv6 specifications have inherent limitations that allow off-path attackers to forge ICMP error messages.

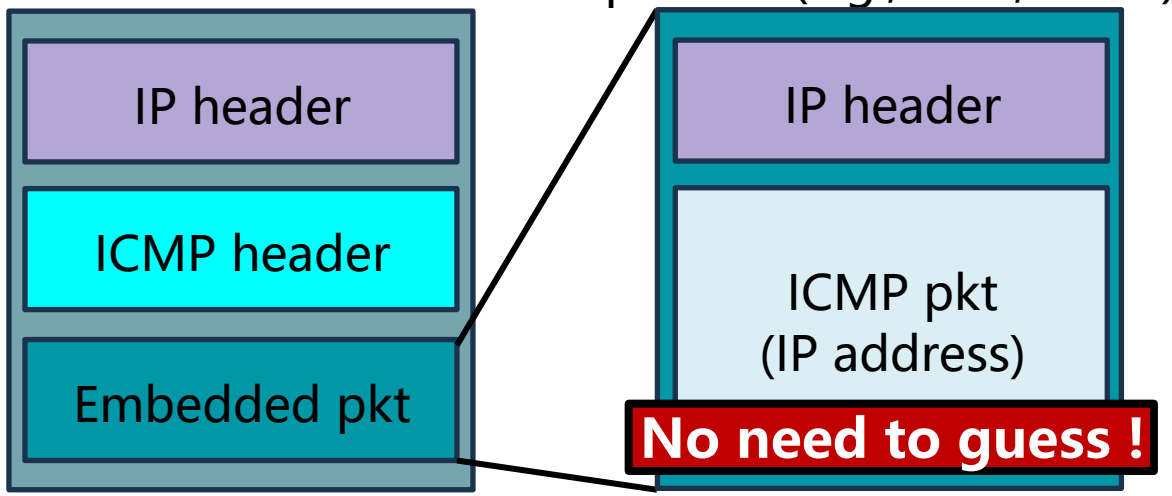
- Check on Embedded Packet is Bypassable
  - For stateful embedded packets (e.g., TCP), **hard to bypass**.
  - For stateless embedded packets (e.g., UDP, ICMP), **easy to bypass**.



Problem

Current ICMP/ICMPv6 specifications have inherent limitations that allow off-path attackers to forge ICMP error messages.

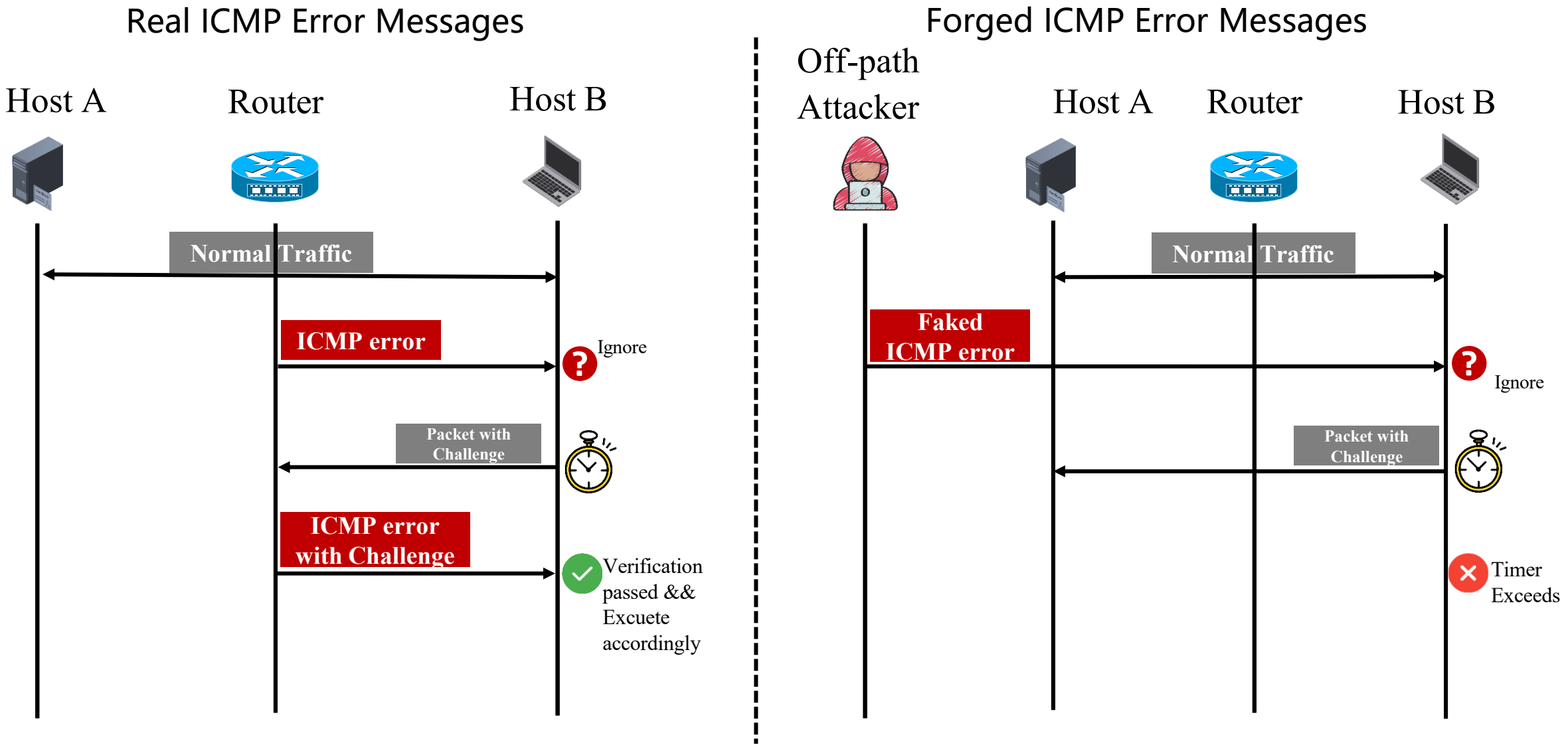
- Check on Embedded Packet is Bypassable
  - ◆For stateful embedded packets (e.g., TCP), **hard to bypass**.
  - ◆For stateless embedded packets (e.g., UDP, ICMP), **easy to bypass**.



Can impact all upper-layer protocols !

We need to design a mechanism to verify the authenticity of ICMP messages!

IETF122: The ICMP Challenge-Confirm Mechanism

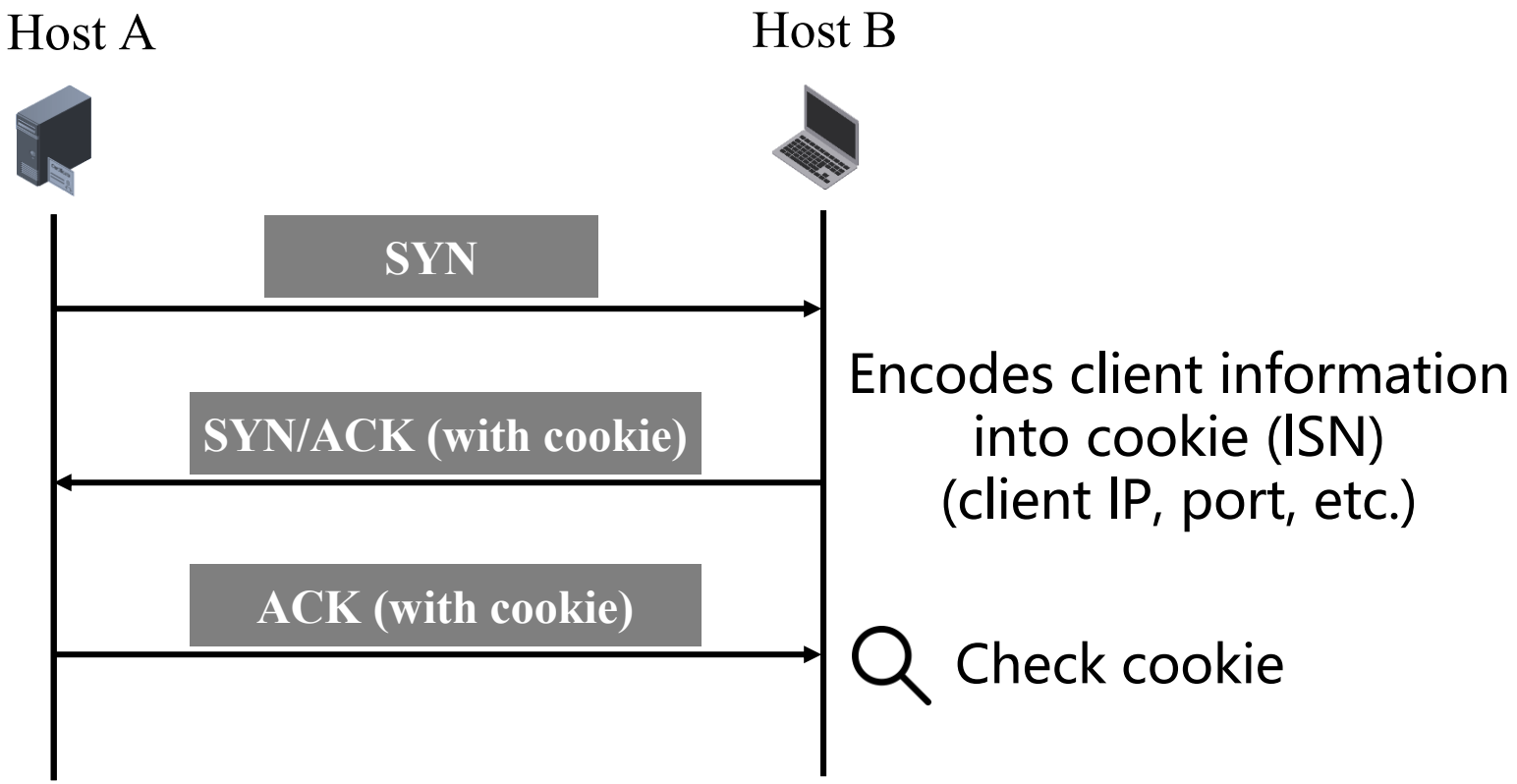


Main Questions

- Question1: Where to store the States, maybe introducing DoS attack?
- Question2: What about amplification Attacks?
- Question3: What if the Challenge or Response packet is lost?

Revised Solution

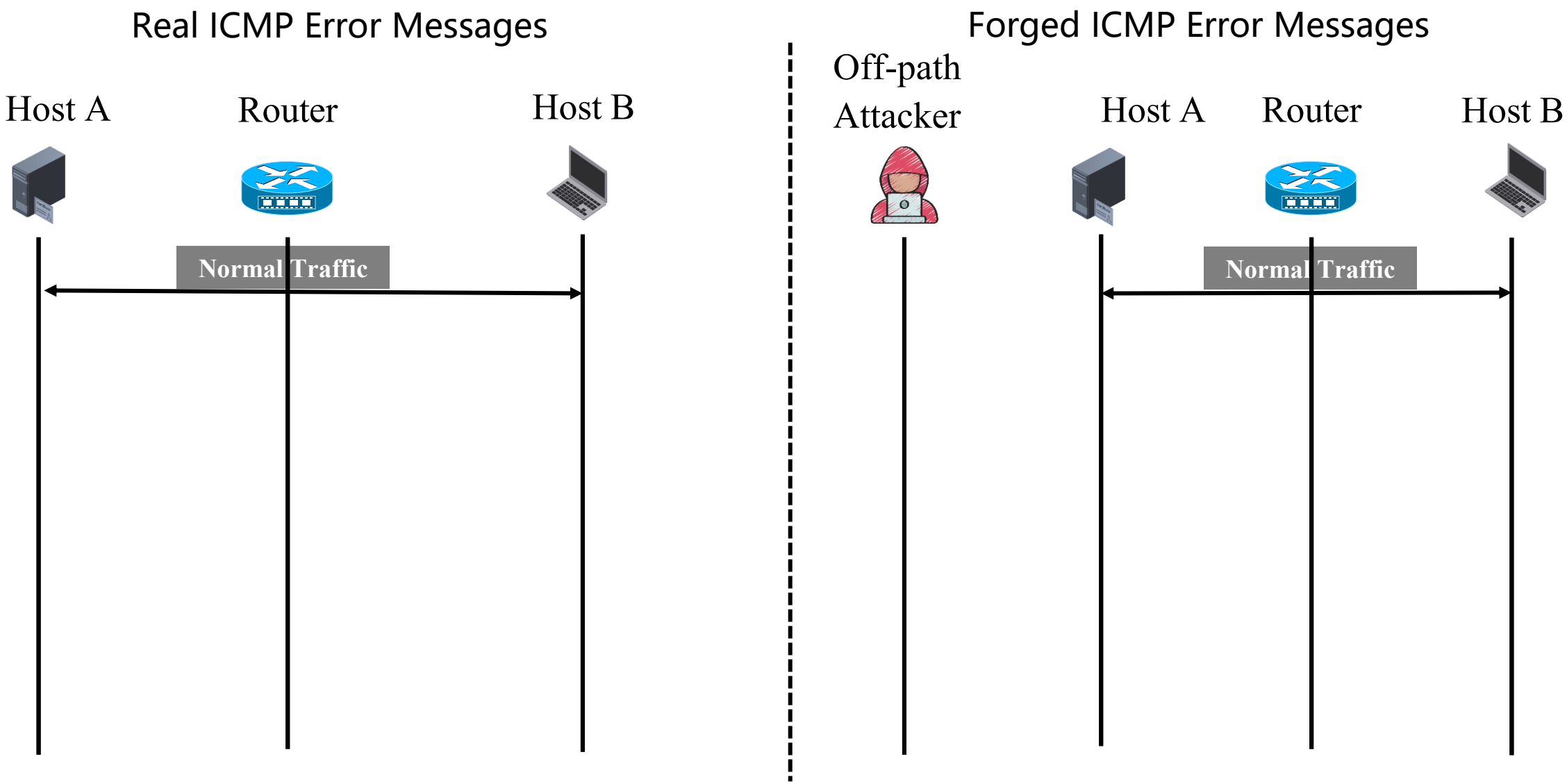
Inspiration: SYN-Cookies



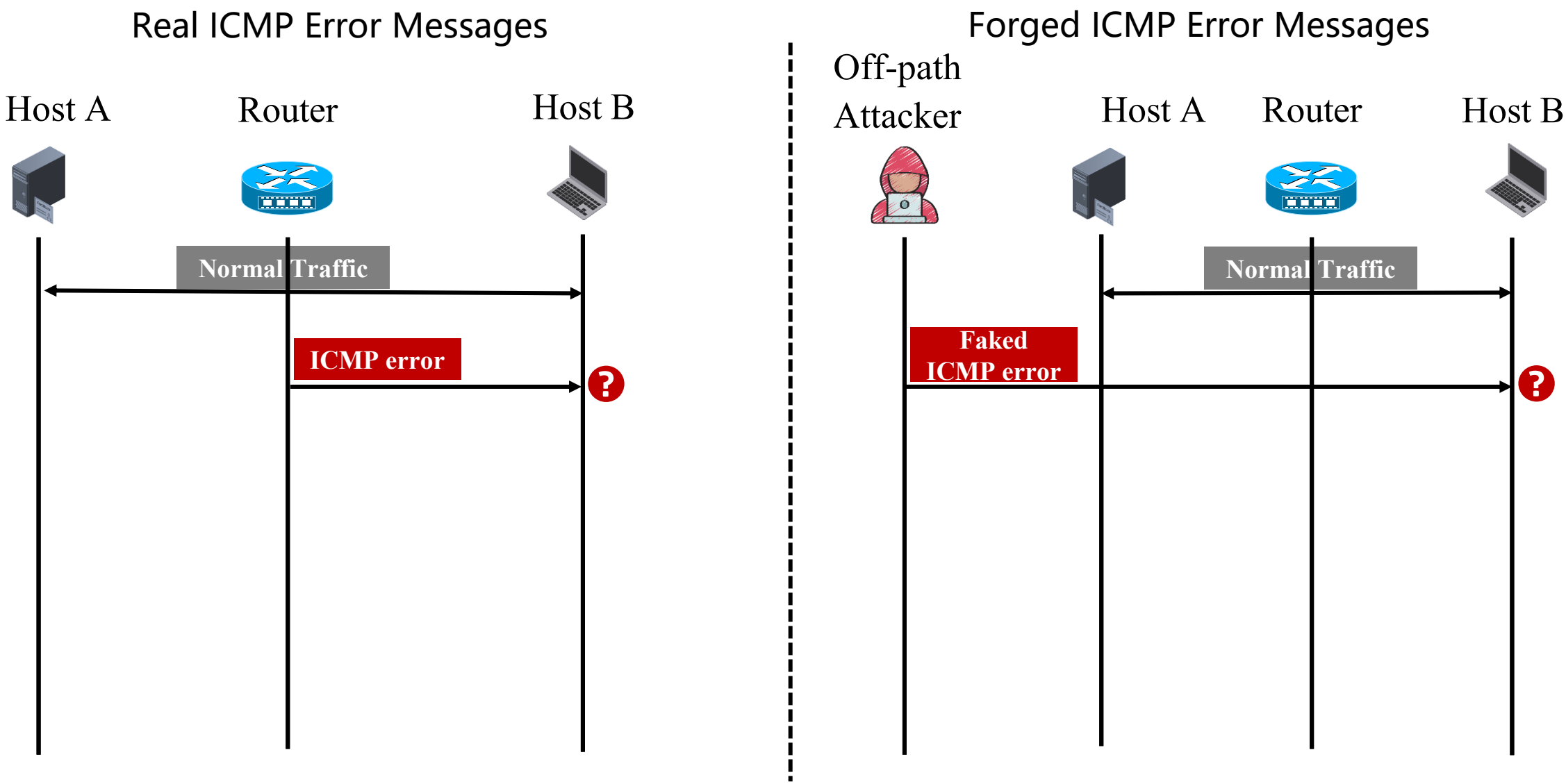
No state of the client is kept in memory

Can we design a similar mechanism to calculate the challenge instead of directly storing the random number?

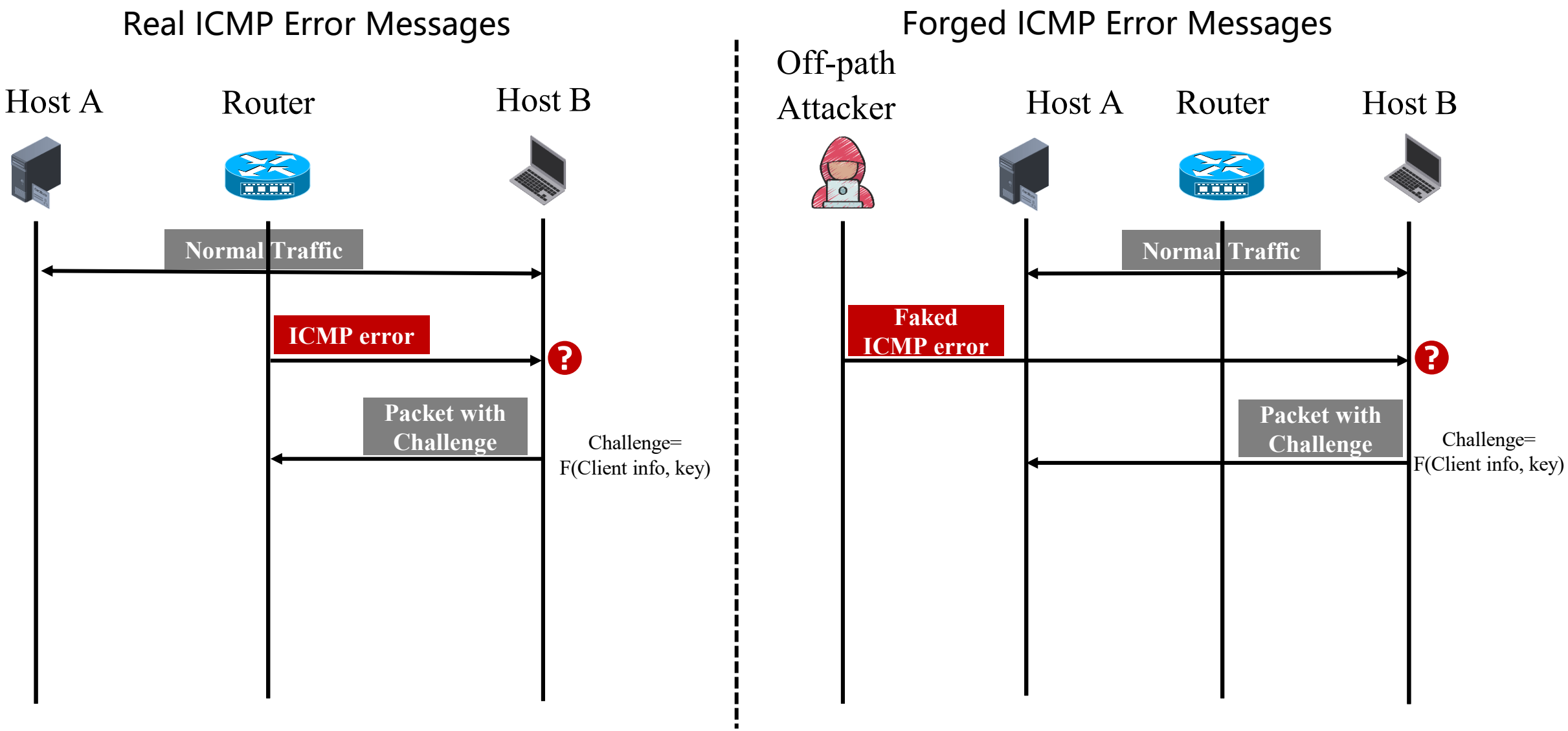
Stateless Challenge-Confirm Mechanism



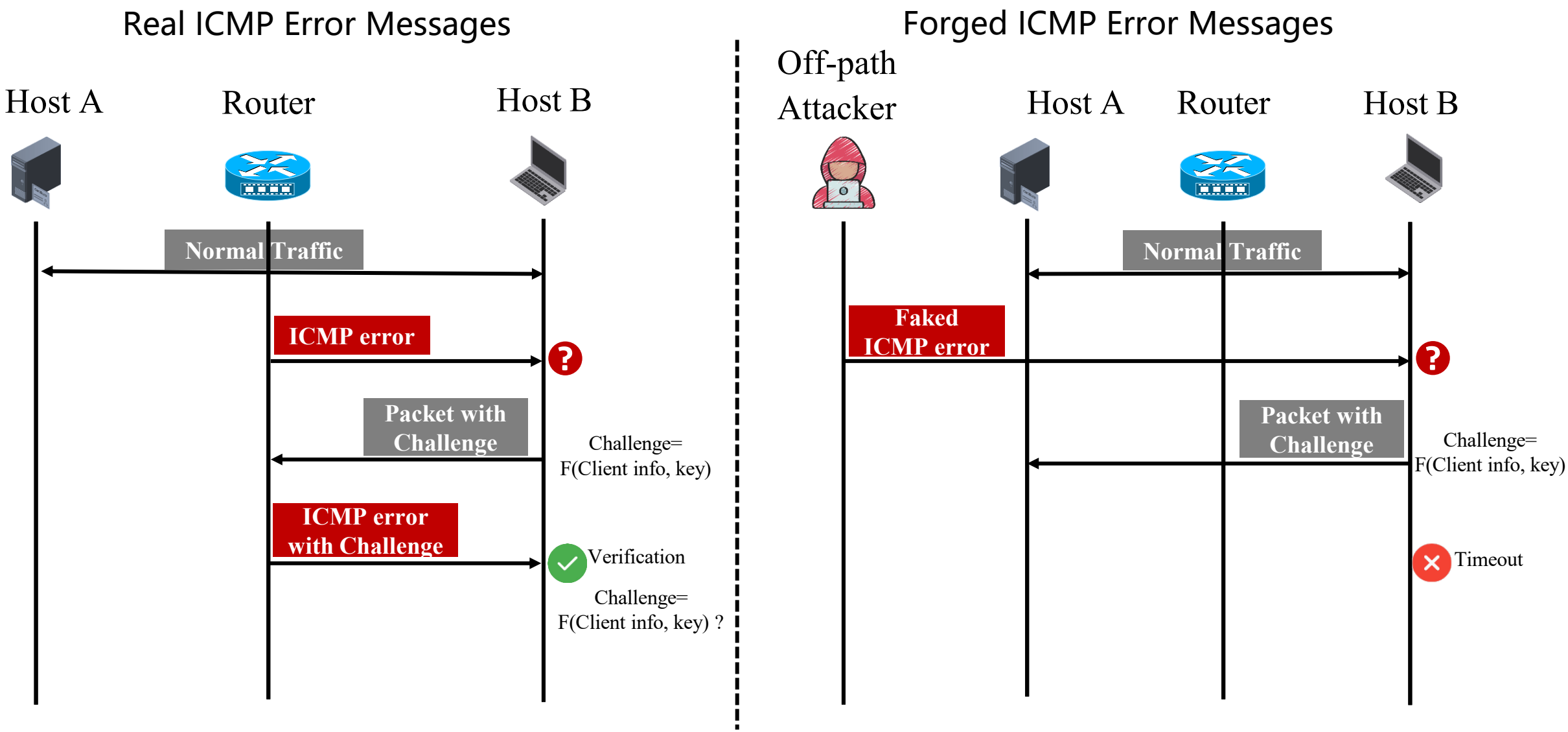
Stateless Challenge-Confirm Mechanism



Stateless Challenge-Confirm Mechanism



Stateless Challenge-Confirm Mechanism



Response to Questions

- **Question 1: State Storage**
  - **Eliminated**: The SYN-cookie style challenge generation method directly eliminates the need for random number storage.

- **Question 2**: **Amplification Attack**
  - **Not So Much**: Challenges are carried in next packets being sent, the only extra overhead is an IP option.

- **Question 3: Packet Loss**
  - **Rare**: We conducted tests on cloud servers in multiple countries and regions and found that no server directly filter packets with challenges.

Next Step

- Collaboration is welcome!
- Your comments and suggestions are welcome

Thanks!