On Path Validation and a Possible Solution

draft-liu-on-network-path-validation-00

OPSEC Meeting @ IETF 117, July 2023

Chunchi Liu (Huawei)

Contents

- Why do we care about Path Validation? What is Path Validation?
- Use Cases
- Our solution based on **Vector Commitments**
- Call for collaboration

Why do we care about path validation?

Routing Security Attacks

- **Routing Hijack**
- **Route Injection**
- **Route Leak**
- **Denial of Service**

Foster

Mitigate

Secure route propagation and authentication in the control plane

- **BGPSec**
- **RPKI**
- **…**
- **Is it enough?**

Cannot guarantee the planned path is *actually* used

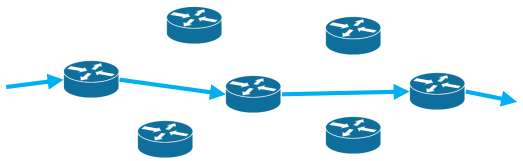
Provide transit proof to complement

Enforcing and verifying the correct transit of traffic in the data plane

- **Path Validation**
- **draft-ietf-sfc-proof-of-transit**
- **…?**

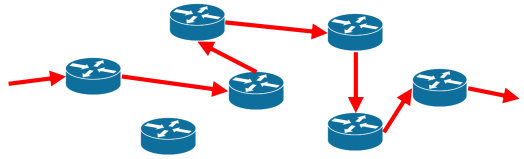
- Path Validation makes sure **the path we chose is the *actual* path the traffic travels on top of.**

The desired path



≠

The actual path

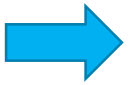


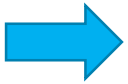
What is Path Validation?

- Path validation "**ensures**" data packets to strictly travel on top of a chosen network path in the data plane.
- Path = designated **nodes** *in* specified **order**

Goals:

1. **Enforce** traffic to follow the path
2. **Validate** traffic indeed traversed the path



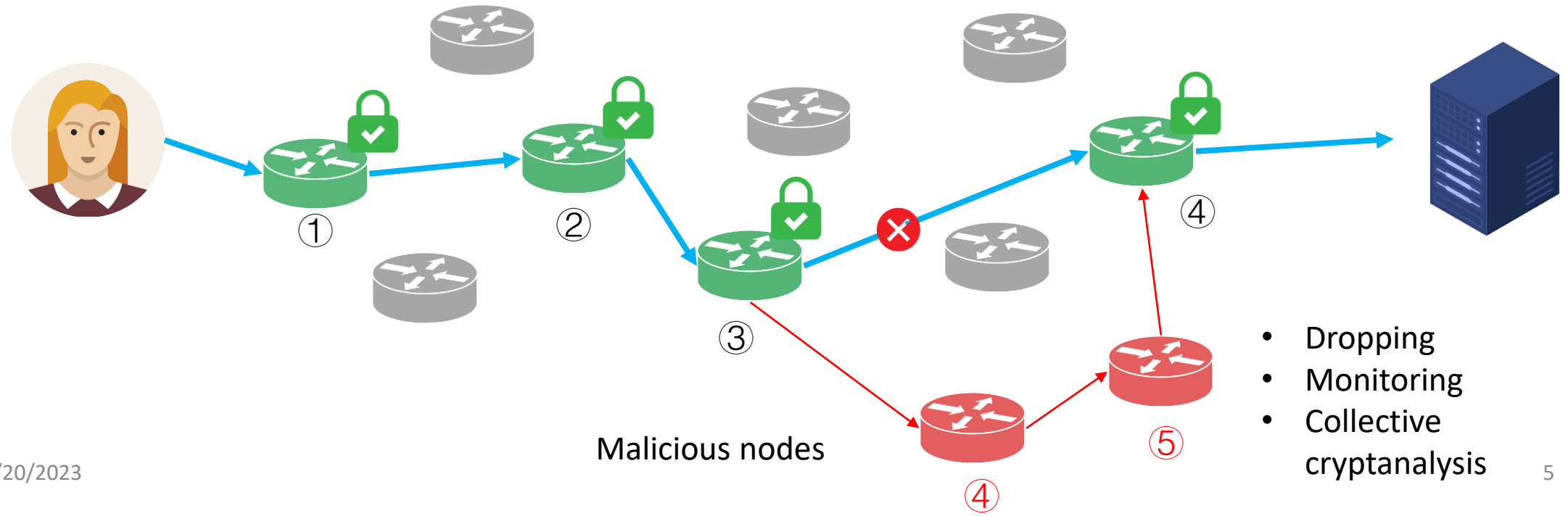


Auxiliary Data in Packet:

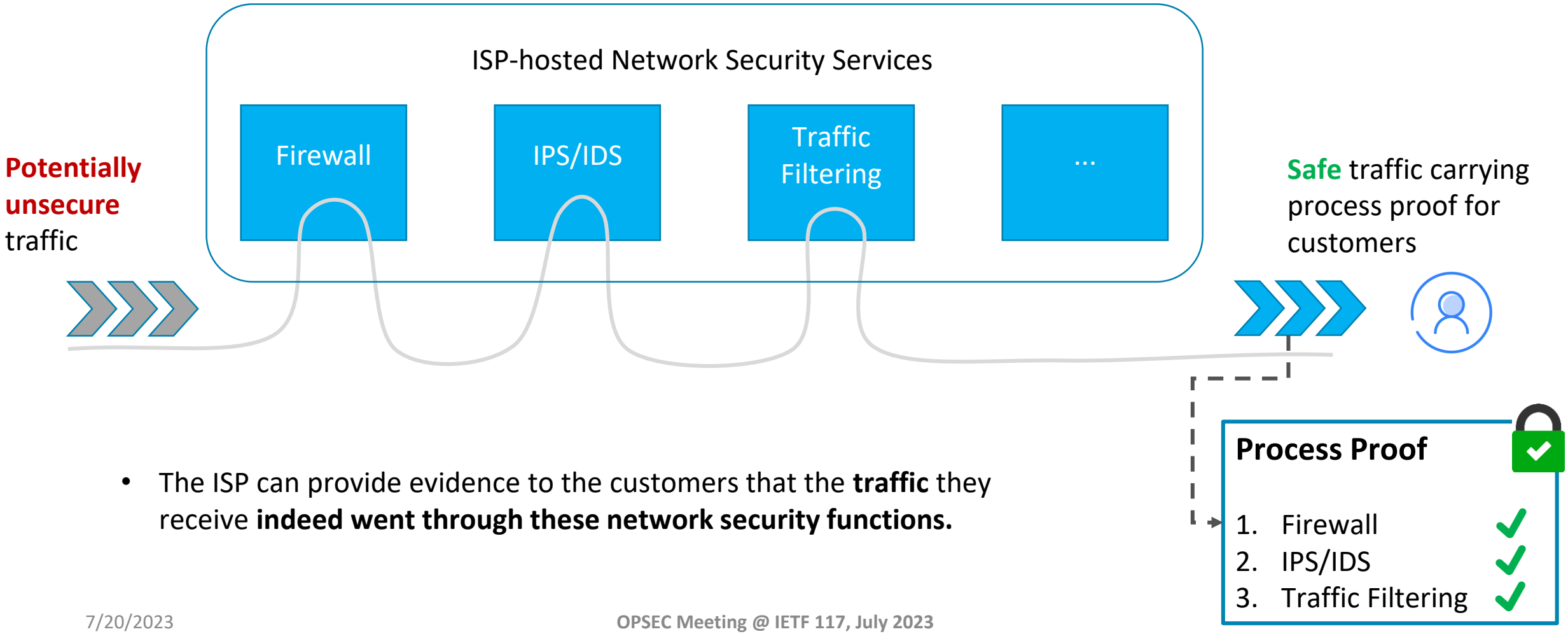
1. **Routing Directive** steers packet forwarding
2. **Transit Proof** logs packet transit history

In Internet routing, the *actual* path the traffic took may **not** be the path we *planned*

- Alice is having a **confidential** business video meeting or VOIP call.
- She doesn't want any data of this connection be detoured and monitored.



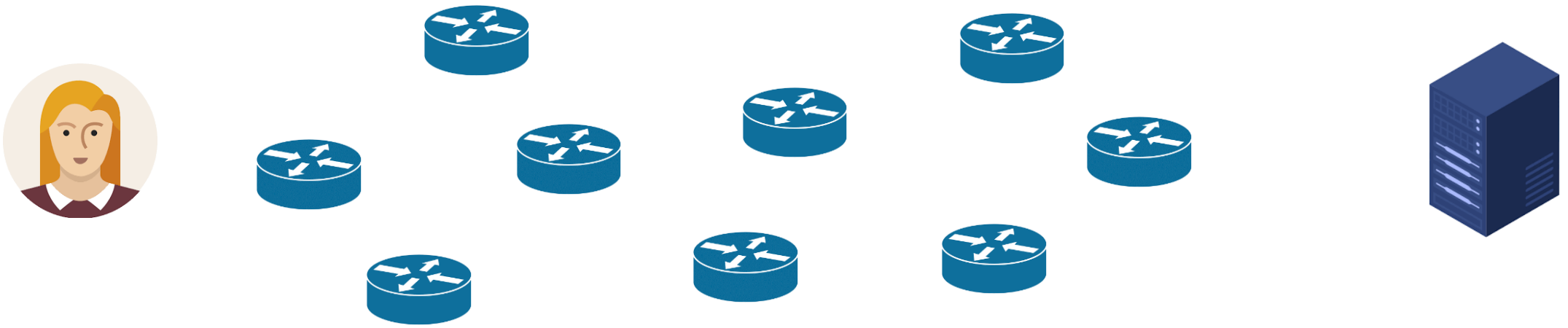
In SFC scenario, proving traffic are ***actually*** processed by our ***planned*** network security service functions



- The ISP can provide evidence to the customers that the **traffic** they receive **indeed went through these network security functions.**

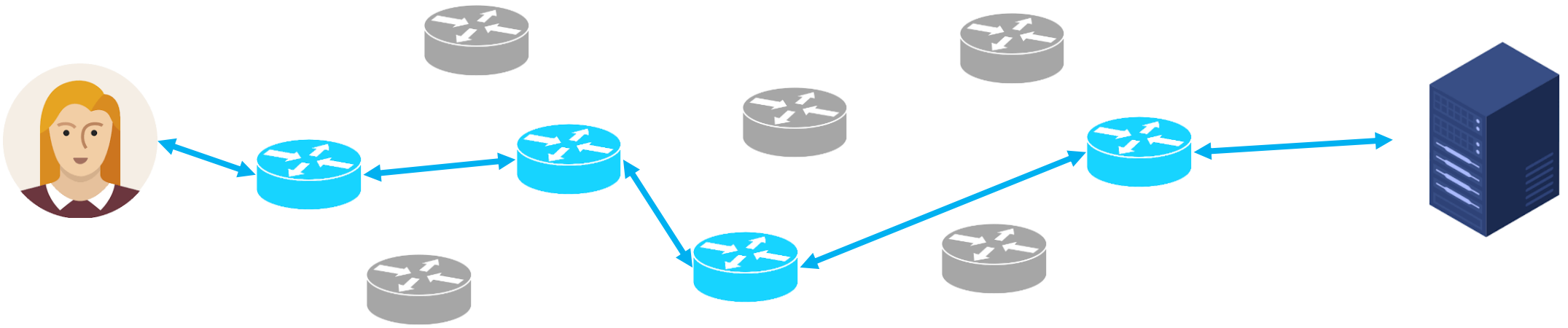
Another Use Case: Proof of SLA connection

- Say Alice purchased a premium Internet plan from ISP A.
- Different E2E connections have different SLA levels.



Another Use Case: Proof of SLA connection

- Say Alice purchased a premium Internet plan from ISP A.
- Different E2E connections have different SLA levels.

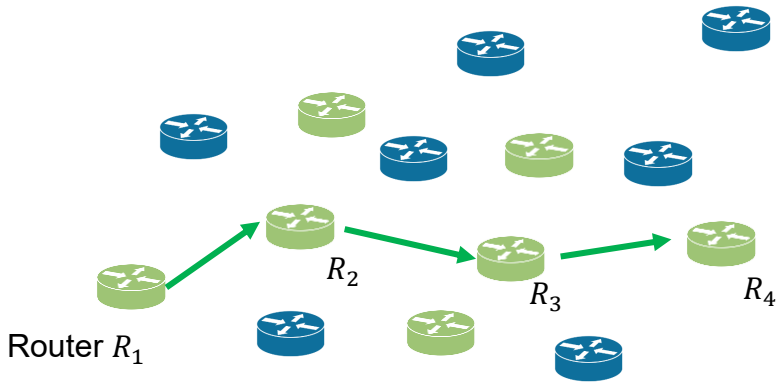


- We **prove** to Alice that her connection was provided by **premium nodes** only.

A Graphical Overview of the VC-based Path Validation Solution

✓ Security

- **Position-binding property**: Transit proof P_i successfully passes verification *iff* it was created by the **right node** n_i at the **right position** i **as previously committed**

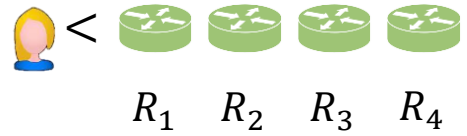


✓ Advantages

- **Efficient:** Proof creation and verification takes **O(1) time**
- **Succinct:** Transit proof and commitment is **O(1) size**
- **Batch-proof** friendly (same efficiency)

Stage 1: Compute Reference Value

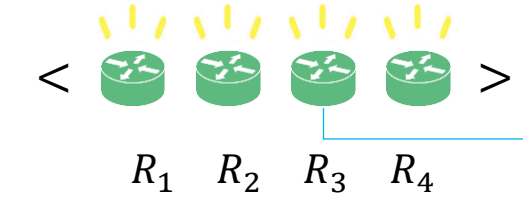
Network Controller



Output 1 **Commitment** → C

- **Controller** selects a path
- Computes a **commitment**

Stage 2: Generate Transit Proof



Output 2 **Transit Proof** → P_i

- **Router** R_i forwards data
- Computes his **transit proof** P_i

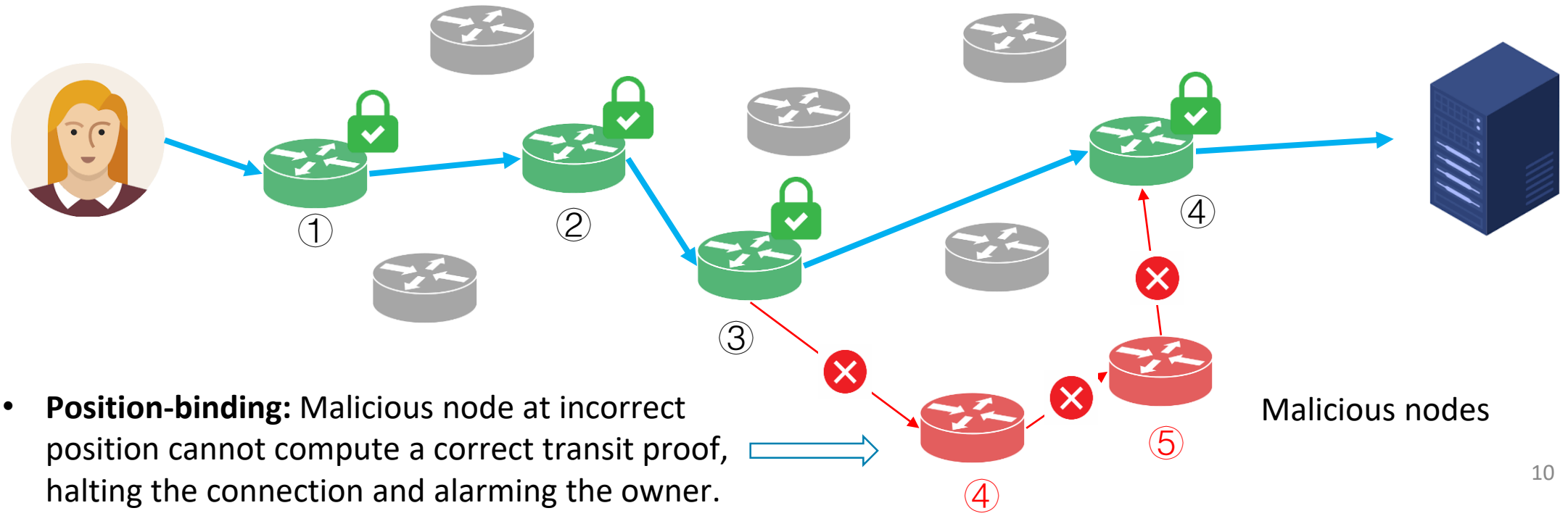
Stage 3: Verification

$$Verify(C, P_i) =^{?} 1$$

- **Observer** verifies P_i against C to check if it was the correct router in correct position.

Anti-detour security-sensitive communication

- Alice is having a **confidential** business video meeting or VOIP call.
- She doesn't want any data of this connection be detoured and monitored.



- **Position-binding:** Malicious node at incorrect position cannot compute a correct transit proof, halting the connection and alarming the owner.

Malicious nodes

Looking for collaboration

- We look for collaborators together to:

1. Work on the draft
2. Extending to various of data plane protocols
3. Joint research
4. Joint PoC implementation and very hopefully, deployment test

On Path Validation and a Possible Solution

Thank you! Quesitons?

draft-liu-on-network-path-validation

OPSEC Meeting @ IETF 117, July 2023

Chunchi Liu (Huawei) liuchunchi@huawei.com

liuchunchi.com