Secure Routing Path Considerations

China Mobile

Meiling Chen

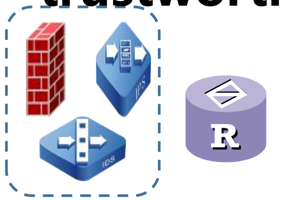
Traditional routing security VS new requirements

- **Traditional** routing attack: Traffic misdirection due to disturbance of routing information propagation
  - Assumption: All devices in a limited domain are trusted; All devices in Internet are untrusted
  - Solution:
    - Limited domain → Intrinsically secure, no additional approaches;
    - Internet → Intrinsically insecure, best effort + announcement security approaches (BGPSEC) ➔ no guarantee of each device's forwarding decision and cumulative forwarding result.

- **New requirements** for routing security: Routing data only on top of trusted/secure devices
  - Assumption: Device trustworthiness is decided by Remote Attestation Procedures (RATS WG)
  - Goal: Dependable forwarding hop-by-hop
  - How?: Routing data only on trusted devices, regardless of domains they are in. Perceive device and path trustworthiness and make routing decisions.

Security requirement of Secure Routing

Node trustworthiness



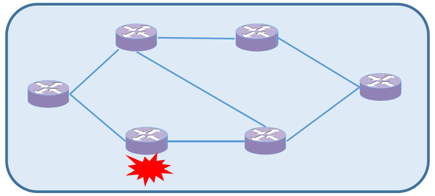
Device&SecFunction Pool

static security

① Is the node dependable/secure or not?

② Does the node have security capabilities or not?

Path computation and orchestration



Network operator

dynamic security

① Is the path dependable/secure or not?

② Is the path have the capabilities to Anti-Cyberattack?

Data Plane Forwarding Auditing/Visibility

Customer

validation

① Is the actually-taken path consistent with the orchestrated path?

② Is the security capabilities/properties consistent with the demand?

	Node trustworthiness	Path computation and orchestration	Data Plane Forwarding Auditing/Visibility
Participant	Cisco、Juniper、China mobile	China mobile、Fujitsu、Cisco、Huawei	Cisco、Huawei
Document	draft-chen-atomized-security-functions draft-chen-idr-bgp-ls-security-capability draft-liu-nasr-requirements	draft-liu-nasr-architecture draft-voit-rats-trustworthy-path-routing Bof: Trust-enhanced networking	draft-liu-path-validation-problem-statement draft-liu-on-network-path-validation draft-ietf-sfc-proof-of-transit

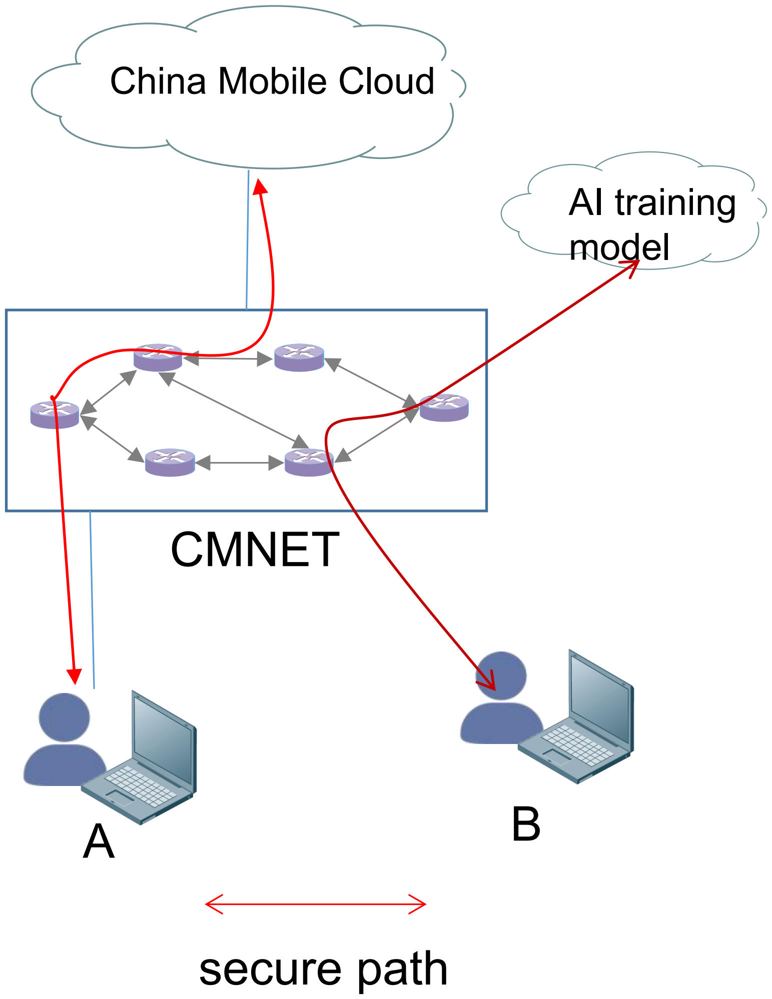
Why routing path needs to be more secure?

Use case for mobile cloud users and AI big model users

- Sensitive user data store in the cloud
- AI large models store in external server

Security requirements

- Data cannot be leaked
- Data not going abroad



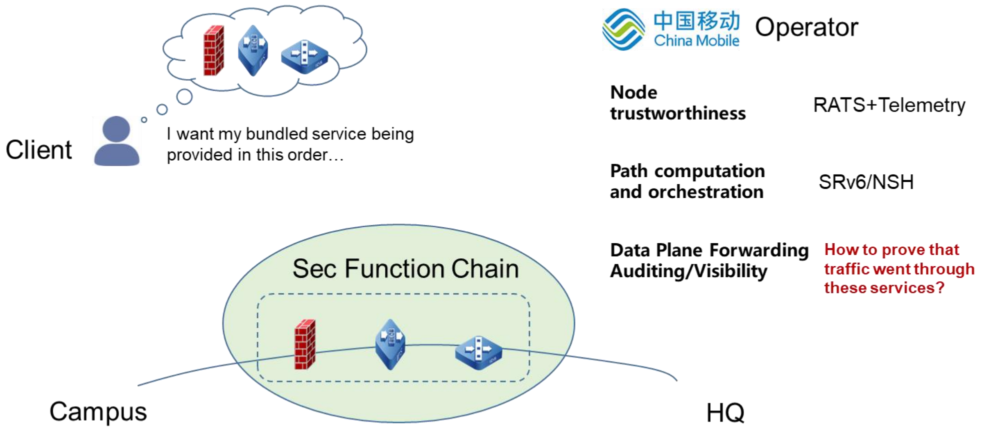
Needs

1. Generate a trustworthy, secure, and controllable forwarding path which can prevent data leakage.
2. Path attestation procedures to prove the path is indeed trustworthy.

Use Cases

Network Path Validation: SFC

- Pass through each security function in sequence

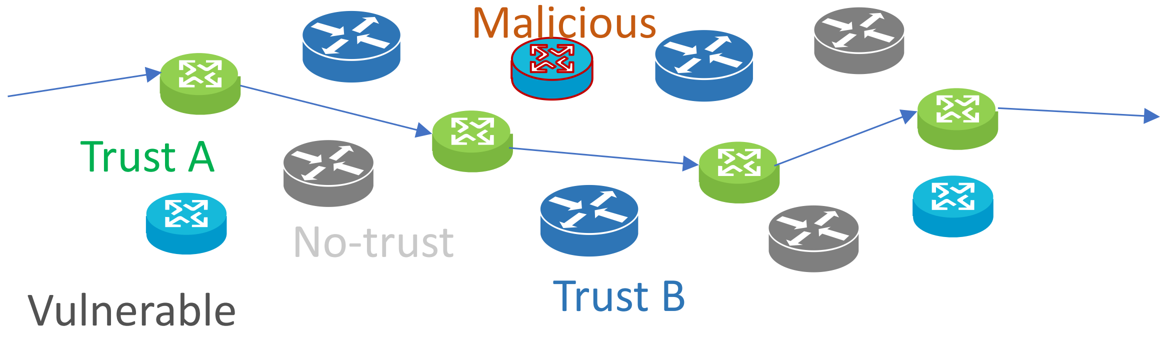


Needs

Orchestrate a path in order and prove the traffic went through these services.

Network Path Validation: Devices with high security guarantees

- Select a trusted path with all trusted nodes



Compute a forwarding path with high security requirements.

Thanks!