Secure Routing Path Consideration

China Mobile

Reason of routing attack

Routing system is important infrastructure in Internet.

There are several routing attack incident towards network operators, cloud service providers and Internet content providers all over the world these 10 years.

Routing attack is a network attack method,hackers modifying the transmission path of network traffic by deceiving network devices such as routers and switches, as a result of controlling the path and destination of network traffic.

Reason of routing attack

① Router is not securely booted

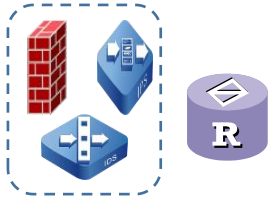
②No pre-designed secure path

③No defense mechanism during the routing process

④ No validation mechanism for the selected path

Security requirement of Routing

Node trustworthiness



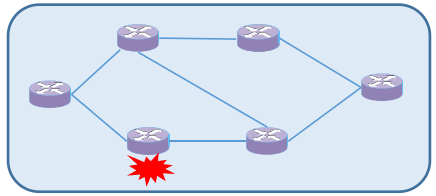
Device&SecFunction Pool

static security

① Is the node dependable/secure or not?

② Does the node have security abilities or not?

Path scheduling



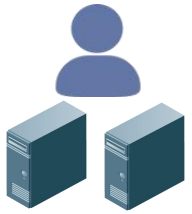
Network opeartor

dynamic security

① Is the path dependable/secure or not?

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

Path Validation



Customer

close-loop validation

① Is the selected Path consistent with the designed path?

② Is the security abilities consistent with the demand?

Participant	Cisco、Juniper、China mobile	China mobile、Fujitsu	Huawei
Document	draft-voit-rats-trustworthy-path-routing draft-chen-atomized-security-functions draft-chen-idr-bgp-ls-security-capability	draft-chen-secure-path-architecture Bof: Trust-enhanced networking	draft-liu-path-validation-problem-statement draft-liu-on-network-path-validation

Architecture of secure path

Introduction of secure path

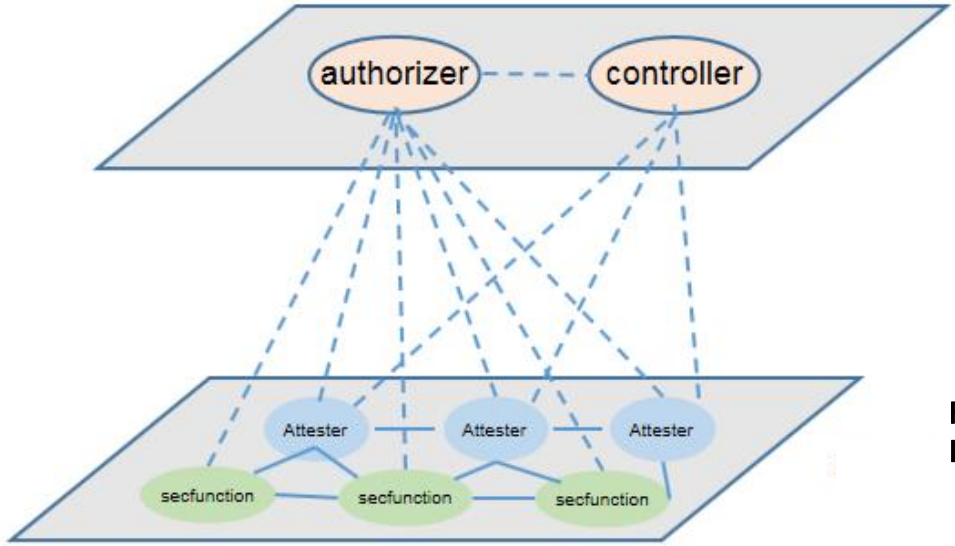
① Problem

No correlation between routing and security resources

② Consideration

Add security factors to routing scheduling

Architecture of secure path



Four roles

- Attester (Router) : Forward user traffic and produce evidence of its own trustworthiness
- Authorizer: verify the claim of attester
- Controller: Generate routing path
- Secfunction: provide security service

Introduce security factors into the routing domain and allocate security resources in the process of routing through unified control and scheduling to meet① routing path security itself ② users security requirement for routing.

Protocol related consideration

① **BGP:** Trustworthiness and security factors collection between Routing nodes by extending the BGP protocol

② **BGP-LS:** Trustworthiness and security factors collection by authorizer and controller by extending the BGP-LS protocol

③ **SRV6:** scheduling routing paths through programming

④ **Restful/yang:** Collect JSON messages carrying security resource information through the restful protocol interface

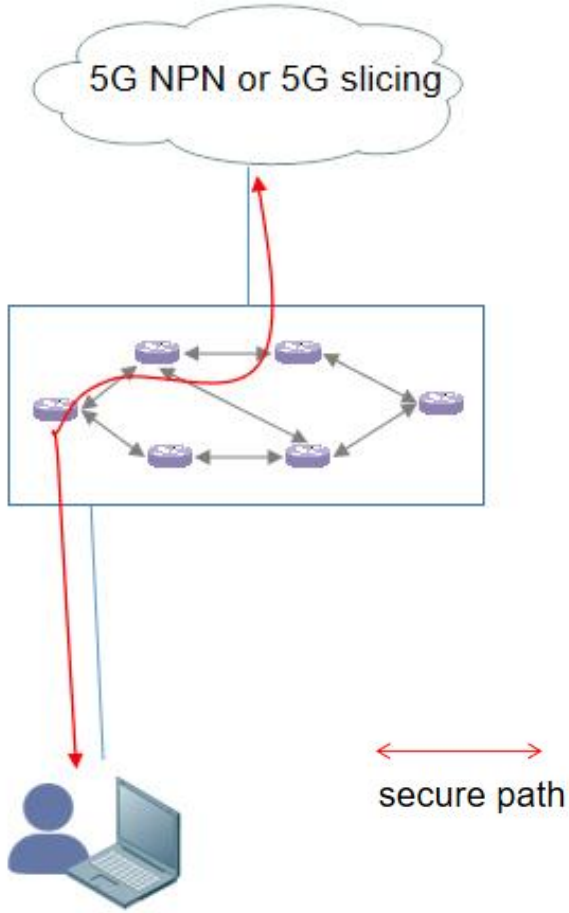
⑤ **Netconf/yang:** Distribute Yang model security policy configuration through the Netconf protocol

⑥ **SFC/SRv6/IOAM:** Extend communication protocols and header data structure to achieve consistency verification of paths and security capabilities

Why routing path needs to be more secure?

Use case for 5G non-public network or 5G network slicing

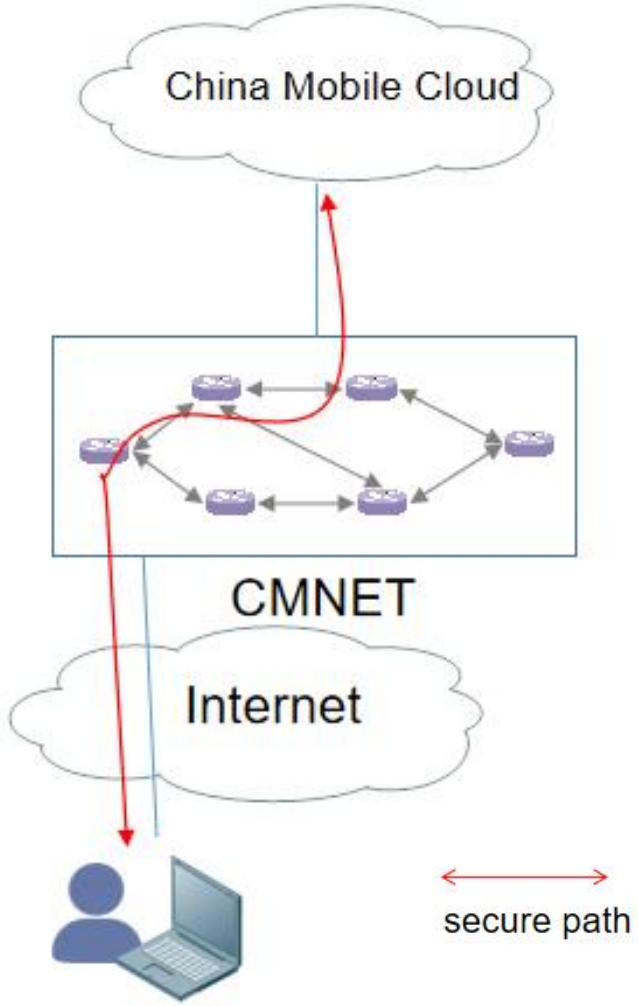
- NPN or 5G slicing vertical users such as bank, stock exchange, electric power company may have requirements on the turstworthiness and anti-attack abilities of the link
- Construct a trusted routing link which meet the customer’s security requirement



Why routing path needs to be more secure?

Use case for mobile cloud users

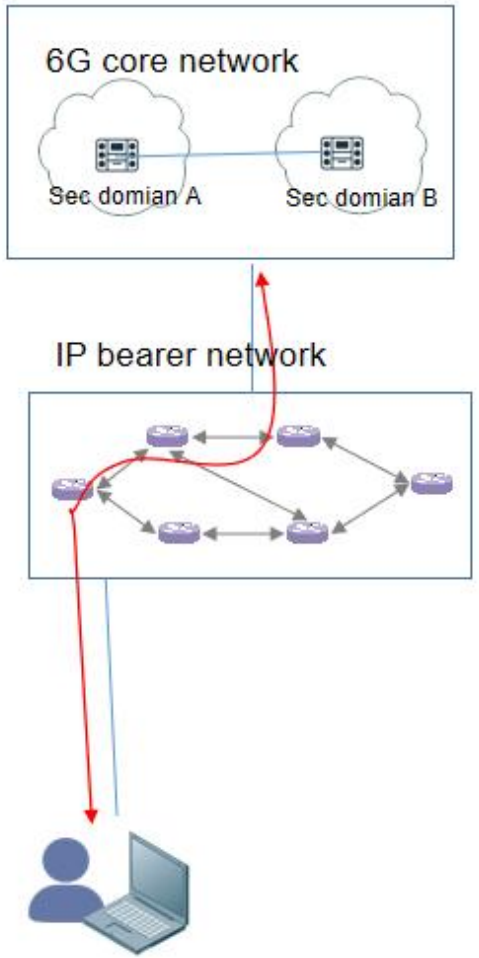
- Sensitive user data store in the cloud
- Users may need high level security protection for the routing link to access to sensitive user data



Why routing path needs to be more secure?

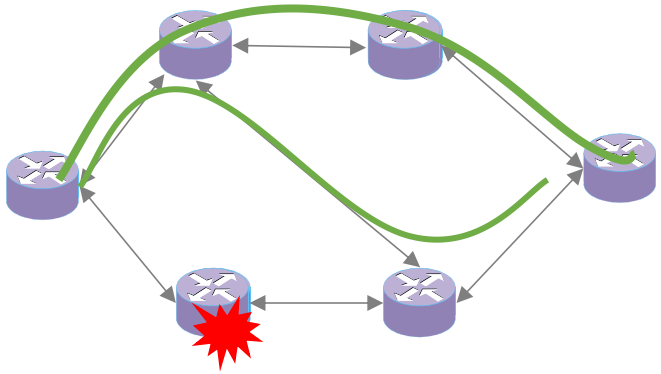
Use case for 6G Distributed Autonomous Network

- 6G core network functions can autonomously find other network functions to communicate
- These 6G NFs may belongs to different security domian and have different security level
- Built-in security in IP bearer network is needed



How to make the routing path more secure?

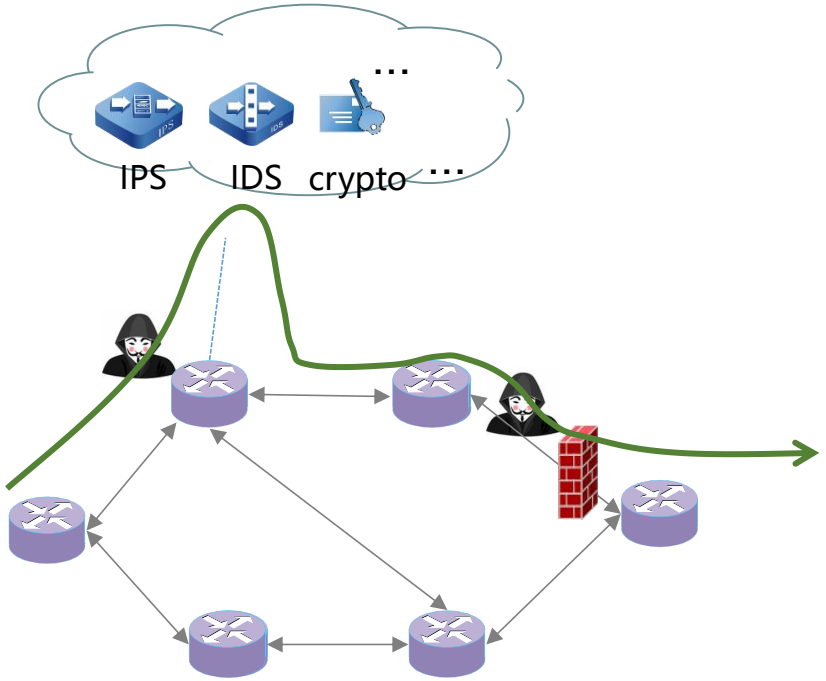
method1: Form secure path



Scheduling routing link with the consideration of :

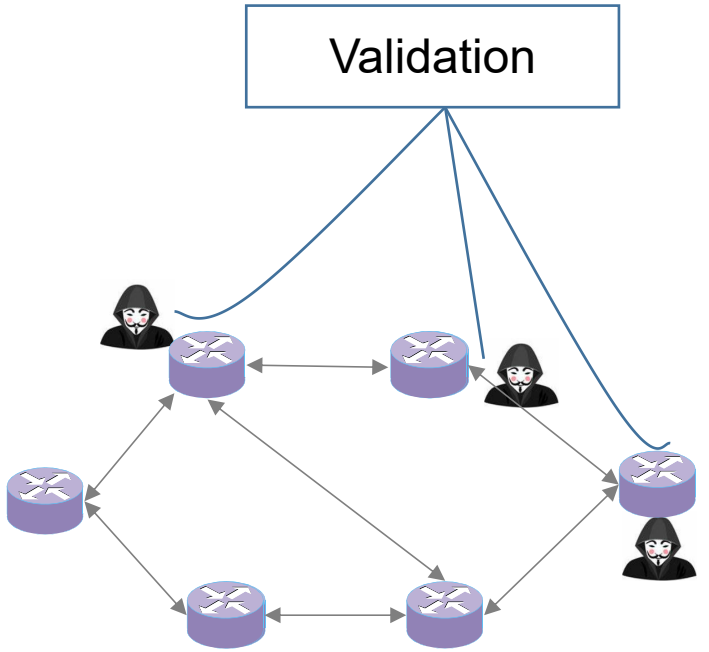
- Attestation of node trustworthiness
- Attestation of node security capabilities

method2: Dispatch security resources



- Dispatch security resources to address the weaknesses of vulnerable network nodes and then ensure network availability;
- Provide dynamic security defense during traffic forwarding for traffic attack sensitive customers

method3: Path validation



Path validation can be used to

- identify the authenticity of the selected path
- indentify the vulnerable nodes of the path

Thanks!