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

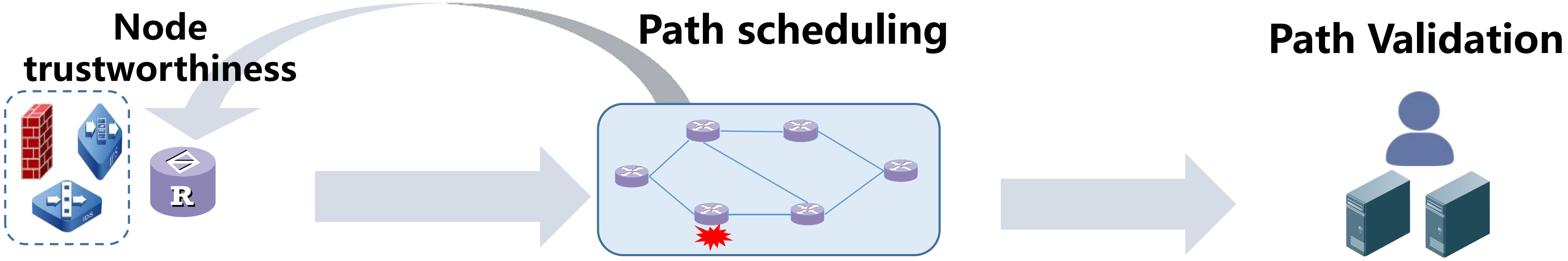
① Router is not securely booted

② No defense mechanism during the routing process

③No pre-designed secure path

④ No validation mechanism for the selected path

Security requirement of Routing



Node trustworthiness

Path scheduling

Path Validation

Device&SecFunction Pool

Network opeartor

Customer

static security

dynamic security

close-loop validation

① Is the node dependable$secure or not?

② Does the node have security abilities or not?

① Is the path dependable$secure or not?

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

① Is the selected Path consistent with the designed path?

② Is the security abilities consistent with the demand?

Parttticipant	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

Goal: By introducing security factors to protect the security of routing, ensure the security of user traffic forwarding during the whole lifecycle

Architecture of secure path

Introduction of secure path

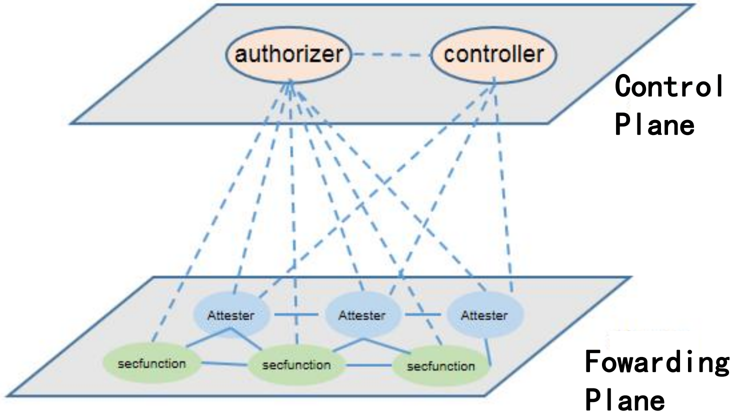
① Problem

No correlation between routing and security resources

② Consideration

Add security factors to routing scheduling

Architecture of secure path



Four roles

- Attester: 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.

Related protocol

① **BGP:** Trustworthiness and security factors collection between 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

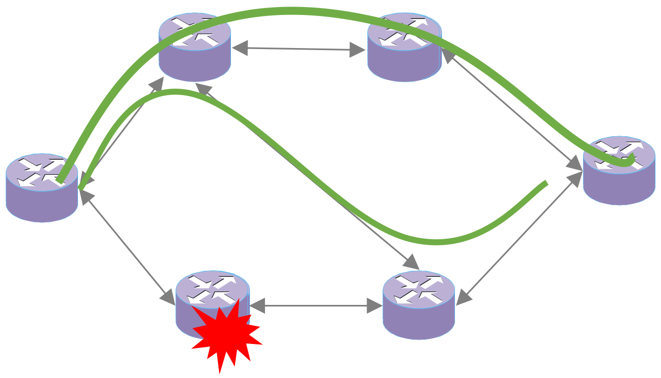
④ **Restful/yang:** Collect JSON messages carrying security resource information through the restful protocol interface

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

Use case of Secure path/Path validation

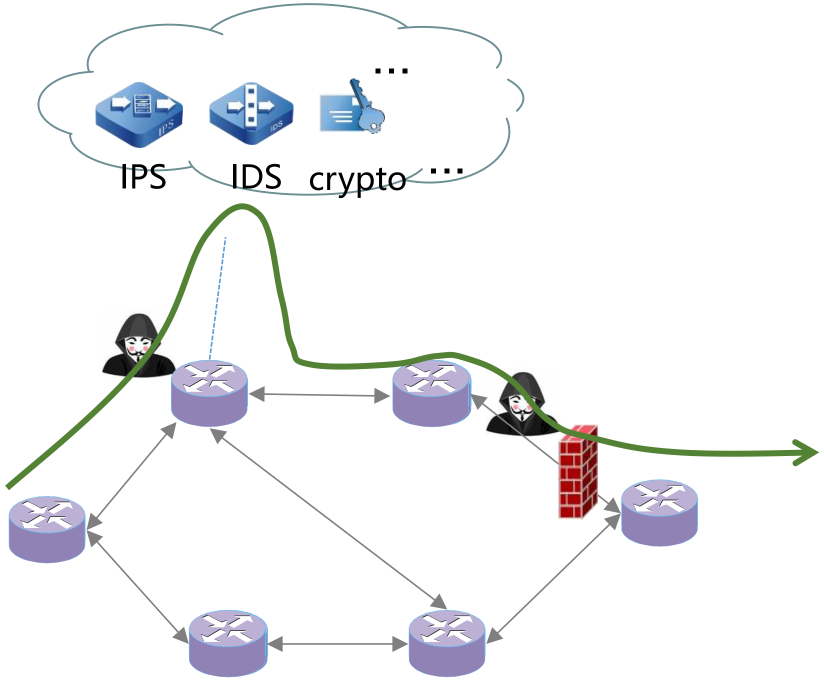
method1： Form secure path



Use cases for method 1：

- For different security domain of operator network
- For non-public network, construct a trusted routing link which meet the customer’s security requirement

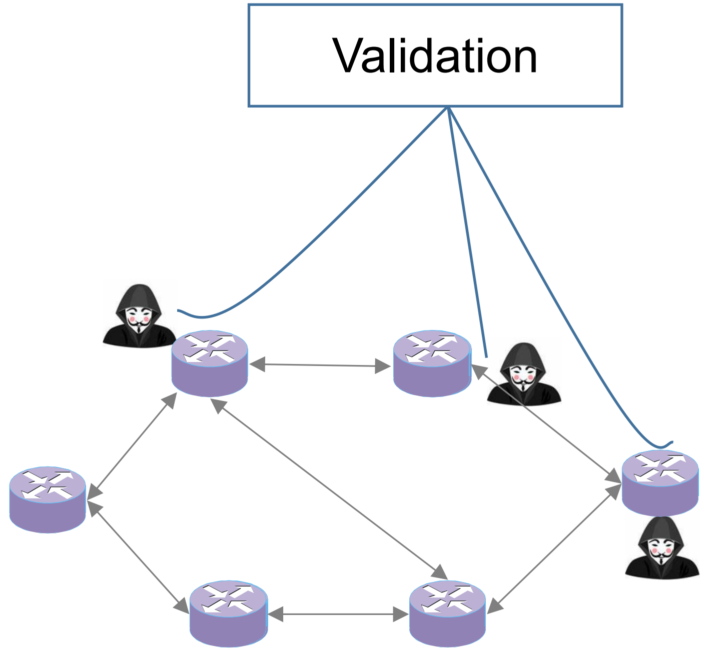
method2：Dispatch security resources



Use cases for method 2：

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

method3：Path validation



Use cases for method 3：

- Path vealidation can identify vulnerable nodes to improve network maintenance security