SRH and IP header protection

draft-chen-spring-srv6-SRH-security-00

IETF111-2021-Spring

Meiling Chen /China Mobile

Objective & Contents

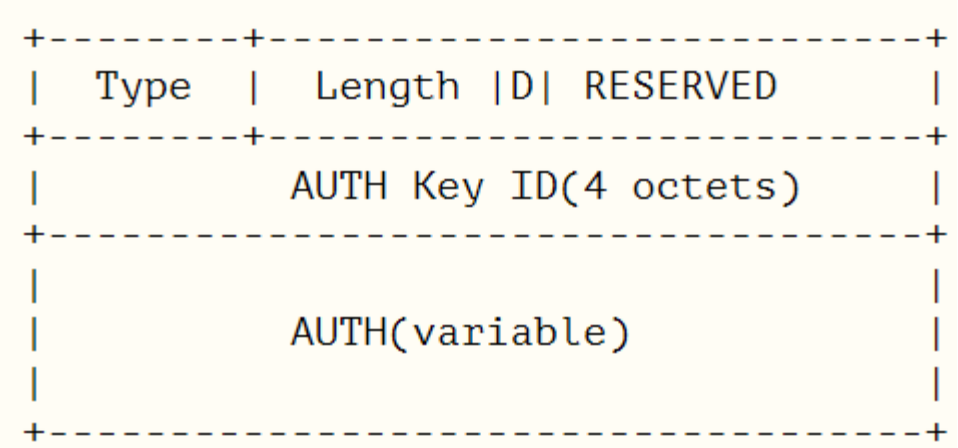
- **Objective**

-an method for Segment Routing Header protection

- **Contents**

- New TLV Type for Signature
- Signing and verifying process
- Optimization process

New TLV Type for Signature(Auth TLV)

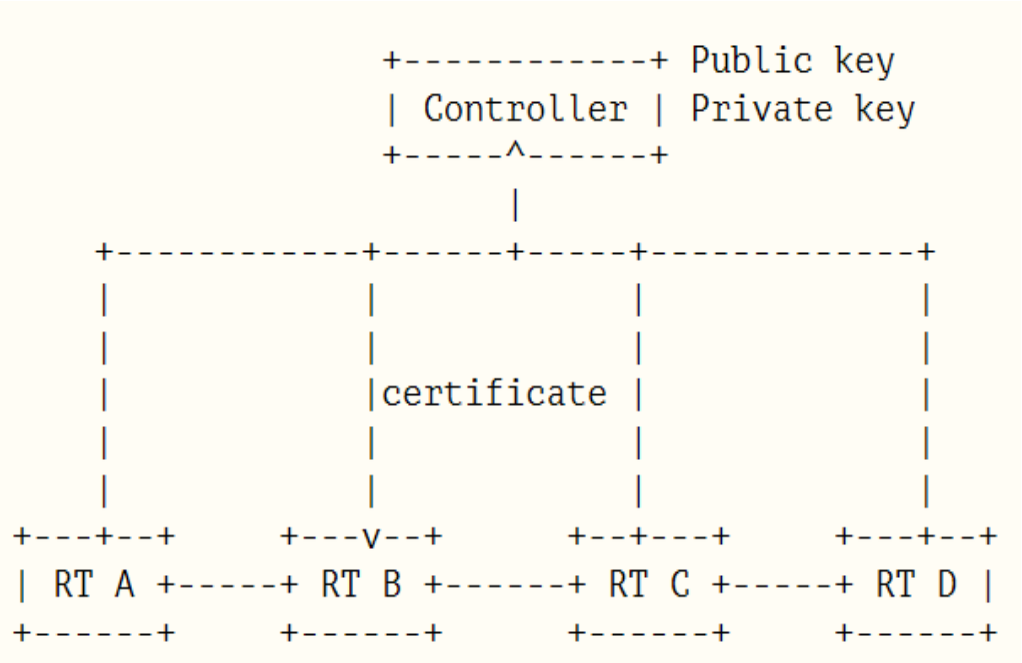


1. A a new type of TLV is defined and the type is 6 which called Auth TLV.
2. The TLV is used for signature protection based on asymmetric secret keys.
3. The AUTH TLV is used to protect IPv6 source address, SRH header.

•AUTH Key ID: A 4-octet opaque number that uniquely identifies the hash algorithm, signature algorithm, and certificate serial number used for signature authentication.

•AUTH: the content of the signature that protects the field, in multiples of 8 octets, at most 32 octets.

Signing and verifying process using a new TLV



The signature process is divided into three steps：

•Step1: Preset certificates, include private keys and controller certificates on SRv6 controllers(or source node), and CA root certificates on key network devices;

•Step2: After the secure connection is established between the controller and the network device on the control plane, perform public key certificate distribution and signature algorithm selection, and inform the key node the selection result.

•Step3: SRv6 controller(or source node) uses the private key, the hash algorithm and the asymmetric algorithm selected in the step2 to sign the packet header, and store the signature results in the TLV, finally sends the routing result which include the signature to the source node(or omit this step), the source node wraps and forwards an SRv6 packet with a signature

Signing and verifying process using a new TLV

Signature verification is required at key network nodes, it's also divided into three steps.

- Step1: Enable signature verification at the key nodes.
- Step2: Request a public key certificate from the controller.
- Step3: calculate the hash value according to the header, and use the public key to decrypt the signature in the message, compare the decryption result with the hash value, if verify successful, forward the message, otherwise, the message is discarded.

Verifying optimization process

When asymmetric key is used to verify on the data plane, the processing efficiency of the forward message will be reduced. An efficient hash table for forwarding and signature verification can be considered. When the network node receives SRv6 packets, it does these steps:

•Step1: Calculates the hash value of the message header, look up the local SRv6 hash table.

•Step2: If the same hash value can find in the local hash table, compare the signature in the hash table and the AUTH in the TLV. If they are same， forward the packet, otherwise, discard.

•Step3: If the same hash value can not find, use the public key to decrypt the. And compare the decryption result with the hash value, if verify failed, discard the packet, otherwise, forward the packet and record the hash value and signature in the local hash table.

ToDo

- Is there anyone interested in the draft? We can detail it together.
- Suggestions for the next step of my draft

- Comments and co-authors are welcome!