A Path Verification Solution based on SRv6

draft-jliu-tpp-srv6-00

Brisbane Meeting @ IETF 119, March 2024

Jun Liu
Tsinghua University

Contents

- What is Path Verification for?
- Existing works.
- Path Verification Solution on SRv6.
- Core Use Case.

What is Path Verification for?

- **Packet tampering and source spoofing.**
- **Path deviation.**
  - Router hop pass.
  - Router addition.
  - Out-of-order forwarding.
- **Denial of Service (DoS).**
- **Privacy leak.**

Existing works-Two ways

- **Verifying the planned paths– if it is trusted and authorized.**
  - [ICING] Naous, J., "Verifying and enforcing network paths with ICING", 2011.
  - [OPT] Kim, T H J., "Lightweight source authentication and path validation", 2014.
- **Verifying the traversed paths-if the packet has actually traversed**.
  - [PPV] Wu, B., "Enabling efficient source and path verification via probabilistic packet marking", 2018.
  - [RFL] Wu, B., ”Robust and lightweight fault localization", 2017.

New Challenge: Ensure that the integrity of the original path is not destroyed when the network flow is forwarded by untrusted nodes

Terminology

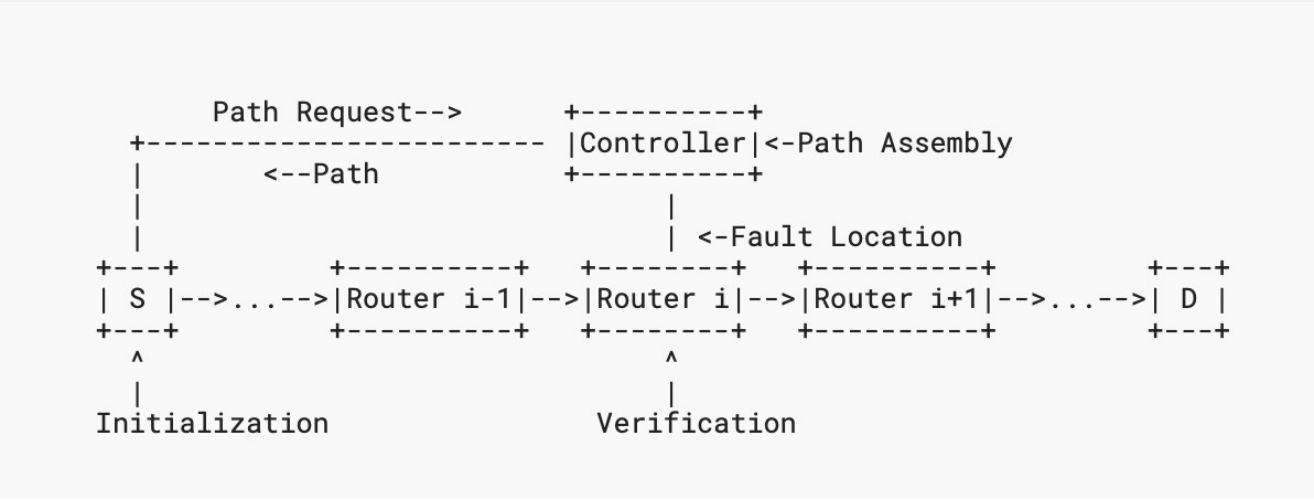
- MAC: Message Authentication Code, a technology to confirm the integrity and conduct certification.
- SRH: [RFC8754]Source Routing Head.
- SRv6: [RFC8986]Segment Routing over IPv6.
- Dos: Denial of Service.
- Tag: Mark a packet as part of a class or group of packets. This field Initialized with a timestamp value to represent a unique session.
- Segments Left: Number of remaining routing segments, defined in [RFC8200] Section 4.4.
- SID: the label of the intermediate router.
- SL: Segments List, an ordered list of SID.
- IR: Intermediate Router, routers participating in packet forwarding in the path.

Path Verification Solution on SRv6

Handle the predetermined forwarding path risks caused by untrusted intermediate routers.

The specific functional goals are as follows:

- **Source and path verification.**
  - Extends the existing SRv6 routing header .
  - Lightweight operations.
- **Privacy protection.**
- **Fault localization.**
  - Provides distributed path verification and centralization-based fault localization.

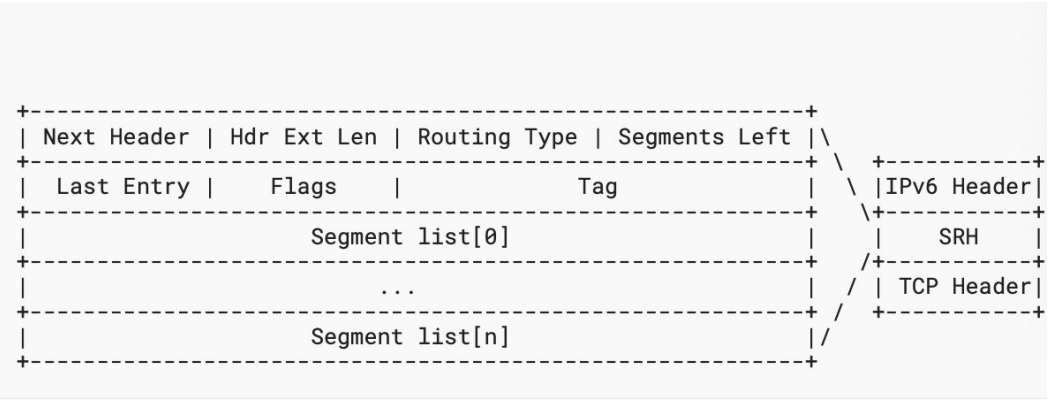


SR-TPP Process

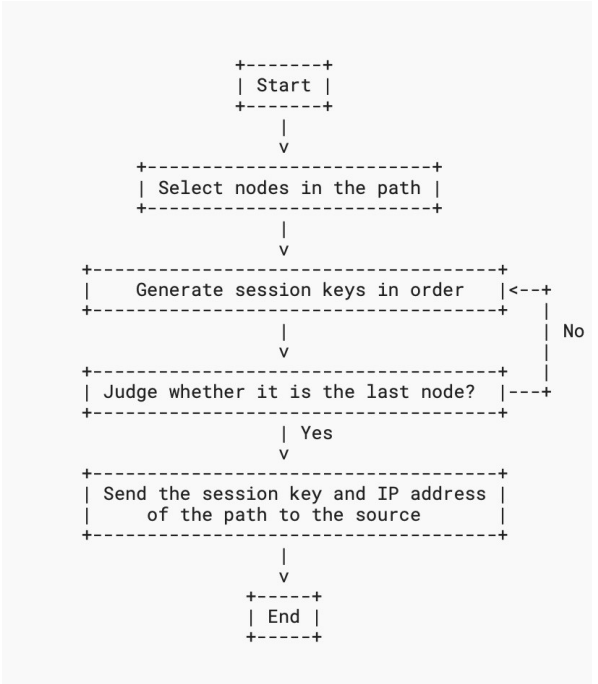
Reduce the header overhead and introduce privacy protection in the path verification mechanism**.**

Initialization

- **Path Initialization.**
  - Use the local key of each SR router and the path creation time-->generate the session key using hash function with session initiation timestamp.
  - Notify the sender of the session key and IP address of the entire path.
- **Package Initialization.**
  - Initialize the Tag field of the SRH when the path was created.
  - Generate its SID and write into the Segment List(SL) .
  - Calculate MAC(SID) and insert into SL for subsequent SID generation.



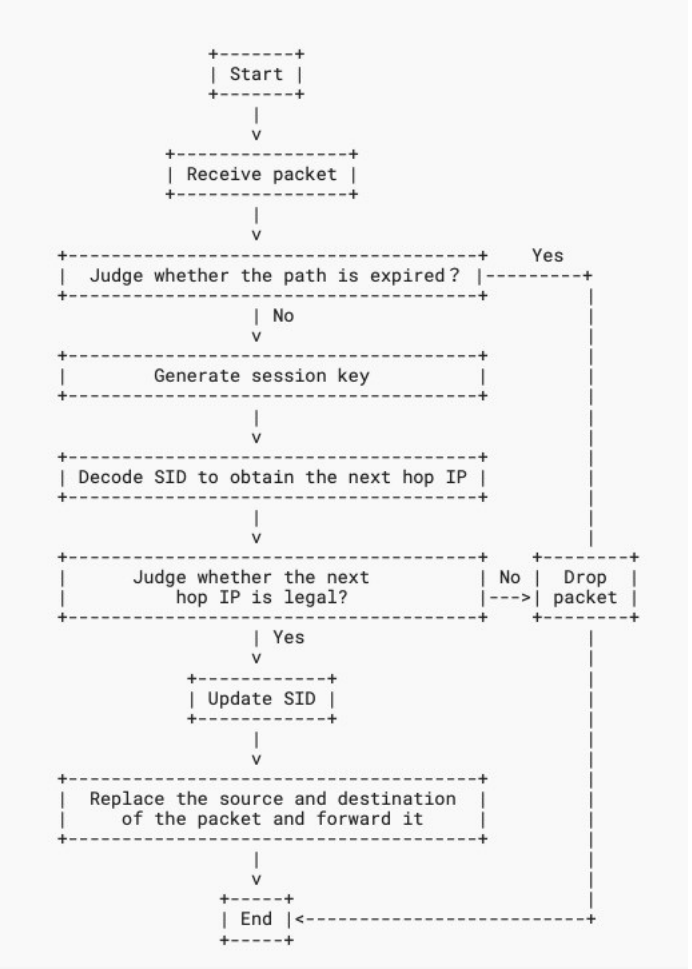
SRv6 header format



Path Initialization Process

Verification

- **Path Initialization Key generation.**
  - Intermediate Router (IR) computes the session key using the IR’s local key and timestamp.
  - The key generation is stateless.
- **Upstream verification.**
  - IR generates a MAC with the partial segment list from the packet Header and the payload.
  - Verifies SL and update by upstream router.
- **Obtain downstream IP address.**
  - IR then parses the SID with K to obtain the IPv6 address of its downstream router.
- **Replace header.**
  - router replaces the source and destination filed of IPv6 Header with itself IPv6 address and its downstream router's IPv6 address.

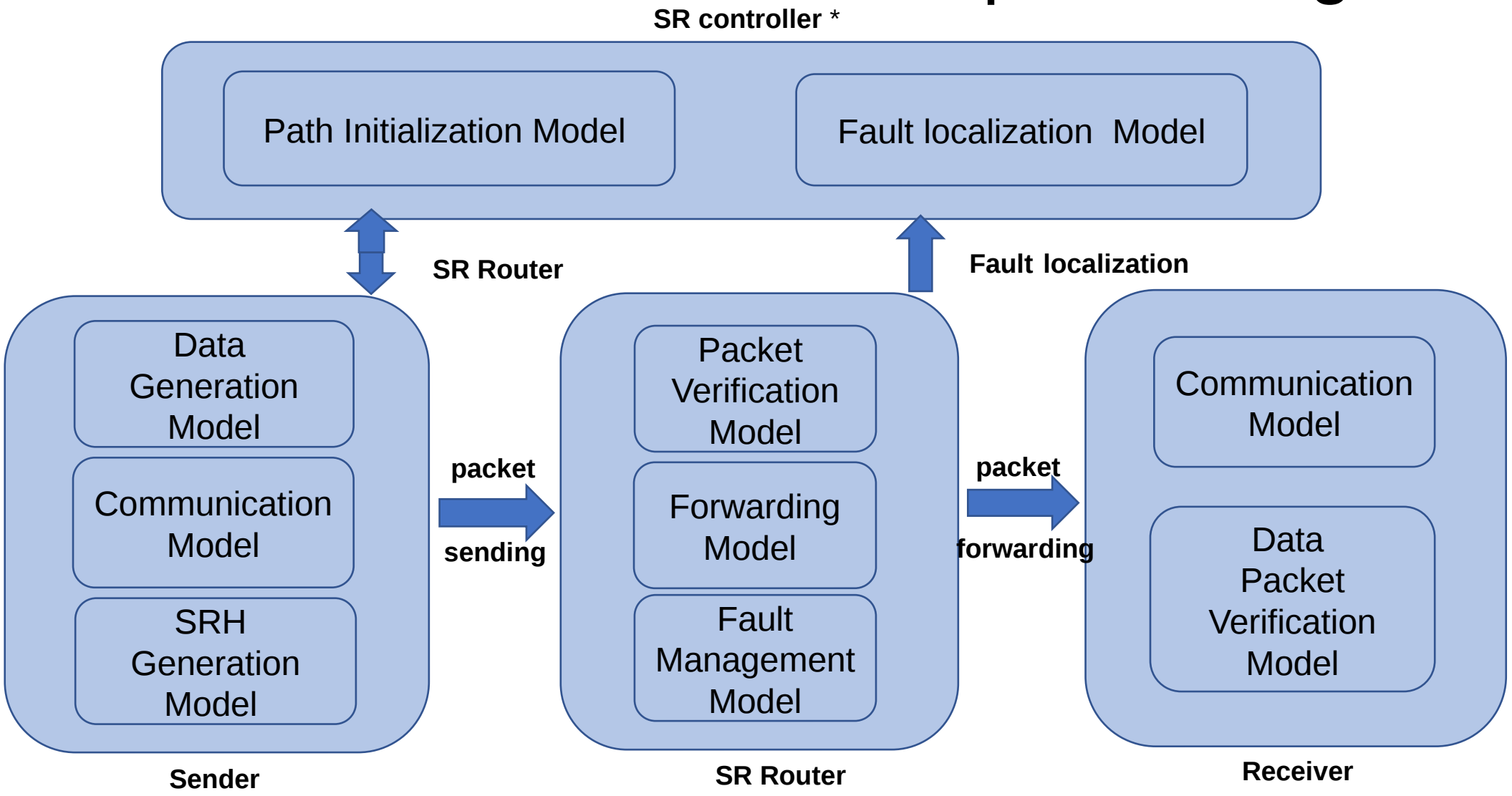


Path Verification Process

Fault location&Security Analysis

- **Fault location.**
  - Payload alteration by the upstream router.
  - Malicious redirection by other routers.
- **Security Analysis.**
  - Packet alteration.
  - Path deviation.
  - Denial-of-Service (DoS).
  - Privacy leaks.

Core Use Case: Proof of TPP-processing



*DELL XPS (IntelCorei 79700, 3GHZ, 8core, 16GB, Ubuntu

Normative References

- [RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/ rfc8200>.
- [RFC8754] Filsfils, C., Ed., Dukes, D., Ed., Previdi, S., Leddy, J., Matsushima, S., and D. Voyer, "IPv6 Segment Routing Header (SRH)", RFC 8754, DOI 10.17487/RFC8754, March 2020, <https://www.rfc-editor.org/info/rfc8754>.
- [RFC8986] Filsfils, C., Ed., Camarillo, P., Ed., Leddy, J., Voyer, D., Matsushima, S., and Z. Li, "Segment Routing over IPv6 (SRv6) Network Programming", RFC 8986, DOI 10.17487/RFC8986, February 2021, <https://www.rfc-editor.org/info/rfc8986>.

Path Verification solution on SRv6

Thank you! Questions?

Brisbane Meeting @ IETF 119, March 2024

Jun Liu

juneliu@tsinghua.edu.cn

draft-jliu-tpp-srv6-00