

Hybrid Two-step telemetry collection method

draft-mirsky-ippm-hybrid-two-step

Greg Mirsky
Wang Lingqiang
Guo Zhui
Haoyu Song

IETF-110 March 2021, Prague(virtual)

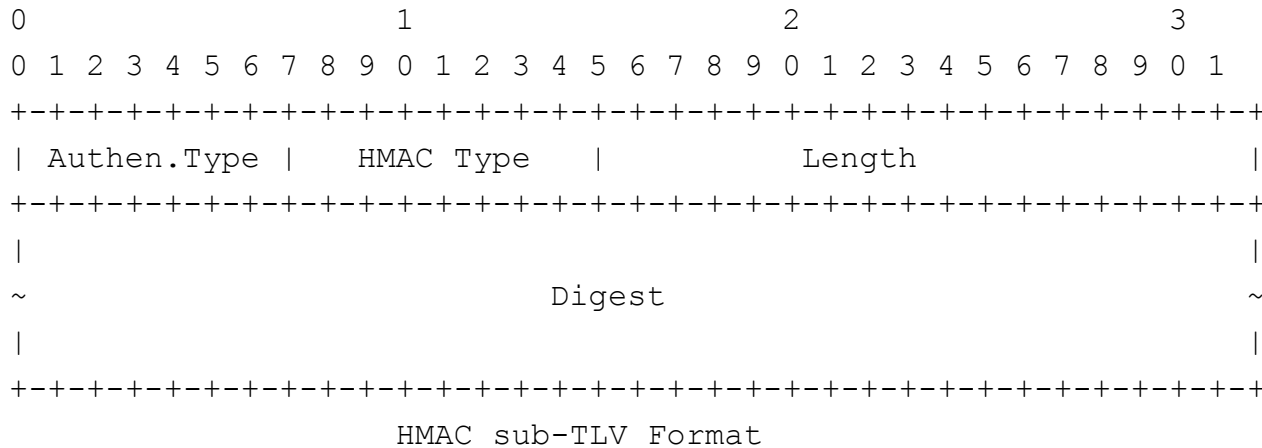
Updates

- HTS as a new IOAM Trace Option-Type
- Authentication in HTS
- Clarify HTS operation at an intermediate node on the reception of a Follow-up packet
- Security Considerations
- IANA registries for HTS

New IOAM Option-Type

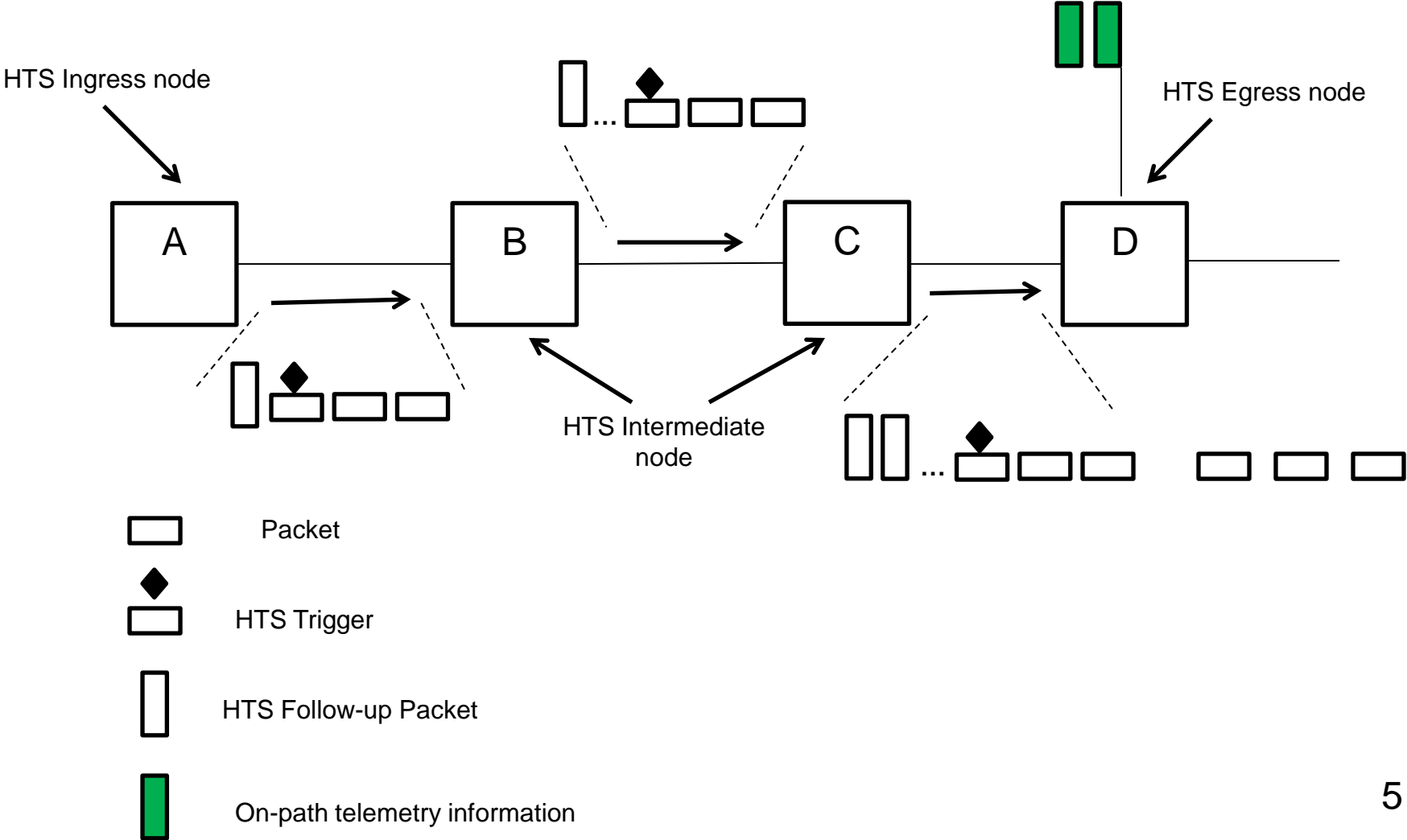
- IOAM Option-Type can be set to the "IOAM Hybrid Two-Step Option-Type"
- IANA is requested to allocate a new code point from the IOAM Option-Type registry
- As a result, a packet that includes the IOAM Header with IOAM HTS Trace Option-Type becomes an HTS trigger packet. IOAM-Trace-Type field determines the set of IOAM data collected and transported in the HTS' Follow-up packet

Authentication in HTS

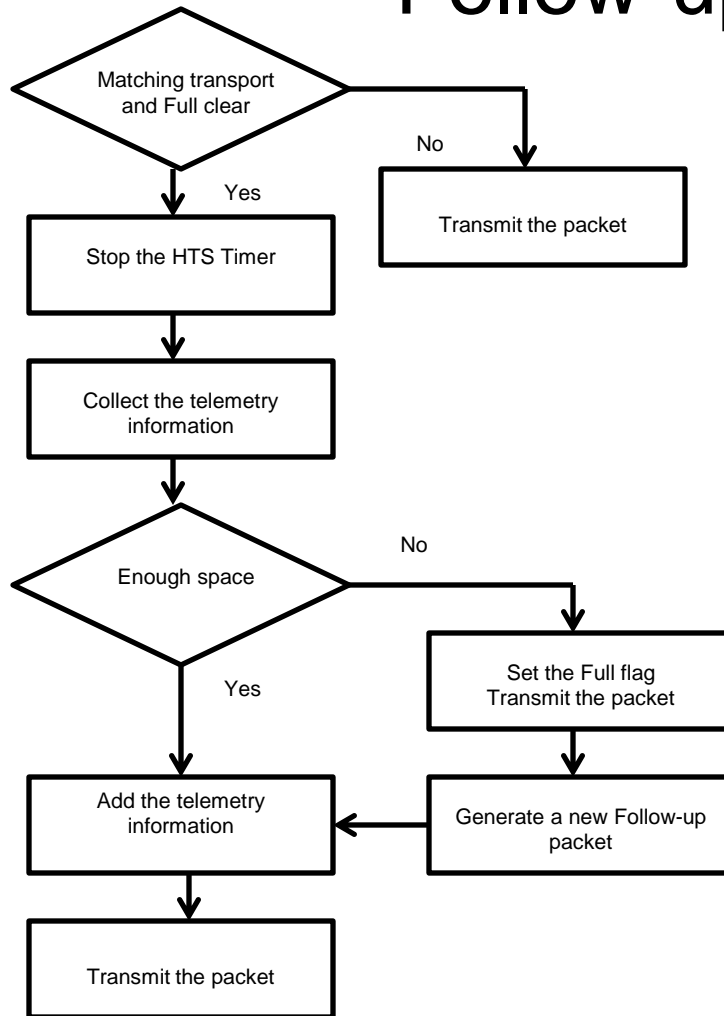


- Use of HMAC-SHA-256 truncated to 128 bits [RFC4868]
- HMAC is calculated over text as the concatenation of the Sequence Number field of the Follow-up packet and the preceding data collected in the Telemetry Data TLV
- The digest MUST be truncated to 128 bits and written into the Digest field
- In the HTS authenticated mode, the Authentication sub-TLV MUST be present in each Telemetry Data TLV, i.e., each node independently authenticates data it appends to the HTS Follow-up packet
- HMAC MUST be verified before using any data in the included Telemetry Data TLV
- If HMAC verification fails, the system MUST stop processing corresponding Telemetry Data TLV and notify an operator

Intermediate HTS node operation on a Follow-up packet



Intermediate HTS node operation on a Follow-up packet



Security Considerations

- HTS nodes belong to a trusted domain
- The integrity protection using the HMAC sub-TLV can be used by each HTS node to protect the collected telemetry information
- Privacy protection can be achieved by sharing the IPsec tunnel traversed by data packets that generate the telemetry information that is collected and transported using HTS

IANA HTS allocations

- IOAM Option-Type code point for HTS
- HTS TLV registry
- HTS sub-TLV registry and allocate the HMAC sub-TLV Type value
- HMAC Type sub-registry and allocate the value for “HMAC-SHA-256 16 octets long” type

Next steps

- Your comments, suggestions, questions always welcome and greatly appreciated
- WG adoption

Thank you