June 2023

FAST EDGE ACCESS CONTROL FOR ROUTED TRAFFIC

Luca Muscariello

Michele Papalini

Giovanna Carofiglio

FAST EDGE ACCESS CONTROL FOR ROUTED TRAFFIC

AUTHORS:
Luca Muscariello
Michele Papalini
Giovanna Carofiglio

ABSTRACT

Real-Time Communication (RTC) traffic typically leverages one or more media bridges (often located in the cloud) and, in order to reduce latency and/or offload cloud resources to the edge, one or more real-time edge relays can be utilized in order to optimize such traffic. Presented herein are techniques to secure a media edge relay node without requiring an authentication for a connection involving the media edge relay node.

DETAILED DESCRIPTION

Real-Time Communication (RTC) traffic usually leverages one or more cascaded media bridges (often located in the cloud) to orchestrate a group communication and switch media across participants involved in the group communication. To reduce latency and offload cloud resources to the edge, one or more real-time edge relays can be deployed in which such edge relays may be considered opportunistic, intermediate nodes located in-path that seek to optimize the traffic (e.g., by sending retransmissions at lower latency, providing cost saving by offloading from the cloud in the case of 'edge-local' participants).

However, migrating RTC traffic to the edge is not without challenges. For example, tasks such as authenticating endpoints and providing access control at the edge can be quite challenging to configure. In addition, the nature of RTC traffic means that any such operations can add unwanted latency to the traffic.

In order to address such issues, this proposal provides techniques for implementing a firewall at edge relay nodes based on Hash-Based Message Authentication Code (HMAC) signature verification. Operations that may be to facilitate such techniques are shown below in Figure 1.

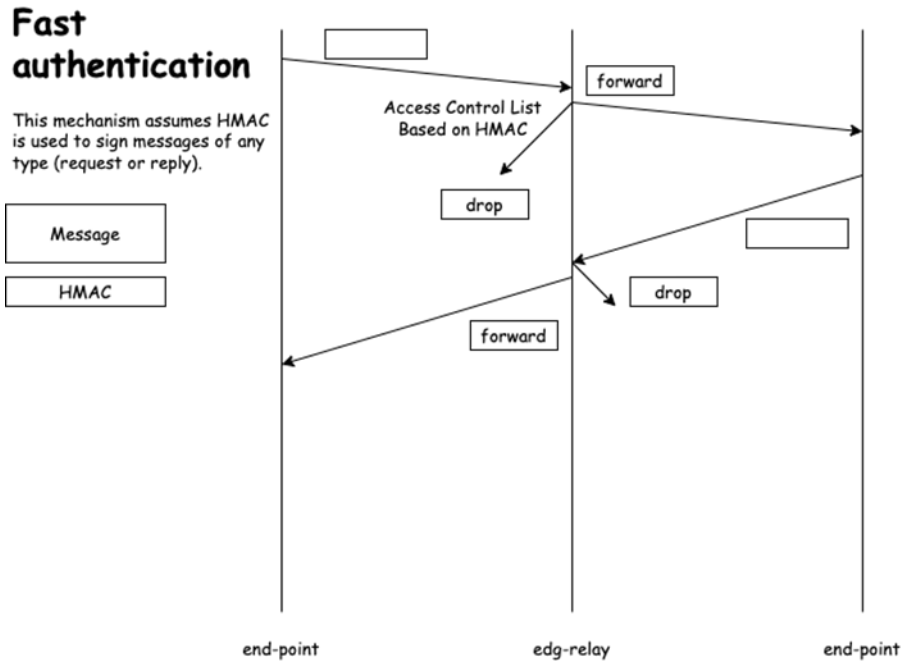

Figure 1: Example Edge Relay HMAC Operations

As shown in Figure 1, a sending endpoint may sign its messages using an HMAC-based signature, which is a keyed hashing mechanism for message authentication. An access control list (ACL) table maintained by the edge relay may be a mirror of the forwarding information base (FIB) in which a lookup is to be performed for each packet received at the ingress against a name-prefix (128 bits) carried in the packet.

If the prefix exists in the FIB and is aggregated, this does not constitute a limitation. Rather, the FIB lookup is used to verify that the 128-bit address is routable for the edge-relay node. Each FIB entry can also store a valid key to verify the signature (HMAC) of the message. Packets that are not authenticated can be dropped.

The per-prefix key can be retrieved by the application control plane, which can also be a member of the group involved in the group communication (e.g., for peer-2-peer (P2P) applications. Every node may apply a key derivation function (KDF) hash in order to obtain the signature key for computation/verification and may rotate the signature key each time the control plane or the data plane triggers a KDF update driven by the sender. The KDF is known in advance and never exchanged.

Accordingly, techniques presented herein may provide for the ability to secure a media edge relay node without requiring an authentication for connections involving the media edge relay node. Thus, the media edge relay node can operate as a Layer 3 (L3) switch, which may both be lightweight and may not store connection status, which can improve scalability. Further, packets that are not authenticated can be dropped.