Media Header Extensions for Wireless Networks

draft-kaippallimalil-tsvwg-media-hdr-wireless-02

Authors: John Kaippallimalil, Sri Gundavelli, Spencer Dawkins

Outline of the draft/presentation:

Slide 3
Motivation & problem statement

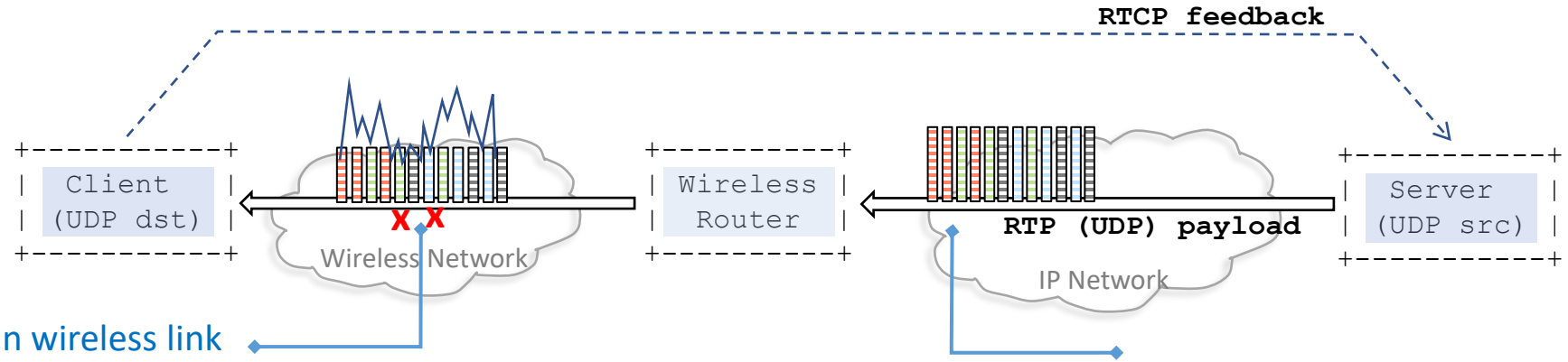
Slide 4
E2E media flow from UDP source to destination

Slide 5
Metadata in the new UDP option

Slide 5
UDP transport for media meta data
(encrypted RTP, RoQ, MoQ)
And, not for media using TCP transport

Slide 3
Outline of solution space and why UDP header extension was chosen.

1. Introduction



Large transient variations in link capacity in wireless access.
Variations will be much more with millimeter wave.

3GPP Rel 18 has specified L4S, selective packet drops for RTP.
L4S/ECN feedback reacts in ~100 ms; selective drops ~1 ms.

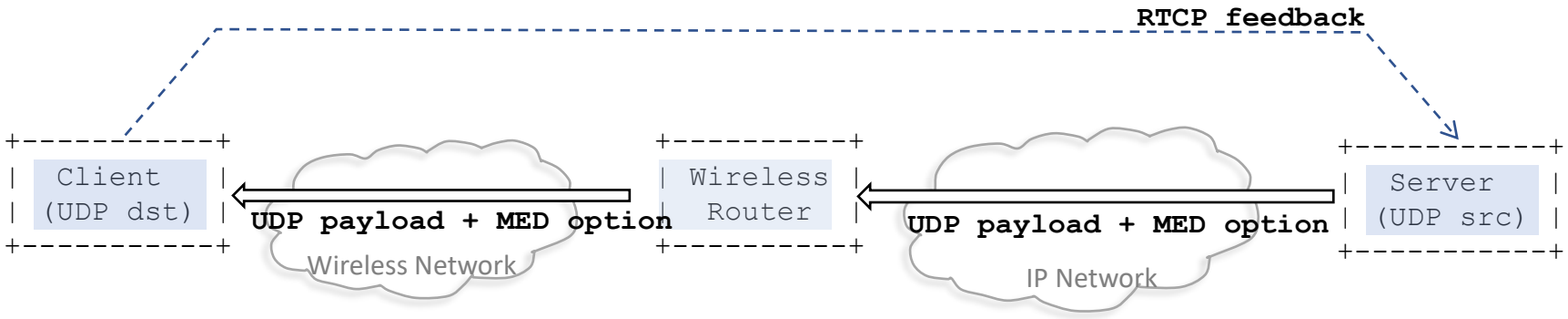
However, encrypted media needs new mechanisms.
- 3GPP Rel 19: companies are interested
- Other accesses (WiFi, Cable?) have similar issues.

Criteria for selecting :
apply (1) priority, (2) burst size, (3) delay budget for an MDU in a flow
(i.e., range of values for burst size, delay budget that change over time, application)
Server may be a node in a Data Center, or a mobile handset.
Should work with all UDP media packets (RTP, QUIC)

timeline:
adds most value for 3GPP if developed in the next 1-2 years.

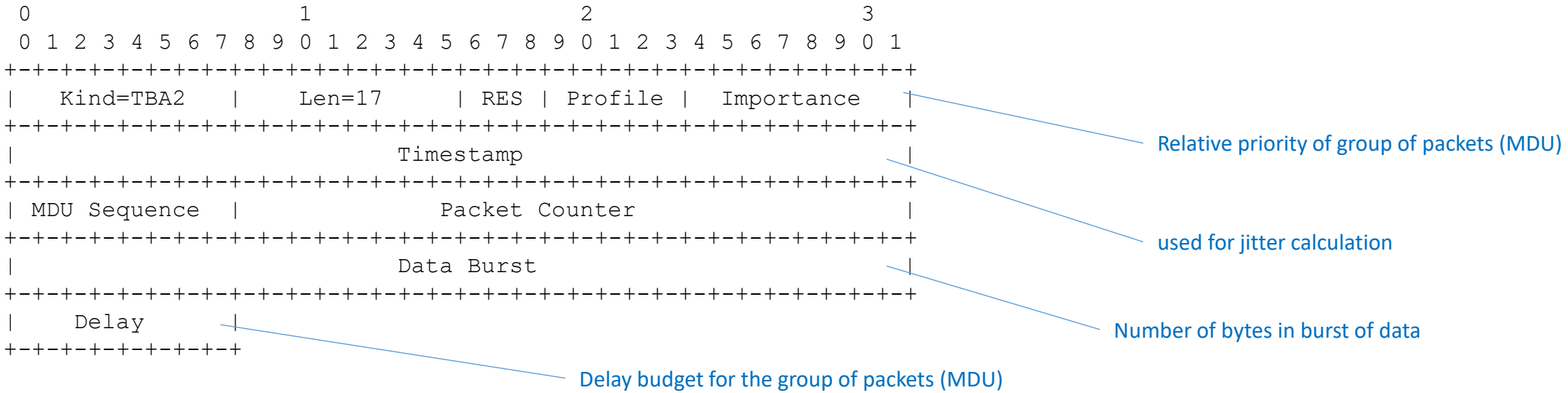
UDP header extensions work with encrypted media (RTP, QUIC) and across accesses (3GPP, WiFi)

1. Architecture



- Application inserts relevant metadata in UDP MED option
  UDP packets carry [Encrypted payload + metadata in MED option]
- Wireless router inspects metadata in MED option and uses to shape, schedule in wireless network.
- Client collects information in UDP metadata, processes and feeds back measurements to Application.
- The Client –> Server feedback loop acts and adjusts rate in the longer timeframe.
- UDP option /metadata is sent from server (UDP source) to client (UDP destination).
  Payload is always encrypted from E2E.
  Metadata is only carried across wireless network and application network that have pre-established trust.
  Across insecure/untrusted network in between, the Security Gateways and complete encryption is required.

3. Metadata, Transport in UDP Option



- New UDP option – MED based on [I-D.ietf-tsvwg-udp-options]
- MED is not altered in transit and is a SAFE UDP option
- MED is sent between UDP source / destination where there is a trust relationship between the wireless network and application network.
- If there is an untrusted/insecure network in between wireless – application networks, the data must be fully encrypted or the UDP option should be policed and dropped.

X. Discussion on the list: why UDP options

Thanks to Sebastian Moeller, Mike Heard, Tom Herbert and Joe Touch for the clear and actionable comments.

Criteria: mechanism to apply (1) priority, (2) burst size, (3) delay budget for an MDU in a flow
(i.e., range of values for burst size, delay budget that change over time, application,)
Server may be a node in a Data Center, or a mobile handset.
timeline: this mechanism would add most value for 3GPP if developed in the next 1-2 years.

DSCP: understanding on the list that DSCP has limited code points while multiple priorities are needed here
And not practical to convey burst size, delay budget

IPv6 Flow Label: a label value corresponding to an MDU.
However, there is no IPv4 flow label. And not easy to convey burst size, delay budget.

IPv6 hop-by-hop hdr extensions: Feasible in managed networks (like 3GPP), but not for open internet and that's ok.
However, while extending IPv4 options may have been possible 30 years ago ...
(wireless network entity (e.g., UPF) are not routers, but application that may run on routers, or an independent node)

UDP options: transport layer mechanism to cover all UDP media (RTP, QUIC, ..)
- How to manage performance of lookups with UDP options in the trailer?
- Opportunity to optimize with IPv6 flow label??

Summary

- Outlines challenges in wireless networks for low latency media applications.
  i.e., how to provide low latency, high bandwidth with large transient variations in capacity
- Fully encrypted media needs additional mechanisms to classify packets.
- 3GPP Rel 19 can be expected to use such a solution if one is available.
  A common solution in IETF can benefit all accesses (3GPP, WiFi) and media transports (sRTP, RoQ, MoQ).
- UDP header extensions developed in this draft seem most promising.

Other comments?

Action for the authors is to act on the comments and update the draft.

Backup Slides

Solution Options for Encrypted UDP Media

Key criteria: evolving media encoding, feedback /packet pacing*, multiple L2 wireless paths, application preferences, performance, security.

1. **DSCP**
   would have been ideal – if it were possible to extend and convey a QoS for group of packets (MDU)

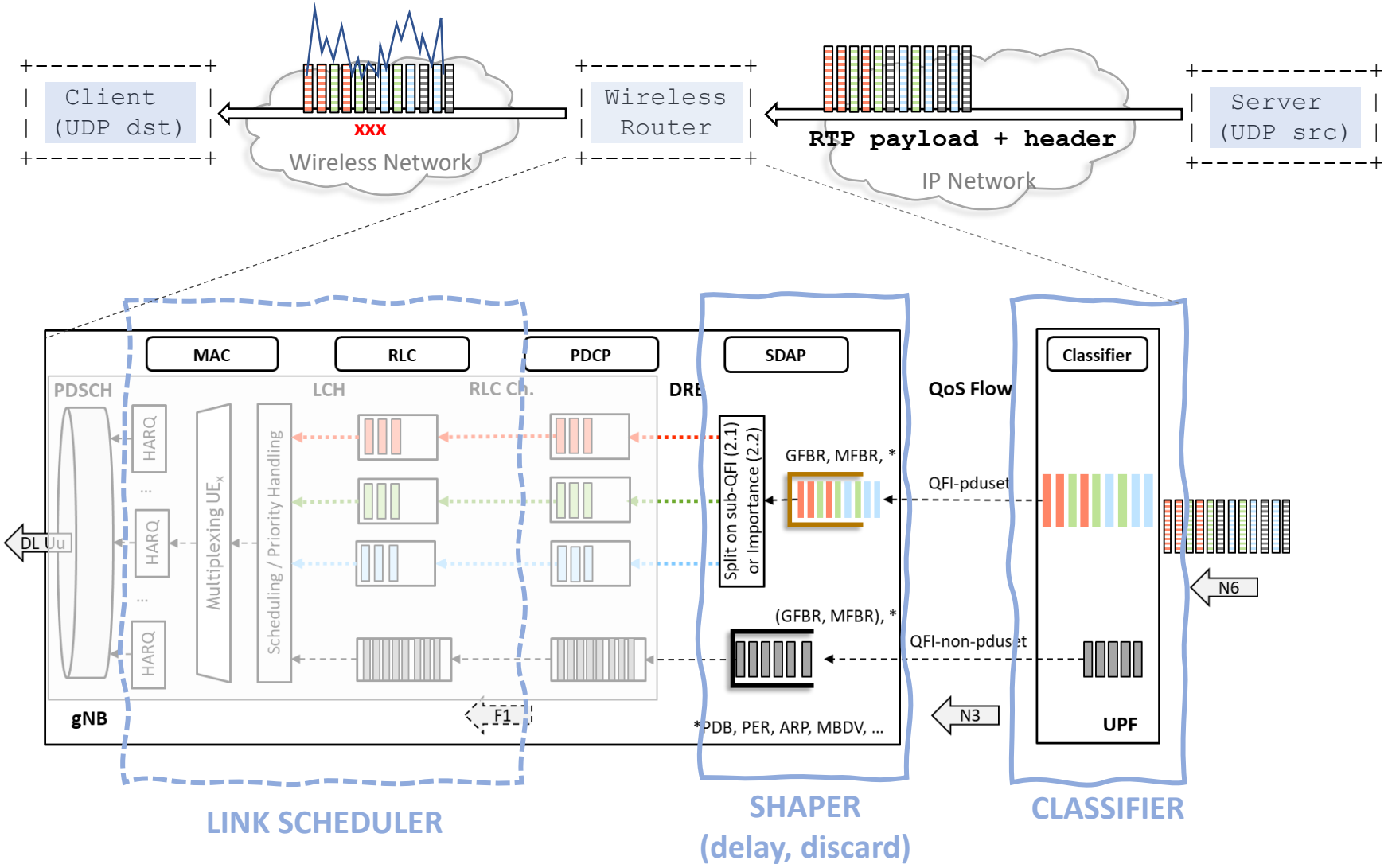
2. **Media Header**
   UDP header extn, in-band with media packet or tunneled mode over "untrusted" network segments.
   - in-band: satisfies most key criteria including performance but assumes trusted networks on path.
   - tunneled: bulk encryption over "untrusted" network segments. No per packet decryption at wireless router.

   MASQUE: tunnel enhanced to carry metadata to wireless router.
   - satisfies criteria except performance (per packet decryption at wireless router is needed).
     No issues with "untrusted" network segments on path.

3. **Multiple congestion Control Segments**
   Media relay at mobile edge, use different/optimal CC for mobile segment: potentially a good long-term solution!
   Media-header + optimal CC are complementary.

4. **Others** a) Media over QUIC Relay: complex key distribution, does not work for RTP.
   b) Terminate GTP at Media server: unlikely that media servers will write to socket for GTP-U
   c) Share keys: Providing keys to wireless network breaks end-to-end security.

3GPP Rel 18 – classification with RTP header



* WiFi /other accesses also benefit if we have a common mechanism for encrypted media.