

# Media Header Extensions for Wireless Networks

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

Authors: John Kaippallimalil, Sri Gundavelli, Spencer Dawkins

# Outline

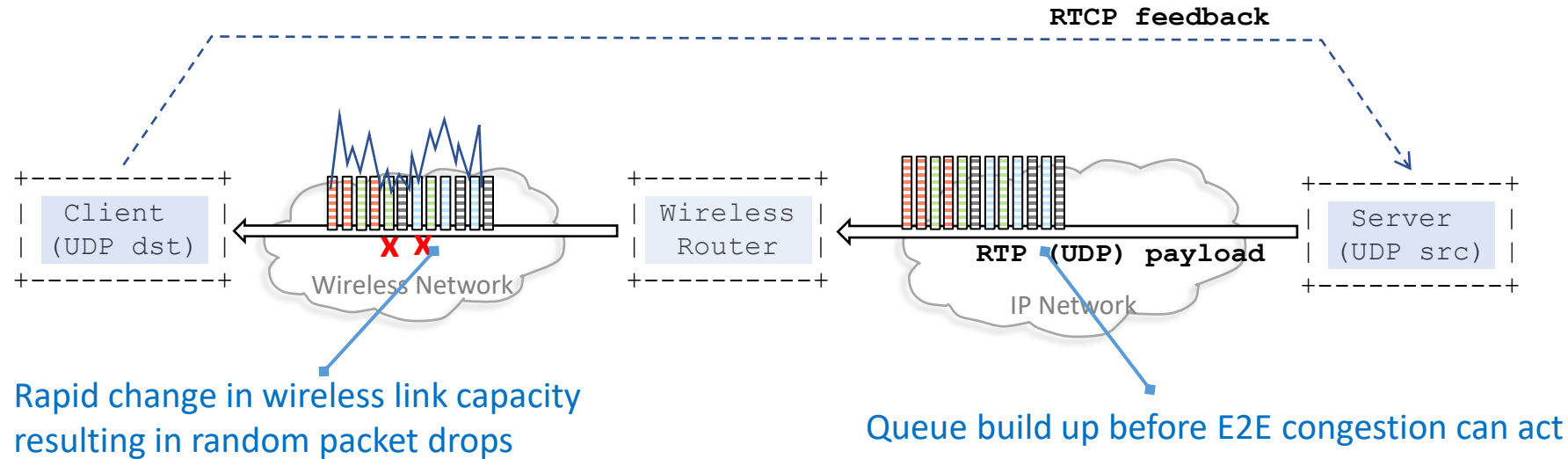
- **Overview**  
latency + bandwidth requirements of media packets  
link capacity variation in wireless networks
- **3GPP Rel 18 classification with RTP header**
- **Solution Options for Encrypted Media**  
DSCP ?, media header, new CC, MoQ relay, shared keys ?, GTP ?.
- **UDP Extension (MED)**  
timestamp, media data unit, packet counter, importance, data burst, delay budget
- **Summary**

## Abstract:

Wireless networks like 5G cellular or Wi-Fi experience significant variations in link capacity over short intervals due to wireless channel conditions, interference, or the end-user's movement. These variations in capacity take place in the order of hundreds of milliseconds and is much too fast for end-to-end congestion signaling by itself to convey the changes for an application to adapt. Media applications on the other hand demand both high throughput and low latency, and are able to dynamically adjust the size and quality of a stream to match available network bandwidth. However, catering to such media flows over a radio link where the capacity changes rapidly requires the buffers and QoS in general to be managed carefully. This draft proposes to provide metadata about the media transported in each packet to allow the wireless network to manage radio resources optimally and to maximize network utilization while also improving application performance.

This draft discusses at a high level potential solution options to this problem and the trade-offs involved. The draft then defines a solution that uses a new UDP option to carry media metadata between a UDP source and destination. This option is compact and has low processing overhead at the wireless router.

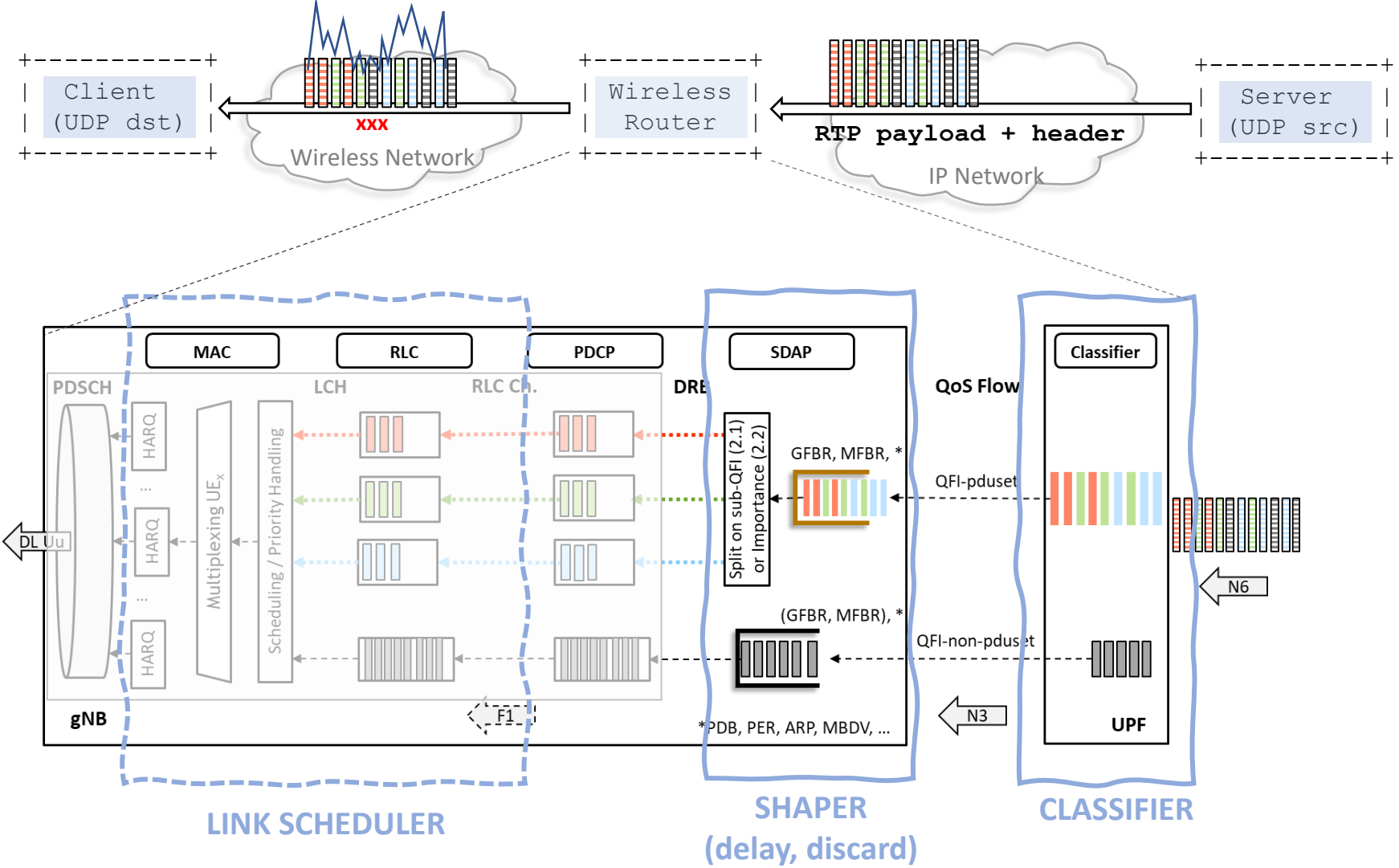
# Overview



- Wireless network accesses experience large transient variations in link capacity. Random or tail drops affect media application performance adversely. It is desirable to drop packets selectively.
- L4S/congestion fed back to application, reacts in  $\sim 100$ s of ms, selective dropping decision in  $\sim 1$ + ms. Note: transient link capacity variation will be much more for millimeter wave radio accesses!
- 3GPP Rel 18 is already specifying use of L4S, selective packet drops for unencrypted RTP media flows. In 3GPP Rel 19, companies are interested in similar mechanism for encrypted media flows (RTP cryptex, RTP over QUIC).
- However, this draft is not only for 3GPP wireless access. Other accesses including WiFi encounter a similar problem. Draft to develop a common mechanism across various accesses (3GPP, WiFi) & media transports (RTP, QUIC) over UDP.

Wireless accesses benefit from packet info to schedule around transient capacity variation.

# 3GPP Rel 18 – classification with RTP header



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

# 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 or tunneled: satisfies criteria above.

MASQUE: satisfies most criteria, except performance (L7, & per packet decryption at wireless router)

### 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.

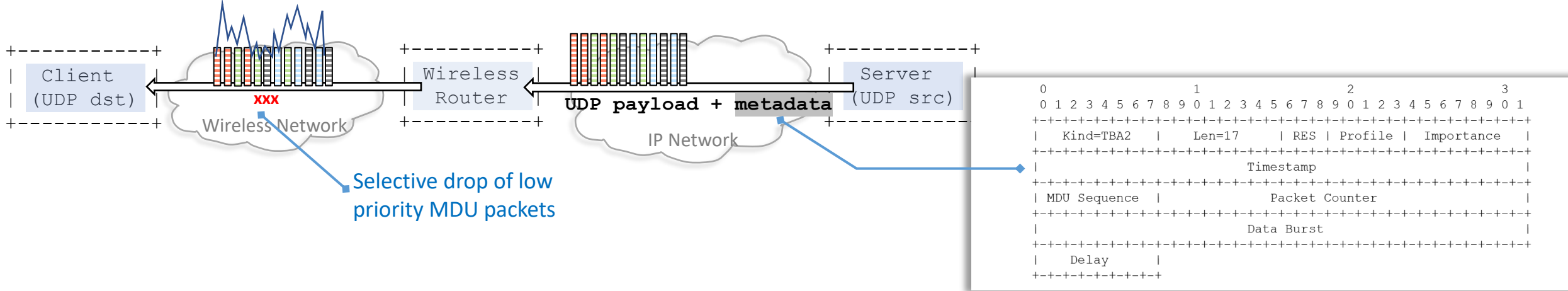
### 4. Others

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.

# UDP Header Extension



- **Application** derives relevant metadata to be added to encrypted UDP payload (e.g., HTTP/3, SRTP cryptex, ..) UDP packets carry [Encrypted payload + metadata]
- **Wireless router** inspects/classifies (MDU, priority, ..) which the wireless network uses in shaping, scheduling. **Client** collects information in UDP metadata, processes/aggregates and feeds back to **Application** (e.g., RTCP).
- For sustained high throughput and low latency:  
The **Server – Client** control loop acts and adjusts rate in the longer timeframe.  
With metadata, **wireless network** handles rate mismatches in short timeframe by selective drops/delays.
- 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.

# 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
- 3GPP Rel 18 identifies this and uses RTP headers for classifying unencrypted RTP media.
- Fully encrypted media needs additional mechanisms to classify packets.
- 3GPP can be expected to consider the problem in Rel 19.  
A common solution in IETF can benefit all accesses (3GPP, WiFi) and media transports (sRTP, RTP-o-QIUC).
- Many solution options considered.  
DSCP, UDP header extensions, MASQUE, new CC (long term?), MoQ relay, GTP@media server, shared keys.  
UDP header extensions seem most promising.

Comments?

How can we move forward?