Media Header Extensions for Wireless Networks

draft-kaippallimalil-tsvwg-media-hdr-wireless-01

Authors: John Kaippallimalil, Sri Gundavelli

Outline

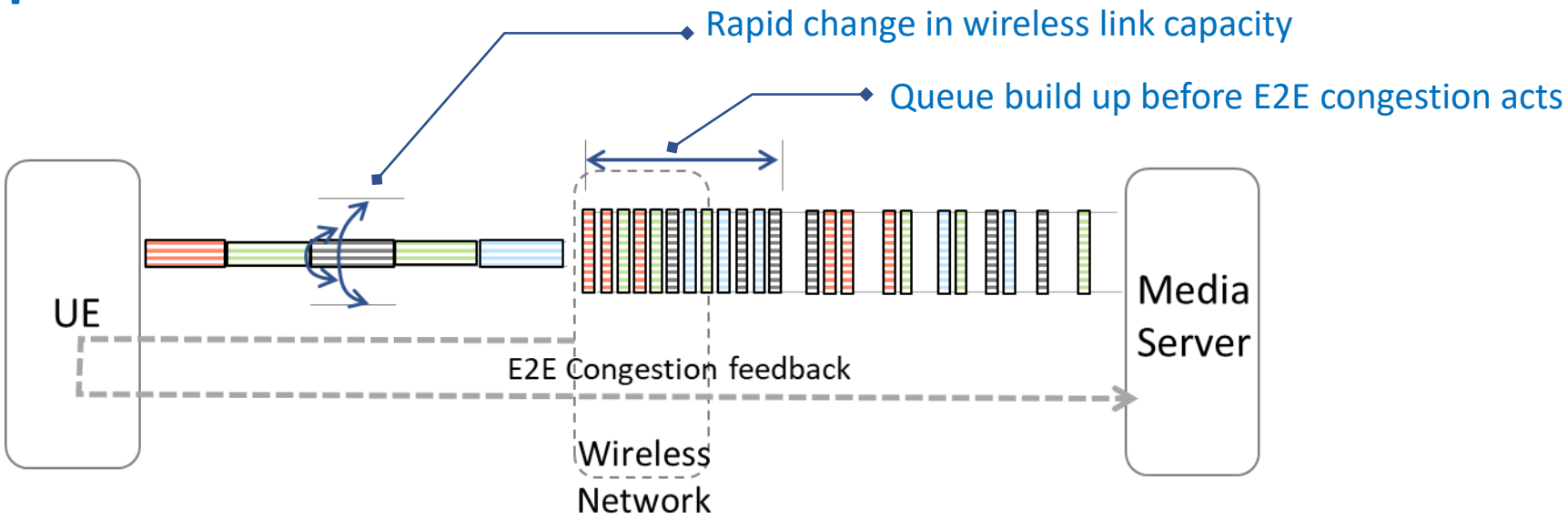
- Motivation for this draft
  latency + bandwidth requirements of media packets
  link capacity variation in wireless networks
- Architecture
  media metadata transport across server, wireless network, client.
- Metadata
  timestamp, media data unit, packet counter, importance, data burst, delay budget
- Transport of Metadata
  new UDP option

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. 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 to be managed carefully. This draft proposes additional information about the media transported in each packet to manage the buffers and optimize the scheduling of radio resources. The set of information proposed here includes relative importance of the packet, burst length and timestamp to be conveyed by the media application in a header extension. This can be used to provide the wireless network the flexibility to prioritize packets that are essential when the radio capacity is temporarily low, defer packets that can tolerate some additional delay, or even drop packets selectively in more extreme conditions.

Another aspect considered here is the means by which the media packet
information is transported. Potential solutions include carrying this information in Media over QUIC extension headers, UDP options, or in a MASQUE encapsulation between the application server and wireless network entity.

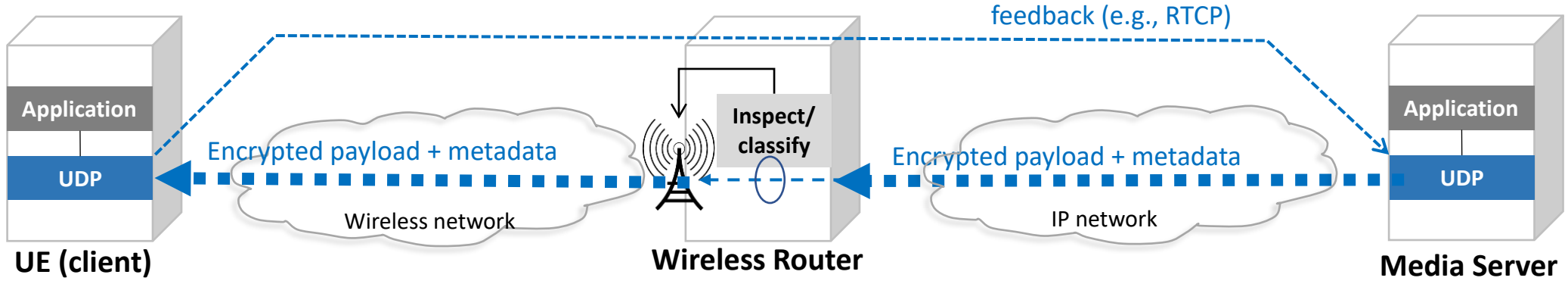
Motivation



- Low latency, high bandwidth media flows, radio networks are scheduled using bounded queue lengths. Random or tail drops affect application performance adversely. It is desirable to drop packets selectively.
- L4S and congestion control (like NADA, GCC) are the key mechanisms, but they work at different time scales. (e.g., RTCP feedback is in 100(s) of ms, while radio channel conditions change in a few ms)
- 3GPP (SA2 – XRM) has already specified both L4S and dropping/deferring of media data units (e.g., I-frame) The current release addresses RTP/SRTP (with extended header) but not fully encrypted media packets.
- The wireless network needs some means by which fully encrypted media packets can be classified.

This draft proposes metadata and a new UDP option to transport the metadata.

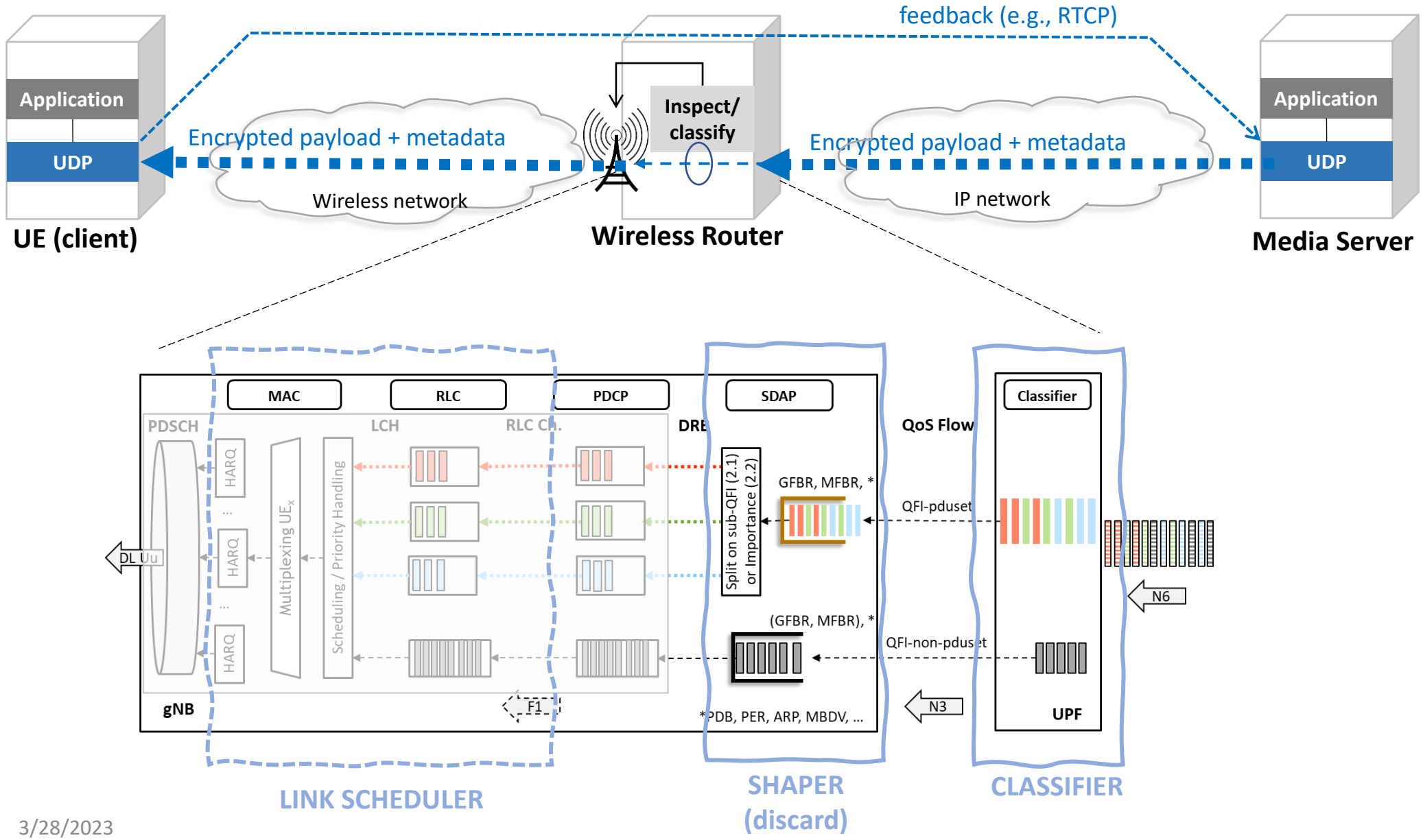
Architecture



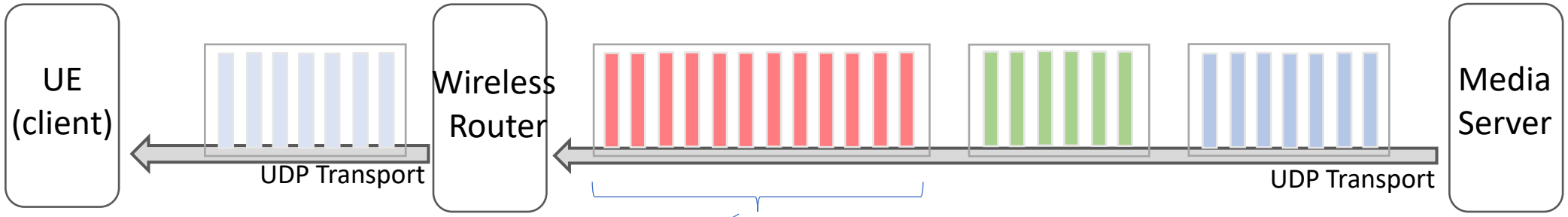
** Assumes media session establishment prior to sending [Encrypted payload + metadata].

- 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.

Application in 3GPP User Plane



Metadata



* Figure shows packets on the wire for 1 transport connection

(same value for each packet of MDU)

Media Data Unit (MDU) sequence number

sequence number for a set of media packets that form an information unit (e.g., a video I-frame)

Importance

relative priority of packets of an MDU

Data Burst

number of bytes in a burst of packets of the MDU

Delay Budget

duration in ms of burst of packets of the MDU

(value changes for each packet of MDU)

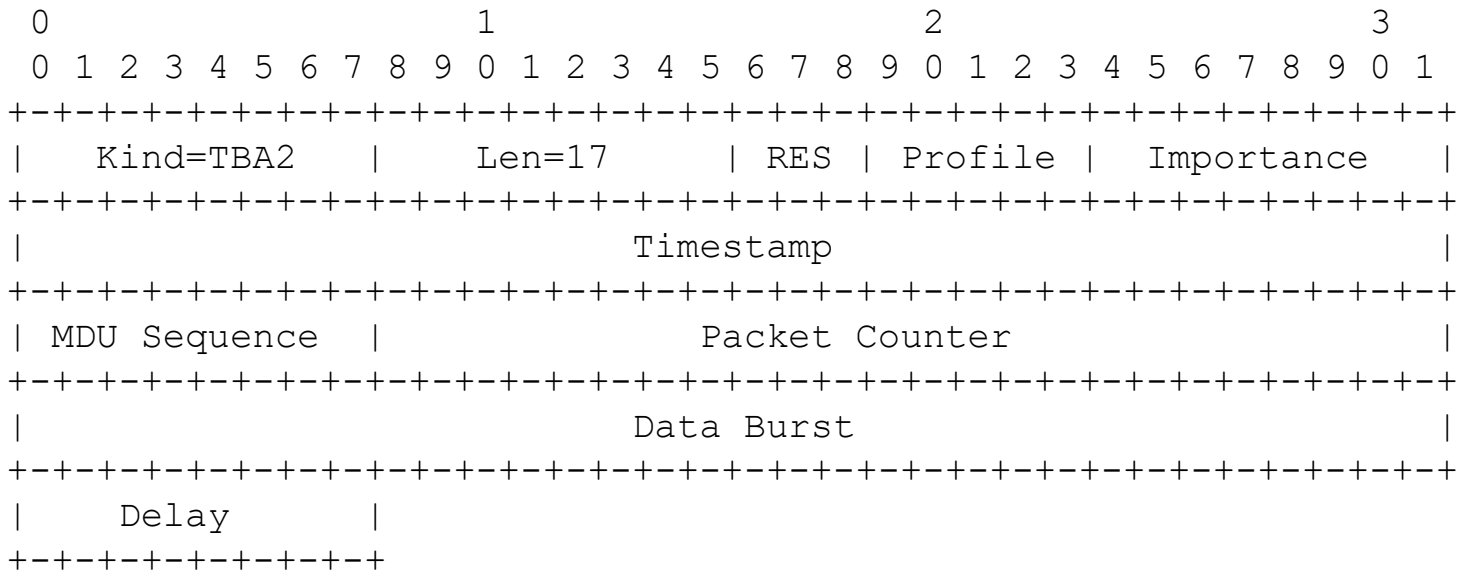
Packet Counter

sequential number of packets in an MDU

Timestamp

time value at sender

MED – 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.

Summary

- Outlines challenges in wireless networks for low latency media applications.
  3GPP SA2 identifies this, addresses aspects in wireless for unencrypted RTP media.
- Fully encrypted media needs additional mechanisms to classify packets.
- This draft proposes:
  - UDP option MED to send metadata between UDP source/destination.
  - Metadata is only carried across networks that have pre-established trust.
  - Wireless network classifies using UDP option, endpoint send feedback to server.
  - Payload is always encrypted from E2E.

Comments?