Formation and Assertion of Data Unit Groups in 3GPP Networks with TSN and PDU Set Support

Sebastian Robitzsch*, Chathura Sarathchandra*, Michael Starsinic† and Xavier de Foy‡
*InterDigital Europe Ltd, London, United Kingdom
†InterDigital Inc., Conshohocken, PA, United States of America
‡InterDigital Canada Lteé, Montreal, Canada
Email: {sebastian.robitzsch, chathura.sarathchandra, michael.starsinic, xavier.defoy}@interdigital.com

***Abstract*—Industrial applications and Extended Reality vertical sectors have expressed the need for dedicated Quality of Service considerations from 3GPP to support time-sensitive, bursty and high throughput communications. Consequently, 3GPP enabled support for Time-Sensitive Networking in Release 17 and started specifying the concept around Packet Data Unit Sets in Release 18. This paper presents a novel solution for any IP-based communication enabling time-sensitive communication while utilising 3GPP Packet Data Unit Set feature. This paper proposes extensions to the IP header that can be utilised by any IP based network. The proposed solutions introduce the concept of a Data Unit Group to describe the entirety of an Application Data Unit and its fragmentation into individual IP packets to be delivered over a packet-switched network. This paper defines Data Unit Group Rules to communicate packet header detection and action rules to Time-Sensitive Networking switches. The rules can be used by Time-Sensitive Networking switches to prioritise and re-order/pre-empt packets and by User Equipments and User Plane Functions to write Packet Data Unit Set Markings.**

***Index Terms*—3GPP, IEEE, Time-Sensitive Networking, Internet Protocol, IETF**

I. Introduction

In the past years we have witnessed a rapid advancement in multi-sensory applications (such as gaming and Extended Reality), increasing the requirements they impose on the networks. Consequently, to keep up with demand, networks have been increasingly optimised to consider application layer information, which allows networks to consider characteristics of the traffic being transferred. Application aware networks aim to transfer data in a way that ultimately reduce network costs while meeting Quality of Service (QoS)/Quality of Experience (QoE) requirements.

Today, the granularity of information used for optimising networks may range from the traffic flow type (e.g. audio, video) to packet-level information (e.g., sequence numbers). Standardisation organisations such as, IETF, IEEE and 3GPP define how such parameters are exposed to the networks and how they may be used for achieving targeted Key Performance Indicators (KPIs). In particular 3GPP's latest 5G offering provides the required network KPIs around throughput, latency and jitter, while offering a tight integration with applications and their QoS requirements [1]. With 5G, 3GPP also integrated support for the vendor-agnostic Time-Sensitive Networking (TSN) standards by IEEE, targeting industrial applications with rather stringent timing requirements for inter-machine or machine-human interactions.

Information related to correlations between data being transferred may enable further improvements through differentiated traffic handling at the granularity of units of data. For example, a single video frame may be transferred through multiple data packets, and all of it must be received at the application for the frame to be fully decodable at the application. Otherwise, it leads to re-transmissions. Moreover, certain frames may be more important than others. Therefore, in the above example, a frame could be considered a Data Unit Group (DUG), and DUG differentiated traffic handling may enable further optimisations in the network. This paper addresses how one could expose DUG-related information to IP networks, how they may be communicated to and used by intermediate network elements.

The paper is structured as follows: Section II provides background on TSN in IEEE, TSN support in 3GPP and PDU Sets. Section III then introduces the Data Unit Group concept and provides insights on how 3GPP and TSN network nodes would operate with the DUG feature. Section IV concludes the paper and provides an outlook on future work.

II. Background

This section presents the background on IEEE's TSN and 3GPP's PDU Sets which form the foundation for the novel concepts presented after.

A. Time-Sensitive Networking

TSN is a collection of IEEE 802.1 and 802.3 standards enabling time-sensitive (aka deterministic) communications for compute nodes, e.g. network switches. In order to achieve timely delivery of data in a packet-switched network, IEEE demands that all TSN-enabled switches are time synchronised, as defined in 802.1AS. All operations within a switch are cycle-based where each cycle has the exact same length with a minimum cycle time of 30µs up to several milliseconds

This work has been partially funded by the European Commission Horizon Europe SNS JU PREDICT-6G project (GA 101095890) and 6G-XR project (GA 101096838). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

(defined in 802.1Qbv). Fig. 1 illustrates the internal workflow of a TSN switch with a description of each component and the related IEEE standard below.

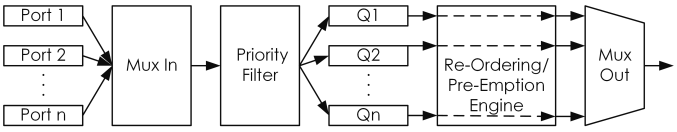

Fig. 1. Internal Workflow of a Time-Sensitive Networking Switch.

The figure above shall be read from left to right; starting with the ports to the very left, these are the switch ports implementing IEEE's 802.3 standard to handle Ethernet frames. Next in the chain is a multiplexer, Mux In, which serialises all incoming packets based on their arrival time and hands them over to a priority filter. This priority filter follows IEEE's 802.1cb specification [2] and aims at identifying the priority of packets by identifying to which stream of packets they belong to. IEEE defines a range of headers to be looked at to make these decisions, i.e. destination/source MAC address, Virtual Local Area Network (VLAN) tag, source/destination IP addresses, transport protocols (User Datagram Protocol (UDP)/Transmission Control Protocol (TCP)), or source/destination port numbers. Based on this configurable prioritisation, the TSN switch places a packet into a set of queues, denoted as Q1, Q2, Q3, ..., Qn in Fig. 1. Each queue represents a different level of configurable priority allowing the re-ordering/pre-emption engine to change the position of each packet within a queue in respect to other packets in other queues. This allows for more important/time-critical packets to be delivered and – if needed – less important packets to be dropped. The last step in this chain is another multiplexer to put the packets out on the respective ports of the switch.

As mentioned above, TSN switches offer flexibility on the chosen priorities, how they are determined and what is placed in which queue. The required configuration can be either done by hand directly on the switch or through programmable methods. IEEE leverages well-established methods and technologies to achieve configuration, i.e. YANG models combined with NETCONF or RESTCONF frameworks. The result is IEEE's YANG model implementing possible identification rules for TSN switches in 802.1cb [2]. To logically centralise the control and management of a TSN network, a Centralised Network Controller (CNC) is defined in [3] to obtain TSN bridge capabilities and to enable the configuration of TSN switches in a more automated fashion.

B. Time-Sensitive Networking-Enabled 3GPP Networks

In Release 16 and 17 3GPP has standardised the support for IEEE 802.1 TSN networks and centres the integration around IEEE's 802.1Q standard [1], which defines the use of VLAN Identifiers to allow switches to perform port-switching based on the Layer 2 identifiers. Figure 2 illustrates 3GPP's support for TSN from a system architecture point of view and depicts the entire 3GPP network exposed as a single TSN bridge with two ports, the Device-Side Translator (DS-TT) and the Network-Side Translator (NW-TT). Furthermore, 3GPP also defines a dedicated TSN Application Function (AF) responsible for the exposed 5G System (5GS) bridge management and the port management for DS-TT and NW-TT. Furthermore, 3GPP supports the Link-Layer Discover Protocol (LLDP) [4] defined by IEEE to discover the topology of a TSN network.

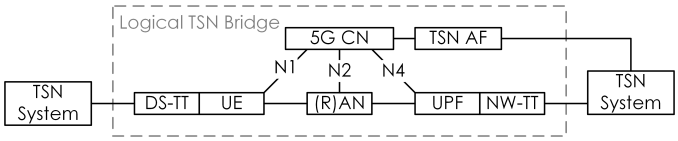

Fig. 2. 3GPP's System Architecture View with Time-Sensitive Networking Support.

All illustrated 3GPP User Plane (UP) components must be sychronised to the same 5G Grand Master Clock, i.e. DS-TT, User Equipment (UE), Access Network (AN), User Plane Function (UPF), NW-TT. This allows the support of the Generic Precision Time Protocol (gPTP), defined in [5], whereby NW-TT and DS-TT can generate ingress gPTP timestamps on the 5GS reference time. Once the gPTP packet leaves the 3GPP system, an egress time is added allowing to determine the residence time of packets in the 5GS. To automate the control and management of TSN bridges, e.g. the 5GS, the TSN AF provides the necessary means to expose TSN bridge capabilities and properties as well as receiving requests to configure rules in internal TSN bridges.

C. Packet Data Unit Sets in 3GPP

3GPP Rel.18 introduced support for Extended Reality (XR) sessions and PDU sets allowing the system to serve different QoS-sensitive service flows to a single or multiple UEs that are collectively participating in a single application. For instance, application layer data formats can range from pure text-based periodic short bursts of numeric values to actual larger chunks (e.g. video or file transfer). Fig. 3 illustrates the Rel.18 feature *PDU Sets*, as described in [1]. PDU Sets can give the 5G network the ability to understand which PDUs belong to the same application-related data unit. PDUs Set related information can be used by the network to ensure that PDUs that are related are delivered to the receiver with an acceptable delay and to make prioritisation decisions.For example, the network can be configured to know whether the entire PDUs Set is needed by the receiver or if a partially received PDUs set may be of use to the receiver. In cases where only an entire PDU Set is useful to the receiver, the network may choose to discard the entire PDUs set if the first PDUs in the set is not successfully delivered.

Table I provides the PDU Set markings specified by 3GPP for identifying Real-Time Transport Protocol (RTP) header fields to fill out PDU Set Markers, as specified in [6].

To mark packets as a PDU Set requires the detection of packet streams using header information. 3GPP studied the dominant protocols used to stream media content in [7,

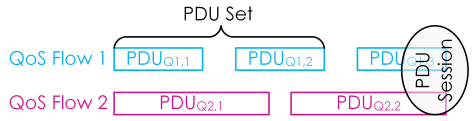

Fig. 3. 3GPP's System Architecture View with Time-Sensitive Networking Support.

TABLE I
MANDATORY PACKET DATA UNIT SET MARKINGS IN 3GPP [6]

PDU Set Marking	**Length**	**Description**
End PDU of the PDU Set	1 bit	If set, it indicates the last PDU of the PDU Set
End of Data Burst	3 bits	While not specified yet in detail, the 3 bits indicate the end of a data burst within a PDU Set
PDU Set Importance	4 bits	This field allows to indicate the importance of this PDU Set compared to other PDU Sets within the same QoS flow. The lower the value the higher the importance. At the moment, the application layer codec level aspects are used to define the importance, i.e. video, audio, text/metadata, image.
PDU Set Seq Num	10 bits	Sequence number that identifies the PDU Set against other PDU Sets
PDU Seq Num	6 bits	Sequence number of a PDU within a PDU Set
PDU Set Size	24 bites	The total size of all PDU in the PDU Set. Note, this field is an option field according to [6, Section 4.4.2.4]

Section 6.7] and covered protocols such as RTP and Hyper-Text Transfer Protocol (HTTP). While for RTP the actual RTP header is extensively analysed to derive the PDU Set Markings, for HTTP the underlying transport protocols UDP and TCP are considered to track streams of packets for the same PDU Set. However, the actual specification work in [6] does not mention any HTTP-based PDU Set markings.

D. Grouping of Packets

There has been an effort in the Transport Services Working Group (TSVWG) to define a UDP solution to convey PDU Set information for application layer protocols that rely on UDP, e.g. HTTP/3 or QUIC. The published draft [8] defines a group of packets that should be handled similarly (e.g. all packets of a video I-frame) as a Media Data Unit (MDU). The draft defines a range of meta parameters as an extension header to UDP: Profile: A profile for added metadata, allowing the proposed extension to enable more metadata profiles then the one covered in this draft; Importance: the importance of the packet (delay tolerance, inter-MDU dependency or a priority level); Burst Size: The number of bytes of data in a continuous stream of packets; Delay Budget: An upper bound in milliseconds between the reception of the first packet of the MDU pot the last packet of the MDU; MDU Sequence: A cyclical counter that has the same value for an MDU; Packet Counter: A counter for the packets within an MDU that increments for each subsequent packet; Timestamp: An absolute data and time as defined in RFC5905 used for network jitter calculations. The sending application is foreseen to inject the UDP header extension.

III. PROPOSED SOLUTIONS

This section describes the solutions for TSN and PDU Set-enabled 3GPP computer networks to extend the PDU Set concept to all application-layer protocols.

A. Data Unit Group Definition

Modern applications often send data which does not fit into a single packet on Layer 2 or 3. As a result, a single Application Data Unit (ADU) is fragmented into a smaller chunks with a maximum length of each chuck determined by the underlying computer network and its Maximum Transmission Unit (MTU), as illustrated in Fig. 4 (for example, ultra high definition video frame may be carried by more than one IP packet). The set of packets that carry the entirety of a single ADU are hereby defined as a *DUG*.

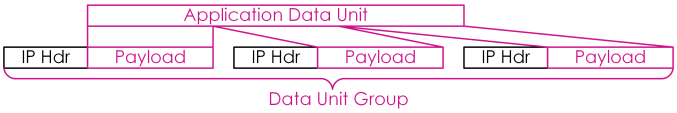

Fig. 4. Relationship between Application Data Unit and Data Unit Group.

Consequently, when the entire DUG is successfully exchanged between the sender and receiver, the receiving application will be able to retrieve the ADU as provided by the sender. In contrary, if a single packet went missing between the sender and receiver, the receiving application might not be able to read the ADU in its entirety.

While the usage of unreliable transport protocols, e.g. UDP, does not fundamentally change the illustration above by which each IP packet carries a fragment of the ADU, when using reliable protocols, such as TCP, the resulting IP stream defining the DUG is split into control packets which carry the necessary Layer 4 control information and the actual data frames. As these control frames are equally important to allow sender and receiver to complete their exchange of the ADU, special considerations will be required to not interfere with the semantics of reliable transport protocols.

B. IP Protocol Header Extension

Over recent decades, packet-switched networks in combination with the IP protocol suite have become the norm in enabling a digital communication across a range of computer networks including mobile networks. Also, the Internet Protocol in its both versions (Version 4 and Version 6) must be seen as the common lowest Open Systems Interconnection (OSI) layer denominator across a wide range of computer networks, making this protocol suite – and the IP protocol itself – an extremely significant component.

When looking at suitable protocol candidates for possible extension to support DUGs and allowing the signalling of DUG information from generic internet applications to lower

layers, the following constraints were identified. The chosen protocol:

- Allows for extension by the IETF without demanding backwards compatibility challenges for devices that do not support any proposed extension
- Is supported by the majority of communication devices
- Does not prevent information access by switches and routers when encryption is used

This paper proposes the introduction of DUG as an extension to the IP header for both dominant IP versions, i.e. Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6). As extending IPv4 and IPv6 headers follow different procedures set out in the IETF, the solutions are presented in separate sub-sections.

1) Internet Protocol Version 6: IPv6 addresses the challenge to allow routers to perform faster in comparison to its earlier Version 4. IPv6 achieves this by allowing network nodes to only parse the IPv6 headers it requires to perform its actions. In order to comply with this requirement and to follow the guidelines on how to design IPv6 header extensions [9], [10], i.e. using Type Length Values (TLVs), new IPv6 TLVs are defined, as illustrated in Figure 5.

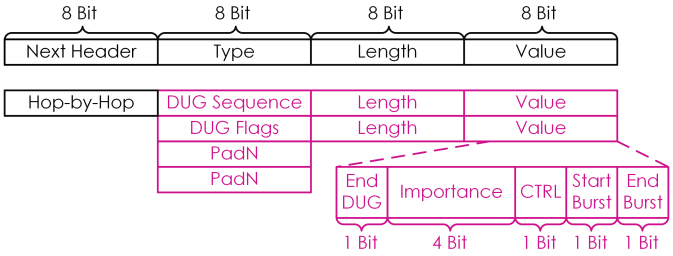

Fig. 5. Proposed Internet Protocol Version 6 Header Protocol Extension for Data Unit Groups.

As the order of extension headers are fixed in IPv6, the DUG-related information must be added to an appropriate IPv6 header. The main purpose of the proposed DUG TLVs is for intermediate node to read the values and perform any sort of traffic engineering upon them. Thus, the Hop-by-Hop options header is identified as the most appropriate one, as intermediate nodes – such as 3GPP UEs/UPFs or TSN switches – shall process the DUG-related information. The two new DUG TLVs defined are described in detail in Table II. The Flags TLV has a set of values which are presented and described in Table III.

2) Internet Protocol Version 4: As all IP modules that receive an IPv4 packet must implement the ability to read each field, making it less versatile to extend it with new header information compared to IPv6. As defined in [11], the Options field in the IPv4 header allows the addition of information to the IPv4 header and is variable in length with a maximum possible length of 40 bytes; all known option-type values are defined by the Internet Assigned Numbers Authority (IANA) [12]. Adding a new option requires to define the option by a 1 octet-long option-type, an option-length octet and the actual

TABLE II
TLVS FOR THE PROPOSED DUG IPV6 EXTENSION HEADER

Type	Length	Value
Sequence	8 bit	An unsigned integer number indicating the order of packets which a Data Unit Group. With each new packet, the sequence number is iterated by 1.
Flags	8 bit	A set of flags providing more contextual information about the application payload this IP packet carries. A detailed list of all flags are provided in Table 3.
PadN	16 bit	Two padding fields of a total length of 2 bytes to make the DUG extension header a multiple of 8 bytes

TABLE III
TLV FLAG FOR THE PROPOSED DUG IPV6 HEADER EXTENSION

Flag Name	Length	Description
End of DUG	1 bit	This bit indicates the end of the DUG.
Importance of DUG	4 bits	These bits indicate the importance of this packet against other packets in the same DUG. Lower values indicate a higher importance and allow to prioritise packets in different DUGs. Importance may be derived from the application type or the sensitivity of applications when not receiving a DUG in their application.
Control	1 bit	When reliable transport protocols are in use, e.g. TCP, or upper-layer control procedures take place, e.g. establishment of a Transport Layer Security (TLS) session, there is no ADU exchanged. However, these control packets are equally important to the delivery of an ADU and depending on their functionality in the communication sometime even more important than the ADU itself.
Start Burst	1 bit	This field indicates the start of a burst of packets within a DUG.
End Burst	1 bit	This field indicates the end of a burst of packets within a DUG.

data in a multiple of 8 bits (1 octet) again. Furthermore, the option-type field comes in a pre-defined three-field octet with 1 bit offering the option to be copied into all fragments in case IP fragmentation takes place, 2 bits to identify the classes the value represents (0: control; 1: reserved for future use; 2: debugging and measurement; 3: reserved for future use), and another 5 bits as the option number to help IP modules that read the header to interpret the meaning and implement a certain usage based on it.

To extend the IPv4 header with DUG-related information, a single 2 octet-long option may be used. The option-type will be set to Copy (1), Class (0) and Value (to be decided based on IANA). The option-length field will indicate 16 bits with the structure of the option-value field as illustrated in Fig. 6. The meaning of each field is identical to the IPv6 fields, as provided in Table II. To indicate the end of the options list, a 1 octet of 0s is added to the end of the options list.

C. Data Unit Group Rules Operations in a 3GPP Environment

This section provides the procedures for identifying a DUG using the proposed IP header extensions with the outcome to

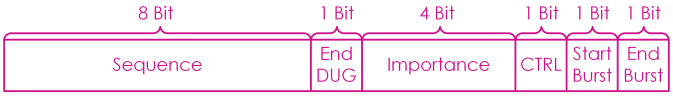

Fig. 6. Proposed IPv4 Header Protocol Extension for DUGs.

map it to PDU Set Markings allowing the 3GPP User Plane to take advantage of the PDU Set capabilities.

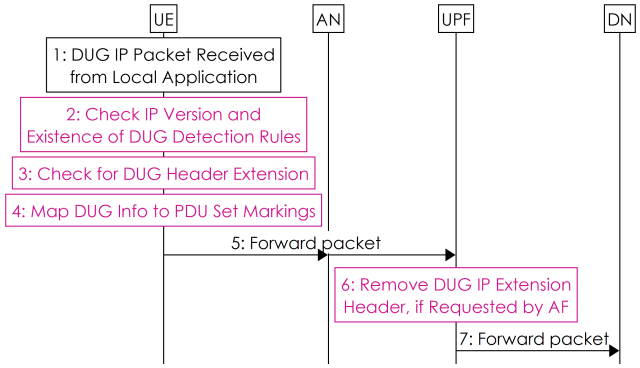

Fig. 7. 3GPP Up-link Procedures for Data Unit Group Internet Protocol Version 4 and Internet Protocol Version 6 Packets.

In Step 1, the UE receives an IP packet from an application with the DUG IP header extension being used (either IPv4 or IPv6) and now in Step 2 checks for the IP version of the packet from the local application based on the configured DUG Rules. The UE identifies the packet as an IP Version 4 or IP Version 6 packet. If the IP packet is identified as Version 4, the UE checks for the existence of the IPv4 DUG TLVs in the options field, following its definition in Section III-B2 (Step 3). If found, Step 4 applies. If the UE identified the IP packet as Version 6, the UE checks for the hop-by-hop header extension and the presence of DUG TLVs, as defined in Section III-B1. If found, Step 4 applies. If the UE cannot find any DUG-related header information, the packet is not identified as a member of a DUG and no further steps apply under this set of DUG Rules. The UE then identifies the DUG extension header information and writes the PDU Set Markings, as indicated in Table IV for IPv4 and in Table V for IPv6. Note that the PDU Set Markings are currently standardised in 3GPP [6] and the tables below merely serves as an example on the DUG to PDU Set Markings mapping based on the current information.

In Step 5, the UE sends the IP packet to the AN where the GPRS Tunnelling Protocol for User Plane (GTP-U) information is written so that the AN can send the IP packet to the UPF. The AN forwards the packet to the UPF via GTP-U signalling. To increase the compatibility with routers in the Data Network (DN) that do not implement the proposed DUG IPv4 or IPv6 header extension, the UPF may have received a configuration indicating that the UPF should remove this extension header for each up-link packet that arrived via N3 before it leaves on N6 (Step 6). Also, if the packet traverses to another UPF via N9, the UPF may remove the DUG header extension (for IPv6)/option (for IPv4). As the last step, the UPF forwards the IP packet towards the DN or alternatively to another UPF.

TABLE IV
INTERNET PROTOCOL VERSION 4 DATA UNIT GROUP HEADER EXTENSION FIELDS TO PACKET DATA UNIT SET MARKING MAPPING

IPv4 Header Field	**PDU Set Marking**
Identifier	PDU Set Sequence Number
DUG Extension Header: Sequence	PDU Sequence Number within a PDU Set
DUG Extension Header: Flags::End of DUG	End PDU of the PDU Set
DUG Extension Header: Flags::End of Burst	End of Data Burst
DUG Extension Header: Flags::Importance	PDU Set Importance

TABLE V
INTERNET PROTOCOL VERSION 6 DATA UNIT GROUP HEADER EXTENSION FIELDS TO PACKET DATA UNIT SET MARKING MAPPING

IPv6 Header Field	**PDU Set Marking**
Flow Label	PDU Set Sequence Number
DUG Extension Header: Sequence	PDU Sequence Number within a PDU Set
DUG Extension Header: Flags::End of DUG	End PDU of the PDU Set
DUG Extension Header: Flags::End of Burst	End of Data Burst
DUG Extension Header: Flags::Importance	PDU Set Importance

The down-link procedures are similar to the up-link ones, depicted in Fig. 7, with the change of the UPF detecting the DUG fields to write the GTP-U header fields for PDU Sets and the UE checking for DUG header fields and their potential removal before the packet is being passed up the protocol stack to a local application or out on a non-3GPP network port, e.g. to a TSN switch (DS-TT).

D. Example Operations in Time-Sensitive Networking Environment

The extension of the DUG concept to the TSN domain is described in this section. In 802.1cb IEEE defines how packet streams can be identified by a TSN switch and besides Layer 2-related header fields, e.g. source/destination Media Access Control (MAC) address or VLAN identifiers, IP header fields are considered already in this specification [2, Section 9.1.5]. Any DUG-related configuration of TSN switches to identify packets belonging to the same information stream should be understood as an extension to 802.1cb.

As described in Section II-A, a TSN switch first assesses the priority of incoming packets before it performs packet (re)scheduling tasks across its priority queues. Fig. 8 visualises in which part of the TSN operations the DUG information could be used to perform appropriate scheduling tasks and in case of timing constraints or time-related congestion, makes decisions which packets have priority based on the knowledge of multiple packets belonging to a DUG. The impacted components are the:

- Priority Filter: The TSN switch allows to be configured which DUG Flags TLV value is used to place a packet into which queue. Depending on how many queues are available and what algorithms are available in the re-ordering and pre-emption engine, the mapping of DUG packets may me a 1:1 to a queue based on the importance field; alternatively, the CTRL bit or start/end of burst fields might be used to prioritise packets of the same DUG differently.
- Re-ordering/Pre-Emption Engine: As the information is available which packets belong to a DUG and their respective importance, the TSN engine may re-schedule or pre-empt all DUG packets within the cycle, or of deemed possible drop an entire DUG to free up resources.

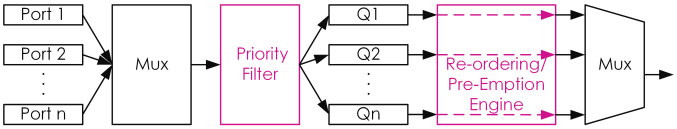

Fig. 8. Internal TSN Switch Flow Operations Using Data Unit Group Information.

E. Configuration of Data Unit Group Rules in Mobile Networks

In a 3GPP system, the Policy Control Function (PCF) may send Policy and Charging Control (PCC) Rules for a PDU Session to the Session Management Function (SMF). The PCC Rules may indicate to the SMF that one or more IP Flows of the PDU Session are expected to carry packets with the DUG extension header.

During a PDU Session Establishment or PDU Session Modification procedure, the SMF may provide DUG Rules to the UE. The DUG Rules may indicate which IP/UDP flows of the PDU Session are expected to carry packets with the DUG extension header. The DUG Rules may be sent to the UE in a PDU Session Establishment Accept message or a PDU Session Modification Command message. The DUG Rules may be part of the QoS rules (likely) or they may be part of any rule that lists IP flows and allows the SMF it indicate for which flows the DUG extension header is enabled (less likely).

The DUG Rules may indicate certain actions that the UE should take when it detects a packet that matches the rule. One example action is whether to forward the matching packet to a local application or a local network port. Another example action is to determine PDU Set information from the packet header and forward the PDU Set Information to the upper-layer (e.g. Service Data Adaptation Protocol (SDAP) or Packet Data Convergence Protocol (PDCP) layer) of the Radio Access Network (RAN) protocol stack. Another example action is to remove the DUG header option before forwarding the packet.

DUG Rules are categorised into detection and action rules for processing packets. DUG Detection Rules indicate the protocol header to check for, i.e. IPv4 or IPv6, and the exact header field, e.g. DUG header extension. The action then defines what to do with the packet once a Detection Rule found the referred header. Exemplary actions are “drop” or “remove DUG header”. Below, an exemplary representation using JavaScript Object Notation (JSON).

```
[{ "detection": {
      "header_type": "ipv4",
      "header_field": "extension",
      "type": "dug" },
   "action": { "remove_extension": "dug" } }]
```

IV. Conclusions and Outlook

This paper presented the novel Layer 3 solution of Data Unit Group, allowing intermediate network nodes to understand the relationship between packets and whether two or more carry a single ADU. The paper introduces extensions to IPv4 and IPv6 headers allowing applications to mark packets according to the ADU type and length. In QoS-constraint scenarios, the new header information is used in 3GPP networks to write PDU Set markings so that the underlying RAN layers can treat the packets according to their belonging to a group; alternatively, if a network node implements the vendor-agnostic TSN standard, pre-emptive packet treatment algorithms can utilise the information presented in the header. Detailed operations upon DUG-extended IP communication in 3GPP networks and TSN switches were presented in the paper.

As the next steps, the authors aim to implement the DUG concept as a standalone user space process in their TSN-enabled 3GPP testbed at Technology Readiness Level (TRL) 4, demonstrating the novel DUG concept in an Integrated Sensing and Communication (ISAC) use case, where non-3GPP sensors generate a range of different data, e.g. periodic single values or point-cloud information (from radar sensors), or even video to post-processing to sensing results in the Core Network.

References

[1] 3GPP. (2023, September) System architecture for the 5g system (release 18), technical specification 23.501.

[2] IEEE. (2022) Yang model for packet stream identification, 802.1cb. [Online]. Available: https://github.com/YangModels/yang/blob/main/standard/ieee/published/802.1/ieee802-dot1cb-stream-identification.yang

[3] ——. (2018) Standard for local and metropolitan area networks – bridges and bridged networks – amendment 31: Stream reservation protocol (srp) enhancements and performance improvements, 802.1qcc.

[4] ——. (2016) Standard for local and metropolitan area networks – station and media access control connectivity discovery, 802.1ab.

[5] ——. (2020) Standard for local and metropolitan area networks – timing and synchronization for time-sensitive applications, 802.1as.

[6] 3GPP. (2023, August) 5g real-time media transport protocol configurations (release 18), technical specification 26.522.

[7] ——. (2022, December) Study on xr (extended reality) and media services (release 18), technical report 23.700-60.

[8] J. Kaippallimalil, S. Gundavelli, and S. Dawkins, “Media Header Extensions for Wireless Networks,” Internet Engineering Task Force, Internet-Draft draft-kaippallimalil-tsvwg-media-hdr-wireless-03, Oct. 2023.

[9] S. Krishnan, james woodyatt, E. Kline, J. Hoagland, and M. Bhatia, “A Uniform Format for IPv6 Extension Headers,” RFC 6564, Apr. 2012.

[10] D. S. E. Deering and B. Hinden, “Internet Protocol, Version 6 (IPv6) Specification,” RFC 8200, Jul. 2017.

[11] “Internet Protocol,” RFC 791, Sep. 1981.

[12] IANA. (2018) Internet protocol version 4 parameters. [Online]. Available: https://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml