RAW WG   CJ. Bernardos
Internet-Draft   UC3M
Intended status: Standards Track   A. Mourad
Expires: August 26, 2021   InterDigital
                                                        February 22, 2021

Terminal-based joint selection and configuration of MEC host and RAW network
draft-bernardos-raw-joint-selection-raw-mec-00

Abstract

There are several scenarios involving multi-hop heterogeneous wireless networks requiring reliable and available features combined with multi-access edge computing, such as Industry 4.0. This document discusses mechanisms to allow a terminal influencing the selection of a MEC host for instantiation of the terminal-targeted MEC applications and functions, and (re)configuring the RAW network lying in between the terminal and the selected MEC host. This document assumes IETF RAW and ETSI MEC integration, fostering discussion about extensions at both IETF and ETSI MEC to better support these scenarios.

Status of This Memo

This Internet-Draft will expire on August 26, 2021.

Copyright Notice

Table of Contents

1. Introduction and Problem Statement

Wireless operates on a shared medium, and transmissions cannot be fully deterministic due to uncontrolled interferences, including self-induced multipath fading. RAW (Reliable and Available Wireless) is an effort to provide Deterministic Networking on across a path that include a wireless interface. RAW provides for high reliability and availability for IP connectivity over a wireless medium. The wireless medium presents significant challenges to achieve deterministic properties such as low packet error rate, bounded consecutive losses, and bounded latency. RAW extends the DetNet Working Group concepts to provide for high reliability and availability for an IP network utilizing scheduled wireless segments and other media, e.g., frequency/time-sharing physical media resources with stochastic traffic: IEEE Std. 802.15.4 timeslotted channel hopping (TSCH), 3GPP 5G ultra-reliable low latency communications (URLLC), IEEE 802.11ax/be, and L-band Digital Aeronautical Communications System (LDACS), etc. Similar to DetNet, RAW technologies aim at staying abstract to the radio layers underneath, addressing the Layer 3 aspects in support of applications requiring high reliability and availability.

As introduced in [I-D.pthubert-raw-architecture], RAW separates the path computation time scale at which a complex path is recomputed from the path selection time scale at which the forwarding decision is taken for one or a few packets. RAW operates at the path selection time scale. The RAW problem is to decide, amongst the redundant solutions that are proposed by the Patch Computation Element (PCE), which one will be used for each packet to provide a Reliable and Available service while minimizing the waste of constrained resources. To that effect, RAW defines the Path Selection Engine (PSE) that is the counter-part of the PCE to perform rapid local adjustments of the forwarding tables within the diversity that the PCE has selected for the Track. The PSE enables to exploit the richer forwarding capabilities with Packet (hybrid) ARQ, Replication, Elimination and Ordering (PAREO), and scheduled transmissions at a faster time scale.

Multi-access Edge Computing (MEC) -- formerly known as Mobile Edge Computing -- capabilities deployed in the edge of the mobile network can facilitate the efficient and dynamic provision of services to mobile users. The ETSI ISG MEC working group, operative from end of 2014, intends to specify an open environment for integrating MEC capabilities with service providers’ networks, including also applications from 3rd parties. These distributed computing capabilities will make available IT infrastructure as in a cloud environment for the deployment of functions in mobile access networks.

One relevant exemplary scenario showing the need for an integration of RAW and MEC is introduced next. One of the main (and distinct) use cases of 5G is Ultra Reliable and Low Latency Communications (URLLC). Among the many so-called "verticals" that require URLLC features, the Industry 4.0 (also referred to as Wireless for Industrial Applications) is probably the one with more short-term potential. As identified in [I-D.ietf-raw-use-cases], this scenario also calls for RAW solutions, as cables are not that suitable for the robots and mobile vehicles typically used in factories. This is also a very natural scenario for MEC deployments, as bounded, and very low latencies are needed between the robots and physical actuators and the control logic managing them.

This scenario includes a wireless domain, involving multiple MEC platforms to ensure low latency to applications, by being able to host MEC applications in several locations, and dynamically migrate the apps as the terminals move around and the serving MEC platform might no longer be capable of meeting the latency requirements.

This document discussess mechanisms to allow the UE to influence/ control jointly the RAW and MEC components deployed in the end-to-end path.

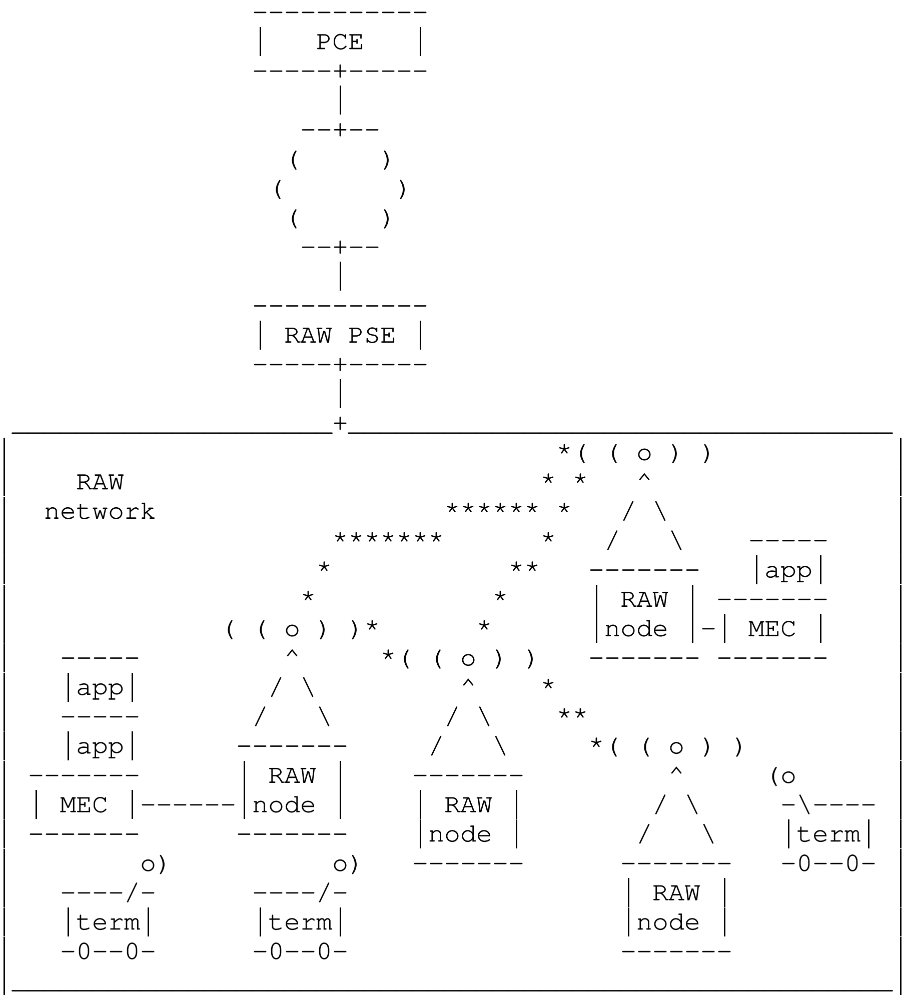

Figure 1: Exemplary scenario depicting MEC and RAW in an industrial environments

Figure 1 depicts an exemplary scenario that integrates a 3GPP 5G network, with ETSI MEC deployed at the edge, and an IETF RAW-capable wireless multi-hop backhaul segment connecting the RAN and the MEC hosts and UPFs. This setup can be used for example in a factory where multiple robots and AGVs are wirelessly connected, and controlled via remote apps. Control applications running in the edge (implemented as MEC applications) require bounded low latencies and a guaranteed availability, despite the mobility of the terminals and the changing wireless conditions. An heterogeneous wireless mesh network is used to provide connectivity inside the factory.

[I-D.bernardos-raw-mec] explores already the integration of RAW and MEC. The current document goes a bit further, proposing solutions to allow terminal-based selection of the MEC platform where to instantiate an app taking into account RAW aspects.

2. Terminology

The following terms used in this document are defined by the ETSI MEC ISG, and the IETF:

MEC host. The mobile edge host is an entity that contains a mobile edge platform and a virtualization infrastructure which provides compute, storage, and network resources, for the purpose of running mobile edge applications.

MEC platform. The mobile edge platform is the collection of essential functionalities required to run mobile edge applications on a particular virtualization infrastructure and enable them to provide and consume mobile edge services.

MEPM. MEC Platform Manager.

MEC applications. Mobile edge applications are instantiated on the virtualization infrastructure of the mobile edge host based on configuration requests validated by the mobile edge management.

PAREO. Packet (hybrid) ARQ, Replication, Elimination and Ordering. PAREO is a superset Of DetNet's PREOF that includes radio-specific techniques such as short range broadcast, MUMIMO, constructive interference and overhearing, which can be leveraged separately or combined to increase the reliability.

PSE. The Path Selection Engine (PSE) is the counter-part of the PCE to perform rapid local adjustments of the forwarding tables within the diversity that the PCE has selected for the Track. The PSE enables to exploit the richer forwarding capabilities with PAREO and scheduled transmissions at a faster time scale over the smaller domain that is the Track, in either a loose or a strict fashion.

UALCMP. The User Application LifeCycle Management Proxy (UALCMP) exposes the Mx2 API to the device application. It allows the device application to request the following application lifecycle management operations from the MEC system: query the available applications, instantiation and deletion of an application and update of an existing application context.

3. Terminal-based joint selection and configuration of MEC host and RAW network

This document defines extensions to: (i) enable a terminal to discover any RAW-enabled network on the path between the terminal and the MEC app host, and the RAW network associated capabilities; (ii) enable the terminal to request desired reliability and availability requirements to be met simultaneously by the MEC+RAW system; and, (iii) enable direct notifications from the RAW network to the terminal, to help with end-to-end application-level optimization. Most of the required extensions are related to ETSI MEC components and interfaces, and therefore are out of the scope of the IETF. However, we still briefly describe them for completeness, putting the main focus on the IETF RAW components and interactions.

Figure 2 shows the components and interfaces impacted by the extensions described in this document. The MEC UALCMP is logically extended with a RAW controller (RAW ctrl) functionality, to enable a terminal to learn about the RAW and MEC capabilities of the 5G network it is attached to, and specify its requirements in terms of availability and reliability for joint MEC app instantiation and RAW network configuration.

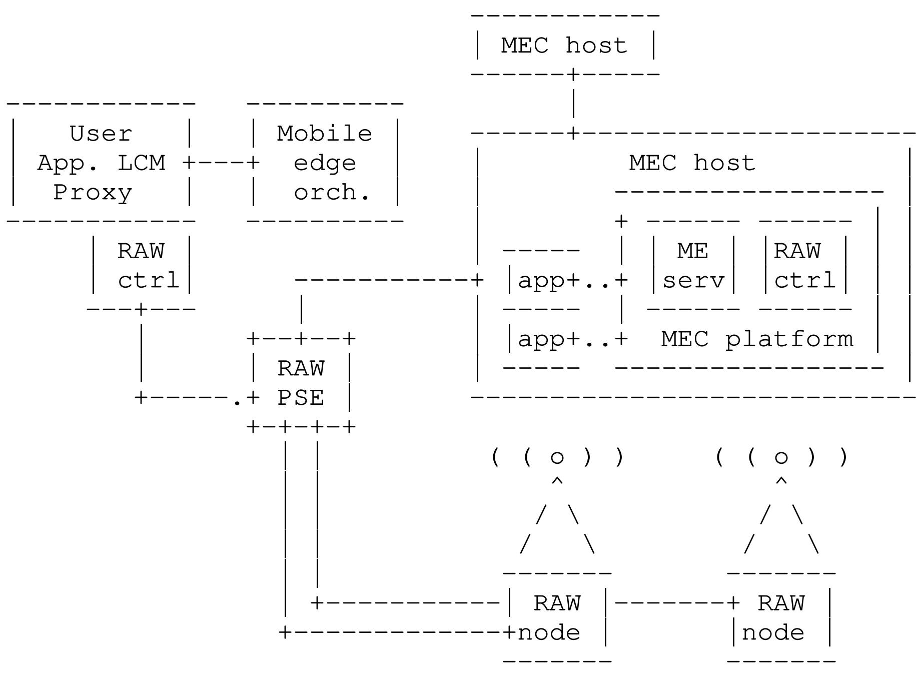

Figure 2: Block diagram

The RAW ctrl - RAW PSE interface was first introduced in [I-D.bernardos-raw-mec].

3.1. Extended User application look-up to support reliability and availability information/capabilities

Here we specify how the terminal/UE is augmented with the additional capability of discovering a RAW network on the path to the hosts of its target MEC applications, and obtaining information about reliability and availability configuration in the RAW network.

Figure 3 shows an exemplary signaling flow diagram.

```
                                                        +--------------+
        +----------+                                    |   MEC host   |
   +--+ |  UALCMP  |    +---+   +----+   +----+  +----+ |       +----+ |
   |UE| +---+----+-+    |RAW|   |MEAO|   |RAW |  |RAW | |  +---+ |RAW | |
   +--+   |  |RAW |      |PSE|   +----+   |node|  |node| |  |MEP| |ctrl| |
    |     |  |ctrl|      +---+     |      +----+  +----+ |  +---+ +----+ |
    |     |  +----+        |       |        |       |    +---|------|---+
    |     |    |          |<...RAW........>|       |        |      |
    |     |    |          |<...signalling.........>|        |      |
    |     |    |          |       |        |       |        |      |
    |1.GET ../app_list    |       |        |       |        |      |
    |....>|    |          |       |        |       |        |      |
    |     |........MEC...........>|.....MEC................>|      |
    |     |<.......signalling.....|<....signalling..........|      |
    |     |    |          |       |        |       |        |      |
    |     |2.RAW info req.|       |        |       |        |      |
    |     |...>|.........>|       |        |       |        |      |
    |     |<...|<.........|       |        |       |        |      |
    |     |    |          |       |        |       |        |      |
    |2.200 OK  |          |       |        |       |        |      |
    |(Application List)   |       |        |       |        |      |
    |     |    |          |       |        |       |        |      |
```

Figure 3: Extended User application look-up

We next explain each of the steps illustrated in the figure:

1. An application that requires use of a MEC app with specific reliability/availability requirements is started at the UE. The UE can either make use of a GET request to the MEC UALCMP extended to indicate that the UE is interested in reliability and availability information, or the UALCMP can decide to include this information based on policies. Either way, the UALCMP authorizes the request from the UE. The MEC system retrieves the list of UE applications available to the requesting UE (this might require interaction with other MEC system level components such as MEAO as depicted optionally in the figure).

2. The UALCMP requests information related to reliability and availability from the RAW PSE through the RAW ctrl logical component.

3. The UALCMP returns the 200 OK response to the device application, following ETSI MEC standards, but with its message body extended to include RAW parameters (namely, Reliability and availability characteristics of the application and its connectivity), such as:

- The assured round trip time in milliseconds supported by the MEC system for the MEC application instance.

- The assured connection bandwidth in kbit/s for the use of the MEC application instance.

- The assured jitter in milliseconds supported by the MEC system for the MEC application instance.

- The maximum percentage of packets failed.

- The assured number of redundant paths supported by the MEC system for the MEC application instance.

3.2. Extended Application context create to support reliability and availability information/capabilities

Here we specify how the UE is augmented with the capability to request the creation of a MEC app including requirements about reliability and availability.

```
                                                        +--------------+
        +----------+                                    |   MEC host   |
   +--+ |  UALCMP  |    +---+   +----+   +----+  +----+ |       +----+ |
   |UE| +---+----+-+    |RAW|   |MEAO|   |RAW |  |RAW | | +---+ |RAW | |
   +--+   | |RAW |      |PSE|   +----+   |node|  |node| | |MEP| |ctrl| |
    |     | |ctrl|      +---+     |      +----+  +----+ | +---+ +----+ |
    |     | +----+        |       |        |       |    +---|------|---+
    |     |    |          |<..RAW.........>|       |        |      |
    |     |    |          |<..signalling..........>|        |      |
    |     |    |          |       |        |       |        |      |
    |1.POST ../app_context|       |        |       |        |      |
    |....>|    |          |       |        |       |        |      |
    |     |..MEC signalling......>|..MEC signalling........>|      |
    |     |    |          |       |        |       |      2.MEC-to-RAW
    |     |    |          |       |        |       |        |.....>|
    |     |    |          |<..2.RAW................................|
    |     |    |<.........|....signalling.>|       |        |      |
    |     |    |          |.......................>|        |      |
    |     |    |          |       |        |       |        |<.....|
    |     |<......MEC.signalling..|<........MEC signalling..|      |
    |     |    |          |       |        |       |        |      |
    |3.201 Created        |       |        |       |        |      |
    |(AppContext)         |       |        |       |        |      |
    |     |    |          |       |        |       |        |      |
```

Figure 4: Application context create

Figure 4 shows an exemplary signaling flow diagram. We next explain each of the steps illustrated in the figure:

1. The UE submits the POST request to the UALCMP. The message body contains the data structure for the application context to be created, which is extended to include reliability and availability attributes:

   * The assured round trip time in milliseconds supported by the MEC system for the MEC application instance.

   * The assured connection bandwidth in kbit/s for the use of the MEC application instance.

   * The assured jitter in milliseconds supported by the MEC system for the MEC application instance.

   * The maximum percentage of packets failed.

   * The assured number of redundant paths supported by the MEC system for the MEC application instance.

   The UALCMP authorizes the request from the device application. The request is forwarded to the MEC system level management, which makes the decision on granting the context creation request. The MEC orchestrator triggers the creation of the application context in the MEC system, including the information about reliability and availability requirements. The UALCMP request the context creation to the MEAO, this request including the reliability and availability requirements of the application. The MEAO selects where to instantiate the application (meaning the MEC host and MEC platform), so it can meet all the requirements.

2. The MEP request to the local RAW ctrl to establish the connectivity between the app and the UE meeting the indicated reliability and availability requirements. This involves additional steps between the RAW ctrl, the RAW PSE and the RAW nodes that are part of the established path(s), as described in [I-D.bernardos-raw-mec].

3. The UALCMP returns the 201 Created response to the UE with the message body containing the data structure of the created application context.

3.3. Extended Application context update to support reliability and availability information/capabilities

Here we specify how the UE is augmented with the capability to request the update of the context of a MEC app including requirements about reliability and availability. One example would be communicating new reliability/availability requirements.

```
                                                        +--------------+
        +----------+                                    |   MEC host   |
   +--+ |  UALCMP  |    +---+   +----+   +----+  +----+ |       +----+ |
   |UE| +---+----+-+    |RAW|   |MEAO|   |RAW |  |RAW | | +---+ |RAW | |
   +--+   |  |RAW |      |PSE|   +----+   |node|  |node| | |MEP| |ctrl| |
    |     |  |ctrl|      +---+     |      +----+  +----+ | +---+ +----+ |
    |     |  +----+        |       |        |       |    +---|------|---+
    |     |    |          |<..RAW.........>|       |        |      |
    |     |    |          |<..signalling..........>|        |      |
    |     |    |          |       |        |       |        |      |
    |1.PUT ../app_contexts|       |        |       |        |      |
    | {contextID} (AppContext)    |        |       |        |      |
    |....>|    |          |       |        |       |        |      |
    |     |..MEC signalling......>|..MEC signalling........>|      |
    |     |    |          |       |        |       |      2.MEC-to-RAW
    |     |    |          |       |        |       |        |.....>|
    |     |    |          |<..2.RAW................................|
    |     |    |<.........|...signalling..>|       |        |      |
    |     |    |          |.......................>|        |      |
    |     |    |          |       |        |       |        |<.....|
    |     |<......MEC.signalling..|<........MEC signalling..|      |
    |     |    |          |       |        |       |        |      |
    |3.204 No Content     |       |        |       |        |      |
    |<....|    |          |       |        |       |        |      |
    |     |    |          |       |        |       |        |      |
```

Figure 5: Application context update

Figure 5 shows an exemplary signaling flow diagram. We next explain each of the steps illustrated in the figure:

1. An application running on the UE making use of a MEC app might change its requirements for the MEC app and associated reliability and availability (for example, in an Industry 4.0 scenario, a robot control app might be required less latency to improve its precision). The UE updates a specific application context by sending a PUT request to the resource within the MEC system that represents it, with the message body containing the modified data structure of AppContext in which only the callback reference and/or application location constraints, and/or the

application reliability and availability requirements (e.g., assured bandwidth, latency and reliability) may be updated.

2. Through interactions with the RAW ctrl, the RAW PSE is indicated to perform the required updates in the RAW network (via signalling with RAW nodes).

3. The UALCMP returns a "204 No Content" response.

3.4. Receiving extended notification events

Here we specify how the UE can receive updates about the RAW connectivity experienced by a MEC application, so it can react in time (e.g., implementing changes at the application level or selecting another point of attachment/slice).

```
                                                        +--------------+
        +----------+                                    |   MEC host   |
   +--+ |  UALCMP  |    +---+   +----+   +----+  +----+ |       +----+ |
   |UE| +---+----+-+    |RAW|   |MEAO|   |RAW |  |RAW | | +---+ |RAW | |
   +--+   |  |RAW |      |PSE|   +----+   |node|  |node| | |MEP| |ctrl| |
    |     |  |ctrl|      +---+     |      +----+  +----+ | +---+ +----+ |
    |     |  +----+        |       |        |       |    +---|------|---+
    |     |    |          |<..RAW.........>|       |        |      |
    |     |    |          |<..signalling..........>|        |      |
    |     |    |          |       |        |       |        |      |
    |     |    |      Event occurs (e.g., it is no longer   |      |
    |     |    |       to keep assured RAW conditions)      |      |
    |     |    |          |       |        |       |        |      |
    |     |    |          |1.MEC-to-RAW    |       |        |      |
    |     |    |          |.......................................>|
    |     |    |          |       |        |       |        |<.....|
    |     |<......MEC signalling..|<........MEC signalling..|      |
    |     |    |          |       |        |       |        |      |
    |2.POST ../callback_ref       |        |       |        |      |
    | ({Notification})    |       |        |       |        |      |
    |<....|    |          |       |        |       |        |      |
    |3.204 No Content     |       |        |       |        |      |
    |....>|    |          |       |        |       |        |      |
    |     |    |          |       |        |       |        |      |
```

Figure 6: Receiving notification events

Figure 5 shows an exemplary signaling flow diagram. We next explain each of the steps illustrated in the figure:

1. If a change of the assured RAW conditions happens (which is detected via RAW OAM mechanisms, out of the scope of this

document, and then notified to the MEC platform), this event reaches the MEC orchestrator, and finally the UALCMP.

2. The UALCMP sends a POST message to the callback reference address provided by the device application as part of application context creation, with the message body containing the {Notification} data structure. The variable {Notification} is replaced with the data type specified for different notification events as specified in ETSI MEC standards, extended to include a modification to the RAW conditions offered to the user application instance:

   * Updated assured round trip time in milliseconds supported by the MEC system for the MEC application instance.

   * Updated assured connection bandwidth in kbit/s for the use of the MEC application instance.

   * Updated maximum percentage of packets failed.

   * Updated assured jitter in milliseconds supported by the MEC system for the MEC application instance.

   * Updated assured number of redundant paths supported by the MEC system for the MEC application instance.

3. The device application sends a "204 No Content" response to the UALCMP.

4. IANA Considerations

TBD.

5. Security Considerations

TBD.

6. Acknowledgments

The work in this draft will be further developed and explored under the framework of the H2020 5Growth (Grant 856709).

7. Informative References

[I-D.bernardos-raw-mec]
Bernardos, C. and A. Mourad, "Extensions to enable wireless reliability and availability in multi- access edge deployments", draft-bernardos-raw-mec-01 (work in progress), January 2021.

[I-D.ietf-raw-use-cases]
Papadopoulos, G., Thubert, P., Theoleyre, F., and C. Bernardos, "RAW use cases", draft-ietf-raw-use-cases-00 (work in progress), October 2020.

[I-D.pthubert-raw-architecture]
Thubert, P., Papadopoulos, G., and R. Buddenberg, "Reliable and Available Wireless Architecture/Framework", draft-pthubert-raw-architecture-05 (work in progress), November 2020.

Authors' Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Alain Mourad
InterDigital Europe

Email: Alain.Mourad@InterDigital.com
URI: http://www.InterDigital.com/

RAW WG
Internet-Draft
Intended status: Standards Track
Expires: July 22, 2021

CJ. Bernardos
UC3M
A. Mourad
InterDigital
January 18, 2021

Extensions to enable wireless reliability and availability in multi-access edge deployments
draft-bernardos-raw-mec-01

Abstract

There are several scenarios involving multi-hop heterogeneous wireless networks requiring reliable and available features combined with multi-access edge computing, such as Industry 4.0. This document describes solutions integrating IETF RAW and ETSI MEC, fostering discussion about extensions at both IETF and ETSI MEC to better support these scenarios.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Wireless operates on a shared medium, and transmissions cannot be fully deterministic due to uncontrolled interferences, including self-induced multipath fading. RAW (Reliable and Available Wireless) is an effort to provide Deterministic Networking on across a path that include a wireless interface. RAW provides for high reliability and availability for IP connectivity over a wireless medium. The wireless medium presents significant challenges to achieve deterministic properties such as low packet error rate, bounded consecutive losses, and bounded latency. RAW extends the DetNet Working Group concepts to provide for high reliability and availability for an IP network utilizing scheduled wireless segments and other media, e.g., frequency/time-sharing physical media resources with stochastic traffic: IEEE Std. 802.15.4 timeslotted channel hopping (TSCH), 3GPP 5G ultra-reliable low latency communications (URLLC), IEEE 802.11ax/be, and L-band Digital Aeronautical Communications System (LDACS), etc. Similar to DetNet, RAW technologies aim at staying abstract to the radio layers underneath, addressing the Layer 3 aspects in support of applications requiring high reliability and availability.

As introduced in [I-D.pthubert-raw-architecture], RAW separates the path computation time scale at which a complex path is recomputed from the path selection time scale at which the forwarding decision is taken for one or a few packets. RAW operates at the path selection time scale. The RAW problem is to decide, amongst the redundant solutions that are proposed by the Patch Computation Element (PCE), which one will be used for each packet to provide a

Reliable and Available service while minimizing the waste of constrained resources. To that effect, RAW defines the Path Selection Engine (PSE) that is the counter-part of the PCE to perform rapid local adjustments of the forwarding tables within the diversity that the PCE has selected for the Track. The PSE enables to exploit the richer forwarding capabilities with Packet (hybrid) ARQ, Replication, Elimination and Ordering (PAREO), and scheduled transmissions at a faster time scale.

Multi-access Edge Computing (MEC) -- formerly known as Mobile Edge Computing -- capabilities deployed in the edge of the mobile network can facilitate the efficient and dynamic provision of services to mobile users. The ETSI ISG MEC working group, operative from end of 2014, intends to specify an open environment for integrating MEC capabilities with service providers' networks, including also applications from 3rd parties. These distributed computing capabilities will make available IT infrastructure as in a cloud environment for the deployment of functions in mobile access networks.

One relevant exemplary scenario showing the need for an integration of RAW and MEC is introduced next. One of the main (and distinct) use cases of 5G is Ultra Reliable and Low Latency Communications (URLLC). Among the many so-called "verticals" that require URLLC features, the Industry 4.0 (also referred to as Wireless for Industrial Applications) is probably the one with more short-term potential. As identified in [I-D.bernardos-raw-use-cases], this scenario also calls for RAW solutions, as cables are not that suitable for the robots and mobile vehicles typically used in factories. This is also a very natural scenario for MEC deployments, as bounded, and very low latencies are needed between the robots and physical actuators and the control logic managing them. Figure 1 depicts an exemplary scenario of a factory where terminals (robots and mobile automated guided vehicles) are wirelessly connected. Control applications running in the edge (implemented as MEC applications) require bounded low latencies and a guaranteed availability, despite the mobility of the terminals and the changing wireless conditions. An heterogeneous wireless mesh network is used to provide connectivity inside the factory.

```
                   -----------
                   |   PCE   |
                   -----+-----
                        |
                      --+--
                     (     )
                    (       )
                     (     )
                      --+--
                        |
                   -----------
                   | RAW PSE |
                   -----+-----
                        |
    ____________________+__________________________________
   |                                  *( ( o ) )           |
   |    RAW                          * *   ^               |
   |  network                  ****** *   / \              |
   |                    *******      *   /   \    -----    |
   |                   *           **   -------   |app|    |
   |                  *           *     | RAW | -------    |
   |             ( ( o ) )*      *      |node |-| MEC |    |
   |   -----         ^     *( ( o ) )   ------- -------    |
   |   |app|        / \         ^    *                     |
   |   -----       /   \       / \    **                   |
   |   |app|      -------     /   \     *( ( o ) )         |
   | -------      | RAW |    -------         ^     (o      |
   | | MEC |------|node |    | RAW |        / \     -\---- |
   | -------      -------    |node |       /   \    |term| |
   |        o)          o)   -------      -------   -0--0- |
   |   ----/-      ----/-                 | RAW |          |
   |   |term|      |term|                 |node |          |
   |   -0--0-      -0--0-                 -------          |
   |                                                       |
   |_______________________________________________________|
```

Figure 1: Exemplary scenario depicting MEC and RAW in an industrial environments

This scenario includes a wireless domain, involving multiple MEC platforms to ensure low latency to applications, by being able to host MEC applications in several locations, and dynamically migrate the apps as the terminals move around and the serving MEC platform might no longer be capable of meeting the latency requirements.

2. Terminology

The following terms used in this document are defined by the ETSI MEC ISG, and the IETF:

MEC host. The mobile edge host is an entity that contains a mobile edge platform and a virtualization infrastructure which provides compute, storage, and network resources, for the purpose of running mobile edge applications.

MEC platform. The mobile edge platform is the collection of essential functionalities required to run mobile edge applications on a particular virtualization infrastructure and enable them to provide and consume mobile edge services.

MEPM. MEC Platform Manager.

MEC applications. Mobile edge applications are instantiated on the virtualization infrastructure of the mobile edge host based on configuration requests validated by the mobile edge management.

PAREO. Packet (hybrid) ARQ, Replication, Elimination and Ordering. PAREO is a superset Of DetNet's PREOF that includes radio-specific techniques such as short range broadcast, MUMIMO, constructive interference and overhearing, which can be leveraged separately or combined to increase the reliability.

PSE. The Path Selection Engine (PSE) is the counter-part of the PCE to perform rapid local adjustments of the forwarding tables within the diversity that the PCE has selected for the Track. The PSE enables to exploit the richer forwarding capabilities with PAREO and scheduled transmissions at a faster time scale over the smaller domain that is the Track, in either a loose or a strict fashion.

3. Problem Statement

With current standards, the MEC platform(s) would have to interact with a Path Computation Element (PCE) for data plane requests and updates. This tremendously limits the capabilities to guarantee real-time forwarding decisions, as it will make it challenging and not possible to manage forwarding decisions in real or near-real time.

RAW solutions and approaches being explored today consider the role of the PSE, which computes at a short time scale which of the available paths (called tracks) -- computed by a PCE -- should be used per flow/packet and also which PAREO functions can be used, in order to provide the flow with the required availability and reliability features. The PSE interacts with the PCE and with the RAW nodes so they can setup the required per-flow state, to recognize the flow and determine the forwarding policy to be applied. These RAW forwarding decisions can be distributed among the necessary nodes using in-band signaling (e.g., extending Segment Routing, BIER-TE or DETNET tagging) or can be taken autonomously by each forwarding node locally (based on its knowledge of the status of the network, gained via OAM RAW-specific mechanisms).

Figure 1 shows an exemplary scenario, depicting an industrial environment where different nodes are wirelessly connected to provide connectivity to several stationary and mobile terminals (i.e., robots). Industry environments are a good example of applications where reliability and availability are critical. Ensuring this in wireless heterogeneous and multi-hop networks requires using multiple paths, using PAREO functions and even using dual or multiple connectivity. Terminal mobility makes it even more challenging to guarantee certain reliability and availability levels, due to the dynamic and fast changes that this needs at the data plane level. The short-time scale forwarding decisions that are required to ensure reliability and availability with terminal mobility cannot be managed if MEC platforms can only interact with the data plane through the PCE.

The PCE is responsible for routing computation and maintenance in a network and it is typically a centralized entity that can even reside outside the network. It is meant to compute and establish redundant paths, but not to be sensitive/reactive to transient changes, and therefore is not capable of ensuring a certain level of reliability and availability in a wireless heterogeneous mesh network, especially if some of the nodes (e.g., the end terminals) might be mobile. With currently standardized solutions, a MEC platform could only interact with the RAW network through the PCE, most possibly through the Mp2 reference point defined by ETSI MEC. This reference point is defined between the MEC platform and the data plane of the virtualization infrastructure to instruct the data plane on how to route traffic among applications, networks, services, etc. This reference point is not further specified by ETSI MEC, but it would be the one that could be used by current solutions to allow for MEC to request the data plane on the RAW network a certain behavior (in terms of availability and reliability) for MEC app traffic flows. With existing solutions, the PCE would be the entry point for configuring and managing the RAW network, probably through the Mp2 reference point. Note that the PCE might reside outside the RAW network, the path between the RAW network and the PCE might be expensive and slow (e.g., it might need to traverse the whole RAW network) and reaching to the PCE can also be slow in regards to the speed of events that affect the forwarding operation at the radio layer.

Additionally, the MEC architecture as currently defined by ETSI does not have any component designed to deal with the specifics of an heterogeneous wireless multi-hop networks (such a RAW one), and therefore, it is very limited in terms of what a MEC app (through the MEC platform) can request to the data plane of an heterogeneous wireless multi-hop network. Besides, this lack of RAW-aware component at the ETSI MEC architecture prevents any enhancement at either the MEC side (e.g., MEC app migrations triggered by RAW status updates) or the RAW side (e.g., PAREO function updates triggered by MEC app/terminal mobility).

Because of all these aforementioned reasons, it is needed to define a new RAW-enabled component at the ETSI MEC architecture, aimed at enabling a more direct interaction between the MEC platform and the RAW network, allowing the MEC platform to notify events and/or request actions to the RAW network quick enough. This involves some challenges, as the RAW PSE has to understand the needs from the running MEC applications, so it can properly configure the RAW nodes so the data plane provides the required reliability and availability.

4. RAW and MEC integration

This document defines a new entity inside the MEC platform: the RAW ctrl. This entity is responsible for computing what to instruct the RAW PSE, based on the requirements of the MEC apps, as well as to take decisions at the MEC side (e.g., migration of apps) based on information about the RAW network status.

As a result of the introduction of the RAW ctrl and the actions it is responsible of, new interactions and interface semantics are added. These interactions and semantics can be terminated at either the PCE or the RAW PSE, depending on the requirements of the MEC apps. For near real-time coordination and control between MEC and RAW mechanisms, the interactions are between the RAW ctrl and the RAW PSE. We mostly refer to this deployment model from now on, as it is the one that allow for near real-time updates on the forwarding plane, but note that an alternative deployment model in which the RAW ctrl interacts with the PCE is also possible, though only supporting non real-time interactions.

The MEC-RAW new interface semantics/extensions depicted in Figure 2 allows the MEC platform to issue requests to the RAW network, through the RAW PSE, so it can behave as required by MEC apps.

```
                ------------                         --- Data plane
                | MEC host |                -------  ... Control plane
   ----------   ------------         .......+ PCE +..
   | Mobile |         .              .      ---+--- .( ( o ) ) ( ( o ) )
   |  edge  |   ------+--------------.------   |    .    ^         ^
   |  orch. |   |         MEC host   .     |   |    .   / \       / \
   ----+-----   |        ------------.---- |   |    .  /   \     /   \
       .      .............+ ------ ---+-- | --+--  ..+------   -------
   ----+----- . | -----  | | ME | |RAW +.....+RAW|    | RAW +...+ RAW |
   | Mobile | . | |app+..+ |serv| |ctrl| | | |PSE+....+node |   |node +
   |  edge  +.. | -----  | ------ ------ | | -----    ---+--+---+------
   |platform|   | |app+..+  MEC platform | |             |
   |manager |   | --+--  ----------------- |             |
   ----------   ----|-----------------------             |
                    |                                    |
                    +------------------------------------+
```

Figure 2: Block diagram

The new semantics of the interface between the MEC platform and the RAW PSE do not only serve to convey the requests, but also to synchronize the status and topology of the RAW (relevant portion of the) network, enabling to perform real-time or near-real time forwarding decisions. In the sequel, we show different exemplary signaling diagrams for the most relevant procedures.

4.1. MEC app request for RAW

Here we specify the interface extensions and signaling procedures needed to enable a MEC app describe and request its needs in terms of availability and reliability. As it will be further developed in other subsections, the wireless network conditions could also have an impact back on the MEC platform (e.g., by triggering the migration of the MEC app).

Figure 3 shows an exemplary signaling flow diagram, in which a certain MEC app request a given behavior for the treatment of the packets the app generates. We consider an industrial wireless application scenario, as the one used in previous sections, as an example for the sake of describing the interface and specified interactions.

The MEC platform is enhanced with a RAW ctrl entity, as introduced in the previous section. The RAW ctrl is a RAW-aware component within the MEC architecture that enables the required interactions with the RAW network, through the RAW PSE. This allows MEC apps to: (i) adapt to RAW conditions (e.g., if the requested reliability and availability is not possible), and (ii) dynamically modify the requested flow forwarding to the RAW network, based on the MEC app and mobility conditions.

```
   +-----------+     +-----+     +----+     +----+     +----+     +----+
   |      RAW  |     | RAW |     |RAW |     |RAW |     |RAW |     |RAW |
   | app  ctrl |     | PSE |     |node|     |node|     |node|     |term|
   +-----------+     +-----+     +----+     +----+     +----+     +----+
      |     |           |           |          |          |         |
   1.MEC app req.       |           |          |          |         |
      |....>|           |           |          |          |         |
      |     |           |           |          |          |         |
      |   2a.MEC-to-RAW req.        |          |          |         |
      |(flow ID,flow spec,reqs.)    |          |          |         |
      |     |..........>|           |          |          |         |
      |     |           |           |          |          |         |
      |   2b.MEC-to-RAW resp.       |          |          |         |
      |   (flow ID,status=OK)       |          |          |         |
      |     |<..........|           |          |          |         |
      |     |           | 3.RAW control        |          |         |
      |     |           | (flow ID,flow spec,PAREO)       |         |
      |     |           |..........>|          |          |         |
      |     |           |.....................>|          |         |
      |     |           |................................>|         |
      |     |           |           |          |          |         |
      | 4a.MEC app      |           |4b.MEC app traffic w/ in-band  |
      |    traffic      |           |  RAW control (flow ID, PAREO) |
      |<--------------------------->|<------------------->|         |
      |     |           |           | (example: packet replication/ |
      |     |           |           |  overhearing, elimination)    |
      |     |           |           |<-------->|<-------->|<------->|
      |     |           |           |          |          |         |
```

Figure 3: MEC app request for RAW

We next explain each of the steps illustrated in the figure:

1. A MEC app which is going to be consumed by a given terminal (or set of terminals, though in this example we show just one consumer), specifies to the MEC platform the characteristics of the traffic is going to generate and its associated requirements.

2. The MEC platform -- namely the RAW ctrl component, which is RAW-aware and knows the characteristics of the deployment -- analyzes the characteristics of the MEC app traffic and the provided requirements, and generates a new request -- over a new interface between the MEC platform and the RAW PSE -- that includes, among others, the following parameters:

- An ID for the given flow, which can be used for future near real-time update/configuration operations on the same flow.

- The flow specification, describing the characteristics of the packets, allowing an efficient identification of flow(s) based on well-known fields in IPv4, IPv6, and transport layer headers like TCP and UDP. An example of how to do this is defined in the Traffic Selectors for Flow Bindings [RFC6088].

- The requirements of the flow in terms of reliability and availability.

3. The RAW PSE processes the request, and based on its knowledge of the network (topology, node capabilities and ongoing flows) computes the best way of transmitting the packets over the RAW network (using the available paths/tracks, previously computed by a PCE). Note that at this point it might be possible that the RAW PSE realizes that it is not possible to provide the requested reliability and availability characteristics, and would report that back to the MEC platform (which might issue a new request with less requirements). The RAW PSE sends control packets to each of the RAW nodes involved, instructing how to deal with the packets belonging to the MEC app flow. This includes:

   - assigning an ID to the flow;

   - instructing the entry point in the RAW network to tag packets with that ID;

   - specific PAREO functions to be used by each of the RAW nodes. This might be signaled to each of the RAW nodes, or just to some of them (e.g., only the entry point) who can then use in-band signaling to specify it.

4. The MEC app generates traffic (step 4a in the figure) which arrives at the RAW entry point in the network, which following the instructions of the RAW PSE, encapsulates and tags the packet, and might also include in-band signaling (e.g., using Segment Routing). Some PAREO functions are applied to the MEC app traffic packets (step 4b in the figure) to achieve the required levels of reliability and availability. In the figure, as an example, packets are replicated (this could be done by means of wireless overhearing) at one point of the network, and then later duplicated packets eliminated.

4.2. RAW OAM triggering MEC app migration

Here we specify the mechanisms for MEC to benefit from RAW OAM information, for example, to trigger the migration of a MEC application to a different MEC platform, to ensure that the requirements of the MEC app continue to be met.

```
   +----+         +--------+     +---+    +----+  +----+  +----+  +----+
   |    |         |    RAW |     |RAW|    |RAW |  |RAW |  |RAW |  |RAW |
   |MEPM|         |app ctrl|     |PSE|    |node|  |node|  |node|  |term|
   +----+         +--------+     +---+    +----+  +----+  +----+  +----+
     |              |    |         |        |       |       |        |
     |              | MEC app      |   MEC app traffic w/ in-band    |
     |              | traffic      |  RAW control (flow ID, PAREO)   |
     |              |<--------------------->|<------------->|        |
     |              |    |         | (example: packet replication/   |
     |              |    |         |    overhearing, elimination)    |
     |              |    |         |        |<----->|<----->|<------>|
     |              |    |         |        |       |       |        |
     |              |    |         |   1.RAW OAM signalling |        |
     |  +--------+  |    |         |<.......|       |       |        |
     |  |    RAW |  | 2.MEC-to-RAW |<...............|       |        |
     |  |app ctrl|  |   (flow ID,  |<.......................|        |
     |  +--------+  |    status=KO)|<................................|
     |    |    |    |    |<........|        |       |       |        |
     |3.MEC app migration|         |        |       |       |        |
     |<.................>|         |        |       |       |        |
     |<.......>|    |    |         |        |       |       |        |
     |    |    |    |    |         |        |       |       |        |
     |    |    | 4a.MEC-to-RAW req.|        |       |       |        |
     |    |   (flow ID,flow spec,reqs.)     |       |       |        |
     |    |    |..................>|        |       |       |        |
     |    |    4b.MEC-to-RAW resp. |        |       |       |        |
     |    |    (flow ID,status=OK) |  5.RAW control |       |        |
     |    |    |<..................|   (flow ID,flow spec,PAREO)     |
     |    |    |    |    |         |.......>|       |       |        |
     |    |    |    |    |         |...............>|       |        |
     |    |    |    |    |         |.......................>|        |
     |    |    |    |    |         |................................>|
     |    |    |    |    |         |        |       |       |        |
     |    6a.MEC app|    |         | 6b.MEC app traffic w/ in-band   |
     |    |  traffic|    |         |    RAW control (flow ID, PAREO) |
     |    |<------------------------------->|<------------->|        |
     |    |    |    |    |         | (example: packet replication/   |
     |    |    |    |    |         |    overhearing, elimination)    |
     |    |    |    |    |         |        |<----->|<----->|<------>|
     |    |    |    |    |         |        |       |       |        |
```

Figure 4: RAW OAM triggering MEC app migration

Figure 4 shows an exemplary signaling flow diagram, in which changes in the RAW network, detected thanks to RAW OAM, trigger the migration of a MEC app. We assume there is already a MEC app deployed and traffic is already flowing (i.e., all the procedures explained in the previous section took already place). We next explain each of the steps illustrated in the figure:

1. RAW OAM signaling is periodically and reactively exchanged between the RAW nodes and the RAW PSE [I-D.theoleyre-raw-oam-support].

2. If the conditions of the network get worse (e.g., because of changes in the radio propagation of a critical link), making it impossible to guarantee the required levels of reliability and availability, this generates a message from the RAW PSE to the MEC platform, indicating that a given MEC app flow can no longer be served.

3. The currently serving MEC platform triggers a MEC app migration to a different MEC platform. This involves the MEC platform manager. Note that the MEC platform might provide suggestions regarding where to migrate the MEC app, based on its knowledge of the RAW network status, acquired by the RAW ctrl through interactions with the PSE.

4. The same steps 2-3-4 specified in the procedure described in Section 4.1 take place. In this step, the MEC platform generates a new request to the RAW PSE.

5. The RAW PSE processes the request, and based on its knowledge of the network computes the best way of transmit the packets over the RAW network. The RAW PSE sends control packets to each of the RAW nodes involved.

6. The MEC app generates traffic, arriving at the RAW entry point in the network, which following the instructions of the RAW PSE, encapsulates and tags the packet.

4.3. MEC OAM for RAW updates

There are scenarios and situations where -- due to the mobility of the terminals or the nodes hosting the MEC platform hosting a given MEC app -- it might be needed to take actions on the RAW network: e.g., to update the paths, apply different PAREO functions, migrate the MEC app (thus involving a change in the RAW forwarding). This triggers the need for mechanisms enabling the RAW PSE to get and use MEC OAM information to update traffic forwarding at the RAW network as needed to adapt to varying conditions, e.g., due to node mobility.

```
   +---------+    +-----+    +----+   +----+   +----+   +----+   +----+
   |     RAW |    | RAW |    |RAW |   |RAW |   |RAW |   |RAW |   |RAW |
   |app  ctrl|    | PSE |    |node|   |node|   |node|   |node|   |term|
   +---------+    +-----+    +----+   +----+   +----+   +----+   +----+
     |     |         |          |        |        |        |       |
     | MEC app       |          | MEC app traffic w/ in-band       |
     | traffic       |          | RAW control (flow ID, PAREO)     |
     |<------------------------>|<--------------->|        |       |
     |     |         |          | (example: packet replication/    |
     |     |         |          |    overhearing, elimination)     |
     |     |         |          |<------>|<------>|<-------------->|
     |     |         |          |        |        |        |       |
     |     |1a.Mobility trigger |        |        |        |       |
     |     |(flow ID,trajectory)|        |        |        |       |
     |     |........>|          |        |        |        |       |
     |     |         |          |        |        |        |       |
     |     |1b.Mobility trigger ACK      |        |        |       |
     |     |(flow ID)|          |        |        |        |       |
     |     |<........|          |        |        |        |       |
     |     |         | 2.RAW control     |        |        |       |
     |     |         | (flow ID,flow spec,PAREO)  |        |       |
     |     |         |.........>|        |        |        |       |
     |     |         |..................>|        |        |       |
     |     |         |...........................>|        |       |
     |     |         |....................................>|       |
     |     |         |............................................>|
     |     |         |          |        |        |        |       |
     | 3a.MEC app    |          |3b.MEC app traffic w/ in-band     |
     |    traffic    |          |  RAW control (flow ID, PAREO)    |
     |<------------------------>|<--------------->|<------>|       |
     |     |         |          | (example: packet replication/    |
     |     |         |          |  overhearing, elimination)       |
     |     |         |          |<-------->|<---->|<------>|<----->|
     |     |         |          |          |      |        |       |
```

Figure 5: MEC OAM for RAW updates

Figure 5 shows an exemplary signaling flow diagram, in which the mobility of the a node (in this case the terminal, but it could have been the MEC platform hosting the MEC app) triggers the need for updating RAW forwarding mechanisms. As in the previous section, we assume there is already a MEC app deployed and traffic is already flowing (i.e., all the procedures explained in Section 4.1 took already place). We next explain each of the steps illustrated in the figure:

1. The MEC platform notifies that the terminal consuming the MEC app is moving (note that it other events can be notified, such as the

mobility of the MEC platform itself), including the expected trajectory (if can be known or predicted in advance, as it will be the case in most cases in several scenarios, such as industrial use cases).

2. The RAW PSE uses this information to re-compute how to best provided the reliability and availability needed by the MEC app traffic flow, and updates the RAW nodes about the PAREO functions that they have to apply.

3. After this, traffic from the MEC app benefits from updated policies, computed according to the new conditions, and ensuring that the requirements of the MEC app continue to be fulfilled.

5. IANA Considerations

TBD.

6. Security Considerations

TBD.

7. Acknowledgments

The work in this draft will be further developed and explored under the framework of the H2020 5Growth (Grant 856709).

8. Informative References

[I-D.bernardos-raw-use-cases]
Papadopoulos, G., Thubert, P., Theoleyre, F., and C. Bernardos, "RAW use cases", draft-bernardos-raw-use-cases-04 (work in progress), July 2020.

[I-D.pthubert-raw-architecture]
Thubert, P., Papadopoulos, G., and R. Buddenberg, "Reliable and Available Wireless Architecture/Framework", draft-pthubert-raw-architecture-05 (work in progress), November 2020.

[I-D.theoleyre-raw-oam-support]
Theoleyre, F., Papadopoulos, G., and G. Mirsky, "Operations, Administration and Maintenance (OAM) features for RAW", draft-theoleyre-raw-oam-support-04 (work in progress), October 2020.

[RFC6088] Tsirtsis, G., Giarreta, G., Soliman, H., and N. Montavont, "Traffic Selectors for Flow Bindings", RFC 6088, DOI 10.17487/RFC6088, January 2011, <https://www.rfc-editor.org/info/rfc6088>.

Authors' Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Alain Mourad
InterDigital Europe

Email: Alain.Mourad@InterDigital.com
URI: http://www.InterDigital.com/

RAW
Internet-Draft
Intended status: Informational
Expires: 21 August 2021

N. Maeurer, Ed.
T. Graeupl, Ed.
German Aerospace Center (DLR)
C. Schmitt, Ed.
Research Institute CODE, UniBwM

17 February 2021

L-band Digital Aeronautical Communications System (LDACS)
draft-ietf-raw-ldacs-07

Abstract

This document provides an overview of the architecture of the L-band Digital Aeronautical Communications System (LDACS), which provides a secure, scalable and spectrum efficient terrestrial data link for civil aviation. LDACS is a scheduled, reliable multi-application cellular broadband system with support for IPv6. LDACS SHALL provide a data link for IP network-based aircraft guidance. High reliability and availability for IP connectivity over LDACS are therefore essential.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

One of the main pillars of the modern Air Traffic Management (ATM) system is the existence of a communication infrastructure that enables efficient aircraft control and safe separation in all phases of flight. Current systems are technically mature but suffering from the VHF band's increasing saturation in high-density areas and the limitations posed by analogue radio communications. Therefore, aviation globally and the European Union (EU) in particular, strives for a sustainable modernization of the aeronautical communication infrastructure.

In the long-term, ATM communication SHALL transition from analogue VHF voice and VDLM2 communication to more spectrum efficient digital data communication. The European ATM Master Plan foresees this transition to be realized for terrestrial communications by the development (and potential implementation) of the L-band Digital Aeronautical Communications System (LDACS). LDACS SHALL enable IPv6 based air- ground communication related to the aviation safety and regularity of flight. The particular challenge is that no additional spectrum can be made available for terrestrial aeronautical communication. It was thus necessary to develop co-existence mechanism/procedures to enable the interference free operation of LDACS in parallel with other aeronautical services/systems in the same frequency band.

Since LDACS SHALL be used for aircraft guidance, high reliability and availability for IP connectivity over LDACS are essential.

1.1. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Terminology

The following terms are used in the context of RAW in this document:

A2A Air-to-Air
AeroMACS Aeronautical Mobile Airport Communication System
A2G Air-to-Ground
ACARS Aircraft Communications Addressing and Reporting System
ADS-C Automatic Dependent Surveillance - Contract
AM(R)S Aeronautical Mobile (Route) Service
ANSP Air Traffic Network Service Provider
AOC Aeronautical Operational Control
AS Aircraft Station
ATC Air-Traffic Control
ATM Air-Traffic Management
ATN Aeronautical Telecommunication Network
ATS Air Traffic Service
CCCH Common Control Channel
COTS IP Commercial Off-The-Shelf
CM Context Management
CNS Communication Navigation Surveillance
CPDLC Controller Pilot Data Link Communication
DCCH Dedicated Control Channel
DCH Data Channel
DLL Data Link Layer
DLS Data Link Service
DME Distance Measuring Equipment
DSB-AM Double Side-Band Amplitude Modulation
FCI Future Communication Infrastructure
FL Forward Link
GNSS Global Navigation Satellite System
GS Ground-Station
G2A Ground-to-Air
HF High Frequency
ICAO International Civil Aviation Organization
IP Internet Protocol
kbit/s kilobit per second
LDACS L-band Digital Aeronautical Communications System
LLC Logical Link Control

LME LDACS Management Entity
MAC Medium Access Layer
MF Multi Frame
OFDM Orthogonal Frequency-Division Multiplexing
OFDMA Orthogonal Frequency-Division Multiplexing Access
OSI Open Systems Interconnection
PHY Physical Layer
RL Reverse Link
SF Super-Frame
SNP Sub-Network Protocol
TDMA Time-Division Multiplexing-Access
VDLM1 VHF Data Link mode 1
VDLM2 VHF Data Link mode 2
VHF Very High Frequency
VI Voice Interface

3. Motivation and Use Cases

Aircraft are currently connected to Air-Traffic Control (ATC) and Aeronautical Operational Control (AOC) via voice and data communications systems through all phases of a flight. Within the airport terminal, connectivity is focused on high bandwidth communications, while during en-route high reliability, robustness, and range is the main focus. Voice communications MAY use the same or different equipment as data communications systems. In the following the main differences between voice and data communications capabilities are summarized. The assumed use cases for LDACS completes the list of use cases stated in [RAW-USE-CASES] and the list of reliable and available wireless technologies presented in [RAW-TECHNOS].

3.1. Voice Communications Today

Voice links are used for Air-to-Ground (A2G) and Air-to-Air (A2A) communications. The communication equipment is either ground-based working in the High Frequency (HF) or Very High Frequency (VHF) frequency band or satellite-based. All VHF and HF voice communications is operated via open broadcast channels without authentication, encryption or other protective measures. The use of well-proven communication procedures via broadcast channels helps to enhance the safety of communications by taking into account that other users MAY encounter communication problems and MAY be supported, if REQUIRED. The main voice communications media is still the analogue VHF Double Side-Band Amplitude Modulation (DSB-AM) communications technique, supplemented by HF Single Side-Band Amplitude Modulation and satellite communications for remote and oceanic areas. DSB-AM has been in use since 1948, works reliably and safely, and uses low-cost communication equipment. These are the main reasons why VHF DSB-AM communications is still in use, and it is likely that this technology will remain in service for many more years. This however results in current operational limitations and impediments in deploying new Air-Traffic Management (ATM) applications, such as flight-centric operation with Point-to-Point communications.

3.2. Data Communications Today

Like for voice, data communications into the cockpit is currently provided by ground-based equipment operating either on HF or VHF radio bands or by legacy satellite systems. All these communication systems are using narrowband radio channels with a data throughput capacity in order of kilobits per second. While the aircraft is on ground some additional communications systems are available, like the Aeronautical Mobile Airport Communication System (AeroMACS) or public cellular networks, operating in the Airport (APT) domain and able to deliver broadband communication capability.

The data communication networks used for the transmission of data relating to the safety and regularity of the flight MUST be strictly isolated from those providing entertainment services to passengers. This leads to a situation that the flight crews are supported by narrowband services during flight while passengers have access to inflight broadband services. The current HF and VHF data links cannot provide broadband services now or in the future, due to the lack of available spectrum. This technical shortcoming is becoming a limitation to enhanced ATM operations, such as Trajectory-Based Operations and 4D trajectory negotiations.

Satellite-based communications are currently under investigation and enhanced capabilities are under development which will be able to provide inflight broadband services and communications supporting the safety and regularity of flight. In parallel, the ground-based broadband data link technology LDACS is being standardized by ICAO and has recently shown its maturity during flight tests [SCH20191]. The LDACS technology is scalable, secure and spectrum efficient and provides significant advantages to the users and service providers. It is expected that both - satellite systems and LDACS - will be deployed to support the future aeronautical communication needs as envisaged by the ICAO Global Air Navigation Plan.

4. Provenance and Documents

The development of LDACS has already made substantial progress in the Single European Sky ATM Research framework, short SESAR, and is currently being continued in the follow-up program SESAR2020 [RIH2018]. A key objective of the this activities is to develop, implement and validate a modern aeronautical data link able to evolve with aviation needs over long-term. To this end, an LDACS specification has been produced [GRA2019] and is continuously updated; transmitter demonstrators were developed to test the spectrum compatibility of LDACS with legacy systems operating in the L-band [SAJ2014]; and the overall system performance was analyzed by computer simulations, indicating that LDACS can fulfil the identified requirements [GRA2011].

LDACS standardization within the framework of the ICAO started in December 2016. The ICAO standardization group has produced an initial Standards and Recommended Practices document [ICA2018]. It defines the general characteristics of LDACS. The ICAO standardization group plans to produce an ICAO technical manual - the ICAO equivalent to a technical standard - within the next years. Generally, the group is open to input from all sources and develops LDACS in the open.

Up to now LDACS standardization has been focused on the development of the physical layer and the data link layer, only recently have higher layers come into the focus of the LDACS development activities. There is currently no "IPv6 over LDACS" specification publicly available; however, SESAR2020 has started the testing of IPv6-based LDACS testbeds.

The IPv6 architecture for the aeronautical telecommunication network is called the Future Communications Infrastructure (FCI). FCI SHALL support quality of service, diversity, and mobility under the umbrella of the "multi-link concept". This work is conducted by ICAO Communication Panel working group WG-I.

In addition to standardization activities several industrial LDACS prototypes have been built. One set of LDACS prototypes has been evaluated in flight trials confirming the theoretical results predicting the system performance [GRA2018] [SCH20191].

5. Applicability

LDACS is a multi-application cellular broadband system capable of simultaneously providing various kinds of Air Traffic Services (including ATS-B3) and AOC communications services from deployed Ground-Stations (GS). The A2G sub-system physical layer and data link layer of LDACS are optimized for data link communications, but the system also supports digital air-ground voice communications.

LDACS supports communication in all airspaces (airport, terminal maneuvering area, and en-route), and on the airport surface. The physical LDACS cell coverage is effectively de-coupled from the operational coverage REQUIRED for a particular service. This is new in aeronautical communications. Services requiring wide-area coverage can be installed at several adjacent LDACS cells. The handover between the involved LDACS cells is seamless, automatic, and transparent to the user. Therefore, the LDACS A2G communications concept enables the aeronautical communication infrastructure to support future dynamic airspace management concepts.

5.1. Advances Beyond the State-of-the-Art

LDACS offers several capabilities that are not provided in contemporarily deployed aeronautical communication systems.

5.1.1. Priorities

LDACS is able to manage services priorities, an important feature not available in some of the current data link deployments. Thus, LDACS guarantees bandwidth, low latency, and high continuity of service for safety critical ATS applications while simultaneously accommodating less safety-critical AOC services.

5.1.2. Security

LDACS is a secure data link with built-in security mechanisms. It enables secure data communications for ATS and AOC services, including secured private communications for aircraft operators and ANSPs (Air Traffic Network Service Providers). This includes concepts for key and trust management, mutual authenticated key exchange protocols, key derivation measures, user and control message-in-transit confidentiality and authenticity protection, secure logging and availability and robustness measures [MAE20181], [MAE20191], [MAE20192].

5.1.3. High Data Rates

The user data rate of LDACS is 315 kbit/s to 1428 kbit/s on the forward link (FL) for the connection Ground-to-Air (G2A), and 294 kbit/s to 1390 kbit/s on the reverse link (RF) for the connection A2G, depending on coding and modulation. This is 50 times the amount terrestrial digital aeronautical communications systems such as VDLM2 provide [SCH20191].

5.2. Application

LDACS SHALL be used by several aeronautical applications ranging from enhanced communication protocol stacks (multi-homed mobile IPv6 networks in the aircraft and potentially ad-hoc networks between aircraft) to classical communication applications (sending GBAS correction data) and integration with other service domains (using the communication signal for navigation).

5.2.1. Air-to-Ground Multilink

It is expected that LDACS together with upgraded satellite-based communications systems will be deployed within the FCI and constitute one of the main components of the multilink concept within the FCI.

Both technologies, LDACS and satellite systems, have their specific benefits and technical capabilities which complement each other. Especially, satellite systems are well-suited for large coverage areas with less dense air traffic, e.g. oceanic regions. LDACS is well-suited for dense air traffic areas, e.g. continental areas or hot-spots around airports and terminal airspace. In addition, both technologies offer comparable data link capacity and, thus, are well-suited for redundancy, mutual back-up, or load balancing.

Technically the FCI multilink concept SHALL be realized by multi-homed mobile IPv6 networks in the aircraft. The related protocol stack is currently under development by ICAO and the Single European Sky ATM Research framework.

5.2.2. Air-to-Air Extension for LDACS

A potential extension of the multi-link concept is its extension to ad-hoc networks between aircraft.

Direct A2A communication between aircrafts in terms of ad-hoc data networks is currently considered a research topic since there is no immediate operational need for it, although several possible use cases are discussed (digital voice, wake vortex warnings, and trajectory negotiation) [BEL2019]. It SHOULD also be noted that currently deployed analog VHF voice radios support direct voice communication between aircraft, making a similar use case for digital voice plausible.

LDACS direct A2A is currently not part of standardization.

5.2.3. Flight Guidance

The FCI (and therefore LDACS) SHALL be used to host flight guidance. This is realized using three applications:

1. Context Management (CM): The CM application SHALL manage the automatic logical connection to the ATC center currently responsible to guide the aircraft. Currently this is done by the air crew manually changing VHF voice frequencies according to the progress of the flight. The CM application automatically sets up equivalent sessions.
2. Controller Pilot Data Link Communication (CPDLC): The CPDLC application provides the air crew with the ability to exchange data messages similar to text messages with the currently responsible ATC center. The CPDLC application SHALL take over most of the communication currently performed over VHF voice and enable new services that do not lend themselves to voice communication (e.g., trajectory negotiation).
3. Automatic Dependent Surveillance - Contract (ADS-C): ADS-C reports the position of the aircraft to the currently active ATC center. Reporting is bound to "contracts", i.e. pre-defined events related to the progress of the flight (i.e. the trajectory). ADS-C and CPDLC are the primary applications used to implement in-flight trajectory management.

CM, CPDLC, and ADS-C are available on legacy datalinks, but not widely deployed and with limited functionality.

Further ATC applications MAY be ported to use the FCI or LDACS as well. A notable application is GBAS for secure, automated landings: The Global Navigation Satellite System (GNSS) based Ground Based Augmentation System (GBAS) is used to improve the accuracy of GNSS to allow GNSS based instrument landings. This is realized by sending GNSS correction data (e.g., compensating ionospheric errors in the GNSS signal) to the aircraft’s GNSS receiver via a separate data link. Currently the VDB data link is used. VDB is a narrow-band single-purpose datalink without advanced security only used to transmit GBAS correction data. This makes VDB a natural candidate for replacement by LDACS.

5.2.4. Business Communication of Airlines

In addition to air traffic services AOC services SHALL be transmitted over LDACS. AOC is a generic term referring to the business communication of airlines. Regulatory this is considered related to the safety and regularity of flight and MAY therefore be transmitted over LDACS.

AOC communication is considered the main business case for LDACS communication service providers since modern aircraft generate significant amounts of data (e.g., engine maintenance data).

5.2.5. LDACS Navigation

Beyond communication radio signals can always also be used for navigation. LDACS takes this into account.

For future aeronautical navigation, ICAO RECOMMENDS the further development of GNSS based technologies as primary means for navigation. However, the drawback of GNSS is its inherent single point of failure - the satellite. Due to the large separation between navigational satellites and aircraft, the received power of GNSS signals on the ground is very low. As a result, GNSS disruptions might occasionally occur due to unintentional interference, or intentional jamming. Yet the navigation services MUST be available with sufficient performance for all phases of flight. Therefore, during GNSS outages, or blockages, an alternative solution is needed. This is commonly referred to as Alternative Positioning, Navigation, and Timing (APNT).

One of such APNT solution consists of integrating the navigation functionality into LDACS. The ground infrastructure for APNT is deployed through the implementation of LDACS's GSs and the navigation capability comes "for free".

LDACS navigation has already been demonstrated in practice in a flight measurement campaign [SCH20191].

6. Requirements to LDACS

The requirements to LDACS are mostly defined by its application area: Communication related to safety and regularity of flight.

A particularity of the current aeronautical communication landscape is that it is heavily regulated. Aeronautical data links (for applications related to safety and regularity of flight) MAY only use spectrum licensed to aviation and data links endorsed by ICAO. Nation states can change this locally, however, due to the global scale of the air transportation system adherence to these practices is to be expected.

Aeronautical data links for the Aeronautical Telecommunication Network (ATN) are therefore expected to remain in service for decades. The VDLM2 data link currently used for digital terrestrial internetworking was developed in the 1990es (the use of the Open Systems Interconnection (OSI) stack indicates that as well). VDLM2 is expected to be used at least for several decades. In this respect aeronautical communication (for applications related to safety and regularity of flight) is more comparable to industrial applications than to the open Internet.

Internetwork technology is already installed in current aircraft. Current ATS applications use either the Aircraft Communications Addressing and Reporting System (ACARS) or the OSI stack. The objective of the development effort LDACS as part of the FCI is to replace legacy OSI stack and proprietary ACARS internetwork technologies with industry standard IP technology. It is anticipated that the use of Commercial Off-The-Shelf (COTS) IP technology mostly applies to the ground network. The avionics networks on the aircraft will likely be heavily modified or proprietary.

AOC applications currently mostly use the same stack (although some applications, like the graphical weather service MAY use the commercial passenger network). This creates capacity problems (resulting in excessive amounts of timeouts) since the underlying terrestrial data links (VDLM1/2) do not provide sufficient bandwidth. The use of non-aviation specific data links is considered a security problem. Ideally the aeronautical IP internetwork and the Internet SHOULD be completely separated.

The objective of LDACS is to provide a next generation terrestrial data link designed to support IP and provide much higher bandwidth to avoid the currently experienced operational problems.

The requirement for LDACS is therefore to provide a terrestrial high-throughput data link for IP internetworking in the aircraft.

In order to fulfil the above requirement LDACS needs to be interoperable with IP (and IP-based services like Voice-over-IP) at the gateway connecting the LDACS network to other aeronautical ground networks (the totality of them being the ATN). On the avionics side in the aircraft aviation specific solutions are to be expected.

In addition to the functional requirements LDACS and its IP stack need to fulfil the requirements defined in RTCA DO-350A/EUROCAE ED-228A [DO350A]. This document defines continuity, availability, and integrity requirements at different scopes for each air traffic management application (CPDLC, CM, and ADS-C). The scope most relevant to IP over LDACS is the CSP (Communication Service Provider) scope.

Continuity, availability, and integrity requirements are defined in [DO350A] volume 1 Table 5-14, and Table 6-13. Appendix A presents the REQUIRED information.

In a similar vein, requirements to fault management are defined in the same tables.

7. Characteristics of LDACS

LDACS will become one of several wireless access networks connecting aircraft to the ATN implemented by the FCI and possibly ACARS/FANS networks [FAN2019].

The current LDACS design is focused on the specification of layer 2.

Achieving stringent the continuity, availability, and integrity requirements defined in [DO350A] will require the specification of layer 3 and above mechanisms (e.g. reliable crossover at the IP layer). Fault management mechanisms are similarly undefined. Input from the working group will be appreciated here.

7.1. LDACS Sub-Network

An LDACS sub-network contains an Access Router (AR) and several GS, each of them providing one LDACS radio cell.

User plane interconnection to the ATN is facilitated by the AR peering with an A2G Router connected to the ATN.

The internal control plane of an LDACS sub-network interconnects the GS. An LDACS sub-network is illustrated in Figure 1.

```
   wireless      user
   link          plane
     AS-------------GS---------------AR---A2G-----ATN
                    .                |   Router
                    . control        |
                    . plane          |
                    .                |
                    GS...............|
                    .                |
                    .                |
                    GS---------------+
```

Figure 1: LDACS sub-network with three GSs and one AS

7.2. Topology

LDACS operating in A2G mode is a cellular point-to-multipoint system. The A2G mode assumes a star-topology in each cell where Aircraft Stations (AS) belonging to aircraft within a certain volume of space (the LDACS cell) is connected to the controlling GS. The LDACS GS is a centralized instance that controls LDACS A2G communications within its cell. The LDACS GS can simultaneously support multiple bi-directional communications to the ASs under its control. LDACS's GSs themselves are connected to each other and the AR.

Prior to utilizing the system an AS has to register with the controlling GS to establish dedicated logical channels for user and control data. Control channels have statically allocated resources, while user channels have dynamically assigned resources according to the current demand. Logical channels exist only between the GS and the AS.

The LDACS wireless link protocol stack defines two layers, the physical layer and the data link layer.

7.3. LDACS Physical Layer

The physical layer provides the means to transfer data over the radio channel. The LDACS GS supports bi-directional links to multiple aircraft under its control. The FL direction at the G2A connection and the RL direction at the A2G connection are separated by Frequency Division Duplex. FL and RL use a 500 kHz channel each. The GS transmits a continuous stream of Orthogonal Frequency-Division Multiplexing (OFDM) symbols on the FL. In the RL different aircraft are separated in time and frequency using a combination of Orthogonal

Frequency-Division Multiple-Access (OFDMA) and Time-Division Multiple-Access (TDMA). Aircraft thus transmit discontinuously on the RL with radio bursts sent in precisely defined transmission opportunities allocated by the GS.

7.4. LDACS Data Link Layer

The data-link layer provides the necessary protocols to facilitate concurrent and reliable data transfer for multiple users. The LDACS data link layer is organized in two sub-layers: The medium access sub-layer and the Logical Link Control (LLC) sub-layer. The medium access sub-layer manages the organization of transmission opportunities in slots of time and frequency. The LLC sub-layer provides acknowledged point-to-point logical channels between the aircraft and the GS using an automatic repeat request protocol. LDACS supports also unacknowledged point-to-point channels and G2A broadcast.

7.5. LDACS Mobility

LDACS supports layer 2 handovers to different LDACS channels. Handovers MAY be initiated by the aircraft (break-before-make) or by the GS (make-before-break). Make-before-break handovers are only supported for GSs connected to each other.

External handovers between non-connected LDACS sub-networks or different aeronautical data links SHALL be handled by the FCI multi-link concept.

8. Reliability and Availability

8.1. Layer 2

LDACS has been designed with applications related to the safety and regularity of flight in mind. It has therefore been designed as a deterministic wireless data link (as far as this is possible).

Based on channel measurements of the L-band channel [SCHN2016] and respecting the specific nature of the area of application, LDACS was designed from the PHY layer up with robustness in mind.

In order to maximize the capacity per channel and to optimally use the available spectrum, LDACS was designed as an OFDM-based Frequency Division Duplex system, supporting simultaneous transmissions in FL at the G2A connection and RF at the A2G connection. The legacy systems already deployed in the L-band limit the bandwidth of both channels to approximately 500 kHz.

The LDACS physical layer design includes propagation guard times sufficient for the operation at a maximum distance of 200 nautical miles from the GS. In actual deployment, LDACS can be configured for any range up to this maximum range.

The LDACS FL physical layer is a continuous OFDM transmission. LDACS RL transmission is based on OFDMA-TDMA bursts, with silence between such bursts. The RL resources (i.e. bursts) are assigned to different ASs on demand by the GS.

The LDACS physical layer supports adaptive coding and modulation for user data. Control data is always encoded with the most robust coding and modulation (QPSK coding rate 1/2).

LDACS medium access on top of the physical layer uses a static frame structure to support deterministic timer management. As shown in Figure 3 and Figure 4, LDACS framing structure is based on Super-Frames (SF) of 240ms duration corresponding to 2000 OFDM symbols. FL and RL boundaries are aligned in time (from the GS perspective) allowing for deterministic sending windows for KEEP ALIVE messages and control and data channels in general.

LDACS medium access is always under the control of the GS of a radio cell. Any medium access for the transmission of user data has to be requested with a resource request message stating the requested amount of resources and class of service. The GS performs resource scheduling on the basis of these requests and grants resources with resource allocation messages. Resource request and allocation messages are exchanged over dedicated contention-free control channels.

The purpose of Quality-of-Service in LDACS medium access is to provide prioritized medium access at the bottleneck (the wireless link). The signaling of higher layer Quality-of-Service requirements to LDACS is yet to be defined. A DiffServ-based solution with a small number of priorities is to be expected.

LDACS has two mechanisms to request resources from the scheduler in the GS.

Resources can either be requested "on demand" with a given priority. On the FL, this is done locally in the GS, on the RL a dedicated contention-free control channel is used called Dedicated Control Channel (DCCH), which is roughly 83 bit every 60 ms. A resource allocation is always announced in the control channel of the FL, short Common Control Channel (CCCH) having variable size. Due to the spacing of the RL control channels every 60 ms, a medium access delay in the same order of magnitude is to be expected.

Resources can also be requested "permanently". The permanent resource request mechanism supports requesting recurring resources in given time intervals. A permanent resource request has to be canceled by the user (or by the GS, which is always in control).

User data transmissions over LDACS are therefore always scheduled by the GS, while control data uses statically (i.e. at cell entry) allocated recurring resources (DCCH and CCCH). The current specification specifies no scheduling algorithm. Scheduling of RL resources is done in physical Protocol Data Units of 112 bit (or larger if more aggressive coding and modulation is used). Scheduling on the FL is done Byte-wise since the FL is transmitted continuously by the GS.

In addition to having full control over resource scheduling, the GS can send forced Handover commands for off-loading or RF channel management, e.g. when the signal quality declines and a more suitable GS is in the AS reach. With robust resource management of the capacities of the radio channel, reliability and robustness measures are therefore also anchored in the LDACS management entity.

In addition, to radio resource management, the LDACS control channels are also used to send keep-alive messages, when they are not otherwise used. Since the framing of the control channels is deterministic, missing keep-alive messages can thus be immediately detected. This information is made available to the multi-link protocols for fault management.

The protocol used to communicate faults is not defined in the LDACS specification. It is assumed that vendors would use industry standard protocols like the Simple Network Management Protocol or the Network Configuration Protocol where security permits.

The LDACS data link layer protocol running on top of the medium access sub-layer uses ARQ to provide reliable data transmission on layer 2.

It employs selective repeat ARQ with transparent fragmentation and reassembly to the resource allocation size to achieve low latency and a low overhead without losing reliability. It ensures correct order of packet delivery without duplicates. In case of transmission errors it identifies lost fragments with deterministic timers synced to the medium access frame structure and initiates retransmission. Additionally, the priority mechanism of LDACS ensures the timely delivery of messages with high importance.

8.2. Beyond Layer 2

LDACS availability can be increased by appropriately deploying LDACS infrastructure: This means proliferating the number of terrestrial base stations. However, the scarcity of aeronautical spectrum for data link communication (in the case of LDACS: tens of MHz in the L-band) and the long range (in the case of LDACS: up to 400 km) make this quite hard. The deployment of a larger number of small cells is certainly possible, suffers, however, also from the scarcity of spectrum. An additional constraint to take into account, is that Distance Measuring Equipment (DME) is the primary user of the aeronautical L-band. That is, any LDACS deployment has to take DME frequency planning into account, too.

The aeronautical community has therefore decided not to rely on a single communication system or frequency band. It is envisioned to have multiple independent data link technologies in the aircraft (e.g., terrestrial and satellite communications) in addition to legacy VHF voice.

However, as of now no reliability and availability mechanisms that could utilize the multi-link have been specified on Layer 3 and above.

Below Layer 2 aeronautics usually relies on hardware redundancy. To protect availability of the LDACS link, an aircraft equipped with LDACS will have access to two L-band antennae with triple redundant radio systems as REQUIRED for any safety relevant aeronautical systems by ICAO.

9. Protocol Stack

The protocol stack of LDACS is implemented in the AS and GS: It consists of the Physical Layer (PHY) with five major functional blocks above it. Four are placed in the Data Link Layer (DLL) of the AS and GS: (1) Medium Access Layer (MAC), (2) Voice Interface (VI), (3) Data Link Service (DLS), and (4) LDACS Management Entity (LME). The last entity resides within the Sub-Network Layer: Sub-Network Protocol (SNP). The LDACS network is externally connected to voice units, radio control units, and the ATN Network Layer.

Figure 2 shows the protocol stack of LDACS as implemented in the AS and GS.

```
            IPv6                   Network Layer
             |
             |
   +------------------+  +----+
   |        SNP       |--|    |   Sub-Network
   |                  |  |    |   Layer
   +------------------+  |    |
             |           | LME|
   +------------------+  |    |
   |        DLS       |  |    |   Logical Link
   |                  |  |    |   Control Layer
   +------------------+  +----+
             |             |
            DCH        DCCH/CCCH
             |         RACH/BCCH
             |             |
   +--------------------------+
   |           MAC            |   Medium Access
   |                          |   Layer
   +--------------------------+
                |
   +--------------------------+
   |           PHY            |   Physical Layer
   +--------------------------+
                |
                |
              ((*))
              FL/RL              radio channels
                                 separated by
                                 Frequency Division Duplex
```

Figure 2: LDACS protocol stack in AS and GS

9.1. MAC Entity Services

The MAC time framing service provides the frame structure necessary to realize slot-based Time Division Multiplex (TDM) access on the physical link. It provides the functions for the synchronization of the MAC framing structure and the PHY Layer framing. The MAC time framing provides a dedicated time slot for each logical channel.

The MAC Sub-Layer offers access to the physical channel to its service users. Channel access is provided through transparent logical channels. The MAC Sub-Layer maps logical channels onto the appropriate slots and manages the access to these channels. Logical channels are used as interface between the MAC and LLC Sub-Layers.

The LDACS framing structure for FL and RL is based on Super-Frames (SF) of 240 ms duration. Each SF corresponds to 2000 OFDM symbols. The FL and RL SF boundaries are aligned in time (from the view of the GS).

In the FL, an SF contains a Broadcast Frame of duration 6.72 ms (56 OFDM symbols) for the Broadcast Control Channel (BCCH), and four Multi-Frames (MF), each of duration 58.32 ms (486 OFDM symbols).

In the RL, each SF starts with a Random Access (RA) slot of length 6.72 ms with two opportunities for sending RL random access frames for the Random Access Channel (RACH), followed by four MFs. These MFs have the same fixed duration of 58.32 ms as in the FL, but a different internal structure

Figure 3 and Figure 4 illustrate the LDACS frame structure.

```
   ^
   |     +------+------------+------------+------------+------------+
   |  FL | BCCH |     MF     |     MF     |     MF     |     MF     |
   F     +------+------------+------------+------------+------------+
   r     <---------------- Super-Frame (SF) - 240ms ----------------->
   e
   q     +------+------------+------------+------------+------------+
   u  RL | RACH |     MF     |     MF     |     MF     |     MF     |
   e     +------+------------+------------+------------+------------+
   n     <---------------- Super-Frame (SF) - 240ms ----------------->
   c
   y
   |
   ----------------------------- Time ------------------------------->
   |
```

Figure 3: SF structure for LDACS

```
   ^
   |     +-------------+------+-------------+
   |  FL |     DCH     | CCCH |     DCH     |
   F     +-------------+------+-------------+
   r     <---- Multi-Frame (MF) - 58.32ms -->
   e
   q     +------+---------------------------+
   u  RL | DCCH |             DCH           |
   e     +------+---------------------------+
   n     <---- Multi-Frame (MF) - 58.32ms -->
   c
   y
   |
   -------------------- Time ------------------>
   |
```

Figure 4: MF structure for LDACS

9.2. DLS Entity Services

The DLS provides acknowledged and unacknowledged (including broadcast and packet mode voice) bi-directional exchange of user data. If user data is transmitted using the acknowledged DLS, the sending DLS entity will wait for an acknowledgement from the receiver. If no acknowledgement is received within a specified time frame, the sender MAY automatically try to retransmit its data. However, after a certain number of failed retries, the sender will suspend further retransmission attempts and inform its client of the failure.

The DLS uses the logical channels provided by the MAC:

1. A GS announces its existence and access parameters in the Broadcast Channel (BC).
2. The RA channel enables AS to request access to an LDACS cell.
3. In the FL the CCCH is used by the GS to grant access to data channel resources.
4. The reverse direction is covered by the RL, where ASs need to request resources before sending. This happens via the DCCH.
5. User data itself is communicated in the Data Channel (DCH) on the FL and RL.

9.3. VI Services

The VI provides support for virtual voice circuits. Voice circuits MAY either be set-up permanently by the GS (e.g., to emulate voice party line) or MAY be created on demand. The creation and selection of voice circuits is performed in the LME. The VI provides only the transmission services.

9.4. LME Services

The mobility management service in the LME provides support for registration and de-registration (cell entry and cell exit), scanning RF channels of neighboring cells and handover between cells. In addition, it manages the addressing of aircraft/ ASs within cells.

The resource management service provides link maintenance (power, frequency and time adjustments), support for adaptive coding and modulation, and resource allocation.

9.5. SNP Services

The DLS provides functions REQUIRED for the transfer of user plane data and control plane data over the LDACS sub-network.

The security service provides functions for secure communication over the LDACS sub-network. Note that the SNP security service applies cryptographic measures as configured by the GS.

10. Security Considerations

10.1. Reasons for Wireless Digital Aeronautical Communications

Aviation will require secure exchanges of data and voice messages for managing the air-traffic flow safely through the airspaces all over the world. Historically Communication Navigation Surveillance (CNS) wireless communications technology emerged from military and a threat landscape where inferior technological and financial capabilities of adversaries were assumed [STR2016]. The main communication method for ATC today is still an open analogue voice broadcast within the aeronautical VHF band. Currently, the information security is purely procedural based by using well-trained personnel and proven communications procedures. This communication method has been in service since 1948. However, since the emergence of civil aeronautical CNS application and today, the world has changed. Civil applications have significant lower spectrum available than military applications. This means several military defence mechanisms such as frequency hopping or pilot symbol scrambling and, thus, a defense-in-depth approach starting at the physical layer is infeasible for civil systems. With the rise of cheap Software Defined Radios, the previously existing financial barrier is almost gone and open source projects such as GNU radio [GNU2012] allow the new type of unsophisticated listeners and possible attackers. Most CNS technology developed in ICAO relies on open standards, thus syntax and semantics of wireless digital aeronautical communications SHOULD be expected to be common knowledge for attackers. With increased digitization and automation of civil aviation the human as control instance is being taken gradually out of the loop. Autonomous transport drones or single piloted aircraft demonstrate this trend. However, without profound cybersecurity measures such as authenticity and integrity checks of messages in-transit on the wireless link or mutual entity authentication, this lack of a control instance can prove disastrous. Thus, future digital communications waveforms will need additional embedded security features to fulfill modern information security requirements like authentication and integrity. These security features require sufficient bandwidth which is beyond the capabilities of a VHF narrowband communications system. For voice and data communications, sufficient data throughput capability is needed to support the security functions while not degrading performance. LDACS is a data link technology with sufficient bandwidth to incorporate security without losing too much user throughput.

As digitalization progresses even further with LDACS and automated procedures such as 4D-Trajectories allowing semi-automated en-route flying of aircraft, LDACS requires stronger cybersecurity measures.

10.2. LADACS Requirements

Overall there are several business goals for cybersecurity to protect in FCI in civil aviation:

1. Safety: The system MUST sufficiently mitigate attacks, which contribute to safety hazards.
2. Flight regularity: The system MUST sufficiently mitigate attacks, which contribute to delays, diversions, or cancellations of flights.
3. Protection of business interests: The system MUST sufficiently mitigate attacks which result in financial loss, reputation damage, disclosure of sensitive proprietary information, or disclosure of personal information.

To further analyze assets and derive threats and thus protection scenarios several Threat-and Risk Analysis were performed for LDACS [MAE20181] , [MAE20191]. These results allowed deriving security scope and objectives from the requirements and the conducted Threat- and Risk Analysis.

10.3. LDACS Security Objectives

Security considerations for LDACS are defined by the official Standards And Recommended Practices (SARPS) document by ICAO [ICA2018]:

1. LDACS SHALL provide a capability to protect the availability and continuity of the system.
2. LDACS SHALL provide a capability including cryptographic mechanisms to protect the integrity of messages in transit.
3. LDACS SHALL provide a capability to ensure the authenticity of messages in transit.
4. LDACS SHOULD provide a capability for nonrepudiation of origin for messages in transit.
5. LDACS SHOULD provide a capability to protect the confidentiality of messages in transit.
6. LDACS SHALL provide an authentication capability.
7. LDACS SHALL provide a capability to authorize the permitted actions of users of the system and to deny actions that are not explicitly authorized.
8. If LDACS provides interfaces to multiple domains, LDACS SHALL provide capability to prevent the propagation of intrusions within LDACS domains and towards external domains.

10.4. LDACS Security Functions

These objectives were used to derive several security functions for LDACS REQUIRED to be integrated in the LDACS cybersecurity architecture: (1) Identification, (2) Authentication, (3) Authorization, (4) Confidentiality, (5) System Integrity, (6) Data Integrity, (7) Robustness, (8) Reliability, (9) Availability, and (10) Key and Trust Management. Several works investigated possible measures to implement these security functions [BIL2017], [MAE20181], [MAE20191]. Having identified security requirements, objectives and functions it MUST be ensured that they are applicable.

10.5. LDACS Security Architecture

The requirements lead to a LDACS security model including different entities for identification, authentication and authorization purposes ensuring integrity, authenticity and confidentiality of data in-transit especially.

10.5.1. Entities

A simplified LDACS architectural modelrequires the following entities: Network operators such as the Societe Internationale de Telecommunications Aeronautiques (SITA) [SIT2020] and ARINC [ARI2020] are providing access to the (1) Ground IPS network via an (2) A2G LDACS Router. This router is attached to a closed off LDACS Access Network, (3) which connects via further (4) Access Routers to the different (5) LDACS Cell Ranges, each controlled by a (6) GS (serving one LDACS cell), with several interconnected GS (7) spanning a local LDACS access network. Via the (8) A2G wireless LDACS data link (9) AS the aircraft is connected to the ground network and via the (10) aircrafts's VI and (11) aircraft's network interface, aircraft's data can be sent via the AS back to the GS and the forwarded back via GSC, LDACS local access network, access routers, LDACS access network, A2G LDACS router to the ground IPS network.

10.5.2. Entity Identification

LDACS needs specific identities for (1) the AS, (2) the GS, (3) the GS, and (4) the Network Operator. The aircraft itself can be identified using the ICAO unique address of an aircraft, the call sign of that aircraft or the recently founded Privacy ICAO Address (PIA) program [FAA2020]. It is conceivable that the LDACS AS will use a combination of aircraft identification, radio component identification such as MAC addresses and even operator features identification to create a unique AS LDACS identification tag. Similar to a 4G's eNodeB Serving Network (SN) Identification tag, a GS could be identified using a similar field. The identification of the network operator is again similar to 4G (e.g., E-Plus, AT&T, and TELUS), in the way that the aeronautical network operators are listed (e.g., ARINC [ARI2020] and SITA [SIT2020]).

10.5.3. Entity Authentication and Key Negotiation

In order to anchor Trust within the system all LDACS entities connected to the ground IPS network SHALL be rooted in an LDACS specific chain-of-trust and PKI solution, quite similar to AeroMACS approach [CRO2016]. These X.509 certificates [RFC5280] residing at the entities and incorporated in the LDACS PKI proof the ownership of their respective public key, include information about the identity of the owner and the digital signature of the entity that has verified the certificate's content. First all ground infrastructures MUST mutually authenticate to each other, negotiate and derive keys and, thus, secure all ground connections. How this process is handled in detail is still an ongoing discussion. However, established methods to secure user plane by IPSec [RFC4301] and IKEv2 [RFC7296] or the application layer via TLS 1.3 [RFC8446] are conceivable. The LDACS PKI with their chain-of-trust approach, digital certificates and public entity keys lay the groundwork for this step. In a second step the AS with the LDACS radio approaches an LDACS cell and performs a cell entry with the corresponding GS. Similar to the LTE cell attachment process [TS33.401], where authentication happens after basic communication has been enabled between AS and GS (step 5a in the UE attachment process [TS33.401]), the next step is mutual authentication and key exchange. Hence, in step three using the identity-based Station-to-Station (STS) protocol with Diffie-Hellman Key Exchange [MAE2020], AS and GS establish mutual trust by authenticating each other, exchanging key material and finally, both ending up with derived key material. A key confirmation is mandatory before the communication channel between the AS and the GS can be opened for user-data communications.

10.5.4. Message-in-transit Confidentiality, Integrity and Authenticity

The subsequent key material from the previous step can then be used to protect LDACS Layer 2 communications via applying encryption and integrity protection measures on the SNP layer of the LDACS protocol stack. As LDACS transports AOC and ATS data, the integrity of that data is most important, while confidentiality only needs to be applied to AOC data to protect business interests [ICA2018]. This possibility of providing low layered confidentiality and integrity protection ensures a secure delivery of user data over the air gap. Furthermore, it ensures integrity protection of LDACS control data.

10.6. LDACS Security Modules

A draft of the cybersecurity architecture of LDACS can be found in [ICA2018] and [MAE20182] and respective updates in [MAE20191], [MAE20192], and [MAE2020].

10.6.1. Placements of Security Functionality in Protocol Stack

Placing protection mechanisms in the LME and SNP entities within the protocol stack of LDACS will be most efficient in securing LDACS. MAC and DLS will also receive new tasks like the measurement performance for control channel protection. Security endpoints for secure user data communication, control data protection and primary entity authentication are the AS and GS.

10.6.2. Trust

The LDACS security concept requires all entities in an LDACS network to authenticate to each other to ascertain that only trusted participants can use the system. To establish trust within the network, inter-operations between all FCI candidates must be possible, thus LDACS will follow AeroMACS lead and also use an FCI specific PKI [RFC5280]. A PKI can solve the problem of having to trust a communication's partner identity claim via involving a trusted third party who verifies the identities of the parties who wish to engage in communication via issuing a digital certificate. As aviation operates worldwide, a hierarchical PKI will have to be deployed with several sub-CAs being distributed over the world.

Basically, there are two proposals on how to achieve worldwide trust coverage:

1. One root CA is installed per geographic region and then it performs cross-certification with distributed root-CAs of all other geo-graphic regions around the world. Subdomains can exist within ATM organizations. Here trust emerges from the assured trustworthiness of each regional root CA cross-certifying other and being cross-certified by other regional CAs
2. The other idea is to have one worldwide (probably offline) root CA, hosted by a trusted worldwide entity, such as ICAO, with several regions sub-CAs distributed around the world. That way, the ICAO hosted root CA serves as trust bridge.

10.6.3. Mutual Authentication and Key Exchange (MAKE)

Via a modified, identity-based STS procedure and digital certificate and public keys pre-deployed during maintenance at the respective end-entities, the MAKE procedure can guarantee (1) Mutual Authentication, (2) Secure Key Agreement, (3) Prefect Forward Secrecy and (4) Key Confirmation [MAE2020]. As Diffie-Hellman Key Exchange (DHKE) procedure, we are currently evaluating the classic ephemeral DHKE [DIF1976] with 3072bit keys, Elliptic Curve DHKE (ECDH) with 256bit keys [KOB1987] and the Supersingular Isogeny DHKE (SIDH) with 2624bit key sizes [JAO2011]. As minimization of security data on the datalink is key, ECDH is currently the favorite way forward. Assuming that an LDACS security header consists of TYPE, ID, UA and PRIO fields, the entire header is of length 48bit [GRA2019]. Cryptographic nonces are 96bit long, signatures 512bit and the public elliptic curve Diffie-Hellman keys 256bit. With these bit sizes, the entire STS-MAKE procedure between AS and GS requires a total of 4 messages and 1920bit [MAE2021].

10.6.4. Key Derivation and Key Hierarchy

Once all parties within the network have successfully authenticated to each other, key derivation is necessary to generate different keys for different purposes. We need different keys for user data protection and keys for control data protection. As key derivation function, we propose the Hash-based Message Authentication Code (HMAC) Key Derivation Function (KDF) - HKDF [RFC5869]. First the input keying material (here: master key/static Diffie Hellman shared key) is taken and a fixed-length pseudo-random key is extracted. We extract a pseudorandom key from the master key by adding a salt value, which can be any fixed non-secret string chosen at random. In the process the pseudo random key becomes indistinguishable from a uniform distribution of bits. As LDACS will be deployed in 2024 with a recommendation of a minimum-security level of 128bit.

10.6.5. User Data Security

It is proposed to secure LDACS Sub-Network Packet Data Units (SN-PDU)s, as their size can vary from 128 to 1536 Byte [GRA2019], which makes them possibly the largest PDUs within LDACS. This helps minimizing security data overhead, in case a Message Authentication Code (MAC) tag is attached to the SN-PDU. For confidentiality protection, it is RECOMMENDED symmetric approaches for data encryption, due to low computational overhead and fast operation times. As encryption algorithm, it is RECOMMENDED to use AES-128-GCM/AES-256-GCM [RFC5288] with Galois Counter Mode (GCM) being a mode of operation on symmetric key block. It provides authenticated encryption and decryption operations and it proves robust against currently known quantum-computer-based algorithms [BER2017]. For message integrity/authenticity protection, it is RECOMMENDED either to use the aforementioned AES-GCM with tag lengths of at least 128bit or HMAC with hash-functions from the SHA-3 family [PRI2014]. At least HMAC-SHA3-128 with a tag length of 128bit is RECOMMENDED. This way the tag security data overhead ranges from 1.04 to 12.50% for user data, depending on the SN-PDU size.

10.6.6. Control Data Security

LDACS has four control channels: AS announce their existence in the RA, at the beginning of each SF in the RL, where each AS can transmit 56bit. GS announce their existence in the BC, at the beginning of each SF in the FL, where the GS can transmit a total of 2304bit. AS can request resources in the DC, where each AS has an 83bit long slot and GS can grant those resources in the CC, with 728bit per CC-PHY-SDU. As the control channels of LDACS are very small-size, it is obvious that protection is challenging. Having security requirements in mind it is RECOMMENDED to introduce group key mechanisms for

LDACS. Thus, after the MAKE procedure of LDACS, a control plane related group key is derived by the GS and shared with all AS in a protected manner. As group key procedure, several approaches are investigated (e.g., G-IKEv2 [I-D.ietf-ipsecme-g-ikev2], CRGT [ZHE2007], CAKE [GUG2018], LKH [SAK2014], and OFT [KUM2020]). As OFT has the least requirements on network operations compared to the other, LDACS will use OFT with a fixed tree of 512-member nodes for a maximum of 512 supported AS in an LDACS cell. All AS and GS use this group key to protect the exchanged control data in the CC/DC slots. As these messages remain valid for a time period in the order of 10 ms and the transmission is distance bound by the MAC protocol of LDACS, very small digest tags of 16 or 32bit can suffice to protect a minimum of integrity of control messages of LDACS. To that end, it is proposed to use blake2b or blake2s and to trim the tag after 4 bytes [RFC7693].

11. Privacy Considerations

LDACS provides a Quality-of-Service, and the generic considerations for such mechanisms apply.

12. IANA Considerations

This memo includes no request to IANA.

13. Acknowledgements

Thanks to all contributors to the development of LDACS and ICAO PT-T.

Thanks to Klaus-Peter Hauf, Bart Van Den Einden, and Pierluigi Fantappie for further input to this draft.

Thanks to SBA Research Vienna for fruitful discussions on aeronautical communications concerning security incentives for industry and potential economic spillovers.

14. Normative References

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/info/rfc5280>.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014, <https://www.rfc-editor.org/info/rfc7296>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/info/rfc8446>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5869] Krawczyk, H. and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)", RFC 5869, DOI 10.17487/RFC5869, May 2010, <https://www.rfc-editor.org/info/rfc5869>.

[RFC5288] Salowey, J., Choudhury, A., and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS", RFC 5288, DOI 10.17487/RFC5288, August 2008, <https://www.rfc-editor.org/info/rfc5288>.

[RFC7693] Saarinen, M-J., Ed. and J-P. Aumasson, "The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC)", RFC 7693, DOI 10.17487/RFC7693, November 2015, <https://www.rfc-editor.org/info/rfc7693>.

15. Informative References

[SCHN2016] Schneckenburger, N., Jost, T., Shutin, D., Walter, M., Thiasiriphet, T., Schnell, M., and U.C. Fiebig, "Measurement of the L-band Air-to-Ground Channel for Positioning Applications", IEEE Transactions on Aerospace and Electronic Systems, 52(5), pp.2281-229 , 2016.

[MAE20191] Maeurer, N., Graeupl, T., and C. Schmitt, "Evaluation of the LDACS Cybersecurity Implementation", IEEE 38th Digital Avionics Systems Conference (DACS), pp. 1-10, San Diego, CA, USA , 2019.

[MAE20192] Maeurer, N. and C. Schmitt, "Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- and Risk Analysis", IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-13, Herndon, VA, USA , 2019.

[GRA2019] Graeupl, T., Rihacek, C., and B. Haindl, "LDACS A/G Specification", SESAR2020 PJ14-02-01 D3.3.030 , 2019.

[FAN2019] Pierattelli, S., Fantappie, P., Tamalet, S., van den Einden, B., Rihacek, C., and T. Graeupl, "LDACS Deployment Options and Recommendations", SESAR2020 PJ14-02-01 D3.4.020 , 2019.

[MAE20182] Maeurer, N. and A. Bilzhause, "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)", IEEE 37th Digital Avionics Systems Conference (DASC), pp. 1-10, London, UK , 2017.

[GRA2011] Graeupl, T. and M. Ehammer, "L-DACS1 Data Link Layer Evolution of ATN/IPS", 30th IEEE/AIAA Digital Avionics Systems Conference (DASC), pp. 1-28, Seattle, WA, USA , 2011.

[GRA2018] Graeupl, T., Schneckenburger, N., Jost, T., Schnell, M., Filip, A., Bellido-Manganell, M.A., Mielke, D.M., Maeurer, N., Kumar, R., Osechas, O., and G. Battista, "L-band Digital Aeronautical Communications System (LDACS) flight trials in the national German project MICONAV", Integrated Communications, Navigation, Surveillance Conference (ICNS), pp. 1-7, Herndon, VA, USA , 2018.

[SCH20191] Schnell, M., "DLR Tests Digital Communications Technologies Combined with Additional Navigation Functions for the First Time", 2019.

[ICA2018] International Civil Aviation Organization (ICAO), "L-Band Digital Aeronautical Communication System (LDACS)", International Standards and Recommended Practices Annex 10 - Aeronautical Telecommunications, Vol. III - Communication Systems , 2018.

[SAJ2014] Haindl, B., Meser, J., Sajatovic, M., Mueller, S., Arthaber, H., Faseth, T., and M. Zaisberger, "LDACS1 Conformance and Compatibility Assessment", IEEE/AIAA 33rd Digital Avionics Systems Conference (DASC), pp. 1-11, Colorado Springs, CO, USA , 2014.

[RIH2018] Rihacek, C., Haindl, B., Fantappie, P., Pierattelli, S., Graeupl, T., Schnell, M., and N. Fistas, "L-band Digital Aeronautical Communications System (LDACS) Activities in SESAR2020", Integrated Communications Navigation and Surveillance Conference (ICNS), pp. 1-8, Herndon, VA, USA , 2018.

[BEL2019] Bellido-Manganell, M. A. and M. Schnell, "Towards Modern Air-to-Air Communications: the LDACS A2A Mode", IEEE/AIAA 38th Digital Avionics Systems Conference (DASC), pp. 1-10, San Diego, CA, USA , 2019.

[TS33.401] Zhang, D., "3GPP System Architecture Evolution (SAE); Security architecture", T33.401, 3GPP , 2012.

[CRO2016] Crowe, B., "Proposed AeroMACS PKI Specification is a Model for Global and National Aeronautical PKI Deployments", WiMAX Forum at 16th Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-19, New York, NY, USA , 2016.

[MAE2020] Maeurer, N., Graeupl, T., and C. Schmitt, "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS", IEEE/AIAA 39th Digital Avionics Systems Conference (DASC), pp. 1-10, San Antonio, TX, USA , 2020.

[STR2016] Strohmeier, M., Schaefer, M., Pinheiro, R., Lenders, V., and I. Martinovic, "On Perception and Reality in Wireless Air Traffic Communication Security", IEEE Transactions on Intelligent Transportation Systems, 18(6), pp. 1338-1357, New York, NY, USA , 2016.

[BIL2017] Bilzhause, A., Belgacem, B., Mostafa, M., and T. Graeupl, "Datalink Security in the L-band Digital Aeronautical Communications System (LDACS) for Air Traffic Management", IEEE Aerospace and Electronic Systems Magazine, 32(11), pp. 22-33, New York, NY, USA , 2017.

[MAE20181] Maeurer, N. and A. Bilzhause, "Paving the Way for an IT Security Architecture for LDACS: A Datalink Security Threat and Risk Analysis", IEEE Integrated Communications, Navigation, Surveillance Conference (ICNS), pp. 1-11, New York, NY, USA , 2018.

[FAA2020] FAA, "Federal Aviation Administration. ADS-B Privacy.", August 2020, <https://www.faa.gov/nextgen/equipadsb/privacy/>.

[GNU2012] GNU Radio project, "GNU radio", August 2012, <http://gnuradio.org>.

[SIT2020] SITA, "Societe Internationale de Telecommunications Aeronautiques", August 2020, <https://www.sita.aero/>.

[ARI2020] ARINC, "Aeronautical Radio Incorporated", August 2020, <https://www.aviation-ia.com/>.

[DO350A] RTCA SC-214, "Safety and Performance Standard for Baseline 2 ATS Data Communications (Baseline 2 SPR Standard)", May 2016, <https://standards.globalspec.com/std/10003192/rtca-do-350-volume-1-2>.

[DIF1976] Diffie, W. and M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory, 22(6):644-654 , November 1976.

[KOB1987] Koblitz, N. and M. Hellman, "Elliptic Curve Cryptosystems", Mathematics of Computation, 48(177):203-209. , January 1987.

[JAO2011] Jao, D. and L. De Feo, "Towards Quantum-Resistant Cryptosystems from Super-singular Elliptic Curve Isogenies", 4th International Workshop on Post-Quantum Cryptography, Springer, Heidelberg, Germany, pp. 19-34 , November 2011.

[MAE2021] Maeurer, N., Graeupl, T., and C. Schmitt, "Cybersecurity for the L-band DigitalAeronautical Communications System (LDACS)", Aviation Cybersecurity: Foundations, Principles, and Applications. H. Song, K. Hopkinson, T. De Cola, T. Alexandrovich, and D. Liu (Eds.), Chapter 07, in printing process , 2021.

[BER2017] Bernstein, D.J. and T. Lange, "Post-Quantum Cryptography", Nature, 549(7671):188-194 , 2017.

[PRI2014] Pritzker, P. and P.D. Gallagher, "SHA-3 standard: Permutation-Based Hash and Extendable-Output Functions", Information Tech Laboratory National Institute of Standards and Technology, pp. 1-35 , 2014.

[ZHE2007] Zheng, X., Huang, C.T., and M. Matthews, "Chinese Remainder Theorem-Based Group Key Management", 45th Annual Southeast Regional Conference, ACM, New York, NY, USA, pp. 266-271 , March 2007.

[GUG2018] Guggemos, T., Streit, K., Knuepfer, M., gentsche Felde, N., and P. Hillmann, "No Cookies, Just CAKE: CRTbased Key Hierarchy for Efficient Key Management in Dynamic Groups", International Conference for Internet Technology and Secured Transactions, Cambridge, UK, pp. 25-32 , December 2018.

[SAK2014] Sakamoto, N., "An Efficient Structure for LKH Key Tree on Secure Multi-Cast Communications", 15th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing, New York, NY, USA, pp. 1-7 , November 2014.

[KUM2020] Kumar, V., Kumar, R., and S.K. Pandey, "A Computationally Efficient Centralized Group Key Distribution Protocol for Secure Multicast Communications Based Upon RSA Public Key Cryptosystem", Journal of King Saud University - Computer and Information Sciences, 32(9):1081-1094 , 2020.

[RAW-TECHNOS]
Thubert, P., Cavalcanti, D., Vilajosana, X., Schmitt, C., and J. Farkas, "Reliable and Available Wireless Technologies", Work in Progress, Internet-Draft, draft-ietf-raw-technologies-00, 20 October 2020, <https://tools.ietf.org/html/draft-ietf-raw-technologies-00>.

[RAW-USE-CASES]
Papadopoulos, G., Thubert, P., Theoleyre, F., and C. Bernardos, "RAW use cases", Work in Progress, Internet-Draft, draft-ietf-raw-use-cases-00, 23 October 2020, <https://tools.ietf.org/html/draft-ietf-raw-use-cases-00>.

[I-D.ietf-ipsecme-g-ikev2]
Smyslov, V. and B. Weis, "Group Key Management using IKEv2", Work in Progress, Internet-Draft, draft-ietf-ipsecme-g-ikev2-02, 11 January 2021, <https://tools.ietf.org/html/draft-ietf-ipsecme-g-ikev2-02>.

Appendix A. Selected Information from DO-350A

This appendix includes the continuity, availability, and integrity requirements interesting for LDACS defined in [DO350A].

The following terms are used here:

CPDLC	Controller Pilot Data Link Communication
DT	Delivery Time (nominal) value for RSP
ET	Expiration Time value for RCP
FH	Flight Hour
MA	Monitoring and Alerting criteria
OT	Overdue Delivery Time value for RSP
RCP	Required Communication Performance

RSP Required Surveillance Performance
TT Transaction Time (nominal) value for RCP

	ECP 130	ECP 130
Parameter	ET	TT95%
Transaction Time (sec)	130	67
Continuity	0.999	0.95
Availability	0.989	0.989
Integrity	1E-5 per FH	1E-5 per FH

Table 1: CPDLC Requirements for ECP

	RCP 240	RCP 240	RCP 400	RCP 400
Parameter	ET	TT95%	ET	TT95%
Transaction Time (sec)	240	210	400	350
Continuity	0.999	0.95	0.999	0.95
Availability	0.989 (safety)	0.989 (efficiency)	0.989	0.989
Integrity	1E-5 per FH	1E-5 per FH	1E-5 per FH	1E-5 per FH

Table 2: CPDLC Requirements for RCP

RCP Monitoring and Alerting Criteria in case of CPDLC:

- MA-1: The system SHALL be capable of detecting failures and configuration changes that would cause the communication service no longer meet the RCP specification for the intended use.
- MA-2: When the communication service can no longer meet the RCP specification for the intended function, the flight crew and/or the controller SHALL take appropriate action.

	RSP 160	RSP 160	RSP 180	RSP 180	RSP 400	RSP 400
Parameter	OT	DT95%	OT	DT95%	OT	DT95%
Transaction Time (sec)	160	90	180	90	400	300
Continuity	0.999	0.95	0.999	0.95	0.999	0.95
Availability	0.989	0.989	0.989 (safety)	0.989 (efficiency)	0.989	0.989
Integrity	1E-5 per FH	1E-5 per FH	1E-5 per FH	1E-5 per FH	1E-5 per FH	1E-5 per FH

Table 3: ADS-C Requirements

RCP Monitoring and Alerting Criteria:

- MA-1: The system SHALL be capable of detecting failures and configuration changes that would cause the ADS-C service no longer meet the RSP specification for the intended function.
- MA-2: When the ADS-C service can no longer meet the RSP specification for the intended function, the flight crew and/or the controller SHALL take appropriate action.

Authors’ Addresses

Nils Maeurer (editor)
German Aerospace Center (DLR)
Muenchner Strasse 20
82234 Wessling
Germany

Email: Nils.Maeurer@dlr.de

Thomas Graeupl (editor)
German Aerospace Center (DLR)
Muenchner Strasse 20
82234 Wessling
Germany

Email: Thomas.Graeupl@dlr.de

Corinna Schmitt (editor)
Research Institute CODE, UniBwM
Werner-Heisenberg-Weg 28
85577 Neubiberg
Germany

Email: corinna.schmitt@unibw.de

RAW
Internet-Draft
Intended status: Informational
Expires: 23 August 2021

P. Thubert, Ed.
Cisco Systems
D. Cavalcanti
Intel
X. Vilajosana
Universitat Oberta de Catalunya
C. Schmitt
Research Institute CODE, UniBwM
J. Farkas
Ericsson

19 February 2021

Reliable and Available Wireless Technologies
draft-ietf-raw-technologies-01

Abstract

This document presents a series of recent technologies that are capable of time synchronization and scheduling of transmission, making them suitable to carry time-sensitive flows with high reliability and availability.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

When used in math or philosophy, the term "deterministic" generally refers to a perfection where all aspect are understood and predictable. A perfectly Deterministic Network would ensure that every packet reach its destination following a predetermined path along a predefined schedule to be delivered at the exact due time. In a real and imperfect world, a Deterministic Network must highly predictable, which is a combination of reliability and availability. On the one hand the network must be reliable, meaning that it will perform as expected for all packets and in particular that it will always deliver the packet at the destination in due time. On the other hand, the network must be available, meaning that it is resilient to any single outage, whether the cause is a software, a hardware or a transmission issue.

RAW (Reliable and Available Wireless) is an effort to provide Deterministic Networking on across a path that include a wireless physical layer. Making Wireless Reliable and Available is even more challenging than it is with wires, due to the numerous causes of loss in transmission that add up to the congestion losses and the delays caused by overbooked shared resources. In order to maintain a similar quality of service along a multihop path that is composed of wired and wireless hops, additional methods that are specific to wireless must be leveraged to combat the sources of loss that are also specific to wireless.

Such wireless-specific methods include per-hop retransmissions (HARQ) and P2MP overhearing whereby multiple receivers are scheduled to receive the same transmission, which balances the adverse effects of the transmission losses that are experienced when a radio is used as pure P2P. Those methods are collectively referred to as PAREO functions in the "Reliable and Available Wireless Architecture/Framework" [I-D.pthubert-raw-architecture].

2. Terminology

This specification uses several terms that are uncommon on protocols that ensure bets effort transmissions for stochastics flows, such as found in the traditional Internet and other statistically multiplexed packet networks.

ARQ: Automatic Repeat Request, enabling an acknowledged transmission and retries. ARQ is a typical model at Layer-2 on a wireless medium. It is typically avoided end-to-end on deterministic flows because it introduces excessive indetermination in latency, but a limited number of retries within a bounded time may be used over a wireless link and yet respect end-to-end constraints.

Available: That is exempt of unscheduled outage, the expectation for a network being that the flow is maintained in the face of any single breakage.

FEC: Forward error correction, sending redundant coded data to help the receiver recover transmission errors without the delays incurred with ARQ.

HARQ: Hybrid ARQ, a combination of FEC and ARQ.

PCE: Path Computation Element.

PAREO (functions): the wireless extension of DetNet PREOF. PAREO functions include scheduled ARQ at selected hops, and expect the use of new operations like overhearing where available.

Reliable: That consistently performs as expected, the expectation for a network being to always deliver a packet in due time.

Track: A DODAG oriented to a destination, and that enables Packet ARQ, Replication, Elimination, and Ordering Functions.

3. On Scheduling

The operations of a Deterministic Network often rely on precisely applying a tight schedule, in order to avoid collision loss and guarantee the worst-case time of delivery. To achieve this, there must be a shared sense of time throughout the network. The sense of time is usually provided by the lower layer and is not in scope for RAW.

3.1. Benefits of Scheduling on Wires

A network is reliable when the statistical effects that affect the packet transmission are eliminated. This involves maintaining at all time the amount of critical packets within the physical capabilities of the hardware and that of the radio medium. This is achieved by controlling the use of time-shared resources such as CPUs and buffers, by shaping the flows and by scheduling the time of transmission of the packets that compose the flow at every hop.

Equipment failure, such as an access point rebooting, a broken radio adapter, or a permanent obstacle to the transmission, is a secondary source of packet loss. When a breakage occurs, multiple packets are lost in a row before the flows are rerouted or the system may recover. This is not acceptable for critical applications such as related to safety. A typical process control loop will tolerate an occasional packet loss, but a loss of several packets in a row will cause an emergency stop (e.g., after 4 packets lost, within a period of 1 second).

Network Availability is obtained by making the transmission resilient against hardware failures and radio transmission losses due to uncontrolled events such as co-channel interferers, multipath fading or moving obstacles. The best results are typically achieved by pseudo randomly cumulating all forms of diversity, in the spatial domain with replication and elimination, in the time domain with ARQ and diverse scheduled transmissions, and in the frequency domain with frequency hopping or channel hopping between frames.

3.2. Benefits of Scheduling on Wireless

In addition to the benefits listed in Section 3.1, scheduling transmissions provides specific value to the wireless medium.

On the one hand, scheduling avoids collisions between scheduled transmissions and can ensure both time and frequency diversity between retries in order to defeat co-channel interference from un-controlled transmitters as well as multipath fading. Transmissions can be scheduled on multiple channels in parallel, which enables to use the full available spectrum while avoiding the hidden terminal problem, e.g., when the next packet in a same flow interferes on a same channel with the previous one that progressed a few hops farther.

On the other hand, scheduling optimizes the bandwidth usage: compared to classical Collision Avoidance techniques, there is no blank time related to inter-frame space (IFS) and exponential back-off in scheduled operations. A minimal Clear Channel Assessment may be needed to comply with the local regulations such as ETSI 300-328, but that will not detect a collision when the senders are synchronized. And because scheduling allows a time-sharing operation, there is no limit to the ratio of isolated critical traffic.

Finally, scheduling plays a critical role to save energy. In IOT, energy is the foremost concern, and synchronizing sender and listener enables to always maintain them in deep sleep when there is no scheduled transmission. This avoids idle listening and long preambles and enables long sleep periods between traffic and resynchronization, allowing battery-operated nodes to operate in a mesh topology for multiple years.

4. IEEE 802.11

4.1. Provenance and Documents

With an active portfolio of nearly 1,300 standards and projects under development, IEEE is a leading developer of industry standards in a broad range of technologies that drive the functionality, capabilities, and interoperability of products and services, transforming how people live, work, and communicate.

The IEEE 802 LAN/MAN Standards Committee (SC) develops and maintains networking standards and recommended practices for local, metropolitan, and other area networks, using an open and accredited process, and advocates them on a global basis. The most widely used standards are for Ethernet, Bridging and Virtual Bridged LANs Wireless LAN, Wireless PAN, Wireless MAN, Wireless Coexistence, Media Independent Handover Services, and Wireless RAN. An individual Working Group provides the focus for each area. Standards produced by the IEEE 802 SC are freely available from the IEEE GET Program after they have been published in PDF for six months.

The IEEE 802.11 LAN standards define the underlying MAC and PHY layers for the Wi-Fi technology. Wi-Fi/802.11 is one of the most successful wireless technologies, supporting many application domains. While previous 802.11 generations, such as 802.11n and 802.11ac, have focused mainly on improving peak throughput, more recent generations are also considering other performance vectors, such as efficiency enhancements for dense environments in 802.11ax, and latency and support for Time-Sensitive Networking (TSN) capabilities in 802.11be.

IEEE 802.11 already supports some 802.1 TSN standards and it is undergoing efforts to support for other 802.1 TSN capabilities required to address the use cases that require time synchronization and timeliness (bounded latency) guarantees with high reliability and availability. The IEEE 802.11 working group has been working in collaboration with the IEEE 802.1 group for several years extending 802.1 features over 802.11. As with any wireless media, 802.11 imposes new constraints and restrictions to TSN-grade QoS, and tradeoffs between latency and reliability guarantees must be considered as well as managed deployment requirements. An overview of 802.1 TSN capabilities and their extensions to 802.11 are discussed in [Cavalcanti_2019].

Wi-Fi Alliance (WFA) is the worldwide network of companies that drives global Wi-Fi adoption and evolution through thought leadership, spectrum advocacy, and industry-wide collaboration. The WFA work helps ensure that Wi-Fi devices and networks provide users the interoperability, security, and reliability they have come to expect.

The following [IEEE Std. 802.11] specifications/certifications are relevant in the context of reliable and available wireless services and support for time-sensitive networking capabilities:

Time Synchronization: IEEE802.11-2016 with IEEE802.1AS; WFA TimeSync Certification.

Congestion Control: IEEE802.11-2016 Admission Control; WFA Admission Control.

Security: WFA Wi-Fi Protected Access, WPA2 and WPA3.

Interoperating with IEEE802.1Q bridges: [IEEE Std. 802.11ak].

Stream Reservation Protocol (part of [IEEE Std. 802.1Qat]): AIEEE802 .11-2016

Scheduled channel access: IEEE802.11ad Enhancements for very high throughput in the 60 GHz band [IEEE Std. 802.11ad].

802.11 Real-Time Applications: Topic Interest Group (TIG) ReportDoc [IEEE_doc_11-18-2009-06].

In addition, major amendments being developed by the IEEE802.11 Working Group include capabilities that can be used as the basis for providing more reliable and predictable wireless connectivity and support time-sensitive applications:

IEEE 802.11ax D4.0: Enhancements for High Efficiency (HE). [IEEE Std. 802.11ax]

IEEE 802.11be Extreme High Throughput (EHT). [IEEE 802.11be WIP]

IEE 802.11ay Enhanced throughput for operation in license-exempt bands above 45 GHz. [IEEE Std. 802.11ay]

The main 802.11ax and 802.11be capabilities and their relevance to RAW are discussed in the remainder of this document.

4.2. 802.11ax High Efficiency (HE)

4.2.1. General Characteristics

The next generation Wi-Fi (Wi-Fi 6) is based on the IEEE802.11ax amendment [IEEE Std. 802.11ax], which includes new capabilities to increase efficiency, control and reduce latency. Some of the new features include higher order 1024-QAM modulation, support for uplink multi-user MIMO, OFDMA, trigger-based access and Target Wake time (TWT) for enhanced power savings. The OFDMA mode and trigger-based access enable scheduled operation, which is a key capability required to support deterministic latency and reliability for time-sensitive flows. 802.11ax can operate in up to 160 MHz channels and it includes support for operation in the new 6 GHz band, which is expected to be open to unlicensed use by the FCC and other regulatory agencies worldwide.

4.2.1.1. Multi-User OFDMA and Trigger-based Scheduled Access

802.11ax introduced a new orthogonal frequency-division multiple access (OFDMA) mode in which multiple users can be scheduled across the frequency domain. In this mode, the Access Point (AP) can initiate multi-user (MU) Uplink (UL) transmissions in the same PHY Protocol Data Unit (PPDU) by sending a trigger frame. This centralized scheduling capability gives the AP much more control of the channel, and it can remove contention between devices for uplink transmissions, therefore reducing the randomness caused by CSMA-based access between stations. The AP can also transmit simultaneously to multiple users in the downlink direction by using a Downlink (DL) MU OFDMA PPDU. In order to initiate a contention free Transmission Opportunity (TXOP) using the OFDMA mode, the AP still follows the typical listen before talk procedure to acquire the medium, which ensures interoperability and compliance with unlicensed band access rules. However, 802.11ax also includes a multi-user Enhanced Distributed Channel Access (MU-EDCA) capability, which allows the AP to get higher channel access priority.

4.2.1.2. Improved PHY Robustness

The 802.11ax PHY can operate with 0.8, 1.6 or 3.2 microsecond guard interval (GI). The larger GI options provide better protection against multipath, which is expected to be a challenge in industrial environments. The possibility to operate with smaller resource units (e.g. 2 MHz) enabled by OFDMA also helps reduce noise power and improve SNR, leading to better packet error rate (PER) performance.

802.11ax supports beamforming as in 802.11ac, but introduces UL MU MIMO, which helps improve reliability. The UL MU MIMO capability is also enabled by the trigger based access operation in 802.11ax.

4.2.1.3. Support for 6GHz band

The 802.11ax specification [IEEE Std. 802.11ax] includes support for operation in the new 6 GHz band. Given the amount of new spectrum available as well as the fact that no legacy 802.11 device (prior 802.11ax) will be able to operate in this new band, 802.11ax operation in this new band can be even more efficient.

4.2.2. Applicability to deterministic flows

TSN capabilities, as defined by the IEEE 802.1 TSN standards, provide the underlying mechanism for supporting deterministic flows in a Local Area Network (LAN). The 802.11 working group has already incorporated support for several TSN capabilities, so that time-sensitive flow can experience precise time synchronization and timeliness when operating over 802.11 links. TSN capabilities supported over 802.11 (which also extends to 802.11ax), include:

1. 802.1AS based Time Synchronization (other time synchronization techniques may also be used)

2. Interoperating with IEEE802.1Q bridges

3. Time-sensitive Traffic Stream identification

The exiting 802.11 TSN capabilities listed above, and the 802.11ax OFDMA and scheduled access provide a new set of tools to better server time-sensitive flows. However, it is important to understand the tradeoffs and constraints associated with such capabilities, as well as redundancy and diversity mechanisms that can be used to provide more predictable and reliable performance.

4.2.2.1. 802.11 Managed network operation and admission control

Time-sensitive applications and TSN standards are expected to operate under a managed network (e.g. industrial/enterprise network). Thus, the Wi-Fi operation must also be carefully managed and integrated with the overall TSN management framework, as defined in the [IEEE8021Qcc] specification.

Some of the random-access latency and interference from legacy/unmanaged devices can be minimized under a centralized management mode as defined in [IEEE8021Qcc], in which admission control procedures are enforced.

Existing traffic stream identification, configuration and admission control procedures defined in [IEEE Std. 802.11] QoS mechanism can be re-used. However, given the high degree of determinism required by many time-sensitive applications, additional capabilities to manage interference and legacy devices within tight time-constraints need to be explored.

4.2.2.2. Scheduling for bounded latency and diversity

As discussed earlier, the [IEEE Std. 802.11ax] OFDMA mode introduces the possibility of assigning different RUs (frequency resources) to users within a PPDU. Several RU sizes are defined in the specification (26, 52, 106, 242, 484, 996 subcarriers). In addition, the AP can also decide on MCS and grouping of users within a given OFMDA PPDU. Such flexibility can be leveraged to support time-sensitive applications with bounded latency, especially in a managed network where stations can be configured to operate under the control of the AP.

As shown in [Cavalcanti_2019], it is possible to achieve latencies in the order of 1msec with high reliability in an interference free environment. Obviously, there are latency, reliability and capacity tradeoffs to be considered. For instance, smaller Resource Units (RU)s result in longer transmission durations, which may impact the minimal latency that can be achieved, but the contention latency and randomness elimination due to multi-user transmission is a major benefit of the OFDMA mode.

The flexibility to dynamically assign RUs to each transmission also enables the AP to provide frequency diversity, which can help increase reliability.

4.3. 802.11be Extreme High Throughput (EHT)

4.3.1. General Characteristics

The [IEEE 802.11be WIP]is the next major 802.11 amendment (after [IEEE Std. 802.11ax]) for operation in the 2.4, 5 and 6 GHz bands. 802.11be is expected to include new PHY and MAC features and it is targeting extremely high throughput (at least 30 Gbps), as well as enhancements to worst case latency and jitter. It is also expected to improve the integration with 802.1 TSN to support time-sensitive applications over Ethernet and Wireless LANs.

The 802.11be Task Group started its operation in May 2019, therefore, detailed information about specific features is not yet available. Only high level candidate features have been discussed so far, including:

1. 320MHz bandwidth and more efficient utilization of non-contiguous spectrum.

2. Multi-band/multi-channel aggregation and operation.

3. 16 spatial streams and related MIMO enhancements.

4. Multi-Access Point (AP) Coordination.

5. Enhanced link adaptation and retransmission protocol, e.g. Hybrid Automatic Repeat Request (HARQ).

6. Any required adaptations to regulatory rules for the 6 GHz spectrum.

4.3.2. Applicability to deterministic flows

The 802.11 Real-Time Applications (RTA) Topic Interest Group (TIG) provided detailed information on use cases, issues and potential solution directions to improve support for time-sensitive applications in 802.11. The RTA TIG report [IEEE_doc_11-18-2009-06] was used as input to the 802.11be project scope.

Improvements for worst-case latency, jitter and reliability were the main topics identified in the RTA report, which were motivated by applications in gaming, industrial automation, robotics, etc. The RTA report also highlighted the need to support additional TSN capabilities, such as time-aware (802.1Qbv) shaping and packet replication and elimination as defined in 802.1CB.

802.11be is expected to build on and enhance 802.11ax capabilities to improve worst case latency and jitter. Some of the enhancement areas are discussed next.

4.3.2.1. Enhanced scheduled operation for bounded latency

In addition to the throughput enhancements, 802.11be will leverage the trigger-based scheduled operation enabled by 802.11ax to provide efficient and more predictable medium access. 802.11be is expected to include enhancements to reduce overhead and enable more efficient operation in managed network deployments [IEEE_doc_11-19-0373-00].

4.3.2.2. Multi-AP coordination

Multi-AP coordination is one of the main new candidate features in 802.11be. It can provide benefits in throughput and capacity and has the potential to address some of the issues that impact worst case latency and reliability. Multi-AP coordination is expected to address the contention due to overlapping Basic Service Sets (OBSS), which is one of the main sources of random latency variations. 802.11be can define methods to enable better coordination between APs, for instance, in a managed network scenario, in order to reduce latency due to unmanaged contention.

Several multi-AP coordination approaches have been discussed with different levels of complexities and benefits, but specific coordination methods have not yet been defined.

4.3.2.3. Multi-band operation

802.11be will introduce new features to improve operation over multiple bands and channels. By leveraging multiple bands/channels, 802.11be can isolate time-sensitive traffic from network congestion, one of the main causes of large latency variations. In a managed 802.11be network, it should be possible to steer traffic to certain bands/channels to isolate time-sensitive traffic from other traffic and help achieve bounded latency.

4.4. 802.11ad and 802.11ay (mmWave operation)

4.4.1. General Characteristics

The IEEE 802.11ad amendment defines PHY and MAC capabilities to enable multi-Gbps throughput in the 60 GHz millimeter wave (mmWave) band. The standard addresses the adverse mmWave signal propagation characteristics and provides directional communication capabilities that take advantage of beamforming to cope with increased attenuation. An overview of the 802.11ad standard can be found in [Nitsche_2015] .

The IEEE 802.11ay is currently developing enhancements to the 802.11ad standard to enable the next generation mmWave operation targeting 100 Gbps throughput. Some of the main enhancements in 802.11ay include MIMO, channel bonding, improved channel access and beamforming training. An overview of the 802.11ay capabilities can be found in [Ghasempour_2017]

4.4.2. Applicability to deterministic flows

The high data rates achievable with 802.11ad and 802.11ay can significantly reduce latency down to microsecond levels. Limited interference from legacy and other unlicensed devices in 60 GHz is also a benefit. However, directionality and short range typical in mmWave operation impose new challenges such as the overhead required for beam training and blockage issues, which impact both latency and reliability. Therefore, it is important to understand the use case and deployment conditions in order to properly apply and configure 802.11ad/ay networks for time sensitive applications.

The 802.11ad standard include a scheduled access mode in which stations can be allocated contention-free service periods by a central controller. This scheduling capability is also available in 802.11ay, and it is one of the mechanisms that can be used to provide bounded latency to time-sensitive data flows. An analysis of the theoretical latency bounds that can be achieved with 802.11ad service periods is provided in [Cavalcanti_2019].

5. IEEE 802.15.4

5.1. Provenance and Documents

The IEEE802.15.4 Task Group has been driving the development of low-power low-cost radio technology. The IEEE802.15.4 physical layer has been designed to support demanding low-power scenarios targeting the use of unlicensed bands, both the 2.4 GHz and sub GHz Industrial, Scientific and Medical (ISM) bands. This has imposed requirements in terms of frame size, data rate and bandwidth to achieve reduced collision probability, reduced packet error rate, and acceptable range with limited transmission power. The PHY layer supports frames of up to 127 bytes. The Medium Access Control (MAC) sublayer overhead is in the order of 10-20 bytes, leaving about 100 bytes to the upper layers. IEEE802.15.4 uses spread spectrum modulation such as the Direct Sequence Spread Spectrum (DSSS).

The Timeslotted Channel Hopping (TSCH) mode was added to the 2015 revision of the IEEE802.15.4 standard [IEEE Std. 802.15.4]. TSCH is targeted at the embedded and industrial world, where reliability, energy consumption and cost drive the application space.

At the IETF, the 6TiSCH Working Group (WG) [TiSCH] deals with best effort operation of IPv6 [RFC8200] over TSCH. 6TiSCH has enabled distributed scheduling to exploit the deterministic access capabilities provided by TSCH. The group designed the essential mechanisms to enable the management plane operation while ensuring IPv6 is supported. Yet the charter did not focus to providing a solution to establish end to end Tracks while meeting quality of service requirements. 6TiSCH, through the RFC8480 [RFC8480] defines the 6P protocol which provides a pairwise negotiation mechanism to the control plane operation. The protocol supports agreement on a schedule between neighbors, enabling distributed scheduling. 6P goes hand-in-hand with a Scheduling Function (SF), the policy that decides how to maintain cells and trigger 6P transactions. The Minimal Scheduling Function (MSF) [I-D.ietf-6tisch-msf] is the default SF defined by the 6TiSCH WG; other standardized SFs can be defined in the future. MSF extends the minimal schedule configuration, and is used to add child-parent links according to the traffic load.

Time sensitive networking on low power constrained wireless networks have been partially addressed by ISA100.11a [ISA100.11a] and WirelessHART [WirelessHART]. Both technologies involve a central controller that computes redundant paths for industrial process control traffic over a TSCH mesh. Moreover, ISA100.11a introduces IPv6 capabilities with a Link-Local Address for the join process and a global unicast addres for later exchanges, but the IPv6 traffic typically ends at a local application gateway and the full power of IPv6 for end-to-end communication is not enabled. Compared to that state of the art, work at the IETF and in particular at RAW could provide additional techniques such as optimized P2P routing, PAREO functions, and end-to-end secured IPv6/CoAP connectivity.

The 6TiSCH architecture [I-D.ietf-6tisch-architecture] identifies different models to schedule resources along so-called Tracks (see Section 5.2.2.2) exploiting the TSCH schedule structure however the focus at 6TiSCH is on best effort traffic and the group was never chartered to produce standard work related to Tracks.

Useful References include:

1. IEEE Std 802.15.4: "IEEE Std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks" [IEEE Std. 802.15.4]. The latest version at the time of this writing is dated year 2015.

2. Morell, A. , Vilajosana, X. , Vicario, J. L. and Watteyne, T. (2013), Label switching over IEEE802.15.4e networks. Trans. Emerging Tel. Tech., 24: 458-475. doi:10.1002/ett.2650" [morell13].

3. De Armas, J., Tuset, P., Chang, T., Adelantado, F., Watteyne, T., Vilajosana, X. (2016, September). Determinism through path diversity: Why packet replication makes sense. In 2016 International Conference on Intelligent Networking and Collaborative Systems (INCoS) (pp. 150-154). IEEE. [dearmas16].

4. X. Vilajosana, T. Watteyne, M. Vucinic, T. Chang and K. S. J. Pister, "6TiSCH: Industrial Performance for IPv6 Internet-of-Things Networks," in Proceedings of the IEEE, vol. 107, no. 6, pp. 1153-1165, June 2019. [vilajosana19].

5.2. TimeSlotted Channel Hopping

5.2.1. General Characteristics

As a core technique in IEEE802.15.4, TSCH splits time in multiple time slots that repeat over time. A set of timeslots constructs a Slotframe (see Section 5.2.2.1.4). For each timeslot, a set of available frequencies can be used, resulting in a matrix-like schedule (see Figure 1).

```
                          timeslot offset
        | 0    1    2    3    4  | 0    1    2    3    4  |    Nodes
        +------------------------+------------------------+   +-----+
        |    |    |    |    |    |    |    |    |    |    |   |  C  |
   CH-1 | EB |    |    |C->B|    | EB |    |    |C->B|    |   |     |
        |    |    |    |    |    |    |    |    |    |    |   +-----+
        +-------------------------------------------------+      |
        |    |    |    |    |    |    |    |    |    |    |      |
   CH-2 |    |    |B->C|    |B->A|    |    |B->C|    |B->A|   +-----+
        |    |    |    |    |    |    |    |    |    |    |   |  B  |
        +-------------------------------------------------+   |     |
    ...                                                       +-----+
                                                                 |
        +-------------------------------------------------+      |
        |    |    |    |    |    |    |    |    |    |    |   +-----+
   CH-15|    |A->B|    |    |    |    |A->B|    |    |    |   |  A  |
        |    |    |    |    |    |    |    |    |    |    |   |     |
        +-------------------------------------------------+   +-----+
   ch.
   offset
```

Figure 1: Slotframe example with scheduled cells between nodes A, B and C

This schedule represents the possible communications of a node with its neighbors, and is managed by a Scheduling Function such as the Minimal Scheduling Function (MSF) [I-D.ietf-6tisch-msf]. Each cell in the schedule is identified by its slotoffset and channeloffset coordinates. A cell's timeslot offset indicates its position in time, relative to the beginning of the slotframe. A cell's channel offset is an index which maps to a frequency at each iteration of the slotframe. Each packet exchanged between neighbors happens within one cell. The size of a cell is a timeslot duration, between 10 to 15 milliseconds. An Absolute Slot Number (ASN) indicates the number of slots elapsed since the network started. It increments at every slot. This is a 5 byte counter that can support networks running for more than 300 years without wrapping (assuming a 10 ms timeslot). Channel hopping provides increased reliability to multi-path fading and external interference. It is handled by TSCH through a channel hopping sequence referred as macHopSeq in the IEEE802.15.4 specification.

The Time-Frequency Division Multiple Access provided by TSCH enables the orchestration of traffic flows, spreading them in time and frequency, and hence enabling an efficient management of the bandwidth utilization. Such efficient bandwidth utilization can be combined to OFDM modulations also supported by the IEEE802.15.4 standard [IEEE Std. 802.15.4] since the 2015 version.

In the RAW context, low power reliable networks should address non-critical control scenarios such as Class 2 and monitoring scenarios such as Class 4 defined by the RFC5673 [RFC5673]. As a low power technology targeting industrial scenarios radio transducers provide low data rates (typically between 50kbps to 250kbps) and robust modulations to trade-off performance to reliability. TSCH networks are organized in mesh topologies and connected to a backbone. Latency in the mesh network is mainly influenced by propagation aspects such as interference. ARQ methods and redundancy techniques such as replication and elimination should be studied to provide the needed performance to address deterministic scenarios.

5.2.2. Applicability to Deterministic Flows

Nodes in a TSCH network are tightly synchronized. This enables to build the slotted structure and ensure efficient utilization of resources thanks to proper scheduling policies. Scheduling is a key to orchestrate the resources that different nodes in a Track or a path are using. Slotframes can be split in resource blocks reserving the needed capacity to certain flows. Periodic and bursty traffic can be handled independently in the schedule, using active and reactive policies and taking advantage of overprovisionned cells to measu reth excursion. Along a Track, resource blocks can be chained so nodes in previous hops transmit their data before the next packet comes. This provides a tight control to latency along a Track. Collision loss is avoided for best effort traffic by overprovisionning resources, giving time to the management plane of the network to dedicate more resources if needed.

5.2.2.1. Centralized Path Computation

In a controlled environment, a 6TiSCH device usually does not place a request for bandwidth between itself and another device in the network. Rather, an Operation Control System (OCS) invoked through an Human/Machine Interface (HMI) iprovides the Traffic Specification, in particular in terms of latency and reliability, and the end nodes, to a Path Computation element (PCE). With this, the PCE computes a Track between the end nodes and provisions every hop in the Track with per-flow state that describes the per-hop operation for a given packet, the corresponding timeSlots, and the flow identification to recognize which packet is placed in which Track, sort out duplicates, etc. In Figure 2, an example of Operational Control System and HMI is depicted.

For a static configuration that serves a certain purpose for a long period of time, it is expected that a node will be provisioned in one shot with a full schedule, which incorporates the aggregation of its behavior for multiple Tracks. The 6TiSCH Architecture expects that the programing of the schedule is done over CoAP as discussed in "6TiSCH Resource Management and Interaction using CoAP" [I-D.ietf-6tisch-coap].

But an Hybrid mode may be required as well whereby a single Track is added, modified, or removed, for instance if it appears that a Track does not perform as expected for, say, Packet Delivery Ratio (PDR). For that case, the expectation is that a protocol that flows along a Track (to be), in a fashion similar to classical Traffic Engineering (TE) [CCAMP], may be used to update the state in the devices. 6TiSCH provides means for a device to negotiate a timeSlot with a neighbor, but in general that flow was not designed and no protocol was selected and it is expected that DetNet will determine the appropriate end-to-end protocols to be used in that case.

Stream Management Entity

```
                         Operational Control System and HMI

      -+-+-+-+-+-+-+ Northbound -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-

                PCE         PCE              PCE              PCE

      -+-+-+-+-+-+-+ Southbound -+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-

              --- 6TiSCH------6TiSCH------6TiSCH------6TiSCH--
     6TiSCH /     Device      Device      Device      Device   \
     Device-                                                    - 6TiSCH
            \     6TiSCH      6TiSCH      6TiSCH      6TiSCH   /  Device
              ----Device------Device------Device------Device--
```

Figure 2

5.2.2.1.1. Packet Marking and Handling

Section "Packet Marking and Handling" of [I-D.ietf-6tisch-architecture] describes the packet tagging and marking that is expected in 6TiSCH networks.

5.2.2.1.1.1. Tagging Packets for Flow Identification

For packets that are routed by a PCE along a Track, the tuple formed by the IPv6 source address and a local RPLInstanceID is tagged in the packets to identify uniquely the Track and associated transmit bundle of timeSlots.

It results that the tagging that is used for a DetNet flow outside the 6TiSCH LLN MUST be swapped into 6TiSCH formats and back as the packet enters and then leaves the 6TiSCH network.

Note: The method and format used for encoding the RPLInstanceID at 6lo is generalized to all 6TiSCH topological Instances, which includes Tracks.

5.2.2.1.1.2. Replication, Retries and Elimination

PRE establishes several paths in a network to provide redundancy and parallel transmissions to bound the end-to-end delay. Considering the scenario shown in Figure 3, many different paths are possible for S to reach R. A simple way to benefit from this topology could be to use the two independent paths via nodes A, C, E and via B, D, F. But more complex paths are possible as well.

```
                            (A)   (C)   (E)

              source (S)                       (R)  (destination)

                            (B)   (D)   (F)
```

Figure 3: A Typical Ladder Shape with Two Parallel Paths Toward the Destination

By employing a Packet Replication function, each node forwards a copy of each data packet over two different branches. For instance, in Figure 4, the source node S transmits the data packet to nodes A and B, in two different timeslots within the same TSCH slotframe.

```
                      ===> (A) => (C) => (E) ===
                    //        \\//   \\//       \\
          source (S)          //\\   //\\         (R)  (destination)
                    \\       //  \\ //  \\      //
                      ===> (B) => (D) => (F) ===
```

Figure 4: Packet Replication: S transmits twice the same data packet, to its DP (A) and to its AP (B).

By employing Packet Elimination function once a node receives the first copy of a data packet, it discards the subsequent copies. Because the first copy that reaches a node is the one that matters, it is the only copy that will be forwarded upward.

Considering that the wireless medium is broadcast by nature, any neighbor of a transmitter may overhear a transmission. By employing the Promiscuous Overhearing function, nodes will have multiple opportunities to receive a given data packet. For instance, in Figure 4, when the source node S transmits the data packet to node A, node B may overhear this transmission.

6TiSCH expects elimination and replication of packets along a complex Track, but has no position about how the sequence numbers would be tagged in the packet.

As it goes, 6TiSCH expects that timeSlots corresponding to copies of a same packet along a Track are correlated by configuration, and does not need to process the sequence numbers.

The semantics of the configuration MUST enable correlated timeSlots to be grouped for transmit (and respectively receive) with a'OR'relations, and then a'AND'relation MUST be configurable between groups. The semantics is that if the transmit (and respectively receive) operation succeeded in one timeSlot in a'OR'group, then all the other timeSLots in the group are ignored. Now, if there are at least two groups, the'AND'relation between the groups indicates that one operation must succeed in each of the groups.

On the transmit side, timeSlots provisioned for retries along a same branch of a Track are placed a same'OR'group. The'OR'relation indicates that if a transmission is acknowledged, then further transmissions SHOULD NOT be attempted for timeSlots in that group. There are as many'OR'groups as there are branches of the Track departing from this node. Different'OR'groups are programmed for the purpose of replication, each group corresponding to one branch of the Track. The'AND'relation between the groups indicates that transmission over any of branches MUST be attempted regardless of whether a transmission succeeded in another branch. It is also possible to place cells to different next-hop routers in a same'OR'group. This allows to route along multi-path Tracks, trying one next-hop and then another only if sending to the first fails.

On the receive side, all timeSlots are programmed in a same'OR'group. Retries of a same copy as well as converging branches for elimination are converged, meaning that the first successful reception is enough and that all the other timeSlots can be ignored.

5.2.2.1.1.3. Differentiated Services Per-Hop-Behavior

Additionally, an IP packet that is sent along a Track uses the Differentiated Services Per-Hop-Behavior Group called Deterministic Forwarding, as described in [I-D.svshah-tsvwg-deterministic-forwarding].

5.2.2.1.2. Topology and capabilities

6TiSCH nodes are usually IoT devices, characterized by very limited amount of memory, just enough buffers to store one or a few IPv6 packets, and limited bandwidth between peers. It results that a node will maintain only a small number of peering information, and will not be able to store many packets waiting to be forwarded. Peers can be identified through MAC or IPv6 addresses.

Neighbors can be discovered over the radio using mechanism such as Enhanced Beacons, but, though the neighbor information is available in the 6TiSCH interface data model, 6TiSCH does not describe a protocol to pro-actively push the neighborhood information to a PCE. This protocol should be described and should operate over CoAP. The protocol should be able to carry multiple metrics, in particular the same metrics as used for RPL operations [RFC6551].

The energy that the device consumes in sleep, transmit and receive modes can be evaluated and reported. So can the amount of energy that is stored in the device and the power that it can be scavenged from the environment. The PCE SHOULD be able to compute Tracks that will implement policies on how the energy is consumed, for instance balance between nodes, ensure that the spent energy does not exceeded the scavenged energy over a period of time, etc...

5.2.2.1.3. Schedule Management by a PCE

6TiSCH supports a mixed model of centralized routes and distributed routes. Centralized routes can for example be computed by a entity such as a PCE [PCE]. Distributed routes are computed by RPL [RFC6550].

Both methods may inject routes in the Routing Tables of the 6TiSCH routers. In either case, each route is associated with a 6TiSCH topology that can be a RPL Instance topology or a Track. The 6TiSCH topology is indexed by a Instance ID, in a format that reuses the RPLInstanceID as defined in RPL.

Both RPL and PCE rely on shared sources such as policies to define Global and Local RPLInstanceIDs that can be used by either method. It is possible for centralized and distributed routing to share a same topology. Generally they will operate in different slotFrames, and centralized routes will be used for scheduled traffic and will have precedence over distributed routes in case of conflict between the slotFrames.

5.2.2.1.4. SlotFrames and Priorities

A slotFrame is the base object that a PCE needs to manipulate to program a schedule into an LLN node. Elaboration on that concept can be fond in section "SlotFrames and Priorities" of [I-D.ietf-6tisch-architecture]

IEEE802.15.4 TSCH avoids contention on the medium by formatting time and frequencies in cells of transmission of equal duration. In order to describe that formatting of time and frequencies, the 6TiSCH architecture defines a global concept that is called a Channel Distribution and Usage (CDU) matrix; a CDU matrix is a matrix of cells with an height equal to the number of available channels (indexed by ChannelOffsets) and a width (in timeSlots) that is the period of the network scheduling operation (indexed by slotOffsets) for that CDU matrix. The size of a cell is a timeSlot duration, and values of 10 to 15 milliseconds are typical in 802.15.4 TSCH to accommodate for the transmission of a frame and an acknowledgement, including the security validation on the receive side which may take up to a few milliseconds on some device architecture.

The frequency used by a cell in the matrix rotates in a pseudo-random fashion, from an initial position at an epoch time, as the matrix iterates over and over.

A CDU matrix is computed by the PCE, but unallocated timeSlots may be used opportunistically by the nodes for classical best effort IP traffic. The PCE has precedence in the allocation in case of a conflict.

In a given network, there might be multiple CDU matrices that operate with different width, so they have different durations and represent different periodic operations. It is recommended that all CDU matrices in a 6TiSCH domain operate with the same cell duration and are aligned, so as to reduce the chances of interferences from slotted-aloha operations. The PCE MUST compute the CDU matrices and shared that knowledge with all the nodes. The matrices are used in particular to define slotFrames.

A slotFrame is a MAC-level abstraction that is common to all nodes and contains a series of timeSlots of equal length and precedence. It is characterized by a slotFrame_ID, and a slotFrame_size. A slotFrame aligns to a CDU matrix for its parameters, such as number and duration of timeSlots.

Multiple slotFrames can coexist in a node schedule, i.e., a node can have multiple activities scheduled in different slotFrames, based on the precedence of the 6TiSCH topologies. The slotFrames may be aligned to different CDU matrices and thus have different width. There is typically one slotFrame for scheduled traffic that has the highest precedence and one or more slotFrame(s) for RPL traffic. The timeSlots in the slotFrame are indexed by the SlotOffset; the first cell is at SlotOffset 0.

The 6TiSCH architecture introduces the concept of chunks ([I-D.ietf-6tisch-architecture]) to operate such spectrum distribution for a whole group of cells at a time. The CDU matrix is formatted into a set of chunks, each of them identified uniquely by a chunk-ID, see Figure 5. The PCE MUST compute the partitioning of CDU matrices into chunks and shared that knowledge with all the nodes in a 6TiSCH network.

```
             +-----+-----+-----+-----+-----+-----+-----+     +-----+
chan.Off. 0  |chnkA|chnkP|chnk7|chnkO|chnk2|chnkK|chnk1| ... |chnkZ|
             +-----+-----+-----+-----+-----+-----+-----+     +-----+
chan.Off. 1  |chnkB|chnkQ|chnkA|chnkP|chnk3|chnkL|chnk2| ... |chnk1|
             +-----+-----+-----+-----+-----+-----+-----+     +-----+
               ...
             +-----+-----+-----+-----+-----+-----+-----+     +-----+
chan.Off. 15 |chnkO|chnk6|chnkN|chnk1|chnkJ|chnkZ|chnkI| ... |chnkG|
             +-----+-----+-----+-----+-----+-----+-----+     +-----+
                0     1     2     3     4     5     6           M
```

Figure 5: CDU matrix Partitioning in Chunks

The appropriation of a chunk can be requested explicitly by the PCE to any node. After a successful appropriation, the PCE owns the cells in that chunk, and may use them as hard cells to set up Tracks. Then again, 6TiSCH did not propose a method for chunk definition and a protocol for appropriation. This is to be done at RAW.

5.2.2.2. 6TiSCH Tracks

A Track at 6TiSCH is the application to wireless of the concept of a path in the Detnet architecture [I-D.ietf-detnet-architecture]. A Track can follow a simple sequence of relay nodes or can be structured as a more complex Destination Oriented Directed Acyclic Graph (DODAG) to a unicast destination. Along a Track, 6TiSCH nodes reserve the resources to enable the efficient transmission of packets while aiming to optimize certain properties such as reliability and ensure small jitter or bounded latency. The Track structure enables Layer-2 forwarding schemes, reducing the overhead of taking routing decisions at the Layer-3.

Serial Tracks can be understood as the concatenation of cells or bundles along a routing path from a source towards a destination. The serial Track concept is analogous to the circuit concept where resources are chained through the multi-hop topology. For example, A bundle of Tx Cells in a particular node is paired to a bundle of Rx Cells in the next hop node following a routing path.

Whereas scheduling ensures reliable delivery in bounded time along any Track, high availability requires the application of PAREO functions along a more complex DODAG Track structure. A DODAG has forking and joining nodes where the concepts such as Replication and Elimination can be exploited. Spatial redundancy increases the oveall energy consumption in the network but improves significantly the availability of the network as well as the packet delivery ratio. A Track may also branch off and rejoin, for the purpose of the so-called Packet Replication and Elimination (PRE), over non congruent branches. PRE may be used to complement layer-2 Automatic Repeat reQuest (ARQ) and receiver-end Ordering to form the PAREO functions. PAREO functions enable to meet industrial expectations in PDR within bounded delivery time over a Track that includes wireless links, even when the Track extends beyond the 6TiSCH network.

```
                     +-----+
                     | IoT |
                     | G/W |
                     +-----+
                        ^  <---- Elimination
                       | |
        Track branch   | |
               +-------+ +--------+ Subnet Backbone
               |                  |
            +--|--+            +--|--+
            |  |  | Backbone   |  |  | Backbone
       o    |  |  | router     |  |  | router
            +--/--+            +--|--+
       o     /    o     o---o----/       o
           o    o---o--/   o      o   o  o   o
      o     \  /     o               o   LLN    o
         o   v  <---- Replication
             o
```

Figure 6: End-to-End deterministic Track

In the example above (see Figure 6), a Track is laid out from a field device in a 6TiSCH network to an IoT gateway that is located on a IEEE802.1 TSN backbone.

The Replication function in the field device sends a copy of each packet over two different branches, and a PCE schedules each hop of both branches so that the two copies arrive in due time at the gateway. In case of a loss on one branch, hopefully the other copy of the packet still makes it in due time. If two copies make it to the IoT gateway, the Elimination function in the gateway ignores the extra packet and presents only one copy to upper layers.

At each 6TiSCH hop along the Track, the PCE may schedule more than one timeSlot for a packet, so as to support Layer-2 retries (ARQ). It is also possible that the field device only uses the second branch if sending over the first branch fails.

In current deployments, a TSCH Track does not necessarily support PRE but is systematically multi-path. This means that a Track is scheduled so as to ensure that each hop has at least two forwarding solutions, and the forwarding decision is to try the preferred one and use the other in case of Layer-2 transmission failure as detected by ARQ.

Methods to implement complex Tracks are described in [I-D.papadopoulos-paw-pre-reqs] and complemented by extensions to the RPL routing protocol in [I-D.ietf-roll-nsa-extension] for best effort traffic, but a centralized routing technique such as promoted in DetNet is still missing.

5.2.2.2.1. Track Scheduling Protocol

Section "Schedule Management Mechanisms" of the 6TiSCH architecture describes 4 paradigms to manage the TSCH schedule of the LLN nodes: Static Scheduling, neighbor-to-neighbor Scheduling, remote monitoring and scheduling management, and Hop-by-hop scheduling. The Track operation for DetNet corresponds to a remote monitoring and scheduling management by a PCE.

Early work at 6TiSCH on a data model and a protocol to program the schedule in the 6TiSCH device was never concluded as the group focussed on best effort traffic. This work would be revived by RAW:

> The 6top interface document [RFC8480] (to be reopened at RAW) was intended to specify the generic data model that can be used to monitor and manage resources of the 6top sublayer. Abstract methods were suggested for use by a management entity in the device. The data model also enables remote control operations on the 6top sublayer.
>
> [I-D.ietf-6tisch-coap] (to be reopened at RAW) was intended to define a mapping of the 6top set of commands, which is described in RFC 8480, to CoAP resources. This allows an entity to interact with the 6top layer of a node that is multiple hops away in a RESTful fashion.
>
> [I-D.ietf-6tisch-coap] also defined a basic set CoAP resources and associated RESTful access methods (GET/PUT/POST/DELETE). The payload (body) of the CoAP messages is encoded using the CBOR format. The PCE commands are expected to be issued directly as CoAP requests or to be mapped back and forth into CoAP by a gateway function at the edge of the 6TiSCH network. For instance, it is possible that a mapping entity on the backbone transforms a non-CoAP protocol such as PCEP into the RESTful interfaces that the 6TiSCH devices support.

5.2.2.2.2. Track Forwarding

By forwarding, this specification means the per-packet operation that allows to deliver a packet to a next hop or an upper layer in this node. Forwarding is based on pre-existing state that was installed as a result of the routing computation of a Track by a PCE. The 6TiSCH architecture supports three different forwarding model, G-MPLS Track Forwarding (TF), 6LoWPAN Fragment Forwarding (FF) and IPv6 Forwarding (6F) which is the classical IP operation [I-D.ietf-6tisch-architecture]. The DetNet case relates to the Track Forwarding operation under the control of a PCE.

A Track is a unidirectional path between a source and a destination. In a Track cell, the normal operation of IEEE802.15.4 Automatic Repeat-reQuest (ARQ) usually happens, though the acknowledgment may be omitted in some cases, for instance if there is no scheduled cell for a retry.

Track Forwarding is the simplest and fastest. A bundle of cells set to receive (RX-cells) is uniquely paired to a bundle of cells that are set to transmit (TX-cells), representing a layer-2 forwarding state that can be used regardless of the network layer protocol. This model can effectively be seen as a Generalized Multi-protocol Label Switching (G-MPLS) operation in that the information used to switch a frame is not an explicit label, but rather related to other properties of the way the packet was received, a particular cell in the case of 6TiSCH. As a result, as long as the TSCH MAC (and Layer-2 security) accepts a frame, that frame can be switched regardless of the protocol, whether this is an IPv6 packet, a 6LoWPAN fragment, or a frame from an alternate protocol such as WirelessHART or ISA100.11a.

A data frame that is forwarded along a Track normally has a destination MAC address that is set to broadcast - or a multicast address depending on MAC support. This way, the MAC layer in the intermediate nodes accepts the incoming frame and 6top switches it without incurring a change in the MAC header. In the case of IEEE802.15.4, this means effectively broadcast, so that along the Track the short address for the destination of the frame is set to 0xFFFF.

A Track is thus formed end-to-end as a succession of paired bundles, a receive bundle from the previous hop and a transmit bundle to the next hop along the Track, and a cell in such a bundle belongs to at most one Track. For a given iteration of the device schedule, the effective channel of the cell is obtained by adding a pseudo-random number to the channelOffset of the cell, which results in a rotation of the frequency that used for transmission. The bundles may be computed so as to accommodate both variable rates and retransmissions, so they might not be fully used at a given iteration of the schedule. The 6TiSCH architecture provides additional means to avoid waste of cells as well as overflows in the transmit bundle, as follows:

In one hand, a TX-cell that is not needed for the current iteration may be reused opportunistically on a per-hop basis for routed packets. When all of the frame that were received for a given Track are effectively transmitted, any available TX-cell for that Track can be reused for upper layer traffic for which the next-hop router matches the next hop along the Track. In that case, the cell that is being used is effectively a TX-cell from the Track, but the short address for the destination is that of the next-hop router. It results that a frame that is received in a RX-cell of a Track with a destination MAC address set to this node as opposed to broadcast must be extracted from the Track and delivered to the upper layer (a frame with an unrecognized MAC address is dropped at the lower MAC layer and thus is not received at the 6top sublayer).

On the other hand, it might happen that there are not enough TX-cells in the transmit bundle to accommodate the Track traffic, for instance if more retransmissions are needed than provisioned. In that case, the frame can be placed for transmission in the bundle that is used for layer-3 traffic towards the next hop along the Track as long as it can be routed by the upper layer, that is, typically, if the frame transports an IPv6 packet. The MAC address should be set to the next-hop MAC address to avoid confusion. It results that a frame that is received over a layer-3 bundle may be in fact associated to a Track. In a classical IP link such as an Ethernet, off-Track traffic is typically in excess over reservation to be routed along the non-reserved path based on its QoS setting. But with 6TiSCH, since the use of the layer-3 bundle may be due to transmission failures, it makes sense for the receiver to recognize a frame that should be re-Tracked, and to place it back on the appropriate bundle if possible. A frame should be re-Tracked if the Per-Hop-Behavior group indicated in the Differentiated Services Field in the IPv6 header is set to Deterministic Forwarding, as discussed in Section 5.2.2.1.1. A frame is re-Tracked by scheduling it for transmission over the transmit bundle associated to the Track, with the destination MAC address set to broadcast.

There are 2 modes for a Track, transport mode and tunnel mode.

5.2.2.2.2.1. Transport Mode

In transport mode, the Protocol Data Unit (PDU) is associated with flow-dependant meta-data that refers uniquely to the Track, so the 6top sublayer can place the frame in the appropriate cell without ambiguity. In the case of IPv6 traffic, this flow identification is transported in the Flow Label of the IPv6 header. Associated with the source IPv6 address, the Flow Label forms a globally unique identifier for that particular Track that is validated at egress before restoring the destination MAC address (DMAC) and punting to the upper layer.

```
                          |                                    ^
      +--------------+    |                                    |
      |     IPv6     |    |                                    |
      +--------------+    |                                    |
      |  6LoWPAN HC  |    |                                    |
      +--------------+  ingress                              egress
      |     6top     |   sets     +----+          +----+     restores
      +--------------+  dmac to   |    |          |    |     dmac to
      |   TSCH MAC   |   brdcst   |    |          |    |      self
      +--------------+    |       |    |          |    |       |
      |   LLN PHY    |    +-------+    +--...-----+    +-------+
      +--------------+
```

Figure 7: Track Forwarding, Transport Mode

5.2.2.2.2.2. Tunnel Mode

In tunnel mode, the frames originate from an arbitrary protocol over a compatible MAC that may or may not be synchronized with the 6TiSCH network. An example of this would be a router with a dual radio that is capable of receiving and sending WirelessHART or ISA100.11a frames with the second radio, by presenting itself as an Access Point or a Backbone Router, respectively.

In that mode, some entity (e.g. PCE) can coordinate with a WirelessHART Network Manager or an ISA100.11a System Manager to specify the flows that are to be transported transparently over the Track.

```
      +--------------+
      |     IPv6     |
      +--------------+
      |  6LoWPAN HC  |
      +--------------+             set            restore
      |     6top     |            +dmac+          +dmac+
      +--------------+          to|brdcst       to|nexthop
      |   TSCH MAC   |            |    |          |    |
      +--------------+            |    |          |    |
      |   LLN PHY    |    +-------+    +--...-----+    +-------+
      +--------------+    |   ingress                 egress   |
                          |                                    |
      +--------------+    |                                    |
      |   LLN PHY    |    |                                    |
      +--------------+    |                                    |
      |   TSCH MAC   |    |                                    |
      +--------------+    | dmac =                             | dmac =
      |ISA100/WiHART |    | nexthop                            v nexthop
      +--------------+
```

Figure 8: Track Forwarding, Tunnel Mode

In that case, the flow information that identifies the Track at the ingress 6TiSCH router is derived from the RX-cell. The dmac is set to this node but the flow information indicates that the frame must be tunneled over a particular Track so the frame is not passed to the upper layer. Instead, the dmac is forced to broadcast and the frame is passed to the 6top sublayer for switching.

At the egress 6TiSCH router, the reverse operation occurs. Based on metadata associated to the Track, the frame is passed to the appropriate link layer with the destination MAC restored.

5.2.2.2.2.3. Tunnel Metadata

Metadata coming with the Track configuration is expected to provide the destination MAC address of the egress endpoint as well as the tunnel mode and specific data depending on the mode, for instance a service access point for frame delivery at egress. If the tunnel egress point does not have a MAC address that matches the configuration, the Track installation fails.

In transport mode, if the final layer-3 destination is the tunnel termination, then it is possible that the IPv6 address of the destination is compressed at the 6LoWPAN sublayer based on the MAC address. It is thus mandatory at the ingress point to validate that the MAC address that was used at the 6LoWPAN sublayer for compression matches that of the tunnel egress point. For that reason, the node that injects a packet on a Track checks that the destination is effectively that of the tunnel egress point before it overwrites it to broadcast. The 6top sublayer at the tunnel egress point reverts that operation to the MAC address obtained from the tunnel metadata.

5.2.2.2.2.4. OAM

An Overview of Operations, Administration, and Maintenance (OAM) Tools [RFC7276] provides an overwiew of the existing tooling for OAM [RFC6291]. Tracks are complex paths and new tooling is necessary to manage them, with respect to load control, timing, and the Packet Replication and Elimination Functions (PREF).

An example of such tooling can be found in the context of BIER [RFC8279] and more specifically BIER Traffic Engineering [I-D.ietf-bier-te-arch] (BIER-TE): [I-D.thubert-bier-replication-elimination] leverages BIER-TE to control the process of PREF, and to provide traceability of these operations, in the deterministic dataplane, along a complex Track. For the 6TiSCH type of constrained environment, [I-D.thubert-6lo-bier-dispatch] enables an efficient encoding of the BIER bitmap within the 6LoRH framework.

6. 5G

6.1. Provenance and Documents

The 3rd Generation Partnership Project (3GPP) incorporates many companies whose business is related to cellular network operation as well as network equipment and device manufacturing. All generations of 3GPP technologies provide scheduled wireless segments, primarily in licensed spectrum which is beneficial for reliability and availability.

In 2016, the 3GPP started to design New Radio (NR) technology belonging to the fifth generation (5G) of cellular networks. NR has been designed from the beginning to not only address enhanced Mobile Broadband (eMBB) services for consumer devices such as smart phones or tablets but is also tailored for future Internet of Things (IoT) communication and connected cyber-physical systems. In addition to eMBB, requirement categories have been defined on Massive Machine-Type Communication (M-MTC) for a large number of connected devices/ sensors, and Ultra-Reliable Low-Latency Communication (URLLC) for connected control systems and critical communication as illustrated in Figure 9. It is the URLLC capabilities that make 5G a great candidate for reliable low-latency communication. With these three corner stones, NR is a complete solution supporting the connectivity needs of consumers, enterprises, and public sector for both wide area and local area, e.g. indoor deployments. A general overview of NR can be found in [TS38300].

```
                                enhanced
                            Mobile Broadband
                                   ^
                                  / \
                                 /   \
                                /     \
                               /       \
                              /   5G    \
                             /           \
                            /             \
                           /               \
                          +-----------------+
                       Massive         Ultra-Reliable
                     Machine-Type       Low-Latency
                    Communication      Communication
```

Figure 9: 5G Application Areas

As a result of releasing the first NR specification in 2018 (Release 15), it has been proven by many companies that NR is a URLLC-capable technology and can deliver data packets at 10^-5 packet error rate within 1ms latency budget [TR37910]. Those evaluations were consolidated and forwarded to ITU to be included in the [IMT2020] work.

In order to understand communication requirements for automation in vertical domains, 3GPP studied different use cases [TR22804] and released technical specification with reliability, availability and latency demands for a variety of applications [TS22104].

As an evolution of NR, multiple studies have been conducted in scope of 3GPP Release 16 including the following two, focusing on radio aspects:

1. Study on physical layer enhancements for NR ultra-reliable and low latency communication (URLLC) [TR38824].

2. Study on NR industrial Internet of Things (I-IoT) [TR38825].

In addition, several enhancements have been done on system architecture level which are reflected in System architecture for the 5G System (5GS) [TS23501].

6.2. General Characteristics

The 5G Radio Access Network (5G RAN) with its NR interface includes several features to achieve Quality of Service (QoS), such as a guaranteeably low latency or tolerable packet error rates for selected data flows. Determinism is achieved by centralized admission control and scheduling of the wireless frequency resources, which are typically licensed frequency bands assigned to a network operator.

NR enables short transmission slots in a radio subframe, which benefits low-latency applications. NR also introduces mini-slots, where prioritized transmissions can be started without waiting for slot boundaries, further reducing latency. As part of giving priority and faster radio access to URLLC traffic, NR introduces preemption where URLLC data transmission can preempt ongoing non-URLLC transmissions. Additionally, NR applies very fast processing, enabling retransmissions even within short latency bounds.

NR defines extra-robust transmission modes for increased reliability both for data and control radio channels. Reliability is further improved by various techniques, such as multi-antenna transmission, the use of multiple frequency carriers in parallel and packet duplication over independent radio links. NR also provides full mobility support, which is an important reliability aspect not only for devices that are moving, but also for devices located in a changing environment.

Network slicing is seen as one of the key features for 5G, allowing vertical industries to take advantage of 5G networks and services. Network slicing is about transforming a Public Land Mobile Network (PLMN) from a single network to a network where logical partitions are created, with appropriate network isolation, resources, optimized topology and specific configuration to serve various service requirements. An operator can configure and manage the mobile network to support various types of services enabled by 5G, for example eMBB and URLLC, depending on the different customers’ needs.

Exposure of capabilities of 5G Systems to the network or applications outside the 3GPP domain have been added to Release 16 [TS23501]. Via exposure interfaces, applications can access 5G capabilities, e.g., communication service monitoring and network maintenance.

For several generations of mobile networks, 3GPP has considered how the communication system should work on a global scale with billions of users, taking into account resilience aspects, privacy regulation, protection of data, encryption, access and core network security, as well as interconnect. Security requirements evolve as demands on trustworthiness increase. For example, this has led to the introduction of enhanced privacy protection features in 5G. 5G also employs strong security algorithms, encryption of traffic, protection of signaling and protection of interfaces.

One particular strength of mobile networks is the authentication, based on well-proven algorithms and tightly coupled with a global identity management infrastructure. Since 3G, there is also mutual authentication, allowing the network to authenticate the device and the device to authenticate the network. Another strength is secure solutions for storage and distribution of keys fulfilling regulatory requirements and allowing international roaming. When connecting to 5G, the user meets the entire communication system, where security is the result of standardization, product security, deployment, operations and management as well as incident handling capabilities. The mobile networks approach the entirety in a rather coordinated fashion which is beneficial for security.

6.3. Deployment and Spectrum

The 5G system allows deployment in a vast spectrum range, addressing use-cases in both wide-area as well as local networks. Furthermore, 5G can be configured for public and non-public access.

When it comes to spectrum, NR allows combining the merits of many frequency bands, such as the high bandwidths in millimeter Waves (mmW) for extreme capacity locally, as well as the broad coverage when using mid- and low frequency bands to address wide-area scenarios. URLLC is achievable in all these bands. Spectrum can be either licensed, which means that the license holder is the only authorized user of that spectrum range, or unlicensed, which means that anyone who wants to use the spectrum can do so.

A prerequisite for critical communication is performance predictability, which can be achieved by the full control of the access to the spectrum, which 5G provides. Licensed spectrum guarantees control over spectrum usage by the system, making it a preferable option for critical communication. However, unlicensed spectrum can provide an additional resource for scaling non-critical communications. While NR is initially developed for usage of licensed spectrum, the functionality to access also unlicensed spectrum was introduced in 3GPP Release 16.

Licensed spectrum dedicated to mobile communications has been allocated to mobile service providers, i.e. issued as longer-term licenses by national administrations around the world. These licenses have often been associated with coverage requirements and issued across whole countries, or in large regions. Besides this, configured as a non-public network (NPN) deployment, 5G can provide network services also to a non-operator defined organization and its premises such as a factory deployment. By this isolation, quality of service requirements, as well as security requirements can be achieved. An integration with a public network, if required, is also possible. The non-public (local) network can thus be interconnected with a public network, allowing devices to roam between the networks.

In an alternative model, some countries are now in the process of allocating parts of the 5G spectrum for local use to industries. These non-service providers then have a choice of applying for a local license themselves and operating their own network or cooperating with a public network operator or service provider.

6.4. Applicability to Deterministic Flows

6.4.1. System Architecture

The 5G system [TS23501] consists of the User Equipment (UE) at the terminal side, and the Radio Access Network (RAN) with the gNB as radio base station node, as well as the Core Network (CN). The core network is based on a service-based architecture with the central functions: Access and Mobility Management Function (AMF), Session Management Function (SMF) and User Plane Function (UPF) as illustrated in Figure 10.

The gNB’s main responsibility is the radio resource management, including admission control and scheduling, mobility control and radio measurement handling. The AMF handles the UE’s connection status and security, while the SMF controls the UE’s data sessions. The UPF handles the user plane traffic.

The SMF can instantiate various Packet Data Unit (PDU) sessions for the UE, each associated with a set of QoS flows, i.e., with different QoS profiles. Segregation of those sessions is also possible, e.g., resource isolation in the RAN and in the CN can be defined (slicing).

```
             +----+  +---+   +---+    +---+    +---+   +---+
             |NSSF|  |NEF|   |NRF|    |PCF|    |UDM|   |AF |
             +--+-+  +-+-+   +-+-+    +-+-+    +-+-+   +-+-+
                |      |       |        |        |       |
           Nnssf|  Nnef|   Nnrf|    Npcf|    Nudm|    Naf|
                |      |       |        |        |       |
             ---+------+-+-----+-+------------+--+-----+-+---
                         |       |            |         |
                    Nausf|   Nausf|        Nsmf|         |
                         |       |            |         |
                      +--+-+   +-+-+        +-+-+     +-+-+
                      |AUSF|   |AMF|        |SMF|     |SCP|
                      +----+   +++-+        +-+-+     +---+
                               / |            |
                              /  |            |
                             /   |            |
                            N1   N2           N4
                           /     |            |
                          /      |            |
                         /       |            |
                     +--+-+   +--+--+      +--+---+      +----+
                     | UE +---+(R)AN+--N3--+ UPF  +--N6--+ DN |
                     +----+   +-----+      ++----++      +----+
                                            |    |
                                            +-N9-+
```

Figure 10: 5G System Architecture

To allow UE mobility across cells/gNBs, handover mechanisms are supported in NR. For an established connection, i.e., connected mode mobility, a gNB can configure a UE to report measurements of received signal strength and quality of its own and neighbouring cells, periodically or event-based. Based on these measurement reports, the gNB decides to handover a UE to another target cell/gNB. Before triggering the handover, it is hand-shaked with the target gNB based on network signalling. A handover command is then sent to the UE and the UE switches its connection to the target cell/gNB. The Packet Data Convergence Protocol (PDCP) of the UE can be configured to avoid data loss in this procedure, i.e., handle retransmissions if needed. Data forwarding is possible between source and target gNB as well. To improve the mobility performance further, i.e., to avoid connection failures, e.g., due to too-late handovers, the mechanism of conditional handover is introduced in Release 16 specifications.

Therein a conditional handover command, defining a triggering point, can be sent to the UE before UE enters a handover situation. A further improvement introduced in Release 16 is the Dual Active Protocol Stack (DAPS), where the UE maintains the connection to the source cell while connecting to the target cell. This way, potential interruptions in packet delivery can be avoided entirely.

6.4.2. Overview of The Radio Protocol Stack

The protocol architecture for NR consists of the L1 Physical layer (PHY) and as part of the L2, the sublayers of Medium Access Control (MAC), Radio Link Control (RLC), Packet Data Convergence Protocol (PDCP), as well as the Service Data Adaption Protocol (SDAP).

The PHY layer handles signal processing related actions, such as encoding/decoding of data and control bits, modulation, antenna precoding and mapping.

The MAC sub-layer handles multiplexing and priority handling of logical channels (associated with QoS flows) to transport blocks for PHY transmission, as well as scheduling information reporting and error correction through Hybrid Automated Repeat Request (HARQ).

The RLC sublayer handles sequence numbering of higher layer packets, retransmissions through Automated Repeat Request (ARQ), if configured, as well as segmentation and reassembly and duplicate detection.

The PDCP sublayer consists of functionalities for ciphering/deciphering, integrity protection/verification, re-ordering and in-order delivery, duplication and duplicate handling for higher layer packets, and acts as the anchor protocol to support handovers.

The SDAP sublayer provides services to map QoS flows, as established by the 5G core network, to data radio bearers (associated with logical channels), as used in the 5G RAN.

Additionally, in RAN, the Radio Resource Control (RRC) protocol, handles the access control and configuration signalling for the aforementioned protocol layers. RRC messages are considered L3 and thus transmitted also via those radio protocol layers.

To provide low latency and high reliability for one transmission link, i.e., to transport data (or control signaling) of one radio bearer via one carrier, several features have been introduced on the user plane protocols for PHY and L2, as explained in the following.

6.4.3. Radio (PHY)

NR is designed with native support of antenna arrays utilizing benefits from beamforming, transmissions over multiple MIMO layers and advanced receiver algorithms allowing effective interference cancellation. Those antenna techniques are the basis for high signal quality and effectiveness of spectral usage. Spatial diversity with up to 4 MIMO layers in UL and up to 8 MIMO layers in DL is supported. Together with spatial-domain multiplexing, antenna arrays can focus power in desired direction to form beams. NR supports beam management mechanisms to find the best suitable beam for UE initially and when it is moving. In addition, gNBs can coordinate their respective DL and UL transmissions over the backhaul network keeping interference reasonably low, and even make transmissions or receptions from multiple points (multi-TRP). Multi-TRP can be used for repetition of data packet in time, in frequency or over multiple MIMO layers which can improve reliability even further.

Any downlink transmission to a UE starts from resource allocation signaling over the Physical Downlink Control Channel (PDCCH). If it is successfully received, the UE will know about the scheduled transmission and may receive data over the Physical Downlink Shared Channel (PDSCH). If retransmission is required according to the HARQ scheme, a signaling of negative acknowledgement (NACK) on the Physical Uplink Control Channel (PUCCH) is involved and PDCCH together with PDSCH transmissions (possibly with additional redundancy bits) are transmitted and soft-combined with previously received bits. Otherwise, if no valid control signaling for scheduling data is received, nothing is transmitted on PUCCH (discontinuous transmission - DTX),and the base station upon detecting DTX will retransmit the initial data.

An uplink transmission normally starts from a Scheduling Request (SR) - a signaling message from the UE to the base station sent via PUCCH. Once the scheduler is informed about buffer data in UE, e.g., by SR, the UE transmits a data packet on the Physical Uplink Shared Channel (PUSCH). Pre-scheduling not relying on SR is also possible (see following section).

Since transmission of data packets require usage of control and data channels, there are several methods to maintain the needed reliability. NR uses Low Density Parity Check (LDPC) codes for data channels, Polar codes for PDCCH, as well as orthogonal sequences and Polar codes for PUCCH. For ultra-reliability of data channels, very robust (low spectral efficiency) Modulation and Coding Scheme (MCS) tables are introduced containing very low (down to 1/20) LDPC code rates using BPSK or QPSK. Also, PDCCH and PUCCH channels support multiple code rates including very low ones for the channel robustness.

A connected UE reports downlink (DL) quality to gNB by sending Channel State Information (CSI) reports via PUCCH while uplink (UL) quality is measured directly at gNB. For both uplink and downlink, gNB selects the desired MCS number and signals it to the UE by Downlink Control Information (DCI) via PDCCH channel. For URLLC services, the UE can assist the gNB by advising that MCS targeting 10^-5 Block Error Rate (BLER) are used. Robust link adaptation algorithms can maintain the needed level of reliability considering a given latency bound.

Low latency on the physical layer is provided by short transmission duration which is possible by using high Subcarrier Spacing (SCS) and the allocation of only one or a few Orthogonal Frequency Division Multiplexing (OFDM) symbols. For example, the shortest latency for the worst case in DL can be 0.23ms and in UL can be 0.24ms according to (section 5.7.1 in [TR37910]). Moreover, if the initial transmission has failed, HARQ feedback can quickly be provided and an HARQ retransmission is scheduled.

Dynamic multiplexing of data associated with different services is highly desirable for efficient use of system resources and to maximize system capacity. Assignment of resources for eMBB is usually done with regular (longer) transmission slots, which can lead to blocking of low latency services. To overcome the blocking, eMBB resources can be pre-empted and re-assigned to URLLC services. In this way, spectrally efficient assignments for eMBB can be ensured while providing flexibility required to ensure a bounded latency for URLLC services. In downlink, the gNB can notify the eMBB UE about pre-emption after it has happened, while in uplink there are two pre-emption mechanisms: special signaling to cancel eMBB transmission and URLLC dynamic power boost to suppress eMBB transmission.

6.4.4. Scheduling and QoS (MAC)

One integral part of the 5G system is the Quality of Service (QoS) framework [TS23501]. QoS flows are setup by the 5G system for certain IP or Ethernet packet flows, so that packets of each flow receive the same forwarding treatment, i.e., in scheduling and admission control. QoS flows can for example be associated with different priority level, packet delay budgets and tolerable packet error rates. Since radio resources are centrally scheduled in NR, the admission control function can ensure that only those QoS flows are admitted for which QoS targets can be reached.

NR transmissions in both UL and DL are scheduled by the gNB [TS38300]. This ensures radio resource efficiency, fairness in resource usage of the users and enables differentiated treatment of the data flows of the users according to the QoS targets of the flows. Those QoS flows are handled as data radio bearers or logical channels in NR RAN scheduling.

The gNB can dynamically assign DL and UL radio resources to users, indicating the resources as DL assignments or UL grants via control channel to the UE. Radio resources are defined as blocks of OFDM symbols in spectral domain and time domain. Different lengths are supported in time domain, i.e., (multiple) slot or mini-slot lengths. Resources of multiple frequency carriers can be aggregated and jointly scheduled to the UE.

Scheduling decisions are based, e.g., on channel quality measured on reference signals and reported by the UE (cf. periodical CSI reports for DL channel quality). The transmission reliability can be chosen in the scheduling algorithm, i.e., by link adaptation where an appropriate transmission format (e.g., robustness of modulation and coding scheme, controlled UL power) is selected for the radio channel condition of the UE. Retransmissions, based on HARQ feedback, are also controlled by the scheduler. If needed to avoid HARQ round-trip time delays, repeated transmissions can be also scheduled beforehand, to the cost of reduced spectral efficiency.

In dynamic DL scheduling, transmission can be initiated immediately when DL data becomes available in the gNB. However, for dynamic UL scheduling, when data becomes available but no UL resources are available yet, the UE indicates the need for UL resources to the gNB via a (single bit) scheduling request message in the UL control channel. When thereupon UL resources are scheduled to the UE, the UE can transmit its data and may include a buffer status report, indicating the exact amount of data per logical channel still left to be sent. More UL resources may be scheduled accordingly. To avoid the latency introduced in the scheduling request loop, UL radio resources can also be pre-scheduled.

In particular for periodical traffic patterns, the pre-scheduling can rely on the scheduling features DL Semi-Persistent Scheduling (SPS) and UL Configured Grant (CG). With these features, periodically recurring resources can be assigned in DL and UL. Multiple parallels of those configurations are supported, in order to serve multiple parallel traffic flows of the same UE.

To support QoS enforcement in the case of mixed traffic with different QoS requirements, several features have recently been introduced. This way, e.g., different periodical critical QoS flows can be served together with best effort transmissions, by the same UE. Among others, these features (partly Release 16) are: 1) UL logical channel transmission restrictions allowing to map logical channels of certain QoS only to intended UL resources of a certain frequency carrier, slot-length, or CG configuration, and 2) intra-UE pre-emption, allowing critical UL transmissions to pre-empt non-critical transmissions.

When multiple frequency carriers are aggregated, duplicate parallel transmissions can be employed (beside repeated transmissions on one carrier). This is possible in the Carrier Aggregation (CA) architecture where those carriers originate from the same gNB, or in the Dual Connectivity (DC) architecture where the carriers originate from different gNBs, i.e., the UE is connected to two gNBs in this case. In both cases, transmission reliability is improved by this means of providing frequency diversity.

In addition to licensed spectrum, a 5G system can also utilize unlicensed spectrum to offload non-critical traffic. This version of NR is called NR-U, part of 3GPP Release 16. The central scheduling approach applies also for unlicensed radio resources, but in addition also the mandatory channel access mechanisms for unlicensed spectrum, e.g., Listen Before Talk (LBT) are supported in NR-U. This way, by using NR, operators have and can control access to both licensed and unlicensed frequency resources.

6.4.5. Time-Sensitive Networking (TSN) Integration

The main objective of Time-Sensitive Networking (TSN) is to provide guaranteed data delivery within a guaranteed time window, i.e., bounded low latency. IEEE 802.1 TSN [IEEE802.1TSN] is a set of open standards that provide features to enable deterministic communication on standard IEEE 802.3 Ethernet [IEEE802.3]. TSN standards can be seen as a toolbox for traffic shaping, resource management, time synchronization, and reliability.

A TSN stream is a data flow between one end station (Talker) to another end station (Listener). In the centralized configuration model, TSN bridges are configured by the Central Network Controller (CNC) [IEEE802.1Qcc] to provide deterministic connectivity for the TSN stream through the network. Time-based traffic shaping provided by Scheduled Traffic [IEEE802.1Qbv] may be used to achieve bounded low latency. The TSN tool for time synchronization is the generalized Precision Time Protocol (gPTP) [IEEE802.1AS]), which provides reliable time synchronization that can be used by end stations and by other TSN tools, e.g., Scheduled Traffic [IEEE802.1Qbv]. High availability, as a result of ultra-reliability, is provided for data flows by the Frame Replication and Elimination for Reliability (FRER) [IEEE802.1CB] mechanism.

3GPP Release 16 includes integration of 5G with TSN, i.e., specifies functions for the 5G System (5GS) to deliver TSN streams such that the meet their QoS requirements. A key aspect of the integration is the 5GS appears from the rest of the network as a set of TSN bridges, in particular, one virtual bridge per User Plane Function (UPF) on the user plane. The 5GS includes TSN Translator (TT) functionality for the adaptation of the 5GS to the TSN bridged network and for hiding the 5GS internal procedures. The 5GS provides the following components:

1. interface to TSN controller, as per [IEEE802.1Qcc] for the fully centralized configuration model

2. time synchronization via reception and transmission of gPTP PDUs [IEEE802.1AS]

3. low latency, hence, can be integrated with Scheduled Traffic [IEEE802.1Qbv]

4. reliability, hence, can be integrated with FRER [IEEE802.1CB]

Figure 10 shows an illustration of 5G-TSN integration where an industrial controller (Ind Ctrlr) is connected to industrial Input/Output devices (I/O dev) via 5G. The 5GS can directly transport Ethernet frames since Release 15, thus, end-to-end Ethernet connectivity is provided. The 5GS implements the required interfaces towards the TSN controller functions such as the CNC, thus adapts to the settings of the TSN network. A 5G user plane virtual bridge interconnects TSN bridges or connect end stations, e.g., I/O devices to the network. Note that the introduction of 5G brings flexibility in various aspects, e.g., more flexible network topology because a wireless hop can replace several wireline hops thus significantly reduce the number of hops end-to-end. [ETR5GTSN] dives more into the integration of 5G with TSN.

```
                 +------------------------------+
                 | 5G System                    |
                 |                         +---+|
                 |     +-+ +-+ +-+ +-+ +-+ |TSN||
                 |     | | | | | | | | | | |AF |......+
                 |     +++ +++ +++ +++ +++ +-+-+|     .
                 |      |   |   |   |   |    |  |     .
                 |     -+---+---++--+-+-+--+-+- |     .
                 |          |    |    |    |    |  +--+--+
                 |         +++  +++  +++  +++   |  | TSN |
                 |         | |  | |  | |  | |   |  |Ctrlr+.......+
                 |         +++  +++  +++  +++   |  +--+--+       .
                 |                              |     .          .
                 |                              |     .          .
                 | +..........................+ |     .          .
                 | .      Virtual Bridge      . |     .          .
+---+            | . +--+--+   +---+ +---+--+ . |  +--+---+       .
|I/O+----------------+DS|UE+---+RAN+-+UPF|NW+------+ TSN  +----+ .
|dev|            | . |TT|  |   |   | |   |TT| . |  |bridge|    | .
+---+            | . +--+--+   +---+ +---+--+ . |  +------+    | .
                 | +..........................+ |     .      +-+-+-+
                 |                              |     .      | Ind |
                 | +..........................+ |     .      |Ctrlr|
                 | .      Virtual Bridge      . |     .      +-+---+
+---+  +------+  | . +--+--+   +---+ +---+--+ . |  +--+---+    |
|I/O+--+ TSN  +------+DS|UE+---+RAN+-+UPF|NW+------+ TSN  +----+
|dev|  |bridge|  | . |TT|  |   |   | |   |TT| . |  |bridge|
+---+  +------+  | . +--+--+   +---+ +---+--+ . |  +------+
                 | +..........................+ |
                 +------------------------------+

    <----------------- end-to-end Ethernet ------------------->
```

Figure 11: 5G - TSN Integration

NR supports accurate reference time synchronization in 1us accuracy level. Since NR is a scheduled system, an NR UE and a gNB are tightly synchronized to their OFDM symbol structures. A 5G internal reference time can be provided to the UE via broadcast or unicast signaling, associating a known OFDM symbol to this reference clock. The 5G internal reference time can be shared within the 5G network, i.e., radio and core network components. For the interworking with gPTP for multiple time domains, the 5GS acts as a virtual gPTP time-aware system and supports the forwarding of gPTP time synchronization information between end stations and bridges through the 5G user plane TTs. These account for the residence time of the 5GS in the time synchronization procedure. One special option is when the 5GS internal reference time in not only used within the 5GS, but also to the rest of the devices in the deployment, including connected TSN bridges and end stations.

Redundancy architectures were specified in order to provide reliability against any kind of failure on the radio link or nodes in the RAN and the core network, Redundant user plane paths can be provided based on the dual connectivity architecture, where the UE sets up two PDU sessions towards the same data network, and the 5G system makes the paths of the two PDU sessions independent as illustrated in Figure 13. There are two PDU sessions involved in the solution: the first spans from the UE via gNB1 to UPF1, acting as the first PDU session anchor, while the second spans from the UE via gNB2 to UPF2, acting as second the PDU session anchor. The independent paths may continue beyond the 3GPP network. Redundancy Handling Functions (RHFs) are deployed outside of the 5GS, i.e., in Host A (the device) and in Host B (the network). RHF can implement replication and elimination functions as per [IEEE802.1CB] or the Packet Replication, Elimination, and Ordering Functions (PREOF) of IETF Deterministic Networking (DetNet) [RFC8655].

```
           +........+
           . Device . +------+      +------+      +------+
           .        . + gNB1 +--N3--+ UPF1 |--N6--+      |
           .        ./+------+      +------+      |      |
           . +----+ /                             |      |
           . |    |/.                             |      |
           . | UE + .                             |  DN  |
           . |    |\.                             |      |
           . +----+ \                             |      |
           .        .\+------+      +------+      |      |
           +........+ + gNB2 +--N3--+ UPF2 |--N6--+      |
                      +------+      +------+      +------+
```

Figure 12: Reliability with Single UE

An alternative solution is that multiple UEs per device are used for user plane redundancy as illustrated in Figure 13. Each UE sets up a PDU session. The 5GS ensures that those PDU sessions of the different UEs are handled independently internal to the 5GS. There is no single point of failure in this solution, which also includes RHF outside of the 5G system, e.g., as per FRER or as PREOF specifications.

```
          +.........+
          .  Device .
          .         .
          . +----+  .  +------+      +------+      +------+
          . | UE +-----+ gNB1 +--N3--+ UPF1 |--N6--+      |
          . +----+  .  +------+      +------+      |      |
          .         .                              |  DN  |
          . +----+  .  +------+      +------+      |      |
          . | UE +-----+ gNB2 +--N3--+ UPF2 |--N6--+      |
          . +----+  .  +------+      +------+      +------+
          .         .
          +.........+
```

Figure 13: Reliability with Dual UE

Note that the abstraction provided by the RHF and the location of the RHF being outside of the 5G system make 5G equally supporting integration for reliability both with FRER of TSN and PREOF of DetNet as they both rely on the same concept.

Note also that TSN is the primary subnetwork technology for DetNet. Thus, the DetNet over TSN work, e.g., [I-D.ietf-detnet-ip-over-tsn], can be leveraged via the TSN support built in 5G.

6.5. Summary

5G technology enables deterministic communication. Based on the centralized admission control and the scheduling of the wireless resources, licensed or unlicensed, quality of service such as latency and reliability can be guaranteed. 5G contains several features to achieve ultra-reliable and low latency performance, e.g., support for different OFDM numerologies and slot-durations, as well as fast processing capabilities and redundancy techniques that lead to achievable latency numbers of below 1ms with reliability guarantees up to 99.999%.

5G also includes features to support Industrial IoT use cases, e.g., via the integration of 5G with TSN. This includes 5G capabilities for each TSN component, latency, resource management, time synchronization, and reliability. Furthermore, 5G support for TSN can be leveraged when 5G is used as subnet technology for DetNet, in combination with or instead of TSN, which is the primary subnet for DetNet. In addition, the support for integration with TSN reliability was added to 5G by making DetNet reliability also applicable, thus making 5G DetNet ready. Moreover, providing IP service is native to 5G.

Overall, 5G provides scheduled wireless segments with high reliability and availability. In addition, 5G includes capabilities for integration to IP networks.

7. L-band Digital Aeronautical Communications System

One of the main pillars of the modern Air Traffic Management (ATM) system is the existence of a communication infrastructure that enables efficient aircraft guidance and safe separation in all phases of flight. Although current systems are technically mature, they are suffering from the VHF band's increasing saturation in high-density areas and the limitations posed by analogue radio. Therefore, aviation globally and the European Union (EU) in particular, strives for a sustainable modernization of the aeronautical communication infrastructure.

In the long-term, ATM communication shall transition from analogue VHF voice and VDL2 communication to more spectrum efficient digital data communication. The European ATM Master Plan foresees this transition to be realized for terrestrial communications by the development and implementation of the L-band Digital Aeronautical Communications System (LDACS). LDACS shall enable IPv6 based air-ground communication related to the safety and regularity of the flight. The particular challenge is that no new frequencies can be made available for terrestrial aeronautical communication. It was thus necessary to develop procedures to enable the operation of LDACS in parallel with other services in the same frequency band.

7.1. Provenance and Documents

The development of LDACS has already made substantial progress in the Single European Sky ATM Research (SESAR) framework, and is currently being continued in the follow-up program, SESAR2020 [RIH18]. A key objective of the SESAR activities is to develop, implement and validate a modern aeronautical data link able to evolve with aviation needs over long-term. To this end, an LDACS specification has been produced [GRA19] and is continuously updated; transmitter demonstrators were developed to test the spectrum compatibility of LDACS with legacy systems operating in the L-band [SAJ14]; and the overall system performance was analyzed by computer simulations, indicating that LDACS can fulfill the identified requirements [GRA11].

LDACS standardization within the framework of the International Civil Aviation Organization (ICAO) started in December 2016. The ICAO standardization group has produced an initial Standards and Recommended Practices (SARPs) document [ICAO18]. The SARPs document defines the general characteristics of LDACS. The ICAO standardization group plans to produce an ICAO technical manual - the ICAO equivalent to a technical standard - within the next years. Generally, the group is open to input from all sources and develops LDACS in the open.

Up to now the LDACS standardization has been focused on the development of the physical layer and the data link layer, only recently have higher layers come into the focus of the LDACS development activities. There is currently no "IPv6 over LDACS" specification; however, SESAR2020 has started the testing of IPv6-based LDACS testbeds. The IPv6 architecture for the aeronautical telecommunication network is called the Future Communications Infrastructure (FCI). FCI shall support quality of service, diversity, and mobility under the umbrella of the "multi-link concept". This work is conducted by ICAO working group WG-I.

In addition to standardization activities several industrial LDACS prototypes have been built. One set of LDACS prototypes has been evaluated in flight trials confirming the theoretical results predicting the system performance [GRA18][SCH19].

7.2. General Characteristics

LDACS will become one of several wireless access networks connecting aircraft to the Aeronautical Telecommunications Network (ATN). The LDACS access network contains several ground stations, each of them providing one LDACS radio cell. The LDACS air interface is a cellular data link with a star-topology connecting aircraft to ground-stations with a full duplex radio link. Each ground-station is the centralized instance controlling all air-ground communications within its radio cell.

The user data rate of LDACS is 315 kbit/s to 1428 kbit/s on the forward link, and 294 kbit/s to 1390 kbit/s on the reverse link, depending on coding and modulation. Due to strong interference from legacy systems in the L-band, the most robust coding and modulation SHOULD be expected for initial deployment i.e. 315/294 kbit/s on the forward/reverse link, respectively.

In addition to the communications capability, LDACS also offers a navigation capability. Ranging data, similar to DME (Distance Measuring Equipment), is extracted from the LDACS communication links between aircraft and LDACS ground stations. This results in LDACS providing an APNT (Alternative Position, Navigation and Timing) capability to supplement the existing on-board GNSS (Global Navigation Satellite System) without the need for additional bandwidth. Operationally, there will be no difference for pilots whether the navigation data are provided by LDACS or DME. This capability was flight tested and proven during the MICONAV flight trials in 2019 [BAT19].

In previous works and during the MICONAV flight campaign in 2019, it was also shown, that LDACS can be used for surveillance capability. Filip et al. [FIL19] shown passive radar capabilities of LDACS and Automatic Dependence Surveillance - Contract (ADS-C) was demonstrated via LDACS during the flight campaign 2019 [SCH19].

Since LDACS has been mainly designed for air traffic management communication it supports mutual entity authentication, integrity and confidentiality capabilities of user data messages and some control channel protection capabilities [MAE18], [MAE191], [MAE192], [MAE20].

Overall this makes LDACS the world’s first truly integrated CNS system and is the worldwide most mature, secure, terrestrial long-range CNS technology for civil aviation.

7.3. Deployment and Spectrum

LDACS has its origin in merging parts of the B-VHF [BRA06], B-AMC [SCH08], TIA-902 (P34) [HAI09], and WiMAX IEEE 802.16e technologies [EHA11]. In 2007 the spectrum for LDACS was allocated at the World Radio Conference (WRC).

It was decided to allocate the spectrum next to Distance Measuring Equipment (DME), resulting in an in-lay approach between the DME channels for LDAC [SCH14].

LDACS is currently being standardized by ICAO and several roll-out strategies are discussed:

The LDACS data link provides enhanced capabilities to existing Aeronautical communications infrastructure enabling them to better support user needs and new applications. The deployment scalability of LDACS allows its implementation to start in areas where most needed to Improve immediately the performance of already fielded infrastructure. Later the deployment is extended based on operational demand. An attractive scenario for upgrading the existing VHF communication systems by adding an additional LDACS data link is described below.

When considering the current VDL Mode 2 infrastructure and user base, a very attractive win-win situation comes about, when the technological advantages of LDACS are combined with the existing VDL mode 2 infrastructure. LDACS provides at least 50 time more capacity than VDL Mode 2 and is a natural enhancement to the existing VDL Mode 2 business model. The advantage of this approach is that the VDL Mode 2 infrastructure can be fully reused. Beyond that, it opens the way for further enhancements which can increase business efficiency and minimize investment risk. [ICAO19]

7.4. Applicability to Deterministic Flows

As LDACS is a ground-based digital communications system for flight guidance and communications related to safety and regularity of flight, time-bounded deterministic arrival times for safety critical messages are a key feature for its successful deployment and roll-out.

7.4.1. System Architecture

Up to 512 Aircraft Station (AS) communicate to an LDACS Ground Station (GS) in the Reverse Link (RL). GS communicate to AS in the Forward Link (FL). Via an Access-Router (AC-R) GSs connect the LDACS sub-network to the global Aeronautical Telecommunications Network (ATN) to which the corresponding Air Traffic Services (ATS) and Aeronautical Operational Control (AOC) end systems are attached.

7.4.2. Overview of The Radio Protocol Stack

The protocol stack of LDACS is implemented in the AS and GS: It consists of the Physical Layer (PHY) with five major functional blocks above it. Four are placed in the Data Link Layer (DLL) of the AS and GS: (1) Medium Access Layer (MAC), (2) Voice Interface (VI), (3) Data Link Service (DLS), and (4) LDACS Management Entity (LME). The last entity resides within the Sub-Network Layer: Sub-Network Protocol (SNP). The LDACS network is externally connected to voice units, radio control units, and the ATN Network Layer.

Figure 14 shows the protocol stack of LDACS as implemented in the AS and GS.

```
            IPv6                   Network Layer
              |
              |
   +------------------+  +----+
   |        SNP       |--|    |   Sub-Network
   |                  |  |    |   Layer
   +------------------+  |    |
              |          | LME|
   +------------------+  |    |
   |        DLS       |  |    |   Logical Link
   |                  |  |    |   Control Layer
   +------------------+  +----+
              |             |
             DCH         DCCH/CCCH
              |          RACH/BCCH
              |             |
   +--------------------------+
   |           MAC            |   Medium Access
   |                          |   Layer
   +--------------------------+
              |
   +--------------------------+
   |           PHY            |   Physical Layer
   +--------------------------+
              |
              |
            ((*))
            FL/RL              radio channels
                               separated by
                               Frequency Division Duplex
```

Figure 14: LDACS protocol stack in AS and GS

7.4.3. Radio (PHY)

The physical layer provides the means to transfer data over the radio channel. The LDACS ground-station supports bi-directional links to multiple aircraft under its control. The forward link direction (FL; ground-to-air) and the reverse link direction (RL; air-to-ground) are separated by frequency division duplex. Forward link and reverse link use a 500 kHz channel each. The ground-station transmits a continuous stream of OFDM symbols on the forward link. In the reverse link different aircraft are separated in time and frequency using a combination of Orthogonal Frequency-Division Multiple-Access (OFDMA) and Time-Division Multiple-Access (TDMA). Aircraft thus transmit discontinuously on the reverse link with radio bursts sent in precisely defined transmission opportunities allocated by the ground-station. The most important service on the PHY layer of LDACS is the PHY time framing service, which indicates that the PHY layer is ready to transmit in a given slot and to indicate PHY layer framing and timing to the MAC time framing service. LDACS does not support beam-forming or Multiple Input Multiple Output (MIMO).

7.4.4. Scheduling, Frame Structure and QoS (MAC)

The data-link layer provides the necessary protocols to facilitate concurrent and reliable data transfer for multiple users. The LDACS data link layer is organized in two sub-layers: The medium access sub-layer and the logical link control sub-layer. The medium access sub-layer manages the organization of transmission opportunities in slots of time and frequency. The logical link control sub-layer provides acknowledged point-to-point logical channels between the aircraft and the ground-station using an automatic repeat request protocol. LDACS supports also unacknowledged point-to-point channels and ground-to-air broadcast. Before going more into depth about the LDACS medium access, the frame structure of LDACS is introduced:

The LDACS framing structure for FL and RL is based on Super-Frames (SF) of 240 ms duration. Each SF corresponds to 2000 OFDM symbols. The FL and RL SF boundaries are aligned in time (from the view of the GS).

In the FL, an SF contains a Broadcast Frame of duration 6.72 ms (56 OFDM symbols) for the Broadcast Control Channel (BCCH), and four Multi-Frames (MF), each of duration 58.32 ms (486 OFDM symbols).

In the RL, each SF starts with a Random Access (RA) slot of length 6.72 ms with two opportunities for sending RL random access frames for the Random Access Channel (RACH), followed by four MFs. These MFs have the same fixed duration of 58.32 ms as in the FL, but a different internal structure

Figure 15 and Figure 16 illustrate the LDACS frame structure.

```
   ^
   |     +------+------------+------------+------------+------------+
   |  FL | BCCH |     MF     |     MF     |     MF     |     MF     |
   F     +------+------------+------------+------------+------------+
   r     <---------------- Super-Frame (SF) - 240ms ---------------->
   e
   q     +------+------------+------------+------------+------------+
   u  RL | RACH |     MF     |     MF     |     MF     |     MF     |
   e     +------+------------+------------+------------+------------+
   n     <---------------- Super-Frame (SF) - 240ms ---------------->
   c
   y
   |
   ----------------------------- Time ------------------------------>
   |
```

Figure 15: SF structure for LDACS

```
   ^
   |     +-------------+------+-------------+
   |  FL |     DCH     | CCCH |     DCH     |
   F     +-------------+------+-------------+
   r     <---- Multi-Frame (MF) - 58.32ms -->
   e
   q     +------+---------------------------+
   u  RL | DCCH |             DCH           |
   e     +------+---------------------------+
   n     <---- Multi-Frame (MF) - 58.32ms -->
   c
   y
   |
   -------------------- Time ------------------>
   |
```

Figure 16: MF structure for LDACS

This fixed frame structure allows for a reliable and dependable transmission of data. Next, the LDACS medium access layer is introduced:

LDACS medium access is always under the control of the ground-station of a radio cell. Any medium access for the transmission of user data has to be requested with a resource request message stating the requested amount of resources and class of service. The ground-station performs resource scheduling on the basis of these requests and grants resources with resource allocation messages. Resource request and allocation messages are exchanged over dedicated contention-free control channels.

LDACS has two mechanisms to request resources from the scheduler in the ground-station. Resources can either be requested "on demand" with a given class of service. On the forward link, this is done locally in the ground-station, on the reverse link a dedicated contention-free control channel is used (Dedicated Control Channel (DCCH); roughly 83 bit every 60 ms). A resource allocation is always announced in the control channel of the forward link (Common Control Channel (CCCH); variable sized). Due to the spacing of the reverse link control channels of every 60 ms, a medium access delay in the same order of magnitude is to be expected.

Resources can also be requested "permanently". The permanent resource request mechanism supports requesting recurring resources in given time intervals. A permanent resource request has to be canceled by the user (or by the ground-station, which is always in control). User data transmissions over LDACS are therefore always scheduled by the ground-station, while control data uses statically (i.e. at net entry) allocated recurring resources (DCCH and CCCH). The current specification documents specify no scheduling algorithm. However performance evaluations so far have used strict priority scheduling and round robin for equal priorities for simplicity. In the current prototype implementations LDACS classes of service are thus realized as priorities of medium access and not as flows. Note that this can starve out low priority flows. However, this is not seen as a big problem since safety related message always go first in any case. Scheduling of reverse link resources is done in physical Protocol Data Units (PDU) of 112 bit (or larger if more aggressive coding and modulation is used). Scheduling on the forward link is done Byte-wise since the forward link is transmitted continuously by the ground-station.

In order to support diversity, LDACS supports handovers to other ground-stations on different channels. Handovers may be initiated by the aircraft (break-before-make) or by the ground-station (make-before-break). Beyond this, FCI diversity shall be implemented by the multi-link concept.

7.5. Summary

LDACS has been designed with applications related to the safety and regularity of the flight in mind. It has therefore been designed as a deterministic wireless data link (as far as possible).

It is a secure, scalable and spectrum efficient data link with embedded navigation capability and thus, is the first truly integrated CNS system recognized by ICAO. During flight tests the LDACS capabilities have been successfully demonstrated. A viable roll-out scenario has been developed which allows gradual introduction of LDACS with immediate use and revenues. Finally, ICAO is developing LDACS standards to pave the way for a successful roll-out in the near future.

8. IANA Considerations

This specification does not require IANA action.

9. Security Considerations

Most RAW technologies integrate some authentication or encryption mechanisms that were defined outside the IETF.

10. Contributors

Georgios Z. Papadopoulos: Contributed to the TSCH section.

Nils M&#228;urer: Contributed to the LDACS section.

Thomas Gr&#228;upl: Contributed to the LDACS section.

Janos Farkas, Torsten Dudda, Alexey Shapin, and Sara Sandberg: Contr ibuted to the 5G section.

11. Acknowledgments

Many thanks to the participants of the RAW WG where a lot of the work discussed here happened.

12. Normative References

[RFC8480] Wang, Q., Ed., Vilajosana, X., and T. Watteyne, "6TiSCH Operation Sublayer (6top) Protocol (6P)", RFC 8480, DOI 10.17487/RFC8480, November 2018, <https://www.rfc-editor.org/info/rfc8480>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC5673] Pister, K., Ed., Thubert, P., Ed., Dwars, S., and T. Phinney, "Industrial Routing Requirements in Low-Power and Lossy Networks", RFC 5673, DOI 10.17487/RFC5673, October 2009, <https://www.rfc-editor.org/info/rfc5673>.

[I-D.ietf-detnet-architecture] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", Work in Progress, Internet-Draft, draft-ietf-detnet-architecture-13, 6 May 2019, <https://tools.ietf.org/html/draft-ietf-detnet-architecture-13>.

[I-D.ietf-6tisch-architecture] Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", Work in Progress, Internet-Draft, draft-ietf-6tisch-architecture-30, 26 November 2020, <https://tools.ietf.org/html/draft-ietf-6tisch-architecture-30>.

13. Informative References

[RFC6550] Winter, T., Ed., Thubert, P., Ed., Brandt, A., Hui, J., Kelsey, R., Levis, P., Pister, K., Struik, R., Vasseur, JP., and R. Alexander, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks", RFC 6550, DOI 10.17487/RFC6550, March 2012, <https://www.rfc-editor.org/info/rfc6550>.

[RFC6551] Vasseur, JP., Ed., Kim, M., Ed., Pister, K., Dejean, N., and D. Barthel, "Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks", RFC 6551, DOI 10.17487/RFC6551, March 2012, <https://www.rfc-editor.org/info/rfc6551>.

[RFC6291] Andersson, L., van Helvoort, H., Bonica, R., Romascanu, D., and S. Mansfield, "Guidelines for the Use of the "OAM" Acronym in the IETF", BCP 161, RFC 6291, DOI 10.17487/RFC6291, June 2011, <https://www.rfc-editor.org/info/rfc6291>.

[RFC7276] Mizrahi, T., Sprecher, N., Bellagamba, E., and Y. Weingarten, "An Overview of Operations, Administration, and Maintenance (OAM) Tools", RFC 7276, DOI 10.17487/RFC7276, June 2014, <https://www.rfc-editor.org/info/rfc7276>.

[RFC8279] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast Using Bit Index Explicit Replication (BIER)", RFC 8279, DOI 10.17487/RFC8279, November 2017, <https://www.rfc-editor.org/info/rfc8279>.

[I-D.ietf-6tisch-msf] Chang, T., Vucinic, M., Vilajosana, X., Duquennoy, S., and D. Dujovne, "6TiSCH Minimal Scheduling Function (MSF)", Work in Progress, Internet-Draft, draft-ietf-6tisch-msf-18, 12 September 2020, <https://tools.ietf.org/html/draft-ietf-6tisch-msf-18>.

[I-D.pthubert-raw-architecture] Thubert, P., Papadopoulos, G., and R. Buddenberg, "Reliable and Available Wireless Architecture/Framework", Work in Progress, Internet-Draft, draft-pthubert-raw-architecture-05, 15 November 2020, <https://tools.ietf.org/html/draft-pthubert-raw-architecture-05>.

[I-D.ietf-roll-nsa-extension] Koutsiamanis, R., Papadopoulos, G., Montavont, N., and P. Thubert, "Common Ancestor Objective Function and Parent Set DAG Metric Container Extension", Work in Progress, Internet-Draft, draft-ietf-roll-nsa-extension-10, 29 October 2020, <https://tools.ietf.org/html/draft-ietf-roll-nsa-extension-10>.

[I-D.papadopoulos-paw-pre-reqs] Papadopoulos, G., Koutsiamanis, R., Montavont, N., and P. Thubert, "Exploiting Packet Replication and Elimination in Complex Tracks in LLNs", Work in Progress, Internet-Draft, draft-papadopoulos-paw-pre-reqs-01, 25 March 2019, <https://tools.ietf.org/html/draft-papadopoulos-paw-pre-reqs-01>.

[I-D.thubert-bier-replication-elimination] Thubert, P., Eckert, T., Brodard, Z., and H. Jiang, "BIER-TE extensions for Packet Replication and Elimination Function (PREF) and OAM", Work in Progress, Internet-Draft, draft-thubert-bier-replication-elimination-03, 3 March 2018, <https://tools.ietf.org/html/draft-thubert-bier-replication-elimination-03>.

[I-D.thubert-6lo-bier-dispatch] Thubert, P., Brodard, Z., Jiang, H., and G. Texier, "A 6loRH for BitStrings", Work in Progress, Internet-Draft,

draft-thubert-6lo-bier-dispatch-06, 28 January 2019, <https://tools.ietf.org/html/draft-thubert-6lo-bier-dispatch-06>.

[I-D.ietf-bier-te-arch]
Eckert, T., Cauchie, G., and M. Menth, "Tree Engineering for Bit Index Explicit Replication (BIER-TE)", Work in Progress, Internet-Draft, draft-ietf-bier-te-arch-09, 30 October 2020, <https://tools.ietf.org/html/draft-ietf-bier-te-arch-09>.

[I-D.ietf-6tisch-coap]
Sudhaakar, R. and P. Zand, "6TiSCH Resource Management and Interaction using CoAP", Work in Progress, Internet-Draft, draft-ietf-6tisch-coap-03, 9 March 2015, <https://tools.ietf.org/html/draft-ietf-6tisch-coap-03>.

[I-D.svshah-tsvwg-deterministic-forwarding]
Shah, S. and P. Thubert, "Deterministic Forwarding PHB", Work in Progress, Internet-Draft, draft-svshah-tsvwg-deterministic-forwarding-04, 30 August 2015, <https://tools.ietf.org/html/draft-svshah-tsvwg-deterministic-forwarding-04>.

[IEEE Std. 802.15.4]
IEEE standard for Information Technology, "IEEE Std. 802.15.4, Part. 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks".

[IEEE Std. 802.11]
"IEEE Standard 802.11 - IEEE Standard for Information Technology - Telecommunications and information exchange between systems Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.".

[IEEE Std. 802.11ak]
"802.11ak: Enhancements for Transit Links Within Bridged Networks", 2017.

[IEEE Std. 802.11ax]
"802.11ax D4.0: Enhancements for High Efficiency WLAN".

[IEEE Std. 802.11ay]
"802.11ay: Enhanced throughput for operation in license-exempt bands above 45 GHz".

[IEEE Std. 802.11ad]
"802.11ad: Enhancements for very high throughput in the 60 GHz band".

[IEEE 802.11be WIP]
"802.11be: Extreme High Throughput".

[IEEE Std. 802.1Qat]
"802.1Qat: Stream Reservation Protocol".

[IEEE8021Qcc]
"802.1Qcc: IEEE Standard for Local and Metropolitan Area Networks--Bridges and Bridged Networks -- Amendment 31: Stream Reservation Protocol (SRP) Enhancements and Performance Improvements".

[Cavalcanti_2019]
Dave Cavalcanti et al., "Extending Time Distribution and Timeliness Capabilities over the Air to Enable Future Wireless Industrial Automation Systems, the Proceedings of IEEE", June 2019.

[Nitsche_2015]
Thomas Nitsche et al., "IEEE 802.11ad: directional 60 GHz communication for multi-Gigabit-per-second Wi-Fi", December 2014.

[Ghasempour_2017]
Yasaman Ghasempour et al., "802.11ay: Next-Generation 60 GHz Communications for 100 Gb/s Wi-Fi", December 2017.

[IEEE_doc_11-18-2009-06]
"802.11 Real-Time Applications (RTA) Topic Interest Group (TIG) Report", November 2018.

[IEEE_doc_11-19-0373-00]
Kevin Stanton et Al., "Time-Sensitive Applications Support in EHT", March 2019.

[morell13] Antoni Morell et al., "Label switching over IEEE802.15.4e networks", April 2013.

[dearmas16]
Jesica de Armas et al., "Determinism through path diversity: Why packet replication makes sense", September 2016.

[vilajosana19]
Xavier Vilajosana et al., "6TiSCH: Industrial Performance for IPv6 Internet-of-Things Networks", June 2019.

[ISA100.11a]
ISA/IEC, "ISA100.11a, Wireless Systems for Automation, also IEC 62734", 2011, <http://www.isa100wci.org/en-US/Documents/PDF/3405-ISA100-WirelessSystems-Future-broch-WEB-ETSI.aspx>.

[WirelessHART]
www.hartcomm.org, "Industrial Communication Networks - Wireless Communication Network and Communication Profiles - WirelessHART - IEC 62591", 2010.

[PCE] IETF, "Path Computation Element", <https://dataTracker.ietf.org/doc/charter-ietf-pce/>.

[CCAMP] IETF, "Common Control and Measurement Plane", <https://dataTracker.ietf.org/doc/charter-ietf-ccamp/>.

[TiSCH] IETF, "IPv6 over the TSCH mode over 802.15.4", <https://dataTracker.ietf.org/doc/charter-ietf-6tisch/>.

[RIH18] Rihacek, C., Haindl, B., Fantappie, P., Pierattelli, S., Gräupl, T., Schnell, M., and N. Fistas, "L-band Digital Aeronautical Communications System (LDACS) Activities in SESAR2020", Proceedings of the Integrated Communications Navigation and Surveillance Conference (ICNS) Herndon, VA, USA, April 2018.

[GRA19] Gräupl, T., Rihacek, C., and B. Haindl, "LDACS A/G Specification", SESAR2020 PJ14-02-01 D3.3.010, February 2019.

[SAJ14] Sajatovic, M., Günzel, H., and S. Müller, "WA04 D22 Test Report for Assessing LDACS1 Transmitter Impact upon DME/TACAN Receivers", April 2014.

[GRA11] Gräupl, T. and M. Ehammer, "L-DACS1 Data Link Layer Evolution of ATN/IPS", Proceedings of the 30th IEEE/AIAA Digital Avionics Systems Conference (DASC) Seattle, WA, USA, October 2011.

[ICAO18] International Civil Aviation Organization (ICAO), "L-Band Digital Aeronautical Communication System (LDACS)", International Standards and Recommended Practices Annex 10 - Aeronautical Telecommunications, Vol. III - Communication Systems, July 2018.

[GRA18] al., T. G. E., "L-band Digital Aeronautical Communications System (LDACS) flight trials in the national German project MICONAV", Proceedings of the Integrated Communications, Navigation, Surveillance Conference (ICNS) Herndon, VA, USA, April 2018.

[SCH19] Schnell, M., "DLR tests digital communications technologies combined with additional navigation functions for the first time", 3 March 2019, <https://www.dlr.de/dlr/en/desktopdefault.aspx/tabid-10081/151_read-32951/#/gallery/33877>.

[TR37910] "3GPP TR 37.910, Study on self evaluation towards IMT-2020 submission", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3190>.

[TR38824] "3GPP TR 38.824, Study on physical layer enhancements for NR ultra-reliable and low latency case (URLLC)", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3498>.

[TR38825] "3GPP TR 38.825, Study on NR industrial Internet of Things (IoT)", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3492>.

[TS22104] "3GPP TS 22.104, Service requirements for cyber-physical control applications in vertical domains", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3528>.

[TR22804] "3GPP TR 22.804, Study on Communication for Automation in Vertical domains (CAV)", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3187>.

[TS23501] "3GPP TS 23.501, System architecture for the 5G System (5GS)", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>.

[TS38300] "3GPP TS 38.300, NR Overall description", <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3191>.

[IMT2020] "ITU towards IMT for 2020 and beyond", <https://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[I-D.ietf-detnet-ip-over-tsn]
Varga, B., Farkas, J., Malis, A., and S. Bryant, "DetNet Data Plane: IP over IEEE 802.1 Time Sensitive Networking (TSN)", Work in Progress, Internet-Draft, draft-ietf-detnet-ip-over-tsn-05, 13 December 2020, <https://tools.ietf.org/html/draft-ietf-detnet-ip-over-tsn-05>.

[IEEE802.1TSN]
IEEE 802.1, "Time-Sensitive Networking (TSN) Task Group", <http://www.ieee802.org/1/pages/tsn.html>.

[IEEE802.1AS]
IEEE, "IEEE Standard for Local and metropolitan area networks -- Timing and Synchronization for Time-Sensitive Applications", IEEE 802.1AS-2020, <https://standards.ieee.org/content/ieee-standards/en/standard/802_1AS-2020.html>.

[IEEE802.1CB]
IEEE, "IEEE Standard for Local and metropolitan area networks -- Frame Replication and Elimination for Reliability", DOI 10.1109/IEEESTD.2017.8091139, IEEE 802.1CB-2017, <https://ieeexplore.ieee.org/document/8091139>.

[IEEE802.1Qbv]
IEEE, "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks -- Amendment 25: Enhancements for Scheduled Traffic", IEEE 802.1Qbv-2015, <https://ieeexplore.ieee.org/document/7440741>.

[IEEE802.1Qcc]
IEEE, "IEEE Standard for Local and metropolitan area networks -- Bridges and Bridged Networks -- Amendment 31:

Stream Reservation Protocol (SRP) Enhancements and Performance Improvements", IEEE 802.1Qcc-2018, <https://ieeexplore.ieee.org/document/8514112>.

[IEEE802.3]
IEEE, "IEEE Standard for Ethernet", IEEE 802.3-2018, <https://ieeexplore.ieee.org/document/8457469>.

[ETR5GTSN] Farkas, J., Varga, B., Miklos, G., and J. Sachs, "5G-TSN integration meets networking requirements for industrial automation", Ericsson Technology Review, Volume 9, No 7, August 2019, <https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-tsn-integration-for-industrial-automation>.

[MAE18] Maeurer, N. and A. Bilzhause, "A Cybersecurity Architecture for the L-band Digital Aeronautical Communications System (LDACS)", IEEE 37th Digital Avionics Systems Conference (DASC), pp. 1-10, London, UK , 2017.

[MAE191] Maeurer, N. and C. Schmitt, "Towards Successful Realization of the LDACS Cybersecurity Architecture: An Updated Datalink Security Threat- and Risk Analysis", IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-13, Herndon, VA, USA , 2019.

[ICAO19] International Civil Aviation Organization (ICAO), "TLDACS White PaperA Roll-out Scenario", Working Paper COMMUNICATIONS PANEL-DATA COMMUNICATIONS INFRASTRUCTURE WORKING GROUP, Montreal, Canada , October 2019.

[MAE192] Maeurer, N., Graeupl, T., and C. Schmitt, "Evaluation of the LDACS Cybersecurity Implementation", IEEE 38th Digital Avionics Systems Conference (DACS), pp. 1-10, San Diego, CA, USA , September 2019.

[MAE20] Maeurer, N., Graeupl, T., and C. Schmitt, "Comparing Different Diffie-Hellman Key Exchange Flavors for LDACS", IEEE 39th Digital Avionics Systems Conference (DACS), pp. 1-10, San Diego, CA, USA , October 2019.

[FIL19] Filip-Dhaubhadel, A. and D. Shutin, "LDACS- Based Non-Cooperative Surveillance Multistatic Radar Design and Detection Coverage Assessment", IEEE 38th Digital Avionics Systems Conference (DACS), pp. 1-10, San Diego, CA, USA , September 2019.

[BAT19] Battista, G., Osechas, O., Narayanan, S., Crespillo, O.G., Gerbeth, D., Maeurer, N., Mielke, D., and T. Graeupl, "Real-Time Demonstration of Integrated Communication and Navigation Services Using LDACS", IEEE Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-12, Herndon, VA, USA , 2019.

[BRA06] Brandes, S., Schnell, M., Rokitansky, C.H., Ehammer, M., Graeupl, T., Steendam, H., Guenach, M., Rihacek, C., and B. Haindl, "B-VHF -Selected Simulation Results and Final Assessment", IEEE 25th Digital Avionics Systems Conference (DACS), pp. 1-12, New York, NY, USA , September 2019.

[SCH08] Schnell, M., Brandes, S., Gligorevic, S., Rokitansky, C.H., Ehammer, M., Graeupl, T., Rihacek, C., and M. Sajatovic, "B-AMC - Broadband Aeronautical Multi-carrier Communications", IEEE 8th Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-13, New York, NY, USA , April 2008.

[HAI09] Haindl, B., Rihacek, C., Sajatovic, M., Phillips, B., Budinger, J., Schnell, M., Kamiano, D., and W. Wilson, "Improvement of L-DACS1 Design by Combining B-AMC with P34 and WiMAX Technologies", IEEE 9th Integrated Communications, Navigation and Surveillance Conference (ICNS), pp. 1-8, New York, NY, USA , May 2009.

[EHA11] Ehammer, M. and T. Graeupl, "AeroMACS - An Airport Communications System", IEEE 30th Digital Avionics Systems Conference (DACS), pp. 1-16, New York, NY, USA , September 2011.

[SCH14] Schnell, M., Epple, U., Shutin, D., and N. Schneckenburger, "LDACS: Future Aeronautical Communications for Air- Traffic Management", IEEE Communications Magazine, 52(5), 104-110 , 2017.

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
06254 MOUGINS - Sophia Antipolis
France

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Dave Cavalcanti
Intel Corporation
2111 NE 25th Ave
Hillsboro, OR, 97124
United States of America

Phone: 503 712 5566
Email: dave.cavalcanti@intel.com

Xavier Vilajosana
Universitat Oberta de Catalunya
156 Rambla Poblenou
08018 Barcelona Catalonia
Spain

Email: xvilajosana@uoc.edu

Corinna Schmitt
Research Institute CODE, UniBwM
Werner-Heisenberg-Weg 39
85577 Neubiberg
Germany

Email: corinna.schmitt@unibw.de

Janos Farkas
Ericsson
Budapest
Magyar tudosok korutja 11
1117
Hungary

Email: janos.farkas@ericsson.com

RAW
Internet-Draft
Intended status: Standards Track
Expires: August 26, 2021

G. Papadopoulos
IMT Atlantique
P. Thubert
Cisco
F. Theoleyre
CNRS
CJ. Bernardos
UC3M

February 22, 2021

RAW use cases
draft-ietf-raw-use-cases-01

Abstract

The wireless medium presents significant specific challenges to achieve properties similar to those of wired deterministic networks. At the same time, a number of use cases cannot be solved with wires and justify the extra effort of going wireless. This document presents wireless use cases demanding reliable and available behavior.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Based on time, resource reservation, and policy enforcement by distributed shapers, Deterministic Networking provides the capability to carry specified unicast or multicast data streams for real-time applications with extremely low data loss rates and bounded latency, so as to support time-sensitive and mission-critical applications on a converged enterprise infrastructure.

Deterministic Networking in the IP world is an attempt to eliminate packet loss for a committed bandwidth while ensuring a worst case end-to-end latency, regardless of the network conditions and across technologies. It can be seen as a set of new Quality of Service (QoS) guarantees of worst-case delivery. IP networks become more deterministic when the effects of statistical multiplexing (jitter and collision loss) are mostly eliminated. This requires a tight control of the physical resources to maintain the amount of traffic within the physical capabilities of the underlying technology, e.g., by the use of time-shared resources (bandwidth and buffers) per circuit, and/or by shaping and/or scheduling the packets at every hop.

Key attributes of Deterministic Networking include:

- time synchronization on all the nodes,

- centralized computation of network-wide deterministic paths,

- multi-technology path with co-channel interference minimization,

- frame preemption and guard time mechanisms to ensure a worst-case delay, and

- new traffic shapers within and at the edge to protect the network.

Wireless operates on a shared medium, and transmissions cannot be fully deterministic due to uncontrolled interferences, including self-induced multipath fading. RAW (Reliable and Available Wireless) is an effort to provide Deterministic Networking Mechanisms on across a path that include a wireless physical layer. Making Wireless Reliable and Available is even more challenging than it is with wires, due to the numerous causes of loss in transmission that add up to the congestion losses and the delays caused by overbooked shared resources.

The wireless and wired media are fundamentally different at the physical level, and while the generic Problem Statement [RFC8557] for DetNet applies to the wired as well as the wireless medium, the methods to achieve RAW necessarily differ from those used to support Time-Sensitive Networking over wires.

So far, Open Standards for Deterministic Networking have prevalently been focused on wired media, with Audio/Video Bridging (AVB) and Time Sensitive Networking (TSN) at the IEEE and DetNet [RFC8655] at the IETF. But wires cannot be used in a number of cases, including mobile or rotating devices, rehabilitated industrial buildings, wearable or in-body sensory devices, vehicle automation and multiplayer gaming.

Purpose-built wireless technologies such as [ISA100], which incorporates IPv6, were developped and deployed to cope for the lack of open standards, but they yield a high cost in OPEX and CAPEX and are limited to very few industries, e.g., process control, concert instruments or racing.

This is now changing [I-D.thubert-raw-technologies]:

- IMT-2020 has recognized Ultra-Reliable Low-Latency Communication (URLLC) as a key functionality for the upcoming 5G.

- IEEE 802.11 has identified a set of real-applications [ieee80211-rt-tig] which may use the IEEE802.11 standards. They typically emphasize strict end-to-end delay requirements.

- The IETF has produced an IPv6 stack for IEEE Std. 802.15.4 TimeSlotted Channel Hopping (TSCH) and an architecture [I-D.ietf-6tisch-architecture] that enables Reliable and Available Wireless (RAW) on a shared MAC.

This draft extends the "Deterministic Networking Use Cases" document [RFC8578] and describes a number of additional use cases which require "reliable/predictable and available" flows over wireless links and possibly complex multi-hop paths called Tracks. This is covered mainly by the "Wireless for Industrial Applications" use case, as the "Cellular Radio" is mostly dedicated to the (wired) transport part of a Radio Access Network (RAN). Whereas the "Wireless for Industrial Applications" use case certainly covers an area of interest for RAW, it is limited to 6TiSCH, and thus its scope is narrower than the use cases described next in this document.

2. Aeronautical Communications

Aircraft are currently connected to ATC (Air-Traffic Control) and AOC (Airline Operational Control) via voice and data communications systems through all phases of a flight. Within the airport terminal, connectivity is focused on high bandwidth communications while during en-route high reliability, robustness and range is the main focus.

2.1. Problem Statement

Up to 2020 civil air traffic has been growing constantly at a compound rate of 5.8% per year [ACI19] and despite the severe impact of the COVID-19 pandemic, air traffic growth is expected to resume very quickly in post-pandemic times [IAT20] [IAC20]. Thus, legacy systems in air traffic management (ATM) are likely to reach their capacity limits and the need for new aeronautical communication technologies becomes apparent. Especially problematic is the saturation of VHF band in high density areas in Europe, the US, and Asia [KEAV20] [FAA20] calling for suitable new digital approaches such as AeroMACS for airport communications, SatCOM for remote domains, and LDACS as long-range terrestrial aeronautical communications system. Making the frequency spectrum’s usage more efficient a transition from analogue voice to digital data communication [PLA14] is necessary to cope with the expected growth of civil aviation and its supporting infrastructure. A promising candidate for long range terrestrial communications, already in the process of being standardized in the International Civil Aviation Organization (ICAO), is the L-band Digital Aeronautical Communications System (LDACS) [ICAO18] [I-D.ietf-raw-ldacs].

2.2. Specifics

During the creation process of new communications system, analogue voice is replaced by digital data communication. This sets a paradigm shift from analogue to digital wireless communications and supports the related trend towards increased autonomous data processing that the Future Communications Infrastructure (FCI) in civil aviation must provide. The FCI is depicted in Figure 1:

```
    Satellite
   #         #
   #          # #
   #            #   #
   #             #      #
   #               #        #
   #                #          #
   #                  #            #
   # Satellite-based   #              #
   #   Communications   #                 #
   #      SatCOM (#)     #                   #
   #                      #                    Aircraft
   #                       #                 %         %
   #                        #              %             %
   #                         #           %     Air-Air     %
   #                          #        %     Communications   %
   #                           #     %         LDACS A/A (%)    %
   #                           #   %                              %
   #                            Aircraft  % % % % % % % % % %  Aircraft
   #                                 |           Air-Ground           |
   #                                 |         Communications         |
   #                                 |           LDACS A/G (|)        |
   #      Communications in          |                                |
   #    and around airports          |                                |
   #         AeroMACS (-)            |                                |
   #                                 |                                |
   #         Aircraft-------------+  |                                |
   #                              |  |                                |
   #                              |  |                                |
   #         Ground network       |  |         Ground network         |
   SatCOM <---------------------> Airport <----------------------> LDACS
   transceiver                     based                             GS
   transceiver
```

Figure 1: The Future Communication Infrastructure (FCI): AeroMACS for APT/TMA domain, LDACS A/G for TMA/ENR domain, LDACS A/G for ENR/ORP domain, SatCOM for ORP domain communications

2.3. Challenges

This paradigm change brings a lot of new challenges:

- Efficiency: It is necessary to keep latency, time and data overhead (routing, security) of new aeronautical datalinks at a minimum.

- Modularity: Systems in avionics usually operate up to 30 years, thus solutions must be modular, easily adaptable and updatable.

- Interoperability: All 192 members of the international Civil Aviation Organization (ICAO) must be able to use these solutions.

2.4. The Need for Wireless

In a high mobility environment such as aviation, the envisioned solutions to provide worldwide coverage of data connections with in-flight aircraft require a multi-system, multi-link, multi-hop approach. Thus air, ground and space-based datalink providing technologies will have to operate seamlessly together to cope with the increasing needs of data exchange between aircraft, air traffic controller, airport infrastructure, airlines, air network service providers (ANSPs) and so forth. Thus, making use of wireless technologies is a MUST in tackling this enormous need for a worldwide digital aeronautical datalink infrastructure.

2.5. Requirements for RAW

Different safety levels need to be supported, from extremely safety critical ones requiring low latency, such as a WAKE warning - a warning that two aircraft come dangerously close to each other - and high resiliency, to less safety critical ones requiring low-medium latency for services such as WXGRAPH - graphical weather data.

Overhead needs to be kept at a minimum since aeronautical data links provide comparatively small data rates in the order of kbit/s.

Policy needs to be supported when selecting data links. The focus of RAW here should be on the selectors, responsible for the routing path a packet takes to reach its end destination. This would minimize the amount of routing information that has to travel inside the network because of precomputed routing tables with the selector being responsible for choosing the most appropriate option according to policy and safety.

3. Amusement Parks

3.1. Use Case Description

The digitalization of Amusement Parks is expected to decrease significantly the cost for maintaining the attractions. Such deployment is a mix between industrial automation (aka. Smart Factories) and multimedia entertainment applications.

Attractions may rely on a large set of sensors and actuators, which react in real time. Typical applications comprise:

- Emergency: safety has to be preserved, and must stop the attraction when a failure is detected.

- Video: augmented and virtual realities are integrated in the attraction. Wearable mobile devices (e.g., glasses, virtual reality headset) need to offload one part of the processing tasks.

- Real-time interactions: visitors may interact with an attraction, like in a real-time video game. The visitors may virtually interact with their environment, triggering actions in the real world (through actuators) [robots].

- Geolocation: visitors are tracked with a personal wireless tag so that their user experience is improved.

- Predictive maintenance: statistics are collected to predict the future failures, or to compute later more complex statistics about the attraction’s usage, the downtime, its popularity, etc.

3.2. Specifics

Amusement parks comprise a variable number of attractions, mostly outdoor, over a large geographical area. The IT infrastructure is typically multi-scale:

- Local area: the sensors and actuators controlling the attractions are co-located. Control loops trigger only local traffic, with a small end-to-end delay, typically inferior than 10 milliseconds, like classical industrial systems [ieee80211-rt-tig].

- Wearable mobile devices are free to move in the park. They exchange traffic locally (identification, personalization, multimedia) or globally (billing, child tracking).

- Computationally intensive applications offload some tasks. Edge computing seems an efficient way to implement real-time applications with offloading. Some non time-critical tasks may rather use the cloud (predictive maintenance, marketing).

3.3. The Need for Wireless

Amusement parks cover large areas and a global interconnection would require a huge length of cables. Wireless also increases the reconfigurability, enabling to update cheaply the attractions. The frequent renewal helps to increase customer loyalty.

Some parts of the attraction are mobile, e.g., trucks of a roller-coaster, robots. Since cables are prone to frequent failures in this situation, wireless transmissions are recommended.

Wearable devices are extensively used for a user experience personalization. They typically need to support wireless transmissions. Personal tags may help to reduce the operating costs [disney-VIP] and to increase the number of charged services provided to the audience (VIP tickets, interactivity, etc.) Some applications rely on more sophisticated wearable devices such as digital glasses or Virtual Reality (VR) headsets for an immersive experience.

3.4. Requirements for RAW

The network infrastructure has to support heterogeneous traffic, with very different critical requirements. Thus, flow isolation has to be provided.

We have to schedule appropriately the transmissions, even in presence of mobile devices. While the [I-D.ietf-6tisch-architecture] already proposes an architecture for synchronized, IEEE Std. 802.15.4 Time-Slotted Channel Hopping (TSCH) networks, we still need multi-technology solutions, able to guarantee end-to-end requirements across heterogeneous technologies, with strict SLA requirements.

Nowadays, long-range wireless transmissions are used mostly for best-effort traffic. On the contrary, [IEEE802.1TSN] is used for critical flows using Ethernet devices. However, we need an IP enabled technology to interconnect large areas, independent of the PHY and MAC layers.

We expect to deploy several different technologies (long vs. short range) which have to cohabit in the same area. Thus, we need to provide layer-3 mechanisms able to exploit multiple co-interfering technologies.

4. Wireless for Industrial Applications

4.1. Use Case Description

A major use case for networking in Industrial environments is the control networks where periodic control loops operate between a sensor that measures a physical property such as the temperature of a fluid, a Programmable Logic Controller (PLC) that decides an action such as warm up the mix, and an actuator that performs the required action, e.g., inject power in a resistor.

4.2. Specifics

4.2.1. Control Loops

Process Control designates continuous processing operations, e.g., heating Oil in a refinery or mixing drinking soda. Control loops in the Process Control industry operate at a very low rate, typically 4 times per second. Factory Automation, on the other hand, deal with discrete goods such as individual automobile parts, and requires faster loops, in the order of 10ms. Motion control that monitors dynamic activities may require even faster rates in the order of a few ms. Finally, some industries exhibit hybrid behaviors, like canned soup that will start as a process industry while mixing the food and then operate as a discrete manufacturing when putting the final product in cans and shipping them.

In all those cases, a packet must flow reliably between the sensor and the PLC, be processed by the PLC, and sent to the actuator within the control loop period. In some particular use cases that inherit from analog operations, jitter might also alter the operation of the control loop. A rare packet loss is usually admissible, but typically 4 losses in a row will cause an emergency halt of the production and incur a high cost for the manufacturer.

4.2.2. Unmeasured Data

A secondary use case deals with monitoring and diagnostics. This so-called unmeasured data is essential to improve the performances of a production line, e.g., by optimizing real-time processing or maintenance windows using Machine Learning predictions. For the lack of wireless technologies, some specific industries such as Oil and Gas have been using serial cables, literally by the millions, to perform their process optimization over the previous decades. But few industries would afford the associated cost and the Holy Grail of the Industrial Internet of Things is to provide the same benefits to all industries, including SmartGrid, Transportation, Building, Commercial and Medical. This requires a cheap, available and scalable IP-based access technology.

Inside the factory, wires may already be available to operate the Control Network. But unmeasured data are not welcome in that network for a number of reasons. On the one hand it is rich and asynchronous, meaning that using they may influence the deterministic nature of the control operations and impact the production. On the other hand, this information must be reported to the carpeted floor over IP, which means the potential for a security breach via the interconnection of the Operational Technology (OT) network with the Internet technology (IT) network and possibly enable a rogue access.

4.3. The Need for Wireless

Ethernet cables used on a robot arm are prone to breakage after a few thousands flexions, a lot faster than a power cable that is wider inn diameter, and more resilient. In general, wired networking and mobile parts are not a good match, mostly in the case of fast and recurrent activities, as well as rotation.

When refurbishing older premises that were built before the Internet age, power is usually available everywhere, but data is not. It is often impractical, time consuming and expensive to deploy an Ethernet fabric across walls and between buildings. Deploying a wire may take months and cost tens of thousands of US Dollars.

Even when wiring exists, e.g., in an existing control network, asynchronous IP packets such as diagnostics may not be welcome for operational and security reasons (see Section 4.2.1). An alternate network that can scale with the many sensors and actuators that equip every robot, every valve and fan that are deployed on the factory floor and may help detect and prevent a failure that could impact the production. IEEE Std. 802.15.4 Time-Slotted Channel Hopping (TSCH) [RFC7554] is a promising technology for that purpose, mostly if the scheduled operations enable to use the same network by asynchronous and deterministic flows in parallel.

4.4. Requirements for RAW

As stated by the "Deterministic Networking Problem Statement" [RFC8557], a Deterministic Network is backwards compatible with (capable of transporting) statistically multiplexed traffic while preserving the properties of the accepted deterministic flows. While the [I-D.ietf-6tisch-architecture] serves that requirement, the work at 6TiSCH was focused on best-effort IPv6 packet flows. RAW should be able to lock so-called hard cells for use by a centralized scheduler, and program so-called end-to-end Tracks over those cells.

Over the course of the recent years, major Industrial Protocols, e.g., [ODVA] with EtherNet/IP [EIP] and [Profinet], have been migrating towards Ethernet and IP. In order to unleash the full power of the IP hourglass model, it should be possible to deploy any application over any network that has the physical capacity to transport the industrial flow, regardless of the MAC/PHY technology, wired or wireless, and across technologies. RAW mechanisms should be able to setup a Track over a wireless access segment such as TSCH and a backbone segment such as Ethernet or WI-Fi, to report a sensor data or a critical monitoring within a bounded latency. It is also important to ensure that RAW solutions are interoperable with existing wireless solutions in place, and with legacy equipment which capabilities can be extended using retrofitting. Maintanability, as a broader concept than reliability is also important in industrial scenarios [square-peg].

5. Pro Audio and Video

5.1. Use Case Description

Many devices support audio and video streaming by employing 802.11 wireless LAN. Some of these applications require low latency capability. For instance, when the application provides interactive play, or when the audio takes plays in real time (i.e. live) for public addresses in train stations or in theme parks.

The professional audio and video industry ("ProAV") includes:

- Virtual Reality / Augmented Reality (VR/AR)

- Public address, media and emergency systems at large venues (airports, train stations, stadiums, theme parks).

5.2. Specifics

5.2.1. Uninterrupted Stream Playback

Considering the uninterrupted audio or video stream, a potential packet losses during the transmission of audio or video flows cannot be tackled by re-trying the transmission, as it is done with file transfer, because by the time the packet lost has been identified it is too late to proceed with packet re-transmission. Buffering might be employed to provide a certain delay which will allow for one or more re-transmissions, however such approach is not efficient in application where delays are not acceptable.

5.2.2. Synchronized Stream Playback

In the context of ProAV, latency is the time between the transmitted signal over a stream and its reception. Thus, for sound to remain synchronized to the movement in the video, the latency of both the audio and video streams must be bounded and consistent.

5.3. The Need for Wireless

The devices need the wireless communication to support video streaming via 802.11 wireless LAN for instance.

During the public address, the deployed announcement speakers, for instance along the platforms of the train stations, need the wireless communication to forward the audio traffic in real time.

5.4. Requirements for RAW

The network infrastructure needs to support heterogeneous types of traffic (including QoS).

Content delivery with bounded (lowest possible) latency.

The deployed network topology should allow for multipath. This will enable for multiple streams to have different (and multiple) paths through the network to support redundancy.

6. Wireless Gaming

6.1. Use Case Description

The gaming industry includes [IEEE80211RTA] real-time mobile gaming, wireless console gaming and cloud gaming. For RAW, wireless console gaming is the most relevant one. We next summarize the three:

- Real-time Mobile Gaming: Different from traditional games, real time mobile gaming is very sensitive to network latency and stability. The mobile game can connect multiple players together in a single game session and exchange data messages between game server and connected players. Real-time means the feedback should present on screen as users operate in game. For good game experience, the end to end latency plus game servers processing time should not be noticed by users as they play the game.

- Wireless Console Gaming: Playing online on a console has 2 types of internet connectivity, which is either wired or Wi-Fi. Most of the gaming consoles today support Wi-Fi 5. But Wi-Fi has an especially bad reputation among the gaming community. The main reasons are high latency, lag spikes and jitter.

- Cloud Gaming: The cloud gaming requires low latency capability as the user commands in a game session need to be sent back to the cloud server, the cloud server would update game context depending on the received commands, and the cloud server would render the picture/video to be displayed at user devices and stream the picture/video content to the user devices. User devices might very likely be connected wirelessly.

6.2. Specifics

While a lot of details can be found on [IEEE80211RTA], we next summarize the main requirements in terms of latency, jitter and packet loss:

- Intra BSS latency: less than 5 ms.

- Jitter variance: less than 2 ms.

- Packet loss: less than 0.1 percent.

6.3. The Need for Wireless

It is clear that gaming is evolving towards wireless, as players demand being able to play anywhere. Besides, the industry is changing towards playing from mobile phones, which are inherently connected via wireless technologies.

6.4. Requirements for RAW

- Time sensitive networking extensions. Extensions, such as time-aware shaping and redundancy (FRE) can be explored to address congestion and reliability problems present in wireless networks.

- Priority tagging (Stream identification). One basic requirement to provide better QoS for time-sensitive traffic is the capability to identify and differentiate time-sensitive packets from other (e.g. best-effort) traffic.

- Time-aware shaping. This capability (defined in IEEE 802.1Qbv) consists of gates to control the opening/closing of queues that share a common egress port within an Ethernet switch. A scheduler defines the times when each queue opens or close, therefore eliminating congestion and ensuring that frames are delivered within the expected latency bounds.

- Dual/multiple link. Due to the competitions and interference are common and hardly in control under wireless network, in order to improve the latency stability, dual/multiple link proposal is brought up to address this issue. Two modes are defined: duplicate and joint.

- Admission Control. Congestion is a major cause of high/variable latency and it is well known that if the traffic load exceeds the capability of the link, QoS will be degraded. QoS degradation maybe acceptable for many applications today, however emerging time-sensitive applications are highly susceptible to increased latency and jitter. In order to better control QoS, it is important to control access to the network resources.

7. UAV platooning and control

7.1. Use Case Description

Unmanned Aerial Vehicles (UAVs) are becoming very popular for many different applications, including military and civil use cases. The term drone is commonly used to refer to a UAV.

UAVs can be used to perform aerial surveillance activities, traffic monitoring (e.g., Spanish traffic control has recently introduced a fleet of drones for quicker reactions upon traffic congestion related events), support of emergency situations, and even transportation of small goods.

UAVs typically have various forms of wireless connectivity:

- cellular: for communication with the control center, for remote maneuvering as well as monitoring of the drone;

- IEEE 802.11: for inter-drone communications (e.g., platooning) and providing connectivity to other devices (e.g., acting as Access Point).

7.2. Specifics

Some of the use cases/tasks involving drones require coordination among drones. Others involve complex compute tasks that might not be performed using the limited computing resources that a drone typically has. These two aspects require continuous connectivity with the control center and among drones.

Remote maneuvering of a drone might be performed over a cellular network in some cased, however, there are situations that need very low latencies and deterministic behavior of the connectivity. Examples involve platooning of drones or share of computing resources among drones (e.g., a drone offload some function to a neighboring drone).

7.3. The Need for Wireless

UAVs cannot be connected through any type of wired media, so it is obvious that wireless is needed.

7.4. Requirements for RAW

The network infrastructure is actually composed by the UAVs themselves, requiring self-configuration capabilities.

Heterogeneous types of traffic need to be supported, from extremely critical ones requiring ultra low latency and high resiliency, to traffic requiring low-medium latency.

When a given service is decomposed into functions -- hosted at different drones -- chained, each link connecting two given functions would have a well-defined set of requirements (latency, bandwidth and jitter) that have to be met.

8. Edge Robotics control

8.1. Use Case Description

The Edge Robotics scenario consists of several robots, deployed in a given area (for example a shopping mall), inter-connected via an access network to a network's edge device or a data center. The robots are connected to the edge so complex computational activities are not executed locally at the robots, but offloaded to the edge. This brings additional flexibility in the type of tasks that the robots do, as well as reducing the costs of robot manufacturing (due to their lower complexity), and enabling complex tasks involving coordination among robots (that can be more easily performed if robots are centrally controlled).

A simple example of the use of multiples robots is cleaning, delivering of goods from warehouses to shops or video surveillance. Multiple robots are simultaneously instructed to perform individual tasks by moving the robotic intelligence from the robots to the network's edge (e.g., data center). That enables easy synchronization, scalable solution and on-demand option to create flexible fleet of robots.

Robots would have various forms of wireless connectivity:

- IEEE 802.11: for connection to the edge and also inter-robot communications (e.g., for coordinated actions).

- Cellular: as an additional communication link to the edge, though primarily as backup, since ultra low latencies are needed.

8.2. Specifics

Some of the use cases/tasks involving robots might benefit from decomposition of a service in small functions that are distributed and chained among robots and the edge. These require continuous connectivity with the control center and among drones.

Robot control is an activity requiring very low latencies between the robot and the location where the control intelligence resides (which might be the edge or another robot).

8.3. The Need for Wireless

Deploying robots in scenarios such as shopping malls for the aforementioned applications cannot be done via wired connectivity.

8.4. Requirements for RAW

The network infrastructure needs to support heterogeneous types of traffic, from robot control to video streaming.

When a given service is decomposed into functions -- hosted at different robots -- chained, each link connecting two given functions would have a well-defined set of requirements (latency, bandwidth and jitter) that have to be met.

9. Emergencies: Instrumented emergency vehicle

9.1. Use Case Description

An instrumented ambulance would be one that has a LAN to which are connected these end systems:

- vital signs sensors attached to the casualty in the ambulance. Relay medical data to hospital emergency room,

- radionavigation sensor to relay position data to various destinations including dispatcher,

- voice communication for ambulance attendant (e.g. consult with ER doctor),

- voice communication between driver and dispatcher,

- etc.

The LAN needs to be routed through radio-WANs to complete the internetwork linkage.

9.2. Specifics

What we have today is multiple communications systems to reach the vehicle:

- A dispatching system,
- a cellphone for the attendant,
- a special purpose telemetering system for medical data,
- etc.

This redundancy of systems, because of its stovepiping, does not contribute to availability as a whole.

Most of the scenarios involving the use of an instrumented ambulance are composed of many different flows, each of them with slightly different requirements in terms of reliability and latency. Destinations might be either at the ambulance itself (local traffic), at a near edge cloud or at the general Internet/cloud.

9.3. The Need for Wireless

Local traffic between the first responders/ambulance staff and the ambulance equipment cannot be doine via wireled connectivity as the responders perform initial treatment outside of the ambulance. The communications from the ambulance to external services has to be wireless as well.

9.4. Requirements for RAW

We can derive some pertinent requirements from this scenario:

- High availability of the internetwork is required.
- The internetwork needs to operate in damaged state (e.g. during an earthquake aftermath, heavy weather, wildfire, etc.). In addition to continuity of operations, rapid restoral is a needed characteristic.
- End-to-end security, both authenticity and confidentiality, is required of traffic. All data needs to be authenticated; some (such as medical) needs to be confidential.
- The radio-WAN has characteristics similar to cellphone -- the vehicle will travel from one radio footprint to another.

10. IANA Considerations

This document has no IANA actions.

11. Security Considerations

This document covers a number of representative applications and network scenarios that are expected to make use of RAW technologies. Each of the potential RAW use cases will have security considerations from both the use-specific perspective and the RAW technology perspective. [I-D.ietf-detnet-security] provides a comprehensive discussion of security considerations in the context of Deterministic Networking, which are generally applicable also to RAW.

12. Acknowledgments

Nils Maeurer, Thomas Graeupl and Corinna Schmitt have contributed significantly to this document, providing input for the Aeronautical communications section. Rex Buddenberg has also contributed to the document, providing input to the Emergency: instrumented emergency vehicle section.

The authors would like to thank Toerless Eckert, Xavi Vilajosana Guillen and Rute Sofia for their valuable comments on previous versions of this document.

The work of Carlos J. Bernardos in this draft has been partially supported by the H2020 5Growth (Grant 856709) and 5G-DIVE projects (Grant 859881).

13. Informative References

[ACI19] Airports Council International (ACI), "Annual World Aitport Traffic Report 2019", November 2019, <https://store.aci.aero/product/annual-world-airport-traffic-report-2019/>.

[disney-VIP] Wired, "Disney's $1 Billion Bet on a Magical Wristband", March 2015, <https://www.wired.com/2015/03/disney-magicband/>.

[EIP] http://www.odva.org/, "EtherNet/IP provides users with the network tools to deploy standard Ethernet technology (IEEE 802.3 combined with the TCP/IP Suite) for industrial automation applications while enabling Internet and enterprise connectivity data anytime, anywhere.", <http://www.odva.org/Portals/0/Library/Publications_Numbered/PUB00138R3_CIP_Adv_Tech_Series_EtherNetIP.pdf>.

[FAA20] U.S. Department of Transportation Federal Aviation Administration (FAA), "Next Generation Air Transportation System", 2019, <https://www.faa.gov/nextgen/ >.

[I-D.ietf-6tisch-architecture]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", draft-ietf-6tisch-architecture-30 (work in progress), November 2020.

[I-D.ietf-detnet-security]
Grossman, E., Mizrahi, T., and A. Hacker, "Deterministic Networking (DetNet) Security Considerations", draft-ietf-detnet-security-13 (work in progress), December 2020.

[I-D.ietf-raw-ldacs]
Maeurer, N., Graeupl, T., and C. Schmitt, "L-band Digital Aeronautical Communications System (LDACS)", draft-ietf-raw-ldacs-06 (work in progress), January 2021.

[I-D.thubert-raw-technologies]
Thubert, P., Cavalcanti, D., Vilajosana, X., Schmitt, C., and J. Farkas, "Reliable and Available Wireless Technologies", draft-thubert-raw-technologies-05 (work in progress), May 2020.

[IAC20] Iacus, S., Natale, F., Santamaria, C., Spyratos, S., and V. Michele, "Estimating and projecting air passenger traffic during the COVID-19 coronavirus outbreak and its socio- economic impact", Safety Science 129 (2020) 104791 , 2020.

[IAT20] International Air Transport Association (IATA), "Economic Performance of the Airline Industry", November 2020, <https://www.iata.org/en/iata-repository/publications/economic-reports/airline-industry-economic-performance---november-2020---report/>.

[ICAO18] International Civil Aviation Organization (ICAO), "L-Band Digital Aeronautical Communication System (LDACS)", International Standards and Recommended Practices Annex 10 - Aeronautical Telecommunications, Vol. III - Communication Systems , 2018.

[IEEE802.1TSN] IEEE standard for Information Technology, "IEEE 802.1AS-2011 - IEEE Standard for Local and Metropolitan Area Networks - Timing and Synchronization for Time-Sensitive Applications in Bridged Local Area Networks".

[ieee80211-rt-tig] IEEE, "IEEE 802.11 Real Time Applications TIG Report", Nov. 2018, <http://www.ieee802.org/11/Reports/rtatig_update.htm>.

[IEEE80211RTA] IEEE standard for Information Technology, "IEEE 802.11 Real Time Applications TIG Report", Nov 2018.

[ISA100] ISA/ANSI, "ISA100, Wireless Systems for Automation", <https://www.isa.org/isa100/>.

[KEAV20] T. Keaveney and C. Stewart, "Single European Sky ATM Research Joint Undertaking", 2019, <https://www.sesarju.eu/>.

[ODVA] http://www.odva.org/, "The organization that supports network technologies built on the Common Industrial Protocol (CIP) including EtherNet/IP.".

[PLA14] Plass, S., Hermenier, R., Luecke, O., Gomez Depoorter, D., Tordjman, T., Chatterton, M., Amirfeiz, M., Scotti, S., Cheng, Y., Pillai, P., Graeupl, T., Durand, F., Murphy, K., Marriott, A., and A. Zaytsev, "Flight Trial Demonstration of Seamless Aeronautical Networking", IEEE Communications Magazine, vol. 52, no. 5 , May 2014.

[Profinet] http://us.profinet.com/technology/profinet/, "PROFINET is a standard for industrial networking in automation.", <http://us.profinet.com/technology/profinet/>.

[RFC7554] Watteyne, T., Ed., Palattella, M., and L. Grieco, "Using IEEE 802.15.4e Time-Slotted Channel Hopping (TSCH) in the Internet of Things (IoT): Problem Statement", RFC 7554, DOI 10.17487/RFC7554, May 2015, <https://www.rfc-editor.org/info/rfc7554>.

[RFC8557] Finn, N. and P. Thubert, "Deterministic Networking Problem Statement", RFC 8557, DOI 10.17487/RFC8557, May 2019, <https://www.rfc-editor.org/info/rfc8557>.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

[robots] Kober, J., Glisson, M., and M. Mistry, "Playing catch and juggling with a humanoid robot.", 2012, <https://doi.org/10.1109/HUMANOIDS.2012.6651623>.

[square-peg] Martinez, B., Cano, C., and X. Vilajosana, "A Square Peg in a Round Hole: The Complex Path for Wireless in the Manufacturing Industry", 2019, <https://ieeexplore.ieee.org/document/8703476>.

Authors' Addresses

Georgios Z. Papadopoulos
IMT Atlantique
Office B00 - 114A
2 Rue de la Chataigneraie
Cesson-Sevigne - Rennes 35510
FRANCE

Phone: +33 299 12 70 04
Email: georgios.papadopoulos@imt-atlantique.fr

Pascal Thubert
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
MOUGINS - Sophia Antipolis 06254
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Fabrice Theoleyre
CNRS
ICube Lab, Pole API
300 boulevard Sebastien Brant - CS 10413
Illkirch 67400
FRANCE

Phone: +33 368 85 45 33
Email: theoleyre@unistra.fr
URI: http://www.theoleyre.eu

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

RAW P. Thubert, Ed.
Internet-Draft Cisco Systems
Intended status: Informational G.Z. Papadopoulos
Expires: 19 May 2021 IMT Atlantique
R. Buddenberg
15 November 2020

Reliable and Available Wireless Architecture/Framework
draft-pthubert-raw-architecture-05

Abstract

Due to uncontrolled interferences, including the self-induced multipath fading, deterministic networking can only be approached on wireless links. The radio conditions may change -way- faster than a centralized routing can adapt and reprogram, in particular when the controller is distant and connectivity is slow and limited. RAW separates the routing time scale at which a complex path is recomputed from the forwarding time scale at which the forwarding decision is taken for an individual packet. RAW operates at the forwarding time scale. The RAW problem is to decide, within the redundant solutions that are proposed by the routing, which will be used for each individual packet to provide a DetNet service while minimizing the waste of resources.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Bringing determinism in a packet network means eliminating the statistical effects of multiplexing that result in probabilistic jitter and loss. This can be approached with a tight control of the physical resources to maintain the amount of traffic within a budgetted volume of data per unit of time that fits the physical capabilities of the underlying technology, and the use of time-shared resources (bandwidth and buffers) per circuit, and/or by shaping and/or scheduling the packets at every hop.

Wireless networks operate on a shared medium where uncontrolled interference, including the self-induced multipath fading, cause random transmission losses and add new dimensions to the statistical effects that affect the delivery. Scheduling can alleviate those effects by enabling diverse transmissions in the spatial, time, code, and frequency domains. Reliable and Available Wireless (RAW) leverages scheduling and all possible forms of diversity to defeat the possible causes of transmission loss while preserving energy and optimizing the use of the shared spectrum.

Deterministic Networking is an attempt to emulate the properties of a serial link over a switched fabric, by providing a bounded latency and eliminating congestion loss, even when co-existing with best-effort traffic. This innovation was introduced on wired networks with IEEE 802.1 TSN (for Ethernet LANs) and IETF DetNet. It is getting traction in various industries including professional A/V, manufacturing, online gaming, and smartgrid automation, enabling cost and performance optimizations (e.g., vs. loads of P2P cables).

The wireless and wired media are fundamentally different at the physical level, and while the generic "Deterministic Networking Problem Statement" [RFC8557] applies to both the wired and the wireless media, the methods to achieve RAW must extend those used to support time-sensitive networking over wires, as a RAW solution has to address less consistent transmissions, energy conservation and shared spectrum efficiency.

Uncontrolled interference and transmission obstacles may impede the wireless transmission, causing rapid variations of the throughput and packet delivery ratio (PDR) of the link. This uncertainty limits the volume and/or duration of traffic that can be safely transmitted on the same link while conforming to a RAW Service Level Agreement (SLA). Techniques such as beamforming with Multi-User MIMO can only alleviate some of those issues, and the term deterministic is usually not associated with a short range radio link, in particular one operated in the ISM band.

This increased complexity explains why the development of deterministic wireless technologies has been lagging behind the similar efforts for wired systems, both at the IEEE and the IETF. But recent progress on scheduled radios such as TSCH and OFDMA indicates that wireless is finally catching up at the lower layers. Sitting at the layer above, RAW takes up the challenge of providing highly available and reliable end-to-end performances in a network with scheduled wireless segments.

RAW provides DetNet elements that are specialized for short range radios. From this inheritance, RAW stays agnostic to the radio layer underneath though the capability to schedule transmissions is assumed. How the PHY is programmed to do so, and whether the radio is single-hop or meshed, are unknown at the IP layer and not part of the RAW abstraction.

The "Deterministic Networking Architecture" [RFC8655] is composed of three planes: the Application (User) Plane, the Controller Plane, and the Network Plane. The RAW Architecture extends the DetNet Network Plane, to accomodate one or multiple hops of homogeneous or heterogeneous wireless technologies, e.g. a Wi-Fi6 Mesh or parallel CBRS access links federated by a 5G backhaul.

The establishment of a path is not in-scope for RAW. It may be the product of a centralized Controller Plane as described for DetNet. As opposed to wired networks, the action of installing a path over a set of wireless links may be very slow relative to the speed at which the radio conditions vary, and it makes sense in the wireless case to provide redundant forwarding solutions along a complex path and to leave it to the Network Plane to select which of those forwarding solutions are to be used for a given packet based on the current conditions.

RAW distinguishes the longer time scale at which routes are computed from the the shorter forwarding time scale where per-packet decisions are made. RAW operates within the Network Plane at the forwarding time scale on one DetNet flow over a complex path called a Track. The Track is preestablished and installed by means outside of the scope of RAW; it may be strict or loose depending on whether each or just a subset of the hops are observed and controlled by RAW.

The RAW Architecture covers Network Plane protocol elements such as Operations, Administration and Maintenance (OAM) to observe some or all hops along a Track as well as the end-to-end packet delivery, and in-band control to optimize the use of redundancy to achieve the required SLA with minimal use of constrained resources.

2. The RAW problem

2.1. Terminology

RAW reuses terminology defined for DetNet in the "Deterministic Networking Architecture" [RFC8655], e.g., PREOF for Packet Replication, Elimination and Ordering Functions.

RAW also reuses terminology defined for 6TiSCH in [6TiSCH-ARCHI] such as the term Track. A Track as a complex path with associated PAREO operations. The concept is abstract to the underlaying technology and applies to any fully or partially wireless mesh, including, e.g., a Wi-Fi mesh. RAW specifies strict and loose Tracks depending on whether the path is fully controlled by RAW or traverses an opaque network where RAW cannot observe and control the individual hops.

RAW uses the term OAM as defined in [RFC6291].

RAW defines the following terms:

PAREO: Packet (hybrid) ARQ, Replication, Elimination and Ordering. PAREO is a superset Of DetNet's PREOF that includes radio-specific techniques such as short range broadcast, MUMIMO, constructive interference and overhearing, which can be leveraged separately or combined to increase the reliability.

Flapping: In the context of RAW, a link flaps when the reliability of the wireless connectivity drops abruptly for a short period of time, typically of a subsecond to seconds duration.

In the context of the RAW work, Reliability and Availability are defined as follows:

Reliability: Reliability is a measure of the probability that an item will perform its intended function for a specified interval under stated conditions. For RAW, the service that is expected is delivery within a bounded latency and a failure is when the packet is either lost or delivered too late. RAW expresses reliability in terms of Mean Time Between Failure (MTBF) and Maximum Consecutive Failures (MCF). More in [NASA].

Availability: Availability is a measure of the relative amount of time where a path operates in stated condition, in other words (uptime)/(uptime+downtime). Because a serial wireless path may not be good enough to provide the required availability, and even 2 parallel paths may not be over a longer period of time, the RAW availability implies a path that is a lot more complex than what DetNet typically envisages (a Track).

2.2. Reliability and Availability

2.2.1. High Availability Engineering Principles

The reliability criteria of a critical system pervade through its elements, and if the system comprises a data network then the data network is also subject to the inherited reliability and availability criteria. It is only natural to consider the art of high availability engineering and apply it to wireless communicaitons in the context of RAW.

There are three principles [pillars] of high availability engineering:

1. elimination of single points of failure
2. reliable crossover
3. prompt detection of failures as they occur.

These principles are common to all high availability systems, not just ones with Internet technology at the center. Examples of both non-Internet and Internet are included.

2.2.1.1. Elimination of Single Points of Failure

Physical and logical components in a system happen to fail, either as the effect of wear and tear, when used beyond acceptable limits, or due to a software bug. It is necessary to decouple component failure from system failure to avoid the latter. This allows failed components to be restored while the rest of the system continues to function.

IP Routers leverage routing protocols to compute alternate routes in case of a failure. There is a rather open-ended issue over alternate routes -- for example, when links are cabled through the same conduit, they form a shared risk link group (SRLG), and will share the same fate if the bundle is cut. The same effect can happen with virtual links that end up in a same physical transport through the games of encapsulation. In a same fashion, an interferer or an obstacle may affect multiple wireless transmissions at the same time, even between different sets of peers.

Intermediate network Nodes such as routers, switches and APs, wire bundles and the air medium itself can become single points of failure. For High Availability, it is thus required to use physically link- and Node-disjoint paths; in the wireless space, it is also required to use the highest possible degree of diversity in the transmissions over the air to combat the additional causes of transmission loss.

From an economics standpoint, executing this principle properly generally increases capitalization expense because of the redundant equipment. In a constrained network where the waste of energy and bandwidth should be minimized, an excessive use of redundant links must be avoided; for RAW this means that the extra bandwidth must be used wisely and with parcimony.

2.2.1.2. Reliable Crossover

Having a backup equipment has a limited value unless it can be reliably switched into use within the down-time parameters. IP Routers execute reliable crossover continuously because the routers will use any alternate routes that are available [RFC0791]. This is due to the stateless nature of IP datagrams and the dissociation of the datagrams from the forwarding routes they take. The "IP Fast Reroute Framework" [FRR] analyzes mechanisms for fast failure detection and path repair for IP Fast-Reroute, and discusses the case of multiple failures and SRLG. Examples of FRR techniques include Remote Loop-Free Alternate [RLFA-FRR] and backup label-switched path (LSP) tunnels for the local repair of LSP tunnels using RSVP-TE [RFC4090].

Deterministic flows, on the contrary, are attached to specific paths where dedicated resources are reserved for each flow. This is why each DetNet path must inherently provide sufficient redundancy to provide the guaranteed SLA at all times. The DetNet PREOF typically leverages 1+1 redundancy whereby a packet is sent twice, over non-congruent paths. This avoids the gap during the fast reroute operation, but doubles the traffic in the network.

In the case of RAW, the expectation is that multiple transient faults may happen in overlapping time windows, in which case the 1+1 redundancy with delayed reestablishment of the second path will not provide the required guarantees. The Data Plane must be configured with a sufficient degree of redundancy to select an alternate redundant path immediately upon a fault, without the need for a slow intervention from the controller plane.

2.2.1.3. Prompt Notification of Failures

The execution of the two above principles is likely to render a system where the user will rarely see a failure. But someone needs to in order to direct maintenance.

There are many reasons for system monitoring (FCAPS for fault, configuration, accounting, performance, security is a handy mental checklist) but fault monitoring is sufficient reason.

"An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks" [STD 62] describes how to use SNMP to observe and correct long-term faults.

"Overview and Principles of Internet Traffic Engineering" [TE] discusses the importance of measurement for network protection, and provides abstract an method for network survivability with the analysis of a traffic matrix as observed by SNMP, probing techniques, FTP, IGP link state advertisements, and more.

Those measurements are needed in the context of RAW to inform the controller and make the long term reactive decision to rebuild a complex path. But RAW itself operates in the Network Plane at a faster time scale. To act on the Data Plane, RAW needs live information from the Operational Plane , e.g., using Bidirectional Forwarding Detection [BFD] and its variants (bidirectional and remote BFD) to protect a link, and OAM techniques to protect a path.

2.2.2. Applying Reliability Concepts to Networking

The terms Reliability and Availability are defined for use in RAW in Section 2.1 and the reader is invited to read [NASA] for more details on the general definition of Reliability. Practically speaking a number of nines is often used to indicate the reliability of a data link, e.g., 5 nines indicate a Packet Delivery Ratio (PDR) of 99.999%.

This number is typical in a wired environment where the loss is due to a random event such as a solar particle that affects the transmission of a particular frame, but does not affect the previous or next frame, nor frames transmitted on other links. Note that the QoS requirements in RAW may include a bounded latency, and a packet that arrives too late is a fault and not considered as delivered.

For a periodic networking pattern such as an automation control loop, this number is proportional to the Mean Time Between Failures (MTBF). When a single fault can have dramatic consequences, the MTBF expresses the chances that the unwanted fault event occurs. In data networks, this is rarely the case. Packet loss cannot never be fully avoided and the systems are built to resist to one loss, e.g., using redundancy with Retries (HARQ) or Packet Replication and Elimination (PRE), or, in a typical control loop, by linear interpolation from the previous measuremnents.

But the linear interpolation method cannot resist multiple consecutive losses, and a high MTBF is desired as a guarantee that this will not happen, IOW that the number of losses-in-a-row can be bounded. In that case, what is really desired is a Maximum

Consecutive Failures (MCF). If the number of losses in a row passes the MCF, the control loop has to abort and the system, e.g., the production line, may need to enter an emergency stop condition.

Engineers that build automated processes may use the network reliability expressed in nines or as an MTBF as a proxy to indicate an MCF, e.g., as described in section 7.4 of the "Deterministic Networking Use Cases" [RFC8578].

2.2.3. Reliability in the Context of RAW

In contrast with wired networks, errors in transmission are the predominant source of packet loss in wireless networks.

The root cause for the loss may be of multiple origins, calling for the use of different forms of diversity:

Multipath Fading: A destructive interference by a reflection of the original signal.

A radio signal may be received directly (line-of-sight) and/or as a reflection on a physical structure (echo). The reflections take a longer path and are delayed by the extra distance divided by the speed of light in the medium. Depending on the frequency, the echo lands with a different phase which may add up to (constructive interference) or cancel the direct signal (destructive interference).

The affected frequencies depend on the relative position of the sender, the receiver, and all the reflecting objects in the environment. A given hop will suffer from multipath fading for multiple packets in a row till the something moves that changes the reflection patterns.

Co-channel Interference: Energy in the spectrum used for the transmission confuses the receiver.

The wireless medium itself is a Shared Risk Link Group (SRLG) for nearby users of the same spectrum, as an interference may affect multiple co-channel transmissions between different peers within the interference domain of the interferer, possibly even when they use different technologies.

Obstacle in Fresnel Zone: The optimal transmission happens when the Fresnel Zone between the sender and the receiver is free of obstacles.

As long as a physical object (e.g., a metallic trolley between peers) that affects the transmission is not removed, the quality of the link is affected.

In an environment that is rich of metallic structures and mobile objects, a single radio link will provide a fuzzy service, meaning that it cannot be trusted to transport the traffic reliably over a long period of time.

Transmission losses are typically not independent, and their nature and duration are unpredictable; as long as a physical object (e.g., a metallic trolley between peers) that affects the transmission is not removed, or as long as the interferer (e.g., a radar) keeps transmitting, a continuous stream of packets will be affected.

The key technique to combat those unpredictable losses is diversity. Different forms of diversity are necessary to combat different causes of loss and the use of diversity must be maximised to optimize the PDR.

A single packet may be sent at different times (time diversity) over diverse paths (spatial diversity) that rely on diverse radio channels (frequency diversity) and diverse PHY technologies, e.g., narrowband vs. spread spectrum, or diverse codes. Using time diversity will defeat short-term interferences; spatial diversity combats very local causes such as multipath fading; narrowband and spread spectrum are relatively innocuous to one another and can be used for diversity in the presence of the other.

2.3. Use Cases and Requirements Served

In order to focus on real-worlds issues and assert the feasibility of the proposed capabilities, RAW focuses on selected technologies that can be scheduled at the lower layers: IEEE Std. 802.15.4 timeslotted channel hopping (TSCH), 3GPP 5G ultra-reliable low latency communications (URLLC), IEEE 802.11ax/be where 802.11be is extreme high throughput (EHT), and L-band Digital Aeronautical Communications System (LDACS). See [RAW-TECHNOS] for more.

"Deterministic Networking Use Cases" [RFC8578] presents a number of wireless use cases including Wireless, such as application to Industrial Applications, Pro-Audio, and SmartGrid Automation. [RAW-USE-CASES] adds a number of use cases that demonstrate the need for RAW capabilities for new applications such as Pro-Gaming and drones. The use cases can be abstracted in two families, Loose Protection, e.g., protecting the first hop in Radio Access Protection and Strict Protection, e.g., providing End-to-End Protection in a wireless mesh.

2.3.1. Radio Access Protection

To maintain the required SLA at all times, a wireless Host may use more than one Radio Access Network (RAN) in parallel.

```
                                      ...   ..
                    RAN 1  -----  ...     ..  ...
                 /              .      ..         ....
   +--------+  /              .                    ....    +-----------+
   |Wireless|-                .                     .....  |  Service  |
   | Device |-***-- RAN 2 -- .       Internet       ....---|     /     |
   |(STA/UE)|-                ..                   .....   |Application|
   +--------+  $$$             .               .......     +-----------+
                 \               ...  ...      .....
                    RAN n  --------  ...   .....

   *** = flapping at this time  $$$ expensive
```

Figure 1: Radio Access Protection

The RANs may be heterogeneous, e.g., 3GPP 5G [RAW-5G] and Wi-Fi [RAW-TECHNOS] for high-speed communication, in which case a Layer-3 abstraction becomes useful to select which of the RANs are used at a particular point of time, and the amount of traffic that is distributed over each RAN.

The idea is that the rest of the path to the destination(s) is protected separately (e.g., uses non-congruent paths, leverages DetNet / TSN, etc...) and is a lot more reliable, e.g., wired. In that case, RAW observes the reliability of the end-to-end operation through each of the RANs but only observes and controls the wireless operation the first hop.

A variation of that use case has a pair of wireless Hosts connected over a wired core / backbone network. In that case, RAW observes and controls the Ingress and Egress RANs, while neglecting the hops in the core. The resulting loose Track may be instanciated, e.g., using tunneling or loose source routing between the RANs.

2.3.2. End-to-End Protection in a Wireless Mesh

In radio technologies that support mesh networking (e.g., Wi-Fi and TSCH), a Track is a complex path with distributed PAREO capabilities. In that case, RAW operates through the multipath and makes decisions either at the Ingress or at every hop (more in Section 3.3).

```
                           A-------B-------C-----D
                          /  \   /       /        \
                   Ingress ----M-------N--zzzzz--- Egress
                          \       \ /             /
                           P--zzz--Q-------------R

                  zzz = flapping now
```

Figure 2: End-to-End Protection

The Protection may be imposed by the source based on end-to-end OAM, or performed hop-by-hop, in which case the OAM must enables the intermediate Nodes to estimate the quality of the rest of the feasible paths in the remainder of the Track to the destination.

2.4. Related Work at The IETF

RAW intersects with protocols or practices in development at the IETF as follows:

* The Dynamic Link Exchange Protocol (DLEP) [RFC8175] from [MANET] can be leveraged at each hop to derive generic radio metrics (e.g., based on LQI, RSSI, queueing delays and ETX) on individual hops.

* OAM work at [detnet] such as [DetNet-IP-OAM] for the case of the IP Data Plane observes the state of DetNet paths, typically MPLS and IPv6 pseudowires [DetNet-DP-FW], in the direction of the traffic. RAW needs feedback that flows on the reverse path and gathers instantaneous values from the radio receivers at each hop to inform back the source and replicating relays so they can make optimized forwarding decisions. The work named ICAN may be related as well.

* [BFD] detect faults in the path between an Ingress and an Egress forwarding engines, but is unaware of the complexity of a path with replication, and expects bidirectionality. BFD considers delivery as success whereas with RAW the bounded latency can be as important as the delivery itself.

* [SPRING] and [BIER] define in-band signaling that influences the routing when decided at the head-end on the path. There’s already one RAW-related draft at BIER [BIER-PREF] more may follow. RAW will need new in-band signaling when the decision is distributed, e.g., required chances of reliable delivery to destination within latency. This signaling enables relays to tune retries and replication to meet the required SLA.

- [CCAMP] defines protocol-independent metrics and parameters (measurement attributes) for describing links and paths that are required for routing and signaling in technology-specific networks. RAW would be a source of requirements for CCAMP to define metrics that are significant to the focus radios.

3. The RAW Framework

3.1. Scope and Prerequisites

A prerequisite to the RAW operation is that an end-to-end routing function computes a complex sub-topology along which forwarding can happen between a source and one or more destinations. The concept of Track is specified in the 6TiSCH Architecture [6TiSCH-ARCHI] to represent that complex sub-topology. Tracks provide a high degree of redundancy and diversity and enable the DetNet PREOF, network coding, and possibly RAW specific techniques such as PAREO, leveraging frequency diversity, time diversity, and possibly other forms of diversity as well.

How the routing operation (e.g., PCE) in the Controller Plane computes the Track is out of scope for RAW. The scope of the RAW operation is one Track, and the goal of the RAW operation is to optimize the use of the Track at the forwarding timescale to maintain the expected SLA while optimizing the usage of constrained resources such as energy and spectrum.

Another prerequisite is that an IP link can be established over the radio with some guarantees in terms of service reliability, e.g., it can be relied upon to transmit a packet within a bounded latency and provides a guaranteed BER/PDR outside rare but existing transient outage windows that can last from split seconds to minutes. The radio layer can be programmed with abstract parameters, and can return an abstract view of the state of the Link to help the Network Layer forwarding decision (think DLEP from MANET).

How the radio interface manages its lower layers is out of control and out of scope for RAW. In the same fashion, the non-RAW portion along a loose Track is by definition out of control and out of scope for RAW. Whether it is a single hop or a mesh is also unknown and out of scope.

3.2. Routing Time Scale vs. Forwarding Time Scale

With DetNet, the Controller Plane Function that handles the routing computation and maintenance (the PCE) can be centralized and can reside outside the network. In a wireless mesh, the path to the PCE can be expensive and slow, possibly going across the whole mesh and back. Reaching to the PCE can also be slow in regards to the speed of events that affect the forwarding operation at the radio layer.

Due to that cost and latency, the Controller Plane is not expected to be sensitive/reactive to transient changes. The abstraction of a link at the routing level is expected to use statistical metrics that aggregate the behavior of a link over long periods of time, and represent its properties as shades of gray as opposed to numerical values such as a link quality indicator, or a boolean value for either up or down.

```
                     +----------------+
                     |  Controller    |
                     |    [PCE]       |
                     +----------------+
                             ^
                             |
                            Slow
                             |
         _‾._‾._‾._‾._‾._‾.  |  ._‾._‾._‾._‾._‾._‾._‾._‾._‾._‾._‾._‾
       _‾._‾._‾._‾._‾._‾._‾. | _‾._‾._‾._‾._‾._‾._‾._‾._‾._‾._‾._‾
                             |
                          Expensive
                             |
                      ....   |  .......
                  ....    .  | .       .......
               ....          v               ...
             ..    A-------B-------C---D        ..
          ...     /  \   /       /      \      ..
         .       I ----M-------N--***-- E        ..
         ..       \      \   /         /         ...
           ..      P--***--Q----------R        ....
             ..                              ....
              .   <----- Fast ------->    ....
               .......                ....
                      .................

      *** = flapping at this time
```

Figure 3: Time Scales

In the case of wireless, the changes that affect the forwarding decision can happen frequently and often for short durations, e.g., a mobile object moves between a transmitter and a receiver, and will cancel the line of sight transmission for a few seconds, or a radar measures the depth of a pool and interferes on a particular channel for a split second.

There is thus a desire to separate the long term computation of the route and the short term forwarding decision. In that model, the routing operation computes a complex Track that enables multiple Non-Equal Cost Multi-Path (N-ECMP) forwarding solutions, and leaves it to the Data Plane to make the per-packet decision of which of these possibilities should be used.

In the wired world, and more specifically in the context of Traffic Engineering (TE), an alternate path can be used upon the detection of a failure in the main path, e.g., using OAM in MPLS-TP or BFD over a collection of SD-WAN tunnels. RAW formalizes a forwarding time scale that is an order(s) of magnitude shorter than the controller plane routing time scale, and separates the protocols and metrics that are used at both scales. Routing can operate on long term statistics such as delivery ratio over minutes to hours, but as a first approximation can ignore flapping. On the other hand, the RAW forwarding decision is made at the scale of the packet rate, and uses information that must be pertinent at the present time for the current transmission(s).

3.3. Wireless Tracks

The "6TiSCH Architecture" [6TiSCH-ARCHI] introduces the concept of Track. RAW extends the concept to any wireless mesh technology, including, e.g., Wi-Fi. A simple Track is composed of a direct sequence of reserved hops to ensure the transmission of a single packet from a source Node to a destination Node across a multihop path.

A Complex Track provides multiple non-equal cost multipath (NECM) forwarding solutions. The Complex Track enables to support multi-path redundant forwarding by employing PRE functions [RFC8655] and the ingress and within the Track. For example, a Complex Track may branch off and rejoin over non-congruent segments.

In the context of RAW, some links or segments in the Track may be reversible, meaning that they can be used in either direction. In that case, an indication in the packet signals the direction of the reversible links or segments that the packet traverses and thus places a constraint that prevents loops from occuring. An indidual packet follows a destination-oriented directed acyclic graph (DODAG) towards a destination Node inside the Complex Track.

3.4. PAREO Functions

RAW may control whether and how to use packet replication and elimination (PRE), Automatic Repeat reQuest (ARQ), Hybrid ARQ (HARQ) that includes Forward Error Correction (FEC) and coding, and other wireless-specific techniques such as overhearing and constructive interferences, in order to increase the reliabiility and availability of the end-to-end transmission.

Collectively, those function are called PAREO for Packet (hybrid) ARQ, Replication, Elimination and Ordering. By tuning dynamically the use of PAREO functions, RAW avoids the waste of critical resources such as spectrum and energy while providing that the guaranteed SLA, e.g., by adding redundancy only when a spike of loss is observed.

In a nutshell, PAREO establishes several paths in a network to provide redundancy and parallel transmissions to bound the end-to-end delay to traverse the network. Optionally, promiscuous listening between paths is possible, such that the Nodes on one path may overhear transmissions along the other path. Considering the scenario shown in Figure 4, many different paths are possible for S to reach R. A simple way to benefit from this topology could be to use the two independent paths via Nodes A, C, E and via B, D, F. But more complex paths are possible by interleaving transmissions from the lower level of the path to the upper level.

```
                             (A) -- (C) -- (E)
                           /                   \
                   Ingress    |      |      |    Egress
                           \                   /
                             (B) -- (D) -- (F)
```

Figure 4: A Ladder Shape with Two Parallel Paths

PAREO may also take advantage of the shared properties of the wireless medium to compensate for the potential loss that is incurred with radio transmissions.

For instance, when the source sends to Node A, Node B may listen promiscuously and get a second chance to receive the frame without an additional transmission. Note that B would not have to listen if it already received that particular frame at an earlier timeslot in a dedicated transmission towards B.

The PAREO model can be implemented in both centralized and distributed scheduling approaches. In the centralized approach, a Path Computation Element (PCE) scheduler calculates a Track and schedules the communication. In the distributed approach, the Track is computed within the network, and signaled in the packets, e.g., using BIER-TE, Segment Routing, or a Source Routing Header.

3.4.1. Packet Replication

By employing a Packet Replication procedure, a Node forwards a copy of each data packet to more than one successor. To do so, each Node (i.e., Ingress and intermediate Node) sends the data packet multiple times as separate unicast transmissions. For instance, in Figure 5, the Ingress Node is transmitting the packet to both successors, nodes A and B, at two different times.

```
                          ===> (A) => (C) => (E) ===
                        //        \\//   \\//       \\
                Ingress           //\\   //\\          Egress
                        \\       //  \\ //  \\      //
                          ===> (B) => (D) => (F) ===
```

Figure 5: Packet Replication

An example schedule is shown in Table 1. This way, the transmission leverages with the time and spatial forms of diversity.

Channel	0	1	2	3	4	5	6
0	S->A	S->B	B->C	B->D	C->F	E->R	F->R
1		A->C	A->D	C->E	D->E	D->F	

Table 1: Packet Replication: Sample schedule

3.4.2. Packet Elimination

The replication operation increases the traffic load in the network, due to packet duplications. This may occur at several stages inside the Track, and to avoid an explosion of the number of copies, a Packet Elimination procedure must be applied as well. To this aim, once a Node receives the first copy of a data packet, it discards the subsequent copies.

The logical functions of Replication and Elimination may be collocated in an intermediate Node, the Node first eliminating the redundant copies and then sending the packet exactly once to each of the selected successors.

3.4.3. Promiscuous Overhearing

Considering that the wireless medium is broadcast by nature, any neighbor of a transmitter may overhear a transmission. By employing the Promiscuous Overhearing operation, the next hops have additional opportunities to capture the data packets. In Figure 6, when Node A is transmitting to its DP (Node C), the AP (Node D) and its sibling (Node B) may decode this data packet as well. As a result, by employing corellated paths, a Node may have multiple opportunities to receive a given data packet.

```
                      ===> (A) ====> (C) ====> (E) ====
                    //     ^ | \\                      \\
             Ingress       | |   \\                      Egress
                    \\     | v     \\                  //
                      ===> (B) ====> (D) ====> (F) ====
```

Figure 6: Unicast with Overhearing

3.4.4. Constructive Interference

Constructive Interference can be seen as the reverse of Promiscuous Overhearing, and refers to the case where two senders transmit the exact same signal in a fashion that the emitted symbols add up at the receiver and permit a reception that would not be possible with a single sender at the same PHY mode and the same power level.

Constructive Interference was proposed on 5G, Wi-Fi7 and even tested on IEEE Std 802.14.5. The hard piece is to synchronize the senders to the point that the signals are emitted at slightly different time to offset the difference of propagation delay that corresponds to the difference of distance of the transmitters to the receiver at the speed of light to the point that the symbols are superposed long enough to be recognizable.

4. The RAW Architecture

4.1. The RAW Conceptual Model

RAW inherits the conceptual model described in section 4 of the DetNet Architecture [RFC8655]. RAW extends the DetNet service layer to provide additional agility against transmission loss.

A RAW Network Plane may be strict or loose, depending on whether RAW observes and takes actions on all hops or not. For instance, the packets between two wireless entities may be relayed over a wired infrastructure such as a Wi-Fi extended service set (ESS) or a 5G Core; in that case, RAW observes and control the transmission over the wireless first and last hops, as well as end-to-end metrics such as latency, jitter, and delivery ratio. This operation is loose since the structure and properties of the wired infrastructure are ignored, and may be either controlled by other means such as DetNet/TSN, or neglected in the face of the wireless hops.

A Controller Plane Function (CPF) called the Path Computation Element (PCE) [RFC4655] interacts with RAW Nodes over a Southbound API. The RAW Nodes are DetNet relays that are capable of additional diversity mechanisms and measurement functions related to the radio interface, in particular the PAREO diversity mechanisms.

The PCE defines a complex Track between an Ingress End System and an Egress End System, and indicates to the RAW Nodes where the PAREO operations may be actionned in the Network Plane. The Track may be expressed loosely to enable traversing a non-RAW subnetwork. In that case, the expectation is that the non-RAW subnetwork can be neglected in the RAW computation, that is, considered infinitely fast, reliable and/or available in comparison with the links between RAW nodes.

```
           CPF               CPF          CPF                CPF


                          Southbound API
      _-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-
    _-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-._-


                    RAW  --z   RAW  --z   RAW  --z   RAW
                z-- Node  z--  Node  z--  Node  z--  Node --z
     Ingress --z    /          /                          z-- Egress
     End           \          \         .. .                  End
     Node   ---z   /          /       .. ..  .            z-- Node
              z-- RAW  --z   RAW     ( non-RAW ) -- RAW --z
                  Node  z--  Node --- ( Nodes  )   Node
                                        ... .
     --z   wireless           wired
      z--  link           --- link
```

Figure 7: RAW Nodes

The Link-Layer metrics are reported to the PCE in a time-aggregated, e.g., statistical fashion. Example Link-Layer metrics include typical Link bandwidth (the medium speed depends dynamically on the PHY mode and the number of users sharing the spectrum) and average and mean squared deviation of availability and reliability figures such as Packet Delivery Ratio (PDR) over long periods of time.

Based on those metrics, the PCE installs the Track with enough redundant forwarding solutions to ensure that the Network Plane can reliably deliver the packets within a System Level Agreement (SLA) associated to the flows that it transports. The SLA defines end-to-end reliability and availability requirements, where reliability may be expressed as a successful delivery in order and within a bounded delay of at least one copy of a packet.

Depending on the use case and the SLA, the Track may comprise non-RAW segments, either interleaved inside the Track, or all the way to the Egress End Node (e.g., a server in the Internet). RAW observes the Lower-Layer Links between RAW nodes (typically, radio links) and the end-to-end Network Layer operation to decide at all times which of the PAREO diversity schemes is actioned by which RAW Nodes.

Once a Track is established, per-segment and end-to-end reliability and availability statistics are periodically reported to the PCE to assure that the SLA can be met or have it recompute the Track if not.

4.2. The Path Selection Engine

RAW separates the path computation time scale at which a complex path is recomputed from the path selection time scale at which the forwarding decision is taken for one or a few packets (more in Section 3.2). RAW operates at the path selection time scale. The RAW problem is to decide, within the redundant solutions that are proposed by the PCE, which will be used for each packet to provide a Reliable and Available service while minimizing the waste of constrained resources.

To that effect, RAW defines the Path Selection Engine (PSE) that is the counter-part of the PCE to perform rapid local adjustments of the forwarding tables within the diversity that the PCE has selected for the Track. The PSE enables to exploit the richer forwarding capabilities with PAREO and scheduled transmissions at a faster time scale over the smaller domain that is the Track, in either a loose or a strict fashion.

Compared to the PCE, the PSE operates on metrics that evolve faster, but that needs to be advertised at a fast rate but only locally, within the Track. The forwarding decision may also change rapidly, but wiht a scope that is also contained within the Track, with no visibility to the other Tracks and flows in the network. This is as opposed to the PCE that needs to observe the whole network, and optimize all the Tracks globally, which can only be done at a slow pace and using long-term statistical metrics, as presented in Table 2.

	PCE (Not in Scope)	PSE (In Scope)
Operation	Centralized	Source-Routed or Distributed
Communication	Slow, expensive	Fast, local
Time Scale	hours and above	seconds and below
Network Size	Large, many Tracks to optimize globally	Small, within one Track
Considered Metrics	Averaged, Statistical, Shade of grey	Instant values / boolean condition

Table 2: PCE vs. PSE

The PSE sits in the DetNet Service sub-Layer of Edge and Relay Nodes. On the one hand, it operates on the packet flow, learning the Track and path selection information from the packet, possibly making local decision and retagging the packet to indicate so. On the other hand, the PSE interacts with the lower layers and with its peers to obtain up-to-date information about its radio links and the quality of the overall Track, respectively, as illustrated in Figure 8.

```
               |
        packet | going
      down the | stack
    +==========v==========+=====================+=====================+
    |   (iOAM + iCTRL)    | (L2 Triggers, DLEP) |       (oOAM)        |
    +==========v==========+=====================+=====================+
    |     Learn from                                 Learn from         |
    |    packet tagging           Maintain           end-to-end         |
    +----------v----------+      Forwarding          OAM packets        |
    | Forwarding decision <        State        +---------^-----------|
    +----------v----------+                     |      Enrich or        |
    +    Retag Packet     |  Learn abstracted   >     Regenerate        |
    |    and Forward      | metrics about Links |     OAM packets       |
    +..........v..........+..........^..........+.........^.v.........+
    |                          Lower layers                           |
    +..........v.....................^....................^.v.........+
         frame | sent           Frame | L2 Ack        oOAM | | packet
          over | wireless         In  |                 In | | and out
               v                      |                    | v
```

Figure 8: PSE

4.3. RAW OAM

The RAW OAM operation in the Network Plane observes either a full Track or subTracks that are being used at this time. This observeation feeds the RAW PSE that makes the decision on which PAREO function in actioned at which RAW Node, for one a small continuous series of packets.

```
                                         ...   ..
                      RAN 1  -----  ...      ..  ...
                   /              .    ..          ....
      +-------+  /              .            ..      ....    +------+
      |Ingress|-                .                     .....  |Egress|
      |  End  |------ RAN 2 -- .       Internet       ....---| End  |
      |System |-                ..                   .....   |System|
      +-------+  \               .               ......      +------+
                   \               ...   ...     .....
                      RAN n  --------  ...   .....

             <------------------> <-------------------->
                Observed by OAM       Opaque to OAM
```

Figure 9: Observed Links in Radio Access Protection

In the case of a End-to-End Protection in a Wireless Mesh, the Track is strict and congruent with the path so all links are observed. Conversely, in the case of Radio Access Protection, the Track is Loose and in that case only the first hop is observed; the rest of the path is abstracted and considered infinitely reliable.

In the case of the Radio Access Protection, only the first hop is protected; the loss of a packet that was sent over one of the possible first hops is attributed to that first hop, even if a particular loss effectively happens farther down the path.

The Links that are not observed by OAM are opaque to it, meaning that the OAM information is carried across and possibly echoed as data, but there is no information capture in intermediate nodes. In the example above, the Internet is opaque and not controlled by RAW; still the RAW OAM measures the end-to-end latency and delivery ratio for packets sent via each if RAN 1, RAN 2 and RAN 3, and determines whether a packet should be sent over either or a collection of those access links.

4.4. Flow Identification vs. Path Identification

Section 4.7 of the DetNet Architecture [RFC8655] ties the app-flow identification which is an appliation layer concept with the network path identification that depends on the networking technology by "exporting of flow identification", e.g., to a MPLS label.

With RAW, this exporting operation is injective but not bijective. e.g., a flow is fully placed within one RAW Track, but not all packets along that Track are necessarily part of the same flow. For instance, out-of-band OAM packets must circulate in the exact same fashion as the flows that they observe. It results that the flow identification that maps to to app-flow at the network layer must be separate from the path identification that is used to forward a packet.

Section 3.4 of the DetNet data-plane framework [DetNet-DP-FW] indicates that for a DetNet IP Data Plane, a flow is identified by an IPv6 6-tuple. With RAW, that 6-tuple is not what indicates the Track, in other words, the flow ID is not the Track ID.

For instance, the 6TiSCH Architecture [6TiSCH-ARCHI] uses a combination of the address of the Egress End System and an instance identifier in a Hop-by-hop option to indicate a Track. This way, if a packet "escapes" the Track, it will reach the Track Egress point through normal routing and be treated at the service layer through, say, elimination and reordering.

The RAW service includes forwarding over a subset of the Links that form the Track (a subTrack). Packets from the same or a different flow that are routed through the same Track will not necessarily traverse the same Links. The PSE selects a subTrack for a packet based on the links that are preferred and those that should be avoided at this time.

Each packet is forwarded within the subTrack that provides the best adequation with the SLA of the flow and the energy and bandwidth constraints of the network.

```
                        Flow 1 (6-tuple) ----+
                                             |
                   Flow 2 (6-tuple)  ---+    |
                                        |    |
                OAM     -----------+    |    |
                                   |    |    |
                                   |    |    |
                              |    |    |    |    |
                              |    v    v    v    |
                              |                   |
                              +---------+---------+
                                        |
                                        |
                        Track i (Egress IP Address, instanceId)
                                        |
                                        |
                                        |
                        +---------+-----+--....-------+
                        |         |                   |
                        |         |                   |
                 subTrack 1    subTrack 2          subTrack n
                        |         |                   |
                        |         |                   |
                        V         V                   V
                     +-----------------------------------+
                     |                                   |
                     |         Destination               |
                     |                                   |
                     +-----------------------------------+
```

Figure 10: Flow Injection

With 6TiSCH, packets are tagged with the same (destination address, instance ID) will experience the same RAW service regardless of the IPv6 6-tuple that indicates the flow. The forwarding does not depend on whether the packets transport application flows or OAM. In the generic case, the Track or the subTrack can be signaled in the packet through other means, e.g., encoded in the suffix of the destination address as a Segment Routing Service Instruction [SR-ARCHI], or leveraging Bit Index Explicit Replication [BIER] Traffic Engineering [BIER-TE].

4.5. Source-Routed vs. Distributed Forwarding Decision

Within a large routed topology, the route-over mesh operation builds a particular complex Track with one source and one or more destinations; within the Track, packets may follow different paths and may be subject to RAW forwarding operations that include replication, elimination, retries, overhearing and reordering.

The RAW forwarding decisions include the selection of points of replication and elimination, how many retries can take place, and a limit of validity for the packet beyond which the packet should be destroyed rather than forwarded uselessly further down the Track.

The decision to apply the RAW techniques must be done quickly, and depends on a very recent and precise knowledge of the forwarding conditions within the complex Track. There is a need for an observation method to provide the RAW Data Plane with the specific knowledge of the state of the Track for the type of flow of interest (e.g., for a QoS level of interest). To observe the whole Track in quasi real time, RAW considers existing tools such as L2-triggers, DLEP, BFD and leverages in-band and out-of-band OAM to capture and report that information to the PSE.

One possible way of making the RAW forwarding decisions within a Track is to position a unique PSE at the Ingress and express its decision in-band in the packet, which requires the explicit signaling of the subTrack within the Track. In that case, the RAW forwarding operation along the Track is encoded by the source, e.g., by indicating the subTrack in the Segment Routing (SRv6) Service Instruction, or by leveraging BIER-TE such as done with [BIER-PREF].

The alternate way is to operate the PSE in each forwarding Node, which makes the RAW forwarding decisions for a packet on its own, based on its knowledge of the expectation (timeliness and reliability) for that packet and a recent observation of the rest of the way across the possible paths based on OAM. Information about the desired service should be placed in the packet and matched with the forwarding Node’s capabilities and policies.

In either case, a per-track/subTrack state is installed in all the intermediate Nodes to recognize the packets that are following a Track and determine the forwarding operation to be applied.

4.6. Encapsulation and Decapsulation

In the generic case where the Track Ingress Node is not the source of the Packet, the Ingress Node needs to encapsulate IP-in-IP to ensure that the Destination IP Address is that of the Egress Node and that the necessary Headers (Routing Header, Segment Routing Header and/or Hop-By-Hop Header) can be added to the packet to signal the Track or the subTrack, conforming [IPv6] that discourages the insertion of a Header on the fly.

In the specific case where the Ingress Node is the source of the packet, the encapsulation can be avoided, provided that the source adds the necessary headers and that the destination is set to the Egress Node. Forwarding to a final destination beyond the Egress Node is possible, e.g., with a Segment Routing Header that signals the rest of the way. In that case a Hop-by-Hop Header is not recommmended since its validity is within the Track only.

5. Security Considerations

RAW uses all forms of diversity including radio technology and physical path to increase the reliability and availability in the face of unpredictable conditions. While this is not done specifically to defeat an attacker, the amount of diversity used in RAW makes an attack harder to achieve.

5.1. Forced Access

RAW will typically select the cheapest collection of links that matches the requested SLA, for instance, leverage free WI-Fi vs. paid 3GPP access. By defeating the cheap connectivity (e.g., PHY-layer interference) the attacker can force an End System to use the paid access and increase the cost of the transmission for the user.

6. IANA Considerations

This document has no IANA actions.

7. Contributors

Xavi Vilajosana: Wireless Networks Research Lab, Universitat Oberta de Catalunya

Remous-Aris Koutsiamanis: IMT Atlantique

Nicolas Montavont: IMT Atlantique

8. Acknowledgments

TBD

9. References

9.1. Normative References

[6TiSCH-ARCHI]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", Work in Progress, Internet-Draft, draft-ietf-6tisch-architecture-29, 27 August 2020, <https://tools.ietf.org/html/draft-ietf-6tisch-architecture-29>.

[RAW-TECHNOS]
Thubert, P., Cavalcanti, D., Vilajosana, X., Schmitt, C., and J. Farkas, "Reliable and Available Wireless Technologies", Work in Progress, Internet-Draft, draft-thubert-raw-technologies-05, 18 May 2020, <https://tools.ietf.org/html/draft-thubert-raw-technologies-05>.

[RAW-USE-CASES]
Papadopoulos, G., Thubert, P., Theoleyre, F., and C. Bernardos, "RAW use cases", Work in Progress, Internet-Draft, draft-bernardos-raw-use-cases-04, 13 July 2020, <https://tools.ietf.org/html/draft-bernardos-raw-use-cases-04>.

[RFC4655] Farrel, A., Vasseur, J.-P., and J. Ash, "A Path Computation Element (PCE)-Based Architecture", RFC 4655, DOI 10.17487/RFC4655, August 2006, <https://www.rfc-editor.org/info/rfc4655>.

[BFD] Katz, D. and D. Ward, "Bidirectional Forwarding Detection (BFD)", RFC 5880, DOI 10.17487/RFC5880, June 2010, <https://www.rfc-editor.org/info/rfc5880>.

[RFC6291] Andersson, L., van Helvoort, H., Bonica, R., Romascanu, D., and S. Mansfield, "Guidelines for the Use of the "OAM" Acronym in the IETF", BCP 161, RFC 6291, DOI 10.17487/RFC6291, June 2011, <https://www.rfc-editor.org/info/rfc6291>.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

[IPv6] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[SR-ARCHI] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

[BIER] Wijnands, IJ., Ed., Rosen, E., Ed., Dolganow, A., Przygienda, T., and S. Aldrin, "Multicast Using Bit Index Explicit Replication (BIER)", RFC 8279, DOI 10.17487/RFC8279, November 2017, <https://www.rfc-editor.org/info/rfc8279>.

[RFC8175] Ratliff, S., Jury, S., Satterwhite, D., Taylor, R., and B. Berry, "Dynamic Link Exchange Protocol (DLEP)", RFC 8175, DOI 10.17487/RFC8175, June 2017, <https://www.rfc-editor.org/info/rfc8175>.

[RFC8557] Finn, N. and P. Thubert, "Deterministic Networking Problem Statement", RFC 8557, DOI 10.17487/RFC8557, May 2019, <https://www.rfc-editor.org/info/rfc8557>.

[RFC8655] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <https://www.rfc-editor.org/info/rfc8655>.

9.2. Informative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[TE] Awduche, D., Chiu, A., Elwalid, A., Widjaja, I., and X. Xiao, "Overview and Principles of Internet Traffic Engineering", RFC 3272, DOI 10.17487/RFC3272, May 2002, <https://www.rfc-editor.org/info/rfc3272>.

[STD 62] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, DOI 10.17487/RFC3411, December 2002, <https://www.rfc-editor.org/info/rfc3411>.

[RFC4090] Pan, P., Ed., Swallow, G., Ed., and A. Atlas, Ed., "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, DOI 10.17487/RFC4090, May 2005, <https://www.rfc-editor.org/info/rfc4090>.

[FRR] Shand, M. and S. Bryant, "IP Fast Reroute Framework", RFC 5714, DOI 10.17487/RFC5714, January 2010, <https://www.rfc-editor.org/info/rfc5714>.

[RLFA-FRR] Bryant, S., Filsfils, C., Previdi, S., Shand, M., and N. So, "Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)", RFC 7490, DOI 10.17487/RFC7490, April 2015, <https://www.rfc-editor.org/info/rfc7490>.

[BIER-PREF]
Thubert, P., Eckert, T., Brodard, Z., and H. Jiang, "BIER-TE extensions for Packet Replication and Elimination Function (PREF) and OAM", Work in Progress, Internet-Draft, draft-thubert-bier-replication-elimination-03, 3 March 2018, <https://tools.ietf.org/html/draft-thubert-bier-replication-elimination-03>.

[DetNet-IP-OAM]
Mirsky, G., Chen, M., and D. Black, "Operations, Administration and Maintenance (OAM) for Deterministic Networks (DetNet) with IP Data Plane", Work in Progress, Internet-Draft, draft-mirsky-detnet-ip-oam-03, 7 August 2020, <https://tools.ietf.org/html/draft-mirsky-detnet-ip-oam-03>.

[DetNet-DP-FW]
Varga, B., Farkas, J., Berger, L., Malis, A., and S. Bryant, "DetNet Data Plane Framework", Work in Progress, Internet-Draft, draft-ietf-detnet-data-plane-framework-06, 6 May 2020, <https://tools.ietf.org/html/draft-ietf-detnet-data-plane-framework-06>.

[RAW-5G] Farkas, J., Dudda, T., Shapin, A., and S. Sandberg, "5G - Ultra-Reliable Wireless Technology with Low Latency", Work in Progress, Internet-Draft, draft-farkas-raw-5g-00, 1 April 2020, <https://tools.ietf.org/html/draft-farkas-raw-5g-00>.

[BIER-TE] Eckert, T., Cauchie, G., and M. Menth, "Tree Engineering for Bit Index Explicit Replication (BIER-TE)", Work in Progress, Internet-Draft, draft-ietf-bier-te-arch-09, 30 October 2020, <https://tools.ietf.org/html/draft-ietf-bier-te-arch-09>.

[NASA] Adams, T., "RELIABILITY: Definition & Quantitative Illustration", <https://kscddms.ksc.nasa.gov/Reliability/Documents/150814-3bWhatIsReliability.pdf>.

[MANET] IETF, "Mobile Ad hoc Networking", <https://dataTracker.ietf.org/doc/charter-ietf-manet/>.

[detnet] IETF, "Deterministic Networking", <https://dataTracker.ietf.org/doc/charter-ietf-detnet/>.

[SPRING] IETF, "Source Packet Routing in Networking", <https://dataTracker.ietf.org/doc/charter-ietf-spring/>.

[BIER] IETF, "Bit Indexed Explicit Replication", <https://dataTracker.ietf.org/doc/charter-ietf-bier/>.

[BFD] IETF, "Bidirectional Forwarding Detection", <https://dataTracker.ietf.org/doc/charter-ietf-bfd/>.

[CCAMP] IETF, "Common Control and Measurement Plane", <https://dataTracker.ietf.org/doc/charter-ietf-ccamp/>.

Authors' Addresses

Pascal Thubert (editor)
Cisco Systems, Inc
Building D
45 Allee des Ormes - BP1200
06254 MOUGINS - Sophia Antipolis
France

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Georgios Z. Papadopoulos
IMT Atlantique
Office B00 - 114A
2 Rue de la Chataigneraie
35510 Cesson-Sevigne - Rennes
France

Phone: +33 299 12 70 04
Email: georgios.papadopoulos@imt-atlantique.fr

Rex Buddenberg
CA
United States of America

Email: buddenbergr@gmail.com

Reliable and Available Wireless Working Group
Internet-Draft
Intended status: Informational
Expires: 8 September 2021

R.C. Sofia
fortiss GmbH
M. Kovatsch
Huawei Technologies
P. Mendes
Airbus

7 March 2021

Requirements for Reliable Wireless Industrial Services
draft-sofia-raw-industrialreq-00

Abstract

This document provides an overview on communication requirements for handling reliable wireless services within the context of industrial environments. The goal of the draft is to bring awareness to communication requirements of current and future wireless industrial services; how can they co-exist with wired infrastructures; key drivers for reliable wireless integration; relevant communication requirements to take into consideration; current and future challenges derived from the use of wireless.

Discussion Venues

This note is to be removed before publishing as an RFC.

Discussion of this document takes place on the mailing list (raw@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/raw/.

Source for this draft and an issue tracker can be found at https://github.com/rute19104/draft-raw-requirements.

Status of This Memo

This Internet-Draft will expire on 4 September 2021.

Copyright Notice

Table of Contents

1. Introduction

Within industrial environments, short-range wireless standards, such as IEEE 802.11ax, are gaining prominence as there exists an increasing need for flexibility in terms of infrastructure layout, of processes support. Wireless, and specifically Wireless Fidelity (Wi-Fi), is now reaching a maturity point where the available transmission rates become highly competitive in comparison to wired environments, thus increasing flexibility, providing a lower cost and higher availability in scenarios requiring, for instance, mobility support. There are, nonetheless, barriers to the integration of wireless in industrial environments. Firstly, being wireless a shared medium, it experiences challenges such as interference and signal strength variability depending on its surroundings. These features raise issues concerning critical services availability, resilience, and security support. Secondly, wireless relies on probabilistic Quality of Service (QoS) and therefore requires tuning to be able to support time-sensitive traffic with bounded latency, low jitter, zero congestion loss. However, the recent advancements of OFDMA-based wireless in the context of IEEE 802.11 standards such as 802.11ax and 802.11be bring in interesting features in the context of supporting critical industrial applications, e.g., a higher degree of flexibility in terms of resource management; frequency allocation aspects that can provide better traffic isolation, or even mechanisms that can assist a tighter time synchronization across wireless environments, thus providing the means to better support traffic in converged networks. Still, being able to address the communication challenges that exist in industrial domains require a better understanding of communication requirements that the existing and future industrial applications may attain. Hence, the focus of this draft is on discussing industrial application requirements, currently and for the future and how to best support time-sensitive applications and services within industrial converged networks. For that purpose, the draft debates on wireless industrial services collected from related normative and informational references on the industrial domain; debates on key drivers for the integration of wireless; debates on specific wireless mechanisms that may assist such integration and challenges thereof; and elaborates on specific requirements to observe both for current wireless services as well as for a subset of future industrial wireless services.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119]. In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying significance described in RFC 2119.

3. Definitions

* Latency (aka bounded latency), concerns the end-to-end transmission delay between a transmitter and a receiver, when a traffic flow is triggered by an application. By definition, latency corresponds to the time interval between sending the first packet of a flow from a source to a destination, until the instant of reception of the last packet of that flow.

* Periodicity stands for whether or not the data transmission is executed in a periodic fashion and whenever possible, the specific periodicity per unit of time has been specified.

* "Transmit data size" corresponds to the data payload in bytes.

* Tolerance to packet loss is presented as "0" (zero congestion loss); tolerant (the application has tolerance to packet loss). Packet loss occurs when packets fail to reach a specific destination on a network. Packet loss is usually measured as a percentage of packets loss in regards to the overall packets sent. In the context of deterministic networking and in particular, of Time-sensitive Networking (TSN), a packet is lost when it is not received within a specific deadline.

* "Time sync" refers to the need to ensure IEEE 1588 synchronization.

* "Node density" provides (wherever available) a glimpse into the number of end-nodes per 20mx20m.

4. Wireless Industrial Services Today

This section describes industrial applications where IEEE 802.11 is already being applied, derived from an analysis of related work.

Industrial wireless services focused on the strengthening of industrial manufacturing environments have been intensively documented via the IEEE Nendica group [NENDICA], the Internet Industrial Consortium [IIC], the OPC FLC working group [OPCFLC]. The IEEE Nendica 2020 report [NENDICA] comprises several end-to-end use-cases and a technical analysis of the identified features and functions supported via wireless/wired deterministic environments. Based on surveys to industry, the report provides a first characterization of wireless services in factories (Wi-Fi 5), characterizing the scenarios in terms of aspects such as as payload size in bytes, communication rate, arrival time tolerance, node density.

The IEEE 802.11 RTA report [IEEERTA] provides additional input concerning the support of wireless for time-sensitive and real-time applications. For each category of application, the report provides a description, basic information concerning topology and packet flow/ traffic model, summarizing the problem statement (main challenges). The industrial applications in this report are a subset and have also considered sources such as IEEE Nendica, IEC/IEEE 60802 Use-cases, as well as 3GPP TR 22.804. The report aggregates the different services in 3 classes (A,B,C) and provides communication requirements for each class categorized as: bounded latency (worst-case one-way latency measured at the application layer); reliability (defined as the percentage of packets expected to be received within the latency bound); time synchronization needs (in the order of micro/ milliseconds); throughput needs (high, moderate, low). The report concludes with guidelines concerning implementation aspects, e.g., traffic classification aspects and new capabilities to support real-time applications.

The Avnu Alliance provides a white paper describing steps for the integration of TSN over WiFi [AVNU2020], briefly describing the integration of Wi-Fi in specific applications such as: closed loop control, mobile robots, power grid control, professional Audio/Video, gaming, AR/VR. The document also raises awareness to the possibility of wireless replacing or being complementary to wired within connected cabines, i.e., in regards to the wiring harness within vehicles (cars, airplanes, trains), which are currently expensive and which require a complex onboarding. Wireless can assist in lowering the costs, if it can be adapted to the critical latency, safety requirements and regulations. Such cases would require 100 micosecond level cycles, according to Avnu. The communication requirements are summarised in terms of whether or not IEEE 1588 synchronisation is required; the typical packet size (data payload); bounded latency; reliability.

Manufacturing wireless use-cases have also been debated in the context of 5G ACIA [ACIA], NICT [NICT], and IETF Deterministic Networking [RFC8578]. These sources provide an overview on user stories, and debate on the challenges brought by the integration of wireless. However, communication requirements are not presented in a systematic way. Lastly, the IETF RAW working group has an active draft which provides an initial overview on the challenges of wireless industrial use-cases [IETFRAW-USECASES].

Derived from the analysis of the aforementioned sources, this section provides a description of categories of applications, and respective communication requirements. The following categories of applications are addressed:

- Equipment and process control.
- Quality supervision.
- Factory resource management.
- Display.
- Human safety.
- Industrial systems.
- Mobile robots.
- Drones/UAV control.
- Power grid control.
- Communication-based train networks.
- Mining industry.
- Connected cabin.

The selected communication requirements and which are presented for each category of applications have been extracted from the different available related work. The parameters are: bounded latency; periodicity; transmit data size; tolerance to packet loss; time synchronization needs; node density characterization.

4.1. Equipment and Process Control Services

This category of industrial wireless services refers to the data exchange required to send, for instance, commands to mobile robots/vehicles, production equipment, and also to receive status information. Reasons for wireless integration concern: flexibility of deployment, reconfigurability, mobility, maintenance cost reduction.

In this category, examples of applications and respective communication requirements are:

- Control of machines and robots.
  - Bounded latency: below 10 ms.
  - Periodic.
  - Transmit data size (bytes): 10-400 (small).
  - Tolerance to packet loss: 0.
  - Time synchronization: IEEE 1588.
  - Node density: 1 to 20 (per 20mx20m area).
- AGVs with rails
  - Bounded latency: 10 ms-100ms.
  - Periodic, once per minute.

  - Transmit data size (bytes): 10-400 (small).
  - Tolerance to packet loss: 0.
  - Time synchronization: IEEE 1588.
  - Node density: 1 to 20 (per 20mx20m area).

* AGVs without rails
  - Bounded latency:1 s.
  - Periodic, once per minute.
  - Transmit data size (bytes): 10-400 (small).
  - Tolerance to packet loss: 0.
  - Time synchronization: IEEE 1588.
  - Node density: 1 to 20 (per 20mx20m area).

* Hard-real time isochronous control, motion control
  - Bounded latency: 250us - 1ms.
  - Periodic.
  - Transmit data size (bytes): 10-400 (small).
  - Tolerance to packet loss: 0.
  - Time synchronization: IEEE 1588.
  - Node density: 1 to 20 (per 20mx20m area).

* Printing, packaging
  - Bounded latency: below 2 ms.
  - Transmit data size (bytes): 10-400 (small).
  - Tolerance to packet loss: 0.
  - Time synchronization: IEEE 1588.
  - Node density: over 50 to 100.

* PLC to PLC communication
  - Bounded latency: 100 us-50 ms.
  - Transmit data size (bytes): 100-700.
  - Tolerance to packet loss: 0.
  - Time synchronization: IEEE 1588.

* Interactive video
  - Bounded latency: 50 -10 ms.

    - Time synchronization: 10-1[micro]s.

- Mobile robotics

    - Bounded latency: 50 -10 ms.

- AR/VR, remote HMI

    - Bounded latency: 10 - 1 ms.

    - Time synchronization: ~1 [micro]s.

    - Time synchronization: 10-1[micro]s.

- Machine, production line controls

    - Bounded latency: 10 - 1 ms.

4.2. Quality Supervision Services

Quality supervision comprises industrial services that collect and assess information related to products and states of machines during production. Reasons for wireless integration concern: flexibility of deployment, maintenance cost reduction.

Examples of applications in this category, and their communication requirements are:

- Inline inspection

    - Bounded latency: bellow 10ms.

    - Time synchronization: 10-1[micro]s.

    - Periodic, once per second.

    - Transmit data size (bytes): 64-1M.

    - Tolerance to packet loss: 0.

    - Node density: 1-10 (per 20mx20m).

- Machine operation recording

    - Bounded latency: over 100 s.

    - Time synchronization: 10-1[micro]s.

    - Periodic, once per second.

    - Transmit data size (bytes): 64-1M.

    - Tolerance to packet loss: 0.

    - Node density: 1-10 (per 20mx20m).

- Logging

    - Bounded latency: over 100s.

    - Time synchronization: 10-1[micro]s.

   - Transmit data size (bytes): 64-1M.

   - Tolerance to packet loss: 0.

   - Node density: 1-10 (per 20mx20m).

4.3. Factory Resource Management Services

Refers to capturing information about whether production is proceeding under proper environmental conditions, and whether staff and devices contributing to productivity enhancement are being managed appropriately. Reasons for wireless integration concern: flexibility of deployment, reconfigurability, maintenance cost reduction.

Services debated in this context are:

* Machine monitoring

   - Bounded latency: 100ms-10s.

   - Periodic.

   - Time synchronization: 10-1[micro]s.

   - Transmit data size (bytes): 10-10M.

   - Tolerance to packet loss: 0.

   - Node density: 1-30.

* Preventive maintenance

   - Bounded latency: over 100ms.

   - Periodic, once per event.

* Positioning, motion analysis

   - Bounded latency: 50ms-10s.

   - Periodic, once per second.

* Inventory control

   - Bounded latency: 50ms-10s.

   - Periodic, once per second.

* Facility control environment

   - Bounded latency: 1s-50s.

   - Periodic, once per minute.

* Checking status of material, small equipment

   - Bounded latency: 100ms-1s.

   - Sporadic, 1 to 10 times per 30 minutes.

4.4. Display Services

This category of services targets workers, allowing them to receive requested support information. It also targets managers in regards to monitoring of production status and processes. Reasons for wireless integration are: scalability, flexibility of deployment, mobility support. Examples of services are:

* Work commands, e.g., wearable displays
  - Bounded latency: 1-10s.
  - Sporadic, once per 10s-1m.
  - Transmit data size (bytes): 10-6K.
  - Tolerance to packet loss: yes.
  - Node density: 1-30
* Display information
  - Bounded latency: 10s.
  - Sporadic, once per hour.
  - Transmit data size (bytes): 10-6K.
  - Tolerance to packet loss: yes.
  - Node density: 1-30.
* Supporting maintenance (video, audio)
  - Bounded latency: 500ms.
  - Sporadic, once per 100ms.
  - Transmit data size (bytes): 10-6K.
  - Tolerance to packet loss: yes.
  - Node density: 1-30.

4.5. Human Safety Services

Refers to industrial wireless services that concern collecting data to infer about potential dangers to workers in industrial environments. The need for wireless integration concerns: support for pervasive deployment; mobility.

Examples of services are:

* Detection of dangerous situations/operations
  - Bounded latency: 1s.
  - Periodic, 10 per second (10 fps).
  - Transmit data size (bytes): 2-100K.
  - Tolerance to packet loss: yes.

- Node density: 1-50.

* Vital sign monitoring, dangerous behaviour detection

  - Bounded latency: 1s-50s.

  - Periodic, once per minute.

  - Transmit data size (bytes): 2-100K.

  - Tolerance to packet loss: 0.

  - Node density: 1-30.

4.6. Mobile Robotics Services

Refers to services that support the communication between robots, e.g., task sharing; guidance control including data processing, AV, alerts. Reasons to consider wireless integration are: the need to support mobility and reconfigurability.

* Video operated remote control

  - Bounded latency: 10-100ms.

  - Transmit data size (bytes): 15-150K.

  - Tolerance to packet loss: yes.

  - Node density: 2-100.

* Assembly of robots or milling machines

  - Bounded latency: 4-8ms.

  - Transmit data size (bytes): 40-250.

  - Tolerance to packet loss: yes.

  - Node density: 2-100.

* Operation of mobile cranes

  - Bounded latency: 12ms.

  - Periodic, once per 2-5ms.

  - Transmit data size (bytes): 40-250.

  - Tolerance to packet loss: yes.

  - Node density: 2-100.

* Drone/UAV air monitoring

  - Bounded latency: 100ms.

  - Tolerance to packet loss: yes.

4.7. Power Grid Control

Power grid control concerns services that support communication links for predictive maintenance and to isolate faults on high voltage lines, transformers, reactors, etc. Reasons to integrate wireless concern: wire replacement maintenance cost reduction.

* Bounded latency: 1-10ms.

* Transmit data size (bytes): 20-50.

* Time synchronization: IEEE 1588.

* Tolerance to packet loss: yes.

* Node density: 2-100.

4.8. Wireless Avionics Intra-communication

Wireless integration is also relevant to industrial environments in the context of replacing cabling. Within the context of avionics [AVIONICS], _Wireless Avionics Intra-communication (WAIC)_ systems [WAIC] are expected to significantly benefit from determinist communications, given their higher criticality. For instance, flight control systems, integrating a large number of endpoints (sensors and actuators), require high reliability and bounded latency to assist in estimating and controlling the state of the aircraft. Real-time data needs to be delivered with strict deadlines for most control systems.

The WAIC standardization process is still ongoing, without a clear indication about the frequencies that would be reserved for such systems, although the frequency band 4.2 GHz to 4.4 GHz is the one that currently seems most popular. Nevertheless, independently of the allocated frequency bands, the determinisc guarantees required by WAIC services may be achieved by means of the integration of functionality developed in current wireless standards.

However, the following requirements are expected to be supported by wireless technology in order to ensure the deterministic operation of WAIC systems:

* Must provide deterministic behaviour in short radio ranges (< 100m).

* Must use low transmit power levels for low rate (10mW) and high rate (50mW) applications.

* Must ensure good system reconfigurability.

* Must support dissimilar redundancy.

In terms of potential KPIs, specific communication requirements can be identified:

* Latency: 20-40ms [PARK2020].

* Packet payload: small (e.g., 50 bytes) and variable bit rate [PARK2020].

* Support between 125 to 4150 nodes [AVIONICS].

* Maximum distance between transmitter and receiver: 15m [AVIONICS].

* Aggregate average data rate of network (kbit/s): 394 to 18385

[AVIONICS].

- Latency: below 5s for High data rate Inside (HI) applications [AVIONICS].

- Jitter: below 50ms for HI applications [AVIONICS].

As an example of current standards that may support the deterministic requirements of WAIC system, we can point to IEEE 802.11ax, which is being devised to operate between 1 and 7GHz (in addition to 2.4 GHz and 5GHz). The WAIC requirement for high reliability and bounded latency may be supported by 802.11ax capability of dividing the spectrum in frequency resource units (RUs), which are assigned to stations for reception and transmission by a central coordinating entity, the wireless Access Point. Reliability can be achieved by assigning more than one RU to the same station, for instance (an aspect that is not covered by IEEE 802.11ax but already under discussion for IEEE 802.11be). Through the central scheduling of the RUs contention overhead can be avoided, which increases efficiency in scenarios of dense deployments as is the case of WAIC applications. In this context, OFDMA and the concept of spatial reuse is relevant, to assist large-scale simultaneous transmission, while at the same time preventing collision and interference, and guaranteeing high throughput [ROBOTS1].

5. Additional Reliable Wireless Industrial Services

This section provides examples of additional wireless industrial services. We have specifically selected three different examples of such use-cases: i) remote AR/VR for maintenance and control; ii) decentralized shop-floor communication and iii) wireless cabin intra-communications. Based on these examples, wireless integration recommendations are debated and a list of specific requirements is provided.

5.1. AR/VR Services within Flexible Factories

5.1.1. Description

While Video is today integrated both into industrial automation systems, and also used with the shop-floor to assist the worker, the integration of AR/VR in the shop-floor in industrial environments is still in the beginning. It is, however, being applied within the electric industry as a way to improve productivity and safety of workers, also overlaying real-time metadata over equipment under maintenance or operation.

In this context, it is important to ensure that the AR/AV traffic does not interfere with the critical traffic of the production system, i.e., performance characteristics like latency and jitter for the critical traffic shall be independent from disturbances. Moreover, it is also important to provide the AR/VR application with low latency, also in the verge of mobility.

5.1.2. Wireless Integration Recommendations

The support of AR/AV in the context of remote maintenance environments is bound to increase within industrial environments, given the relevancy in terms of remote maintenance and equipment operations. It is also relevant to consider its use within the context of worker safety and it can be foreseen that AV-based remote maintenance will, in the future, be supported via mobile devices carried by workers on the go. Wireless is therefore a key communication asset for this type of applications. In terms of traffic in a converged network, AR/AV is a bandwidth intensive real-time service. It therefore requires specific handling (other than Best Effort, BE). Moreover, the AR/AV traffic flows must not create disturbance when transmitted via wireless. Hence, traffic isolation is an important aspect to ensure for this type of traffic profile.

A third aspect to address in the future concerns the fact that there will most likely be the need to support multiple AR/AV streams from different end-users within a single Wireless Local Area Network (WLAN), thus increasing the need for traffic isolation. A fourth aspect concerns the fact that VR systems, if not adequately support, result in VR sickness. Specific network and non-network requirements have already been identified by IEEE 802, MPEG, 3GPP. Such requirements contemplate, for instance, support of higher frame rates, reducing the motion-to-photon latency, higher data transmission rates, low jitter, etc.

5.1.3. Requirements Considerations

In such applications, to ensure minimum interference, a few aspects need to be ensured:

- The AR/AV traffic needs to be isolated in order to prevent interference, i.e., it SHOULD have a specific CoS assigned (downlink and uplink).

- Between wireless devices (stations) and AP, there is the need to ensure that the AR/AV traffic is handled in a way that does not hinder critical traffic.

- Low mobility SHOULD be supported.

- Multiple user support SHOULD be provided.

- VR sickness MUST be prevented [IEEERTA].

- A tight integration of the AR/VR systems with production systems SHOULD be address in way compatible with the deterministic wired infrastructure. For instance, Audio Video Bridging (AVB) in the wired TSN infrastructure. Specifically, AVB is usually blocked by the time-aware shaper, and impacted by: TAS, CBS, FIFO and FPNS (fixed priority non-preemptive scheduling).

- A software-based mechanism on the AP SHOULD support an adequate mapping of CoS to the wireless QoS (e.g., EDCA UPs).

- MAC layer contention MUST be mitigated for all wireless stations within the area (within the range of the same AP or not).

Specific communication requirements:

- Latency: 3-10ms [IEEERTA].

- Bandwidth, 0.1-2Gbps [IEEERTA].

- Data payload, over 4Kbytes [IEEERTA].

5.2. Decentralized Shop-floor Communication Services

5.2.1. Description

The increasing automation of industrial environments implies an increase in the number of integrated nodes, including mobile nodes. Wireless is, for instance, a key driver for scenarios involving mobile vehicles [NICT]. NICT also describes already production environments, in particular environments with elevated temperatures, where wireless communication is used to support safety of workers and to remotely monitor production status. Such environments comprise different applications (e.g., safety of workers, mobile robots, factory resource management) and debate on the interconnection of different wireless technologies and devices, from PLCs, to autonomous mobile robots, e.g., UAVs, AGVs. Wireless/wired integration mechanisms have also been debated in the cost of self-organizing production lines [DIETRICH2018]. Therefore, the notion of flexible and heterogeneous shop-floor communication is already present in industrial environments, based on hybrid wired/wireless systems and the integration of multi-AP environments.

5.2.2. Wireless Integration Recommendations

Prior related work debates on centralized communication architectures (infrastructure mode), and for this case, the issue of connectivity is usually circumvented via multiple AP coordination mechanisms. Within the context of multi-AP coordination and assuming TDMA-based communication, a well-organized schedule can prevent collisions [FERN2019]. Hence, for this specific type of scenario, the main issue concerns handling handovers in a timely and precise way, capable of providing deterministic guarantees. However, with an increase on the number of nodes on a shop-floor, connectivity issues become more complex.

Therefore, it is relevant to explore also the possibility of a "decentralized" approach to shop-floor communication, considering both mobile and static nodes. In this case, and from a topology perspective, wireless industrial services are expected to be provided over both ad-hoc and infrastructure mode. Within the ad-hoc communication areas, there is control-based traffic integrated with sensing (critical, non-critical), with real-time traffic, as well as time-triggered traffic. Each node is responsible for managing its access to the medium, thus requiring a cooperative protocol approach.

5.2.3. Requirements Considerations

In such environment, connectivity becomes more complex requiring additional support:

* A wider variety of traffic profiles MUST be supported, thus increasing the management complexity.

* Devices communicating via ad-hoc mode MUST integrate a collaborative communication approach, e.g., relaying, cluster-based scheduling approach.

* Low mobility MUST be supported (e.g., up to 2 m/s within a BSS).

* Multi-AP coordination MUST still be integrated.

* Frequent handover MUST be supported, ideally with a make-before-break approach.

* Neighbor detection and coverage problem detection MUST be implemented in ad-hoc nodes.

Specific communication requirements: * Latency: 20-40ms [ROBOTS1]. * Packet payload: small (e.g., 50 bytes) and variable bit rate [ROBOTS1].

5.3. Autonomous Airborne Services

Description

Over the last decade several services emerged that rely on the autonomous (total or partial) operation of airborne systems. Examples of such systems are: logistic drones; swarm of drones (e.g. for surveillance); urban Air Mobility [UAM18]; single Pilot operation of commercial aircrafts [BBN8436].

Such autonomous airborne systems rely on advances in communications, navigation, and air traffic management to mitigate the significant workload of autonomous operations, namely by means of air-ground collaborative decision making. Such decision making processes rely on expanding the role of ground operators, including tactical (re-routing) and emergency flight phases, as well as higher levels of decision support including systems monitoring in real-time.

Such air-ground collaborative decision making process can only be possible with the support of a reliable wireless network able to assist in the required data exchange (of different types of traffic) within significant constraints in terms of delay and error avoidance.

5.3.1. Wireless Integration Recommendations

Independently of the type of application (logistics, surveillance, urban air mobility, single pilot operation), an autonomous airborne system can be models as a multi-agent system, in which agents need to use a wireless network to communicate reliably between them and in possible with a control entity. The nature and position of such agentes differ from application to application. For instance, all agents may be collocated in the same or different flying vehicles.

A high-performance and reliable wireless network has an important role in meeting the challenges of autonomous airborne systems, such as coordination and collaboration strategies, control mechanisms, and mission planning algorithms. Hence, wireless technologies plan a central role in the creation of the needed networking system, including air-to-air communications (single or multi-hop) but air-to-ground communications.

Air-to-air communications allow all airborne agents to establish efficient communication, allowing the reception of error prune data exchanged within the required time frames. For instance, in a swarm drones can either communicate with each other directly, or indirectly by constructing multi-hop communication paths with other drones.

In what concerns air-to-ground communications, airborne agents communicate with a control center, such as a ground station, to obtain real-time updated information (e.g. mission related). Air-to-ground communication is usually direct communication.

The air-to-air and air-to-ground communications are combined through a communication architecture, which can be of different types. In small autonomous systems (single drones used for logistics), a central control station is deployed with enough powerf to communicate with the drone. In autonomous systems with a large number of agents, a decentralized approach should be used.

5.3.2. Requirements Considerations

When analysing the major properties of wireless communication architectures, the first priority should go to requirements of high coverage and maintaining connectivity. The former plays an important role in gathering the information needed for the operation of the autonomous system, while maintaining connectivity ensures the real-time communication within the system.

However, autonomous systems may operate in unknown environments, with the unpredicted appearance of threats and obstacles in time and space. Hence such systems should rely on wireless technology that has a high level of reliability and availability. For instance, wireless technology that is able to keep two neighbour agents connected, even when their direct link drops below the required minimum signal-to-noise ratio (SNR) or receive signal strength indicators (RSSI) range. On a system level, wireless network technologies, such as routing, should be able to react cognitively to changes of the environment to adapt the communication system in order to ensure the needed coverage and connectivity levels.

In this sense it is required the investigation of routing protocols able to ensure the desirable level or reliability and availability of complete system. This means that the wireless routing function should fulfill a set of requirements, including: * Suitable for dynamic topologies. * Scalable with the number of networked agents. * Ensure low values of packet delays (KPI depends upon the specific application). * Ensure high values of packet delivery (KPI depends upon the specific application). * Ensure fast recovery in the presence of interrupted communications. * Ensure low cost in terms of the utilization of network resources (e.g. network queues, transmission opportunities). * Ensure high robustness to link failure.

6. Security Considerations

This document describes industrial application communication requirements for the integration of reliable Wi-Fi technologies. The different applications have security considerations which have been described in the respective sources [IEEERTA], [NICT], [IIC], [AVNU2020], [ACIA].

7. IANA Considerations

This document has no IANA actions.

8. Acknowledgments

The research leading to these results received funding from joint fortiss GmbH and Huawei project TSNWiFi (https://www.fortiss.org/en/research/projects/detail/tsnwifi(https://www.fortiss.org/en/research/projects/detail/tsnwifi))

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997,

<https://www.rfc-editor.org/info/rfc2119>.

9.2. Informative References

[ACIA] 5G ACIA, ., "5G for Connected Industries and Automation", November 2019.

[AVIONICS] Fischione, P.Park, P.Di Marco, J.Nah, and C., "Wireless Avionics Intra-Communications, A Survey of Benefits, Challenges, and Solutions, pp. 1-24", 2020.

[AVNU2020] Bush, S., "Avnu Alliance White Paper Wireless TSN-Definitions, Use Cases & Standards Roadmap", 2020.

[BBN8436] Pew, Deutsch, Stephen, and Richard W., "Single pilot commercial aircraft operation. BBN Report.", 2005.

[DIETRICH2018]
, & Fohler, G, Dietrich, S., May, G., von Hoyningen-Huene, J., Mueller, A., "Frame conversion schemes for cascaded wired/wireless communication networks of factory automation, Mobile Networks and Applications, 23(4), 817-827", 2018.

[FERN2019] Fernández Ganzabal, Z., "Analysis of the Impact of Wireless Mobile Devices in Critical Industrial Applications", May 2019.

[IEEERTA] Meng, K., "IEEE 802.11 Real Time Applications TIG Report", 2018.

[IETFRAW-USECASES]
Bernardos, G.P.P.T.F.T.a.C., "RAW use cases," IETF draft - RAW working group", 2020, <https://datatracker.ietf.org/doc/draft-ietf-raw-use-cases/>.

[IIC] Linehan, M., "Time Sensitive Networks for Flexible Manufacturing Testbed Characterization and Mapping of Converged Traffic Types", 2020.

[NENDICA] Zein, Ed, N., "IEEE 802 Nendica Report, Flexible Factory IoT-Use Cases and Communication Requirements for Wired and Wireless Bridged Networks", 2020.

[NICT] NICT, "Wireless use cases and communication requirements in factories (abridged edition), Flex. Factories Proj", February 2018.

[OPCFLC] "OPC Foundation Field Level Communications (FLC) Initiative", September 2020, <https://opcfoundation.org/flc/>.

[PARK2020] Park, Pangun, et al, ., "Wireless Avionics Intra-Communications, A Survey of Benefits, Challenges, and Solutions. IEEE Internet of Things Journal", 2020.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

[ROBOTS1] Hoebeke, J.Haxhibeqiri, E.A.Jarchlo, I.Moerman, and J., "Flexible Wi-Fi Communication among Mobile Robots in Indoor Industrial Environments, Mob. Inf. Syst.", 2018.

[UAM18] Shamiyeh, Michael, Raoul Rothfeld, and Mirko Hornung, ., "A performance benchmark of recent personal air vehicle concepts for urban air mobility. Proceedings of the 31st Congress of the International Council of the Aeronautical Sciences, Belo Horizonte, Brazil", 2018.

[WAIC] International Telecommunication Union, "Technical characteristics and operational objectives for wireless avionics intra-communications, Policy, vol. 2197, p. 58,".

Authors' Addresses

Rute C. Sofia
fortiss GmbH
Guerickestr. 25
80805 Munich
Germany

Email: sofia@fortiss.org

Matthias Kovatsch
Huawei Technologies
Riesstr. 25 C, 3.0G
80992 Munich
Germany

Email: ietf@kovatsch.net

Paulo Milheiro Mendes
Airbus
Willy-Messerschmitt Strasse 1
81663 Munich
Germany

Email: paulo.mendes@airbus.com