RAW
Internet-Draft
Intended status: Standards Track
Expires: January 12, 2021

G. Papadopoulos
IMT Atlantique
P. Thubert
Cisco
F. Theoleyre
CNRS
CJ. Bernardos
UC3M
July 11, 2020

RAW use cases
draft-bernardos-raw-use-cases-04

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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 12, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
2. Aeronautical Communications 5
2.1. Problem Statement 5
2.2. Specifics 5
2.3. Challenges 6
2.4. The Need for Wireless 7
2.5. Requirements for RAW 7
3. Amusement Parks 7
3.1. Use Case Description 7
3.2. Specifics 8
3.3. The Need for Wireless 8
3.4. Requirements for RAW 9
4. Wireless for Industrial Applications 9
4.1. Use Case Description 9
4.2. Specifics 10
4.2.1. Control Loops 10
4.2.2. Unmeasured Data 10
4.3. The Need for Wireless 11
4.4. Requirements for RAW 11
5. Pro Audio and Video 12
5.1. Use Case Description 12
5.2. Specifics 12
5.2.1. Uninterrupted Stream Playback 12
5.2.2. Synchronized Stream Playback 12
5.3. The Need for Wireless 12
5.4. Requirements for RAW 13
6. Wireless Gaming 13
6.1. Use Case Description 13
6.2. Specifics 14
6.3. The Need for Wireless 14
6.4. Requirements for RAW 14
7. UAV platooning and control 15
7.1. Use Case Description 15
7.2. Specifics 15
7.3. The Need for Wireless 15
7.4. Requirements for RAW 16
8. Edge Robotics control 16
8.1. Use Case Description 16
8.2. Specifics 17

8.3. The Need for Wireless 17
8.4. Requirements for RAW 17
9. Emergencies: Instrumented emergency vehicle 17
9.1. Use Case Description 17
9.2. Specifics 18
9.3. The Need for Wireless 18
9.4. Requirements for RAW 18
10. IANA Considerations 19
11. Security Considerations 19
12. Acknowledgments 19
13. Informative References 19
Authors' Addresses 22

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:

- o time synchronization on all the nodes,
- o centralized computation of network-wide deterministic paths,
- o multi-technology path with co-channel interference minimization,
- o frame preemption and guard time mechanisms to ensure a worst-case delay, and
- o 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

Worldwide civil air traffic is expected to grow by 84% until 2040 compared to 2017 [EURO20]. 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.maeurer-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.

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

- o 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:

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

- o 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.

- o 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].

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

- o 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:

- o 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].

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

- o 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:

- o Virtual Reality / Augmented Reality (VR/AR)

- o 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:

- o Intra BSS latency: less than 5 ms.
- o Jitter variance: less than 2 ms.
- o 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

- o 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.
- o 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.
- o 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.
- o 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.
- o 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:

- o vital signs sensors attached to the casualty in the ambulance. Relay medical data to hospital emergency room,
- o radionavigation sensor to relay position data to various destinations including dispatcher,
- o voice communication for ambulance attendant (e.g. consult with ER doctor),
- o voice communication between driver and dispatcher,
- o 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:

- o A dispatching system,
- o a cellphone for the attendant,
- o a special purpose telemetering system for medical data,
- o 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:

- o High availability of the internetwork is required.
- o 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.
- o 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.
- o 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

[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>.

[EURO20] EUROCONTROL, "EUROCONTROL's Challenges of Growth 2018 Study Report", 2018, <https://www.eurocontrol.int/sites/default/files/content/documents/officialdocuments/reports/challenges-of-growth-2018.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-28 (work in progress), October 2019.

[I-D.ietf-detnet-security] Mizrahi, T. and E. Grossman, "Deterministic Networking (DetNet) Security Considerations", draft-ietf-detnet-security-10 (work in progress), May 2020.

[I-D.maeurer-raw-ldacs] Maeurer, N., Graeupl, T., and C. Schmitt, "L-band Digital Aeronautical Communications System (LDACS)", draft-maeurer-raw-ldacs-04 (work in progress), July 2020.

[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.

[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
Internet-Draft
Intended status: Informational
Expires: 10 September 2020

J. Farkas, Ed.
T. Dudda
A. Shapin
S. Sandberg
Ericsson

9 March 2020

5G - Ultra-Reliable Wireless Technology with Low Latency
draft-farkas-5g-raw-00

Abstract

This document describes the features of 5G that make it a wireless technology providing ultra-reliability, high availability, and low latency; and looks out to possibilities on the application of 5G together with IETF Deterministic Networking (DetNet).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 10 September 2020.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Provenance and Documents 2
3. General Characteristics 4
4. Deployment and Spectrum 5
5. Applicability to Deterministic Flows 6
5.1. System Architecture 6
5.2. Overview of The Radio Protocol Stack 8
5.3. Radio (PHY) 9
5.4. Scheduling and QoS (MAC) 10
5.5. Time-Sensitive Networking (TSN) Integration 12
6. Summary 16
7. IANA Considerations 17
8. Security Considerations 17
9. Acknowledgments 17
10. Informative References 17
Authors' Addresses 19

1. Introduction

5G is a highly predictable scheduled wireless technology. Equipped with Ultra-Reliable Low-Latency Communication (URLLC) features, 5G provides ultra reliability and high availability as well as low latency for critical communications. That is, 5G is a Reliable Available Wireless (RAW) technology. Its characteristics make 5G perfectly suitable to be part of deterministic networks, e.g., industrial automation networks. Furthermore, 5G already includes features and capabilities for integration with deterministic wireline technologies such as IEEE 802.1 Time-Sensitive Networking (TSN) [IEEE802.1TSN] and IETF Deterministic Networking (DetNet) [RFC8655].

2. 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 1. 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 1: 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].

3. 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.

4. 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.

5. Applicability to Deterministic Flows

5.1. 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 2.

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 2: 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.

5.2. 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.

5.3. 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.

5.4. 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.

5.5. 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 2 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 3: 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 5. 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 4: Reliability with Single UE

An alternative solution is that multiple UEs per device are used for user plane redundancy as illustrated in Figure 5. 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 5: 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. 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. IANA Considerations

This document does not require IANA action.

8. Security Considerations

5G includes security mechanisms as defined by 3GPP.

9. Acknowledgments

The authors acknowledge the work of all from Ericsson Research who contributed to the subject in any form.

10. Informative References

[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-02, 6 March 2020, <https://tools.ietf.org/html/draft-ietf-detnet-ip-over-tsn-02>.

[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>.

Authors' Addresses

Janos Farkas (editor)
Ericsson
Budapest
Magyar tudosok korutja 11
1117
Hungary

Email: janos.farkas@ericsson.com

Torsten Dudda
Ericsson
Ericsson Allee 1
52134 Herzogenrath
Germany

Email: torsten.dudda@ericsson.com

Alexey Shapin
Ericsson
Laboratoriegrand 11
SE-977 53 Lulea
Sweden

Email: alexey.shapin@ericsson.com

Sara Sandberg
Ericsson
Laboratoriegrand 11

SE-977 53 Lulea
Sweden

Email: sara.sandberg@ericsson.com

RAW
Internet-Draft
Intended status: Informational
Expires: 5 April 2021

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

2 October 2020

L-band Digital Aeronautical Communications System (LDACS)
draft-maeurer-raw-ldacs-06

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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 5 April 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights

and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Motivation and Use Cases 5
3.1. Voice Communications Today 5
3.2. Data Communications Today 6
4. Provenance and Documents 7
5. Applicability 8
5.1. Advances Beyond the State-of-the-Art 8
5.1.1. Priorities 8
5.1.2. Security 8
5.1.3. High Data Rates 9
5.2. Application 9
5.2.1. Air-to-Ground Multilink 9
5.2.2. Air-to-Air Extension for LDACS 9
5.2.3. Flight Guidance 10
5.2.4. Business Communication of Airlines 11
5.2.5. LDACS Navigation 11
6. Requirements to LDACS 12
7. Characteristics of LDACS 15
7.1. LDACS Sub-Network 16
7.2. Topology 16
7.3. LDACS Physical Layer 17
7.4. LDACS Data Link Layer 17
7.5. LDACS Mobility 17
8. Reliability and Availability 18
8.1. Layer 2 18
8.2. Beyond Layer 2 20
9. Protocol Stack 21
9.1. Medium Access Control (MAC) Entity Services 22
9.2. Data Link Service (DLS) Entity Services 24
9.3. Voice Interface (VI) Services 25
9.4. LDACS Management Entity (LME) Services 25
9.5. Sub-Network Protocol (SNP) Services 25
10. Security Considerations 25
10.1. Reasons for Wireless Digital Aeronautical Communications 25
10.2. Requirements for LDACS 26
10.3. Security Objectives for LDACS 27
10.4. Security Functions for LDACS 27
10.5. Security Architectural Details for LDACS 28
10.5.1. Entities in LDACS Security Model 28

10.5.2. Matter of LDACS Entity Identification 28
10.5.3. Matter of LDACS Entity Authentication and Key Negotiation 29
10.5.4. Matter of LDACS Message-in-transit Confidentiality, Integrity and Authenticity 29
10.6. Security Architecture for LDACS 30
11. Privacy Considerations 30
12. IANA Considerations 30
13. Acknowledgements 30
14. Normative References 30
15. Informative References 31
Authors' Addresses 34

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.

2. Terminology

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

A2A Air-to-Air
LDACS A2A LDACS 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
FAA Federal Aviation Administration
FCI Future Communication Infrastructure
FDD Frequency Division Duplex
FL Forward Link
GANP Global Air Navigation Plan
GNSS Global Navigation Satellite System
GS Ground Station
GSC Ground-Station Controller
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 Layer
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
PDU Protocol Data Units
PHY Physical Layer
QoS Quality of Service
RL Reverse Link

SARPs Standards And Recommended Practices
SDR Software Defined Radio
SESAR Single European Sky ATM Research
SF Super-Frame
SNP Sub-Network Protocol
SSB-AM Single Side-Band Amplitude Modulation
TBO Trajectory-Based Operations
TDM Time Division Multiplexing
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 (SSB-AM) 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 Aeronautical Mobile Airport Communication System (AeroMACS; as of now not widely used) 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 (TBO) 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 (GANP).

4. 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 [RIH2018]. 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 [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 (SARPs) document [ICA2018]. 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 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 Aeronautical Operational Control (AOC) communications services from deployed Ground Stations (GS). The LDACS A2G sub-system physical layer and data link layer 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 Navigation 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 (Ground-to-Air), and 294 kbit/s to 1390 kbit/s on the reverse link (Air-to-Ground), 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 Future Communication Infrastructure (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 SESAR.

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 Air-to-Air (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 airborne 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 Global Navigation Satellite System (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 ground stations 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 OSI internetwork 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 Open Systems Interconnection (OSI) stack. The objective of the development effort LDACS is part of (FCI) is to replace legacy (OSI) 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 e.g. VoIP) 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.

The upcoming Figures Figure 1 and Figure 2 summarize the main seetings based on volume 1 Table 5-14, and Table 6-13 defined in [DO350A]. In a similar vein, requirements to fault management are defined in the same tables.

	ECP 130		RCP 240		RCP 400	
Parameter	ET	TT_95%	ET	TT_95%	ET	TT_95%
Transaction Time (Sec)	130	67	240	210	400	350
Continuity	0.999	0.95	0.999	0.95	0.999	0.95
Availability	0.989		0.989 (safety) 0.9899 (efficiency)		0.989	
Integrity	1E-5 per FH		1E-5 per FH		1E-5 per FH	
RCP Monitoring and Alerting Criteria						
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.					

Figure 1: Requirements for CPDLC

	RSP 160		RSP 180		RSP 400	
Parameter	OT	DT 95%	OT	DT 95%	OT	DT 95%
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 (safety) 0.9899 (efficiency)		0.989	
Integrity	1E-5 per FH		1E-5 per FH		1E-5 per FH	
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.					

Figure 2: Requirements for ADS-C

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), a Ground-Station Controller (GSC), and several Ground-Stations (GS), each of them providing one LDACS radio cell.

User plane interconnection to the ATN is facilitated by the Access Router (AR) peering with an Air-to-Ground Router (A2G Router) connected to the ATN. It is up to implementer's choice to keep Access Router and Air-Ground Router functions separated, or to merge them.

The internal control plane of an LDACS sub-network is managed by the GSC. An LDACS sub-network is illustrated in Figure 3.

```
wireless      user
link          plane
  A--------------G-------------Access---A2G-----ATN
  S..............S             Router   Router
                 . control      . |
                 . plane        . |
                 .              . |
                 GSC.............|
                 .               |
                 .               |
                 GS---------------+
```

Figure 3: LDACS sub-network with two 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 ground stations themselves are connected to a GSC controlling the LDACS sub-network.

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 forward link direction (FL; G2A) and the reverse link direction (RL; A2G) 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 Orthogonal Frequency-Division Multiplexing (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.

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 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 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 ground-stations connected to the same GSC.

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 FDD system, supporting simultaneous transmissions in Forward Link (FL; G2A) and Reverse Link (RL; A2G). 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 users (ASs) on demand by the ground station (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 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 QoS in LDACS medium access is to provide prioritized medium access at the bottleneck (the wireless link). The signaling of higher layer QoS 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 forward link, this is done locally in the GS, on the reverse link a dedicated contention-free control channel is used called 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); variably sized). Due to the spacing of the reverse link 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 ground-station, 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 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 GS.

In addition to having full control over resource scheduling, the GS can send forced Handover (HO) 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 SatCom) 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 system by ICAO.

9. Protocol Stack

The protocol stack of LDACS is implemented in the AS, GS, and GSC: 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), (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 4 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 FDD
```

Figure 4: LDACS protocol stack in AS and GS

9.1. Medium Access Control (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 reverse link 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 5 and Figure 6 illustrates 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 5: LDACS super-frame structure

```
   ^
   |     +-------------+------+-------------+
   |  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 6: LDACS multi-frame (MF) structure

9.2. Data Link Service (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 data link service, 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 data link service uses the logical channels provided by the MAC:

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

9.3. Voice Interface (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. LDACS Management Entity (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. It is controlled by the network management service in the GSC.

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

9.5. Sub-Network Protocol (SNP) Services

The data link service 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 ground station controller.

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. First of all civil applications have significant lower spectrum available than military applications. This means several military defense

mechanisms such as frequency hopping or pilot symbol scrambling and thus a defense-in-depth approach starting at the physical layer is impossible for civil systems. With the rise of cheap Software Defined Radios (SDR), 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. Furthermore most CNS technology developed in ICAO relies on open standards, thus syntax and semantics of wireless digital aeronautical communications can be common knowledge for attackers. Finally 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. However, 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. Requirements for LDACS

Overall there are several business goals for cybersecurity to protect in future communication infrastructure 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. Security Objectives for LDACS

Security considerations for LDACS are defined by the official ICAO SARPS [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. Security Functions for LDACS

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 now we must look at the scope of the applicability of these functions.

10.5. Security Architectural Details for LDACS

With requirements out of the way, we want to have a look at the scope of the LDACS security model. This includes looking at the entities, identification, authentication and authorization of entities, integrity, authenticity and confidentiality of data in-transit and more.

10.5.1. Entities in LDACS Security Model

First of all the question is what entities do we have in a simplified LDACS architectural model: 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) Ground Station Controller (GSC) and spanning a local LDACS Access Network connecting to the (7) Ground Stations (GS) that serve one LDACS cell. Via the (8) A2G wireless LDACS data link (9) Airborne Stations (AS) the aircraft is connected to the ground network and via the (10) airborne voice interface and (11) airborne network interface, airborne 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. Matter of LDACS Entity Identification

Each entity described in the sections above must be uniquely identified within the LDACS network thus we need LDACS specific identities for (1) the Aircraft Station (AS), (2) Ground Station (GS), (3) Ground Station Controller (GSC) and (4) Network Operator (NO). 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. And again similar to 4G’s Mobility Management Entities (MME), a GSC could be identified using similar identification fields within the LDACS network. The identification of the network operator is again similar to 4G (e.g., E-Plus, AT&T, TELUS, ...), in the way that the aeronautical network operators are listed (e.g., ARINC [ARI2020] and SITA [SIT2020]).

10.5.3. Matter of LDACS 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 aircraft with the LDACS radio (AS) approaches an LDACS cell and performs a cell entry with the corresponding groundstation (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. Thus 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 AS-GS can be opened for user-data communications.

10.5.4. Matter of LDACS 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. Security Architecture for LDACS

Summing up all previous paragraphs, a draft of the cybersecurity architecture of LDACS can be found in [ICA2018], [MAE20182] and updates in [MAE20191], [MAE20192], [MAE2020]. It proposes the use of an own LDACS PKI, identity management based on aircraft identities and network operator identities (e.g., SITA and ARINC), public key certificates incorporated in the PKI based chain-of-trust and stored in the entities allowing for mutual authentication and key exchange procedures, key derivation mechanisms for perfect forward secrecy and user/control plane message-in-transit integrity and confidentiality protection. This secures data traveling over the airgap between aircraft and groundstation and also between groundstation and Air Navigation Service Provider regardless of the secure or unsecure nature of application data. Of course application data itself must be additionally secured to achieve end-to-end security (secure dialogue service), however the LDACS datalinks aims to provide an additional layer of protection just for this network segment.

11. Privacy Considerations

LDACS provides a Quality of Service (QoS), 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>.

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>.

[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>.

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: 25 April 2020

P. Thubert, Ed.
Cisco Systems
G.Z. Papadopoulos
IMT Atlantique
23 October 2019

Reliable and Available Wireless Problem Statement
draft-pthubert-raw-problem-statement-04

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 forwarded 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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 25 April 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
2. Terminology 4
3. Use Cases and Requirements Served 5
4. Routing Time Scale vs. Forwarding Time Scale 5
5. Prerequisites 7
6. Related Work at The IETF 7
7. Problem Statement 8
8. Security Considerations 9
9. IANA Considerations 9
10. References 9
10.1. Normative References 9
10.2. Informative References 10
Authors' Addresses 11

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, adds another dimension to the statistical effects that affect the delivery. Scheduling transmissions can alleviate those effects by leveraging diversity in the spatial, time, code, and frequency domains, and provide a Reliable and Available service while preserving energy and optimizing the use of the shared spectrum.

Deterministic Networking is an attempt to mostly eliminate packet loss for a committed bandwidth with a guaranteed worst-case end-to-end latency, even when co-existing with best-effort traffic in a shared network. This innovation is enabled by recent developments in

technologies including IEEE 802.1 TSN (for Ethernet LANs) and IETF DetNet (for wired IP networks). It is getting traction in various industries including manufacturing, online gaming, professional A/V, cellular radio and others, making possible many cost and performance optimizations.

The DetNet architecture [DetNet-ARCH] is composed of three planes: a (User)Application Plane, a Controller Plane, and a Network Plane. Reliable and Available Wireless (RAW) extends DetNet to focus on issues that are mostly a concern on wireless links, and inherits the architecture and the planes. A RAW Network Plane is thus a Network Plane inherited by RAW from DetNet.

RAW networking aims at providing highly available and reliable end-to-end performances in a network with scheduled wireless segments. Uncontrolled interference and transmission obstacles may impede the transmission, and techniques such as beamforming with Multi-User MIMO can only alleviate some of those issues, so the term "deterministic" is usually not associated with short range radios, in particular in the ISM band. This uncertainty places limits to the amount of traffic that can be transmitted on a link while conforming to a RAW Service Level Agreement (SLA) that may vary rapidly.

The wireless and wired media are fundamentally different at the physical level, and while the generic Problem Statement for DetNet applies to the wired as well as the wireless medium, the methods to achieve RAW will differ from those used to support time-sensitive networking over wires, as a RAW solution will need to address less consistent transmissions, energy conservation and shared spectrum efficiency.

The development of RAW technologies has been lagging behind deterministic efforts for wired systems both at the IEEE and the IETF. But recent efforts at the IEEE and 3GPP indicate that wireless is finally catching up at the lower layer and that it is now possible for the IETF to extend DetNet for wireless segments that are capable of scheduled wireless transmissions.

The intent for RAW is to provide 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.

Still, in order to focus on real-worlds issues and assert the feasibility of the proposed capabilities, RAW will focus 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.

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 at the forwarding time scale on one DetNet flow over one path that is preestablished and installed by means outside of the scope of RAW. The scope of the RAW WG comprises Network plane protocol elements such as OAM and in-band control to improve the RAW operation at the Service and at the forwarding sub-layers, e.g., controlling whether to use packet replication, Hybrid ARQ and coding, with a constraint to limit the use of redundancy when it is really needed, e.g., when a spike of loss is observed. This is discussed in more details in Section 4 and the next sections.

2. Terminology

RAW reuses terminology defined for DetNet in [DetNet-ARCH], e.g., PREOF for Packet Replication, Elimination and Ordering Functions.

RAW also reuses terminology defined for 6TiSCH in [6TiSCH-ARCH] such as Track. 6TiSCH defined the term Track for that complex path with associated PAREO operations.

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 wireles connectivity is interrupted for short transient times, typically of a subsecond duration.

This document reuses terms that are well-defined in the context of automation to networking and packet delivery, in particular for reliability and availability. In the context of the RAW work, they 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).

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).

3. Use Cases and Requirements Served

[RFC8578] presents a number of wireless use cases including Wireless for Industrial Applications. [RAW-USE-CASES] adds a number of use cases that demonstrate the need for RAW capabilities in Pro-Audio, gaming and robotics.

4. Routing Time Scale vs. Forwarding Time Scale

With DetNet, the end-to-end routing can be centralized and can reside outside the network. In wireless, and in particular in a wireless mesh, the path to the controller that performs the route computation and maintenance expensive in terms of critical resources such as air time and energy.

Reaching to the routing computation can also be slow in regards to the speed of events that affect the forwarding operation at the radio layer. Due to the cost and latency to perform a route computation, 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 operational metrics that aggregate the behavior of a link over long periods of time, and represent its availability as shades of gray as opposed to either up or down.

```
                    +----------------+
                    |  Controller    |
                    |    (PCE)       |
                    |  [Routing ]    |
                    |  [Function]    |
                    +----------------+
                            ^
                            |
                          Slow
                            |
      _-._-._-._-._-._-.    |  ._-._-._-._-._-._-._-._-._-._-._-._-
    _-._-._-._-._-._-._-.   | _-._-._-._-._-._-._-._-._-._-._-._-
                            |
                        Expensive
                     ....   |  .......
                 ....    .  | .       .....
              ....          v            ...
           ..   A-------B-------C---D     ..
        ...    /  \   /       /      \     ..
      .      I ----M-------N--zzz-- E  ..
      ..      \      \   /         /     .
        ..     P--zzz--Q----------R   ..
          ..                          ..
            .......               ...
                   ...............
     zzz = flapping now
```

Figure 1: 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 such a 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 forwarding plane to make the per-packet decision of which of these possibilities should be used.

In the case of wires, the concept is known in traffic engineering where 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 controler 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 packet speed, and uses information that must be pertinent at the present time for the current transmission.

5. Prerequisites

A prerequisite to the RAW work 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. For 6TiSCH, this is a Track. The concept of Track is specified in the 6TiSCH Architecture [6TiSCH-ARCH]. Tracks provide a high degree of redundancy and diversity and enable DetNet PREOF, end-to-end network coding, and possibly radio-specific abstracted techniques such as ARQ, overhearing, frequency diversity, time slotting, and possibly others.

How the routing operation 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 service 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 forwarding decision (think DLEP from MANET). In the layered approach, how the radio manages its PHY layer is out of control and out of scope. Whether it is single hop or meshed is also unknown and out of scope.

6. 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.

* Operations, Administration and Maintenance (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.

7. Problem Statement

Within a large routed topology, the routing 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 forwarding 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 will consider existing tools such as L2-triggers, DLEP, BFD and in-band and out-of-band OAM.

One possible way of making the RAW forwarding decisions is to make them all at the ingress and express them in-band in the packet, which requires new loose or strict Hop-by-hop signaling. To control the RAW forwarding operation along a Track for the individual packets, RAW may leverage and extend known techniques such as DetNet tagging, Segment Routing (SRv6) or BIER-TE such as done with [BIER-PREF].

An alternate way is to enable each forwarding node to make 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 within the Track. Information about the service should be placed in the packet and matched with the forwarding node's capabilities and policies.

In either case, a per-flow state is installed in all intermediate nodes to recognize the flow and determine the forwarding policy to be applied.

8. Security Considerations

This document is a problem statement and does not propose a solution that could yield security issues.

9. IANA Considerations

This document has no IANA actions.

10. References

10.1. Normative References

[6TiSCH-ARCH]
Thubert, P., "An Architecture for IPv6 over the TSCH mode of IEEE 802.15.4", Work in Progress, Internet-Draft, draft-ietf-6tisch-architecture-27, 18 October 2019, <https://tools.ietf.org/html/draft-ietf-6tisch-architecture-27>.

[DetNet-ARCH]
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>.

[RAW-TECHNOS]
Thubert, P., Cavalcanti, D., Vilajosana, X., and C.

Schmitt, "Reliable and Available Wireless Technologies", Work in Progress, Internet-Draft, draft-thubert-raw-technologies-03, 1 July 2019, <https://tools.ietf.org/html/draft-thubert-raw-technologies-03>.

[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-00, 5 July 2019, <https://tools.ietf.org/html/draft-bernardos-raw-use-cases-00>.

[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>.

[RFC8578] Grossman, E., Ed., "Deterministic Networking Use Cases", RFC 8578, DOI 10.17487/RFC8578, May 2019, <https://www.rfc-editor.org/info/rfc8578>.

10.2. Informative References

[BFD] IETF, "Bidirectional Forwarding Detection", October 2019, <https://dataTracker.ietf.org/doc/charter-ietf-bfd/>.

[BIER] IETF, "Bit Indexed Explicit Replication", October 2019, <https://dataTracker.ietf.org/doc/charter-ietf-bier/>.

[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>.

[CCAMP] IETF, "Common Control and Measurement Plane", October 2019, <https://dataTracker.ietf.org/doc/charter-ietf-ccamp/>.

[DetNet] IETF, "Deterministic Networking", October 2019, <https://dataTracker.ietf.org/doc/charter-ietf-detnet/>.

[DetNet-DP-FW]
Varga, B., Farkas, J., Berger, L., Fedyk, D., Malis, A., Bryant, S., and J. Korhonen, "DetNet Data Plane

Framework", Work in Progress, Internet-Draft, draft-ietf-detnet-data-plane-framework-02, 13 September 2019, <https://tools.ietf.org/html/draft-ietf-detnet-data-plane-framework-02>.

[DetNet-IP-OAM]
Mirsky, G. and M. Chen, "Operations, Administration and Maintenance (OAM) for Deterministic Networks (DetNet) with IP Data Plane", Work in Progress, Internet-Draft, draft-mirsky-detnet-ip-oam-00, 8 July 2019, <https://tools.ietf.org/html/draft-mirsky-detnet-ip-oam-00>.

[MANET] IETF, "Mobile Ad hoc Networking", October 2019, <https://dataTracker.ietf.org/doc/charter-ietf-manet/>.

[SPRING] IETF, "Source Packet Routing in Networking", October 2019, <https://dataTracker.ietf.org/doc/charter-ietf-spring/>.

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

RAW
Internet-Draft
Intended status: Standards Track
Expires: May 6, 2020

F. Theoleyre
CNRS
G. Papadopoulos
IMT Atlantique

November 3, 2019

Operations, Administration and Maintenance (OAM) features for RAW
draft-theoleyre-raw-oam-support-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 some of these use-cases.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on May 6, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of

the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 2
1.1. Terminology 3
2. Needs for OAM in RAW 3
3. Operation 4
3.1. Connectivity Verification 4
3.2. Route Tracing 4
3.3. Fault verification / detection 4
3.4. Fault isolation / identification 5
4. Administration 5
4.1. Worst-case metrics 6
4.2. Energy efficiency constraint 6
5. Maintenance 6
5.1. Multipath 7
5.2. Replication / Elimination 7
5.3. Resource Reservation 7
5.4. Soft transition after reconfiguration 7
6. Informative References 8
Authors' Addresses 8

1. Introduction

Reliable and Available Wireless (RAW) is an effort that extends DetNet to approach end-to-end deterministic performances over a network that includes scheduled wireless segments. The wireless and wired media are fundamentally different at the physical level. Enabling thus reliable and available wireless communications is even more challenging than it is in wired IP networks, due to the numerous causes of loss in transmission that add up to the congestion losses and the delays caused by overbooked shared resources. To provide quality of service along a multihop path that is composed of wired and wireless hops, additional methods needs to be considered to leverage the potential lossy wireless communication.

Traceability belongs to Operations, Administration, and Maintenance (OAM) which is the toolset for fault detection and isolation, and for performance measurement. More can be found on OAM Tools in [RFC7276].

The main purpose of this document is to detail the requirements of the OAM features recommended to construct a predictable communication infrastructure on top of a collection of wireless segments. This document describes the benefits, problems, and trade-offs for using OAM in wireless networks to provide availability and predictability.

In this document, the term OAM will be used according to its definition specified in [RFC6291]. We expect to implement an OAM framework in RAW networks to maintain a real-time view of the network infrastructure, and its ability to respect the Service Level Agreements (SLA), such as delay and reliability, assigned to each data flow.

1.1. Terminology

- o OAM entity: a data flow to be controlled;
- o OAM end-devices: the source or destination of a data flow;
- o defect: a temporary change in the network characteristics (e.g. link quality degradation because of temporary external interference, a mobile obstacle)
- o fault: a definite change which may affect the network performance, e.g. a node runs out of energy,

2. Needs for OAM in RAW

RAW networks expect to make the communications reliable and predictable on top of a wireless network infrastructure. Most critical applications will define a SLA to respect for the data flows it generates. RAW considers network plane protocol elements such as OAM to improve the RAW operation at the service and at the forwarding sub-layers.

To respect strict guarantees, RAW relies on a Path Computation Element (PCE) which will be responsible to schedule the transmissions in the deployed network. Thus, resources have to be provisioned a priori to handle any defect. OAM represents the core of the over provisioning process, and maintains the network operational by updating the schedule dynamically.

Fault-tolerance also assumes that multiple path have to be provisioned so that an end-to-end circuit keeps on existing whatever the conditions. OAM is in charge of controlling the replication/ elimination processes.

To be energy-efficient, reserving some dedicated out-of-band resources for OAM seems idealistic, and only in-band solutions are considered here.

RAW supports both proactive and on-demand troubleshooting.

3. Operation

OAM features will enable RAW with robust operation both for forwarding and routing purposes.

3.1. Connectivity Verification

We need to verify that two endpoints are connected with each other. Since we reserve resources along the path independently for each flow, we must be able to verify that the path exists for a given flow label.

The control and data packets may not follow the same path, and the connectivity verification has to be triggered in-band without impacting the data traffic. In particular, the control plane may work while the data plane may be broken.

The ping packets must be labeled in the same way as the data packets of the flow to monitor.

3.2. Route Tracing

Ping and traceroute are two very common tools for diagnostic. They help to identify the list of routers in the route. However, to be predictable, resources are reserved per flow in RAW. Thus, we need to define route tracing tools able to track the route for a specific flow.

Because the network has to be fault-tolerant, multipath can be considered, with multiple Maintenance Intermediate Endpoints for each hop in the path. Thus, all the possible paths between two maintenance endpoints should be retrieved.

3.3. Fault verification / detection

RAW expects to operate fault-tolerant networks. Thus, we need mechanisms able to detect faults, before they impact the network performance.

The network has to detect when a fault occurred, i.e. the network has deviated from its expected behavior. While the network must report an alarm, the cause may not be identified precisely. For instance, the end-to-end reliability has decreased significantly, or a buffer overflow occurs.

We have to minimize the amount of statistics / measurements to exchange:

- o energy efficiency: low-power devices have to limit the volume of monitoring information since every bit consumes energy.

- o bandwidth: wireless networks exhibit a bandwidth significantly lower than wired, best-effort networks.

- o per-packet cost: is is often more expensive to send several packets instead of combining them in a single link-layer frame.

Thus, localized and centralized mechanisms have to be combined together, and additional control packets have to be triggered only after a fault detection.

3.4. Fault isolation / identification

The network has isolated and identified the cause of the fault. For instance, the quality of a specific link has decreased, requiring more retransmissions, or the level of external interference has locally increased.

4. Administration

To take proper decisions, the network has to expose a collection of metrics, including:

- o Packet losses: the time-window average and maximum values of the number of packet losses has to be measured. Many critical applications stop to work if a few consecutive packets are dropped;

- o Received Signal Strength Indicator (RSSI) is a very common metric in wireless to denote the link quality. The radio chipset is in charge of translating a received signal strength into a normalized quality indicator;

- o Delay: the time elapsed between a packet generation / enqueuing and its reception by the next hop;

- o Buffer occupancy: the number of packets present in the buffer, for each of the existing flows.

These metrics should be collected:

- o per virtual circuit to measure the end-to-end performance for a given flow. Each of the paths has to be isolated in multipath strategies;

- o per radio channel to measure e.g. the level of external interference, and to be able to apply counter-measures (e.g. blacklisting)

- o per device to detect misbehaving node, when it relays the packets of several flows.

4.1. Worst-case metrics

RAW aims to enable real-time communications on top of an heterogeneous architecture. Since wireless networks are known to be lossy, RAW has to implement strategies to improve the reliability on top of unreliable links. Hybrid Automatic Repeat reQuest (ARQ) has typically to enable retransmissions based on the end-to-end reliability and latency requirements.

To take correct decisions, the controller needs to know the distribution of packet losses for each flow, and for each hop of the paths. In other words, average end-to-end statistics are not enough. They must allow the controller to predict the worst-case.

4.2. Energy efficiency constraint

RAW targets also low-power wireless networks, where energy represents a key constraint. Thus, we have to cake care of the energy and bandwidth consumption. The following techniques aim to reduce the cost of such maintenance:

piggybacking: some control information are inserted in the data packets if they do not fragment the packet (i.e. the MTU is not exceeded). Information Elements represent a standardized way to handle such information;

flags/fields: we have to set-up flags in the packets to monitor to be able to monitor the forwarding process accurately. A sequence number field may help to detect packet losses. Similarly, path inference tools such as [ipath] insert additional information in the headers to identify the path followed by a packet a posteriori.

5. Maintenance

RAW needs to implement a self-healing and self-optimization approach. The network must continuously retrieve the state of the network, to judge about the relevance of a reconfiguration, quantifying:

the cost of the sub-optimality: resources may not be used optimally (e.g. a better path exists);

the reconfiguration cost: the controller needs to trigger some reconfigurations. For this transient period, resources may be twice reserved, and control packets have to be transmitted.

Thus, reconfiguration may only be triggered if the gain is significant.

5.1. Multipath

To be fault-tolerant, several paths can be reserved between two maintenance endpoints. They must be node-disjoint, so that a path can be available at any time.

5.2. Replication / Elimination

When multiple paths are reserved between two maintenance endpoints, they may decide to replicate the packets to introduce redundancy, and thus to alleviate transmission errors and collisions. For instance, in Figure 1, the source node S is transmitting the packet to both parents, nodes A and B. Each maintenance endpoint will decide to trigger the replication / elimination process when a set of metrics passes through a threshold value.

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

Figure 1: Packet Replication: S transmits twice the same data packet, to its DP (A) and to its AP (B).

5.3. Resource Reservation

Because the QoS criteria associated to a path may degrade, the network has to provision additional resources along the path. We need to provide mechanisms to patch a schedule (changing the channel offset, allocating more timeslots, changing the path, etc.).

5.4. Soft transition after reconfiguration

Since RAW expects to support real-time flows, we have to support soft-reconfiguration, where the novel ressources are reserved before the ancient ones are released. Some mechanisms have to be proposed so that packets are forwarded through the novel track only when the

resources are ready to be used, while maintaining the global state consistent (no packet re-ordering, duplication, etc.)

6. Informative References

[ipath] Gao, Y., Dong, W., Chen, C., Bu, J., Wu, W., and X. Liu, "iPath: path inference in wireless sensor networks.", 2016, <https://doi.org/10.1109/TNET.2014.2371459>.

[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>.

Authors' Addresses

Fabrice Theoleyre
CNRS
Building B
300 boulevard Sebastien Brant - CS 10413
Illkirch - Strasbourg 67400
FRANCE

Phone: +33 368 85 45 33
Email: theoleyre@unistra.fr
URI: http://www.theoleyre.eu

Georgios Z. Papadopoulos
IMT Atlantique
Office B00 - 102A
2 Rue de la Chataigneraie
Cesson-Sevigne - Rennes 35510
FRANCE

Phone: +33 299 12 70 04
Email: georgios.papadopoulos@imt-atlantique.fr

RAW
Internet-Draft
Intended status: Standards Track
Expires: April 28, 2021

F. Theoleyre
CNRS
G. Papadopoulos
IMT Atlantique
G. Mirsky
ZTE Corp.

October 25, 2020

Operations, Administration and Maintenance (OAM) features for RAW
draft-theoleyre-raw-oam-support-04

Abstract

Some critical applications may use a wireless infrastructure. However, wireless networks exhibit a bandwidth of several orders of magnitude lower than wired networks. Besides, wireless transmissions are lossy by nature; the probability that a packet cannot be decoded correctly by the receiver may be quite high. In these conditions, guaranteeing the network infrastructure works properly is particularly challenging, since we need to address some issues specific to wireless networks. This document lists the requirements of the Operation, Administration, and Maintenance (OAM) features recommended to construct a predictable communication infrastructure on top of a collection of wireless segments. This document describes the benefits, problems, and trade-offs for using OAM in wireless networks to achieve Service Level Objectives (SLO).

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on April 28, 2021.

Copyright Notice

Copyright (c) 2020 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
  1.1. Terminology 4
  1.2. Acronyms 5
  1.3. Requirements Language 5
2. Role of OAM in RAW 5
  2.1. Link concept and quality 6
  2.2. Broadcast Transmissions 6
  2.3. Complex Layer 2 Forwarding 7
3. Operation 7
  3.1. Information Collection 7
  3.2. Continuity Check 7
  3.3. Connectivity Verification 7
  3.4. Route Tracing 8
  3.5. Fault Verification/detection 8
  3.6. Fault Isolation/identification 8
4. Administration 9
  4.1. Worst-case metrics 9
  4.2. Efficient data retrieval 10
5. Maintenance 10
  5.1. Dynamic Resource Reservation 11
  5.2. Reliable Reconfiguration 11
6. IANA Considerations 11
7. Security Considerations 11
8. Acknowledgments 11
9. Informative References 11
Authors' Addresses 13

1. Introduction

Reliable and Available Wireless (RAW) is an effort that extends DetNet to approach end-to-end deterministic performances over a network that includes scheduled wireless segments. In wired networks, many approaches try to enable Quality of Service (QoS) by implementing traffic differentiation so that routers handle each type of packets differently. However, this differentiated treatment was expensive for most applications.

Deterministic Networking (DetNet) [RFC8655] has proposed to provide a bounded end-to-end latency on top of the network infrastructure, comprising both Layer 2 bridged and Layer 3 routed segments. Their work encompasses the data plane, OAM, time synchronization, management, control, and security aspects.

However, wireless networks create specific challenges. First of all, radio bandwidth is significantly lower than for wired networks. In these conditions, the volume of signaling messages has to be very limited. Even worse, wireless links are lossy: a layer 2 transmission may or may not be decoded correctly by the receiver, depending on a broad set of parameters. Thus, providing high reliability through wireless segments is particularly challenging.

Wired networks rely on the concept of _links_. All the devices attached to a link receive any transmission. The concept of a link in wireless networks is somewhat different from what many are used to in wireline networks. A receiver may or may not receive a transmission, depending on the presence of a colliding transmission, the radio channel's quality, and the external interference. Besides, a wireless transmission is broadcast by nature: any _neighboring_ device may be able to decode it. The document includes detailed information on what the implications for the OAM features are.

Last but not least, radio links present volatile characteristics. If the wireless networks use an unlicensed band, packet losses are not anymore temporally and spatially independent. Typically, links may exhibit a very bursty characteristic, where several consecutive packets may be dropped. Thus, providing availability and reliability on top of the wireless infrastructure requires specific Layer 3 mechanisms to counteract these bursty losses.

Operations, Administration, and Maintenance (OAM) Tools are of primary importance for IP networks [RFC7276]. It defines a toolset for fault detection, isolation, and performance measurement.

The primary purpose of this document is to detail the specific requirements of the OAM features recommended to construct a

predictable communication infrastructure on top of a collection of wireless segments. This document describes the benefits, problems, and trade-offs for using OAM in wireless networks to provide availability and predictability.

In this document, the term OAM will be used according to its definition specified in [RFC6291]. We expect to implement an OAM framework in RAW networks to maintain a real-time view of the network infrastructure, and its ability to respect the Service Level Objectives (SLO), such as delay and reliability, assigned to each data flow.

1.1. Terminology

We re-use here the same terminology as [detnet-oam]:

- o OAM entity: a data flow to be controlled;
- o Maintenance End Point (MEP): OAM devices crossed when entering/ exiting the network. In RAW, it corresponds mostly to the source or destination of a data flow. OAM message can be exchanges between two MEPs;
- o Maintenance Intermediate endPoint (MIP): OAM devices along the flow; OAM messages can be exchanged between a MEP and a MIP;
- o control/data plane: while the control plane expects to configure and control the network (long-term), the data plane takes the individual decision;
- o passive / active methods (as defined in [RFC7799]): active methods send additionnal control information (inserting novel fields, generating novel control packets). Passive methods infer information just by observing unmodified existing flows.
- o active methods may implement one of these two strategies:
  - * In-band: control information follows the same path as the data packets. In other words, a failure in the data plane may prevent the control information to reach the destination (e.g., end-device or controller).
  - * out-of-band: control information is sent separately from the data packets. Thus, the behavior of control vs. data packets may differ;

We also adopt the following terminology, which is particularly relevant for RAW segments.

- o piggybacking vs. dedicated control packets: control information may be encapsulated in specific (dedicated) control packets. Alternatively, it may be piggybacked in existing data packets, when the MTU is larger than the actual packet length. Piggybacking makes specifically sense in wireless networks: the cost (bandwidth and energy) is not linear with the packet size.

- o router-over vs. mesh under: a control packet is either forwarded directly to the layer-3 next hop (mesh under) or handled hop-by-hop by each router. While the latter option consumes more resource, it allows to collect additionnal intermediary information, particularly relevant in wireless networks.

- o Defect: a temporary change in the network (e.g., a radio link which is broken due to a mobile obstacle);

- o Fault: a definite change which may affect the network performance, e.g., a node runs out of energy.

1.2. Acronyms

OAM Operations, Administration, and Maintenance

DetNet Deterministic Networking

SLO Service Level Objective

QoS Quality of Service

SNMP Simple Network Management Protocol

SDN Software-Defined Network

1.3. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

2. Role of OAM in RAW

RAW networks expect to make the communications reliable and predictable on top of a wireless network infrastructure. Most critical applications will define an SLO to be required for the data flows it generates. RAW considers network plane protocol elements

such as OAM to improve the RAW operation at the service and the forwarding sub-layers.

To respect strict guarantees, RAW relies on an orchestrator able to monitor and maintain the network. Typically, a Software-Defined Network (SDN) controller is in charge of scheduling the transmissions in the deployed network, based on the radio link characteristics, SLO of the flows, the number of packets to forward. Thus, resources have to be provisioned a priori to handle any defect. OAM represents the core of the pre-provisioning process and maintains the network operational by updating the schedule dynamically.

Fault-tolerance also assumes that multiple paths have to be provisioned so that an end-to-end circuit keeps on existing whatever the conditions. The Packet Replication and Elimination Function ([PREF-draft]) on a node is typically controlled by a central controller/orchestrator. OAM mechanisms can be used to monitor that PREOF is working correctly on a node and within the domain.

To be energy-efficient, reserving some dedicated out-of-band resources for OAM seems idealistic, and only in-band solutions are considered here.

RAW supports both proactive and on-demand troubleshooting.

The specific characteristics of RAW are discussed below.

2.1. Link concept and quality

In wireless networks, a _link_ does not exist physically. A common convention is to define a wireless link as a pair of devices that have a non-null probability of exchanging a packet that the receiver can decode. Similarly, we designate as *neighbor* any device with a radio link with a specific transmitter.

Each wireless link is associated with a link quality, often measured as the Packet Delivery Ratio (PDR), i.e., the probability that the receiver can decode the packet correctly. It is worth noting that this link quality depends on many criteria, such as the level of external interference, the presence of concurrent transmissions, or the radio channel state. This link quality is even time-variant.

2.2. Broadcast Transmissions

In modern switching networks, the unicast transmission is delivered uniquely to the destination. Wireless networks are much closer to the ancient *shared access* networks. Practically, unicast and broadcast frames are handled similarly at the physical layer. The

link layer is just in charge of filtering the frames to discard irrelevant receptions (e.g., different unicast MAC address).

However, contrary to wired networks, we cannot be sure that a packet is received by *all* the devices attached to the layer-2 segment. It depends on the radio channel state between the transmitter(s) and the receiver(s). In particular, concurrent transmissions may be possible or not, depending on the radio conditions (e.g., do the different transmitters use a different radio channel or are they sufficiently spatially separated?)

2.3. Complex Layer 2 Forwarding

Multiple neighbors may receive a transmission. Thus, anycast layer-2 forwarding helps to maximize the reliability by assigning multiple receivers to a single transmission. That way, the packet is lost only if *none* of the receivers decode it. Practically, it has been proven that different neighbors may exhibit very different radio conditions, and that reception independency may hold for some of them [anycast-property].

3. Operation

OAM features will enable RAW with robust operation both for forwarding and routing purposes.

3.1. Information Collection

The model to exchange information should be the same as for detnet network, for the sake of inter-operability. YANG may typically fulfill this objective.

However, RAW networks imply specific constraints (e.g., low bandwidth, packet losses, cost of medium access) that may require to minimize the volume of information to collect. Thus, we discuss in Section 4.2 the different ways to collect information, i.e., transfer physically the OAM information from the emitter to the receiver.

3.2. Continuity Check

Similarly to detnet, we need to verify that the source and the destination are connected (at least one valid path exists)

3.3. Connectivity Verification

As in detnet, we have to verify the absence of misconnection. We will focus here on the RAW specificities.

Because of radio transmissions' broadcast nature, several receivers may be active at the same time to enable anycast Layer 2 forwarding. Thus, the connectivity verification must test any combination. We also consider priority-based mechanisms for anycast forwarding, i.e., all the receivers have different probabilities of forwarding a packet. To verify a delay SLO for a given flow, we must also consider all the possible combinations, leading to a probability distribution function for end-to-end transmissions. If this verification is implemented naively, the number of combinations to test may be exponential and too costly for wireless networks with low bandwidth.

3.4. Route Tracing

Wireless networks are meshed by nature: we have many redundant radio links. These meshed networks are both an asset and a drawback: while several paths exist between two endpoints, and we should choose the most efficient one(s), concerning specifically the reliability, and the delay.

Thus, multipath routing can be considered to make the network fault-tolerant. Even better, we can exploit the broadcast nature of wireless networks to exploit meshed multipath routing: we may have multiple Maintenance Intermediate Endpoints (MIE) for each hop in the path. In that way, each Maintenance Intermediate Endpoint has several possible next hops in the forwarding plane. Thus, all the possible paths between two maintenance endpoints should be retrieved, which may quickly become untractable if we apply a naive approach.

3.5. Fault Verification/detection

Wired networks tend to present stable performances. On the contrary, wireless networks are time-variant. We must consequently make a distinction between _normal_ evolutions and malfunction.

3.6. Fault Isolation/identification

The network has isolated and identified the cause of the fault. While detnet already expects to identify malfunctions, some problems are specific to wireless networks. We must consequently collect metrics and implement algorithms tailored for wireless networking.

For instance, the decrease in the link quality may be caused by several factors: external interference, obstacles, multipath fading, mobility. It it fundamental to be able to discriminate the different causes to make the right decision.

4. Administration

The RAW network has to expose a collection of metrics to support an operator making proper decisions, including:

- o Packet losses: the time-window average and maximum values of the number of packet losses have to be measured. Many critical applications stop to work if a few consecutive packets are dropped;

- o Received Signal Strength Indicator (RSSI) is a very common metric in wireless to denote the link quality. The radio chipset is in charge of translating a received signal strength into a normalized quality indicator;

- o Delay: the time elapsed between a packet generation / enqueuing and its reception by the next hop;

- o Buffer occupancy: the number of packets present in the buffer, for each of the existing flows.

These metrics should be collected per device, virtual circuit, and path, as detnet already does. However, we have to face in RAW to a finer granularity:

- o per radio channel to measure, e.g., the level of external interference, and to be able to apply counter-measures (e.g., blacklisting).

- o per link to detect misbehaving link (assymetrical link, fluctuating quality).

- o per resource block: a collision in the schedule is particularly challenging to identify in radio networks with spectrum reuse. In particular, a collision may not be systematic (depending on the radio characteristics and the traffic profile)

4.1. Worst-case metrics

RAW inherits the same requirements as detnet: we need to know the distribution of a collection of metrics. However, wireless networks are know to be highly variable. Changes may be frequent, and may exhibit a periodical pattern. Collecting and analyzing this amount of measurements is challenging.

Wireless networks are known to be lossy, and RAW has to implement strategies to improve reliability on top of unreliable links. Hybrid Automatic Repeat reQuest (ARQ) has typically to enable

retransmissions based on the end-to-end reliability and latency requirements.

4.2. Efficient data retrieval

We have to minimize the number of statistics / measurements to exchange:

- o energy efficiency: low-power devices have to limit the volume of monitoring information since every bit consumes energy.

- o bandwidth: wireless networks exhibit a bandwidth significantly lower than wired, best-effort networks.

- o per-packet cost: it is often more expensive to send several packets instead of combining them in a single link-layer frame.

In conclusion, we have to take care of power and bandwidth consumption. The following techniques aim to reduce the cost of such maintenance:

on-path collection: some control information is inserted in the data packets if they do not fragment the packet (i.e., the MTU is not exceeded). Information Elements represent a standardized way to handle such information;

flags/fields: we have to set-up flags in the packets to monitor to be able to monitor the forwarding process accurately. A sequence number field may help to detect packet losses. Similarly, path inference tools such as [ipath] insert additional information in the headers to identify the path followed by a packet a posteriori.

hierarchical monitoring; localized and centralized mechanisms have to be combined together. Typically, a local mechanism should contiuously monitor a set of metrics and trigger distant OAM exchances only when a fault is detected (but possibly not identified). For instance, local temporary defects must not trigger expensive OAM transmissions.

5. Maintenance

RAW needs to implement a self-healing and self-optimization approach. The network must continuously retrieve the state of the network, to judge about the relevance of a reconfiguration, quantifying:

the cost of the sub-optimality: resources may not be used optimally (e.g., a better path exists);

the reconfiguration cost: the controller needs to trigger some reconfigurations. For this transient period, resources may be twice reserved, and control packets have to be transmitted.

Thus, reconfiguration may only be triggered if the gain is significant.

5.1. Dynamic Resource Reservation

Wireless networks exhibit time-variant characteristics. Thus, the network has to provide additional resources along the path to fit the worst-case performance. This time-variant characteristics make the resource reservation very challenging: over-reaction waste radio and energy resources. Inversely, under-reaction jeopardize the network operations, and some SLO may be violated.

5.2. Reliable Reconfiguration

Wireless networks are known to be lossy. Thus, commands may be received or not by the node to reconfigure. Unfortunately, inconsistent states may create critical misconfigurations, where packets may be lost along a path because it has not been properly configured.

We have to propose mechanisms to guarantee that the network state is always consistent, even if some control packets are lost. Timeouts and retransmissions are not sufficient since the reconfiguration duration would be, in that case, unbounded.

6. IANA Considerations

This document has no actionable requirements for IANA. This section can be removed before the publication.

7. Security Considerations

This section will be expanded in future versions of the draft.

8. Acknowledgments

TBD

9. Informative References

[anycast-property]
Teles Hermeto, R., Gallais, A., and F. Theoleyre, "Is Link-Layer Anycast Scheduling Relevant for IEEE 802.15.4-TSCH Networks?", 2019, <https://doi.org/10.1109/LCNSymposium47956.2019.9000679>.

[detnet-oam]
Theoleyre, F., Papadopoulos, G. Z., Mirsky, G., and C. J. Bernardos, "Operations, Administration and Maintenance (OAM) features for detnet", 2020, <https://tools.ietf.org/html/draft-theoleyre-detnet-oam-support>.

[ipath] Gao, Y., Dong, W., Chen, C., Bu, J., Wu, W., and X. Liu, "iPath: path inference in wireless sensor networks.", 2016, <https://doi.org/10.1109/TNET.2014.2371459>.

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

[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>.

[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>.

[RFC7799] Morton, A., "Active and Passive Metrics and Methods (with Hybrid Types In-Between)", RFC 7799, DOI 10.17487/RFC7799, May 2016, <https://www.rfc-editor.org/info/rfc7799>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[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>.

Authors' Addresses

Fabrice Theoleyre
CNRS
Building B
300 boulevard Sebastien Brant - CS 10413
Illkirch - Strasbourg 67400
FRANCE

Phone: +33 368 85 45 33
Email: theoleyre@unistra.fr
URI: http://www.theoleyre.eu

Georgios Z. Papadopoulos
IMT Atlantique
Office B00 - 102A
2 Rue de la Chataigneraie
Cesson-Sevigne - Rennes 35510
FRANCE

Phone: +33 299 12 70 04
Email: georgios.papadopoulos@imt-atlantique.fr

Greg Mirsky
ZTE Corp.

Email: gregimirsky@gmail.com