Demonstration of Data-Sovereign Telemetry Broker for Open and Disaggregated Optical Networks

Haydar Qarawlus[1], Steffen Biehs[1], Behnam Shariati[2], José Juan Pedreño Manresa[3], Ayoub Bouchedoub[1], Hendrik Haße[1], Pooyan Safari[2], Achim Autenrieth[3], Johannes Fischer[2]

(1) Fraunhofer ISST, Dortmund, Germany
(2) Fraunhofer HHI, Berlin, Germany
(3) ADVA Optical Networking, Munich, Germany
Corresponding author: haydar.qarawlus@isst.fraunhofer.de

Abstract: We demonstrate a novel and modular telemetry broker that allows remote collection and exchange of telemetry data. Our proposal enforces data sovereignty principles powered by International Data Spaces components and enables unprecedented data ownership control.

1. Overview

The transformation towards network disaggregation requires an exceptional level of interoperability, cooperation, and intelligence at various levels of the networking stack [1][2]. It also necessitates the vendors to expose their device-specific parameters to telemetry collectors. However, the generated data usually comprises confidential information and business-critical data of the involved vendors and operators [3][4]. Currently, the equipment status and telemetry data are retrieved using protocols (e.g., gRPC/gNMI, NETCONF) and data models (e.g., OpenConfig, OpenROADM, ONF T-API) [5] that are entirely data ownership agnostic and do not offer any usage control and policy enforcement functionalities, much like the proposed telemetry brokers based on Apache Kafka [6][7].

In recent years, the aspects of data sovereignty as well as the control and ownership of data post-exchange has been heavily researched. A number of standards and protocols have been created to address the various aspects of the topic, the most defined of which is the International Data Spaces (IDS) communication standard [8]. This standard, along with its components, is defined and maintained by the International Data Spaces Association (IDSA).

In this work, we propose a novel telemetry brokering solution based on IDS components that focuses on data sovereignty, thus offering unprecedented data usage control and policy enforcement features [8]. In the demo zone, we perform live demonstrations of the proposed solution for two distinct use cases that require data sharing and telemetry streaming among multiple data providers and consumers. The demonstration will be performed on a partially dis-aggregated optical networking testbed with commercial equipment [2].

2. Innovation

Our innovative proposal incorporates data sovereignty principles in telemetry streaming workflow. We achieve this by employing several IDS components, such as the IDS Metadata Broker [9] and Dataspace Connector [10] in addition to various self-developed components to allow sovereign and secure data exchange that are presented next.

2.1. Data Sovereignty and Dataspace Connectivity

The creation of a dedicated dataspace in the IDS and establishing a connection with other participants requires the use of different IDS components, the most important of which is the IDS Connector. The IDS Connector communicates using a set of standardized IDS messages defined according to the IDS Reference Architecture Model (IDS RAM) [8][11]. Each participating connector in a dataspace must be certified and obtain a certificate from an IDS Certificate Authority (CA), thus allowing other dataspace participants to validate their identity. As an added level of security, each IDS message sent from a connector must contain a valid bearer access token issued by an IDS Dynamic Attribute Provisioning Service (DAPS) [11].

In addition to the use and adaptation of standard IDS components, we developed a framework consisting of several specialized components to enable the connection between the IDS components and the network appliances, which are contained within the Wrapper and the Device Agent applications (see Figure 1). On the one hand, the Device Agent is designed to operate on the lowest level of our Data Marketplace Connector application shown in Figure 2. Each Agent is designed for a specific protocol and data model (e.g., NETCONF and OpenConfig) and communicates with the appliances directly to obtain the telemetry data. On the other hand, the Wrapper is designed to facilitate the communication between the Agent and the Dataspace Connector, as the connector has a strictly defined interface and communication sequence required to offer data to other dataspace participants. The Dataspace Connector stores a comprehensive list of metadata about the data being offered in addition to the usage constraints applied to them.

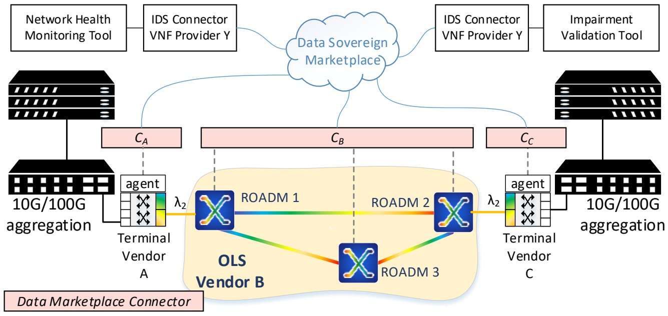

Figure 1: Data Marketplace Connector Components

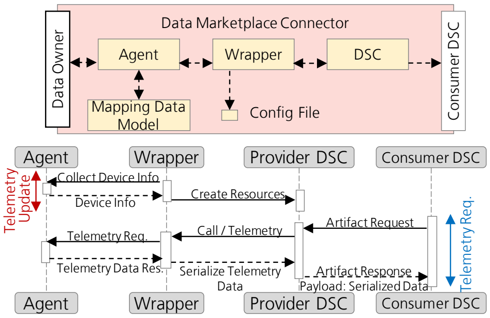

Figure 2: Data Marketplace Connector and Message Exchange

The Wrapper is responsible for the creation and maintenance of this metadata list, in addition to providing the connector with various endpoints, at which the telemetry data contained within the Agent can be easily accessed. The data offered at a connector can be registered at an IDS Metadata Broker, the main component of the Data Marketplace illustrated in Figure 1. The broker maintains an indexed and searchable list of metadata from dataspace connectors, allowing other dataspace participants to easily locate data of interest at a central location. In order to maintain data sovereignty principles, the broker does not contain the actual data being shared, rather its descriptive metadata and the address of the connector, at which the data is hosted [11]. Once the data provider decides to offer data at through the connector, the Wrapper component triggers the required communication sequence in the connector to register the data at the broker, thus allowing the data to be offered at the data marketplace. The separation of the Agent and Wrapper components allows for a simplified change and addition of communication protocols to support various appliances and use cases. The communication between the components is defined through protocol buffer messages and the exchange is done with gRPC.

For our demonstration, we use the aforementioned components to focus on the following two main use cases to highlight how a streamlined data exchange pipeline following data sovereignty principles can facilitate the data exchange process and allow for various applications.

2.2. Impairment Validation Use-case

End-to-end QoT estimation in a partially disaggregated network where third party terminals running over alien OLS requires a significant level of information sharing among the vendors providing the end-to-end optical line system and the terminals. To our knowledge, there is little literature that considers the constraint of information sharing while approaching the QoT estimation problem [3][4]. However, the proposed solutions are limited and cannot be generalized. We demonstrate how our novel framework allows QoT estimation while adhering to data sovereignty principles and secure information sharing among vendors. The developed framework will enable a network controller or a third party to calculate an end-to-end QoT metric without directly accessing the details of the optical line system or maintain access to data without the permission of the data provider.

2.3. Network Health Monitoring Use-case:

Due to the heterogeneous nature of the open disaggregated network, each piece of collected telemetry needs to be identified and contextualized, not only to ensure its ownership and sovereignty but also for better classification for the consumer. We focus on network health monitoring related parameters and demonstrate their constant streaming through our proposed telemetry broker. The Agent application defined in the previous section collects all relevant parameters from a particular device at regular intervals; it is then parsed and pre-processed (to avoid spurious or corrupted values) to be pushed to the Wrapper. Upon instantiation and before the telemetry polling starts, the Wrapper requests initial information from the Agent. The reply message contains hierarchical information to identify not only the physical/logical interfaces which originate the telemetry data, but also the device serial number, software version, supported protocols, and unique identifier. The reply message also includes additional information about the vendor and the data center (DC), such as its name, location, etc. The Agent is responsible to inform the Wrapper once a new batch of telemetry data is available for requires. This information is used by the Wrapper to trigger the update sequence at the Dataspace Connector. This process informs any potential data consumer about the availability of a new version of the monitoring data, thus allowing them to request the data again while upholding the usage constraints defined by the provider.

3. OFC Relevance

Our demonstration proposes a novel approach towards the realization of the network telemetry data sharing among vendors, operators, and other interested third parties that might have conflict of interests to freely exchange data with each other. The tools and mechanisms demonstrated will enable a sovereign and secure exchange of telemetry data. Furthermore, the demonstrated technologies can be adapted and extended to become fully automated, allowing for a sovereign exchange of data without operator interaction. This would be essential in data-centric network management and service provisioning models. OFC is the medium of choice to showcase our demonstration, as its attendees consisting of experts and the research community represent a large part of our target audience.

4. Demo content & implementation

We perform our demonstration on a partially disaggregated metro networking testbed hosted at Fraunhofer HHI premises and composed of commercial network elements from ADVA [2]. The collected telemetry data originate from transponders and OLS devices. The other components are deployed as containers running on the cloud.

Figure 1 illustrates the general architecture of our demonstration. The terminals connected to the OLS are the source of the data. The data generated is collected and offered at our sovereign marketplace. For our use-case demonstration described above, data consumer applications will request the telemetry data from the provider through the marketplace and process them accordingly.

As part of the telemetry collection framework, we developed software components as part of our telemetry data connector highlighted in Figure 2. A “Collector” application connects directly to the terminals and collects telemetry data through NETCONF and OpenConfig. The data is then processed and filtered through an “agent” application, which is designed to communicate with the specific protocol on the south-bound interface and communicate with a “wrapper” application through the northbound interface using gRPC. The main task of the “wrapper” is to be informed of the availability of networking components offering telemetry data, and to coordinate and manage the externally developed DSC through its direct communication with the agent. The wrapper additionally provides a set of REST API endpoints for the DSC that allow it to request the data whenever a data consumer wishes to access the data. Furthermore, the wrapper manages the creation and maintenance of IDS resources that describe the telemetry data being shared in the IDS. The wrapper communicates with the DSC through a set of pre-defined REST API endpoints. After the resources are created in the DSC, the wrapper component signals it to send the metadata to the IDS Metadata Broker powering the data marketplace. This allows consumers to easily find and request the data through an IDS connector, which ensures data sovereignty conditions are met. The messages exchanged between IDS components follow the IDS-Message format.

Figure 2 also highlights the startup and request processes of the connector systems. Upon startup or when updates occur, the agent informs the wrapper and provides the changes. The wrapper in turn manages the necessary resource creation at the DSC and the following registration at the IDS Metadata broker. Once a request from a consumer arrives, the DSC performs the sovereignty checks to ensure the consumer can access the data and forwards the request to the endpoints available in the wrapper application. The wrapper maps the request to one of the available agents and forwards the request to the agent. The agent collects the data from the network devices and the response is then forwarded back in the chain until its serialization and transmission over the IDS back to the consumer.

5. Acknowledgement

This work was partly funded by the German Federal Ministry of Education and Research (BMBF) in the framework of AI-NET PROTECT (Funding Numbers: KIS8CEL010, FKZ 16KIS1282).

6. References

[1] Telecom Infra Project whitepaper, “TIP OOPT MUST optical whitepaper,” Jul 2021.
[2] B. Shariati, *et al*., “Demonstration of latency-aware 5G network slicing on optical metro networks,” JOCN, 14(1), Jan 2022.
[3] K. Kaeval, *et al*., “QoT assessment of the optical spectrum as a service in disaggregated network scenarios,” JOCN. 13(10), May 2021.
[4] N. Hashemi, *et al*., “Vertical federated learning for privacy-preserving ML model development in partially disaggregated networks,” ECOC, 2021.
[5] R. Vilalta, *et al*., “Experimental evaluation of control and monitoring protocols for optical SDN networks and equipment,” JOCN, 13(8), 2021.
[6] A. Sgambelluri, *et al*., “Reliable and scalable Kafka-based framework for optical network telemetry,” JOCN, 13(10), 2021.
[7] M. Balanici, *et al*., “Demonstration of a real-time ml pipeline for traffic forecasting in AI-assisted F5G optical access networks,” ECOC, 2022.
[8] B. Otto, et al., “IDS Reference Architecture Model 3.0,” Berlin, Germany, 2019
[9] International Data Spaces Association, “IDS Metadata Broker,” GitHub Repository, 2022. [Online]. Available: https://github.com/International-Data-Spaces-Association/metadata-broker-open-core (Accessed Nov. 1, 2022)
[10] International Data Spaces Association, “Dataspace Connector,” GitHub Repository, 2022. [Online]. Available: https://github.com/International-Data-Spaces-Association/DataspaceConnector (Accessed Nov. 1, 2022)
[11] H. Pettenpohl, et al., “International Data Spaces in a Nutshell,” 2022. 10.1007/978-3-030-93975-5_3.