Telemetry Framework with Data Sovereignty Features

B. Shariati[1], H. Qarawlus[2], S. Biehs[2], J.-J. Pedreno-Manresa[3], P. Safari[1], M. Balanici[1], A. Bouchedoub[2], H. Haße[2], A. Autenrieth[3], J. K. Fischer[1], R. Freund[1]

(1) Fraunhofer HHI, Berlin, Germany
(2) Fraunhofer ISST, Dortmund, Germany
(3) ADVA Optical Networking, Munich, Germany
Corresponding author: behnam.shariati@hhi.fraunhofer.de

Abstract: We propose a novel framework that enables data ecosystem and regulated telemetry streaming in open and disaggregated optical networks. We review its requirements, present its architecture, and discuss two demonstrated use-cases in our testbeds. © 2022 The Author(s)

1. Introduction

The realization of autonomous networks requires an unprecedented level of infrastructure monitoring and telemetry streaming to provide the necessary inputs to network applications (NetApp) that are expected to take over all the manually handled processes [1]. In this regard, there has been a significant progress in the development of open protocols (e.g. RESTCONF, NETCONF, and gRPC) and data models to enable programmable network elements and monitoring devices to expose their telemetry data [2-3]. Considering the tremendous amount of telemetry data each network element produces, it is absolutely necessary to decide what to collect, when to collect, and how to collect. Moreover, in view of the increasing interest of telecom operators in network openness/disaggregation and the co-existence of a multitude of players (i.e., vendors and solution providers), cross-player telemetry sharing as well as exposing telemetry data to external players, which intend to develop added-value services and NetApp, should be enabled. Therefore, for some particular scenarios and parameters, there should be data usage control and policy enforcement mechanisms [4] as well as data anonymization and encryption [5-6] tools that address confidentiality/regulatory concerns (e.g. data relevant to actual location and identification of an element sensitive to national security) and conflict of interests' issues (e.g., vendor-specific data tied to non-disclosure agreements).

In this work, we propose a novel *Telemetry Framework* that encompasses all these features. In the remaining of this paper, we review the requirements for such a framework, present its architecture and building blocks, discuss potential use-cases, and conclude by presenting two demonstrated use-cases of the proposed telemetry framework.

2. Telemetry Framework

We design the telemetry framework based on the reference optical network architecture illustrated in Fig1, which itself follows the target architecture defined by OOPT working group of Telecom Infra Project [7]. The telemetry framework is envisioned to operate in access/metro/core networks; support numerous technologies from different vendors; accept different protocols, data models, and subscription modes for telemetry streaming; offer autonomous subscription configuration for optimized telemetry retrieval; incorporate International Data Spaces (IDS)-based data marketplace with data sovereignty features to perform control usage and policy enforcement; as well as data APPs to perform telemetry data anonymization, encryption, and abstraction. The telemetry framework offers several APIs to expose/share/trade (raw/anonymized/encrypted/abstracted) telemetry data to different points of presence.

The architecture of the telemetry framework together with the supported south bound and north bound APIs are presented in Fig2a. The primary task of the controller module is to activate and (re)configure the telemetry

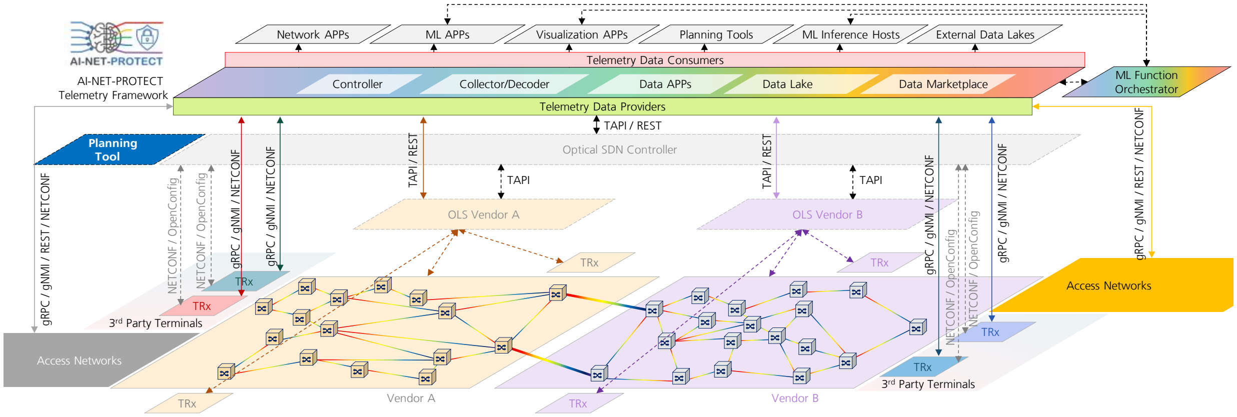

Fig. 1: Reference optical network architecture of the project AI-NET-PROTECT [8]

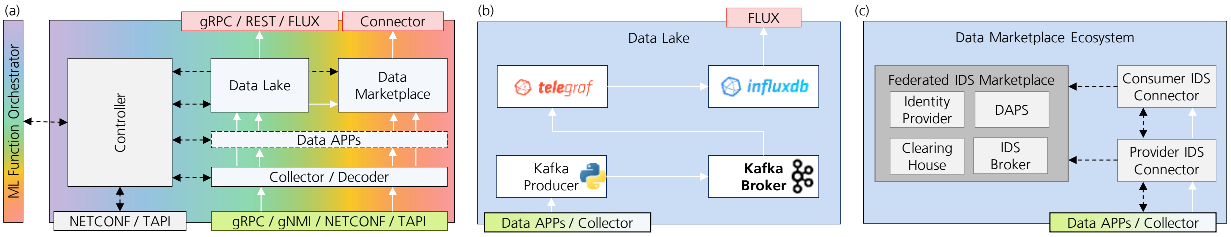

Fig. 2: (a) Telemetry framework architecture; (b) an implementation of the data lake; and (c) IDS-based data marketplace ecosystem [9]. (Dashed black arrows → control messages, white arrows → telemetry data flow)

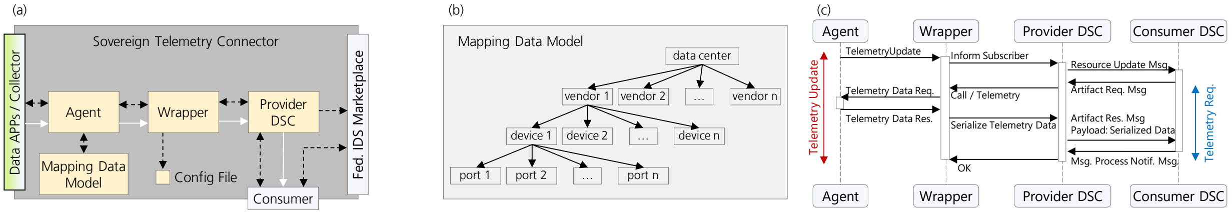

Fig. 3: (a) IDS connector architecture; (b) information mode of the marketplace; and (c) telemetry request (update) workflow of the marketplace

functionality and subscriptions of the network elements. Moreover, based on a request submitted by a Machine Learning (ML) Function Orchestrator (MLFO) and/or the internal data APPs, it could trigger modification of the telemetry flow. The collector/decoder module receives, and decode (e.g., Protobuf-to-JSON) if necessary, the telemetry events, and writes them to the data lake, unless any data APP is triggered to pre-process the telemetry data beforehand. The data lake is the telemetry storage database that could be implemented in various forms depending on the network design and operator expectations. Our implementation is illustrated in Fig2b [10], which has been also contributed to the ETSI ISG F5G telemetry work item [11]. One of the most innovative aspects of our telemetry framework is the incorporation of a data marketplace with data sovereignty features.

Data sovereignty is a feature that enables data providers to determine what happens to their data and define how, when and at what price others may use it across the value chain [9]. Data sovereignty assigns binding usage restrictions to data and establishes an ecosystem for secure and trusted data exchange. In order to do that, IDS attaches additional metainformation to the data, which unambiguously defines usage policies at each level of the data value chain. We develop an IDS-based data marketplace ecosystem that offers various usage control and policy enforcement for telemetry data sharing. The data marketplace ecosystem (shown in Fig2c) comprises several subsystems. IDS Connectors enable the participation (data providers and consumers) in the ecosystem. The IDS Broker serves as the core of the federated marketplace component and contains metadata about the registered resources from the data providers. DAPS (dynamic attribute provisioning service) provides the data providers with tokens to be validated by the data recipients. The Clearing House serves as a logging station for transactions between IDS components. In order to develop the marketplace ecosystem, we use the currently most feature-complete version of the IDS connector, namely the Dataspace Connector (DSC) originally developed and made open-source by Fraunhofer ISST. The DSC offers the most compatibility with other IDS components and as such is most suitable for communication with the Federated Marketplace's IDS Broker [9].

We present the architecture of the IDS Connector in Fig3a. The DSC forms the core system of the Sovereign Telemetry Connector which allows the various stakeholders to communicate and share resources within the marketplace ecosystem. In order to allow external components to communicate and share resources, an IDS wrapper is developed to align and map the communication between the various components. The IDS wrapper serves as an internal component in the Sovereign Telemetry Connector system and maps the communication originating from the components using for example NETCONF/gRPC/gNMI protocols to a suitable format that is understood by the IDS Connector and the recipients. In order for IDS to handle different data formats uniformly, the wrapper uses the unified hierarchical data model represented in Fig3b. Each agent must first convert its data into the format of the Mapping Data Model before it can be sent to the wrapper. *Datacenter* is the top class within the data model and represents a catalog within the IDS information model. Besides an id, name, location, and description field, it contains a list of vendors. A *vendor* represents a resource within the IDS information model. In addition to a name and description fields, it contains a list of devices. A *device* represents a resource representation within the IDS information model. Additionally, it contains an id, *supportedProtocols*, *versionNumber*, and *softwareVersionNumber* field, and a list of ports. A *port* represents an artifact within the IDS information model. One port contains an id and a field *portNumber*. Finally, Fig3c shows the telemetry request/update workflow of the

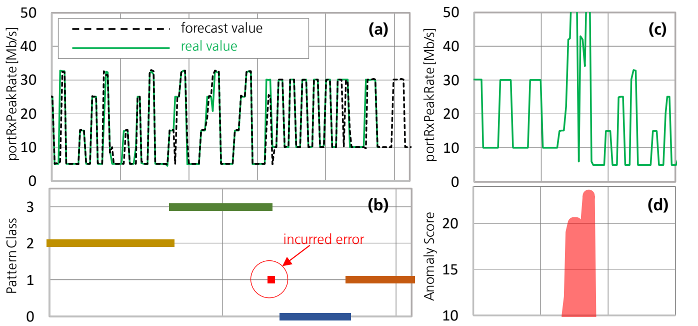

Fig. 4: (a) Traffic forecasting 10 steps into horizon; (b) traffic pattern recognition; (c) traffic anomaly by turning on an additional traffic source; and (d) outcome of the anomaly detection model.

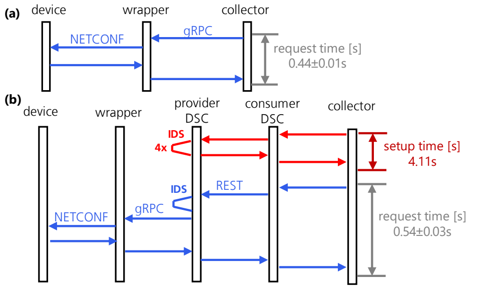

Fig. 5: Telemetry data request workflow and time (a) without DSC, and (b) with DSC. Incorporation of data sovereignty adds an overhead that renders also in a longer telemetry retrieval time around ~0.1s.

marketplace. A consumer DSC sends an IDS *ArtifactRequestMessage* to the provider DSC. To obtain the telemetry data from the agent, the DSC calls the telemetry interface in the Wrapper. The Wrapper in turn sends a request to the agent in the form of a *TelemetryDataRequest*. The agent retrieves data from other systems or internally and packages it in a *TelemetryDataResponse* message. This message is then returned to the other components to eventually be received by the consumer DSC. Our proposed framework offers numerous features and functionalities for telemetry streaming, processing, sharing, usage control, and policy enforcement that enables the players of a telco ecosystem to form a regulated data ecosystem, which is necessary for the future data-driven autonomous networks. We briefly review two demonstrated use-cases of our framework in the next section.

3. Demonstrated Use Cases

3.1. Real-time ML Pipeline for Optical Network Automation

We used the proposed telemetry framework and demonstrated a real-time ML pipeline for traffic analysis in our passive optical networking (PON) testbed [10]. In the demonstration, the data lake (Fig2b) of the framework was adapted to stream telemetry data (sampled every 5 seconds) from a gRPC-capable PON to the ML inference host, which runs three distinct ML APPs for traffic forecasting (Fig4a), traffic pattern recognition (Fig4b), and anomaly detection (Fig4c). The details of the pipeline are presented in [10] and a recording of the demo is available at [8,12].

3.2. Regulated Telemetry Sharing between Optical Line System (OLS) and 3rd Party Terminal

The impairment validation procedure for provisioning of services using 3rd party terminals across foreign OLSs requires certain level of information sharing among vendors that might not be straightforward due to conflict of interests [6]. We used the data marketplace ecosystem (Fig2c) of the telemetry framework to share OLS-specific telemetry data from a set of NETCONF-capable devices with the impairment validation tool for a limited amount of time (an example of usage control). This was carried out on the partially disaggregated testbed described in [13]. As shown in Fig5, the incorporation of data sovereignty makes it longer for the telemetry data to be retrieved, which can be considered as a measure of additional metainformation introducing data sovereignty into the workflow. Note that, there is also a single time setup procedure that establishes the trust between the DSC provider and consumer.

4. Concluding Remarks

We presented a novel telemetry framework comprising a data marketplace ecosystem that allows contractual/regulated telemetry sharing among different players in an open and disaggregated optical network.

5. Acknowledgement

This work was partly funded by BMBF in the framework of AI-NET PROTECT (KIS8CEL010, FKZ 16KIS1282). The authors would like to thank Anders Lindgren from Telia Company for the fruitful discussion.

6. References

[1] 5G-PPP SW Network WG, “NetApp: opening up 5G and beyond networks,” Version 1.0, Sep 2022.
[2] R. Casellas, *et al*., “Advances in SDN control and telemetry for beyond 100G disaggregated optical networks,” JOCN, 14(6), Jun 2022.
[3] J. Kundrat, *et al*., “Opening up ROADMs: streaming telemetry,” JOCN, 13(10), Oct 2021.
[4] IDSA Position Paper, “Usage control in the International Data Spaces,” Version 3.0, Mar 2021.
[5] B. Eckhard (Wien, AT), et al., “Reversible anonymous telemetry data collection,” U.S. Patent 20200117831, Apr 2020.
[6] N. Hashemi, *et al*., “Vertical federated learning for privacy-preserving ML development in partially disaggregated networks,” ECOC, 2021.
[7] TIP OOPT MUST Optical Whitepaper, “Target architecture: disaggregated open optical networks,” Version 1.0, Jul 2021.
[8] Celtic-Next Flagship Project AI-NET-PROTECT [Accessed Online: https://protect.ai-net.tech/].
[9] IDSA Whitepaper, “Reference Architecture Model,” Version 3.0, Apr 2019.
[10] M. Balanici, *et al*., “Demo of a real-time ML pipeline for traffic forecasting in AI-assisted F5G optical access networks,” ECOC 2022.
[11] ETSI White Paper No. #50, “Fixed 5th generation advanced and beyond,” ETSI, 1st Edition, Sep 2022.
[12] Fraunhofer HHI YouTube Channel, [https://youtu.be/5moNFa7uhzc, Accessed Online: Nov 2022].
[13] B. Shariati, *et al*., “Demonstration of latency-aware 5G network slicing on optical metro networks,” JOCN, 14(1), Jan 2022.