Toward Building a Context-Aware Data Aggregation Framework for Network Monitoring

July 2021

IETF 111 - NMRG

Ignacio Dominguez (UPM), Daniel Gonzalez (UPM)

Diego R. Lopez (TID)

Index

1. Introduction

2. Context Modeling

3. Semantic Data Aggregator (SDA) Framework

4. Real Use Case

5. Conclusions

Introduction

Main Ideas

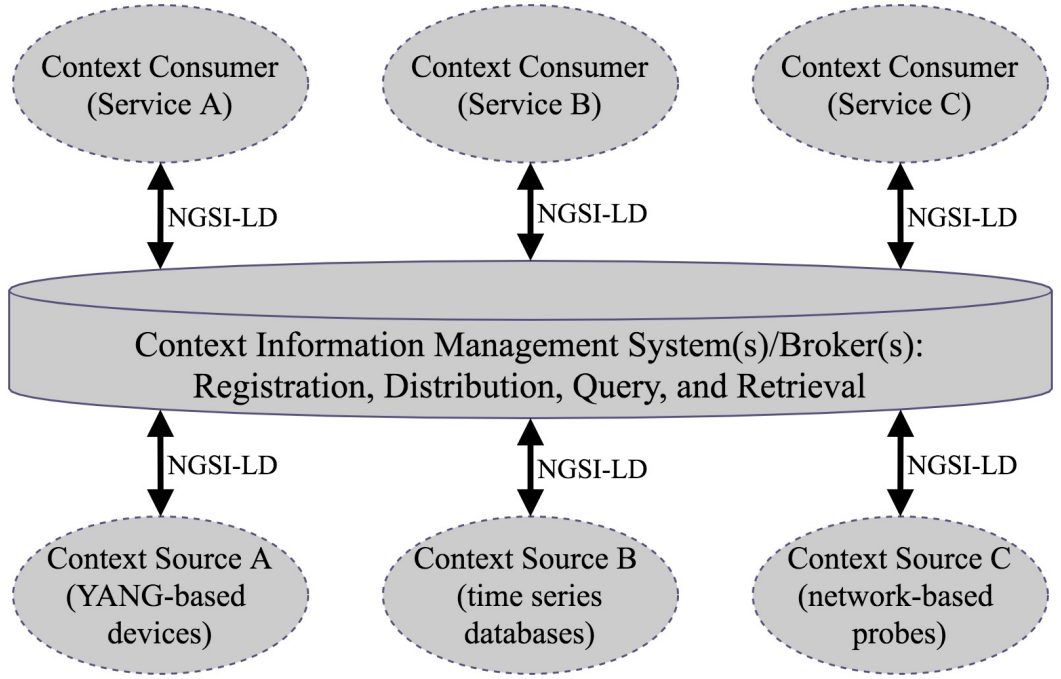
- Deal with **heterogeneous** data sources
  - Multi-domain, multi-technology, multi-…
  - Transport protocols
  - Encoding formats
  - Subscription mechanisms (pull vs push)
- Metadata to characterize the data sources
  - **Context information management** based on **ETSI CIM**
- Semantic framework for network monitoring
  - Applies **streaming telemetry** techniques
  - Leverages metadata for configuration/description of **data pipelines**
  - **Transformation** between data models

ETSI ISG CIM

- Focused on mechanisms to deal with context information
  - Information shared through data publication platforms (Context Brokers)
- Standardizes the **NGSI-LD protocol** for exchanging context information:
  - NGSI-LD information models describing entities, properties, and relationships (property graphs)
  - Definition of NGSI-LD API based on REST
- Mainly applied to IoT scenarios

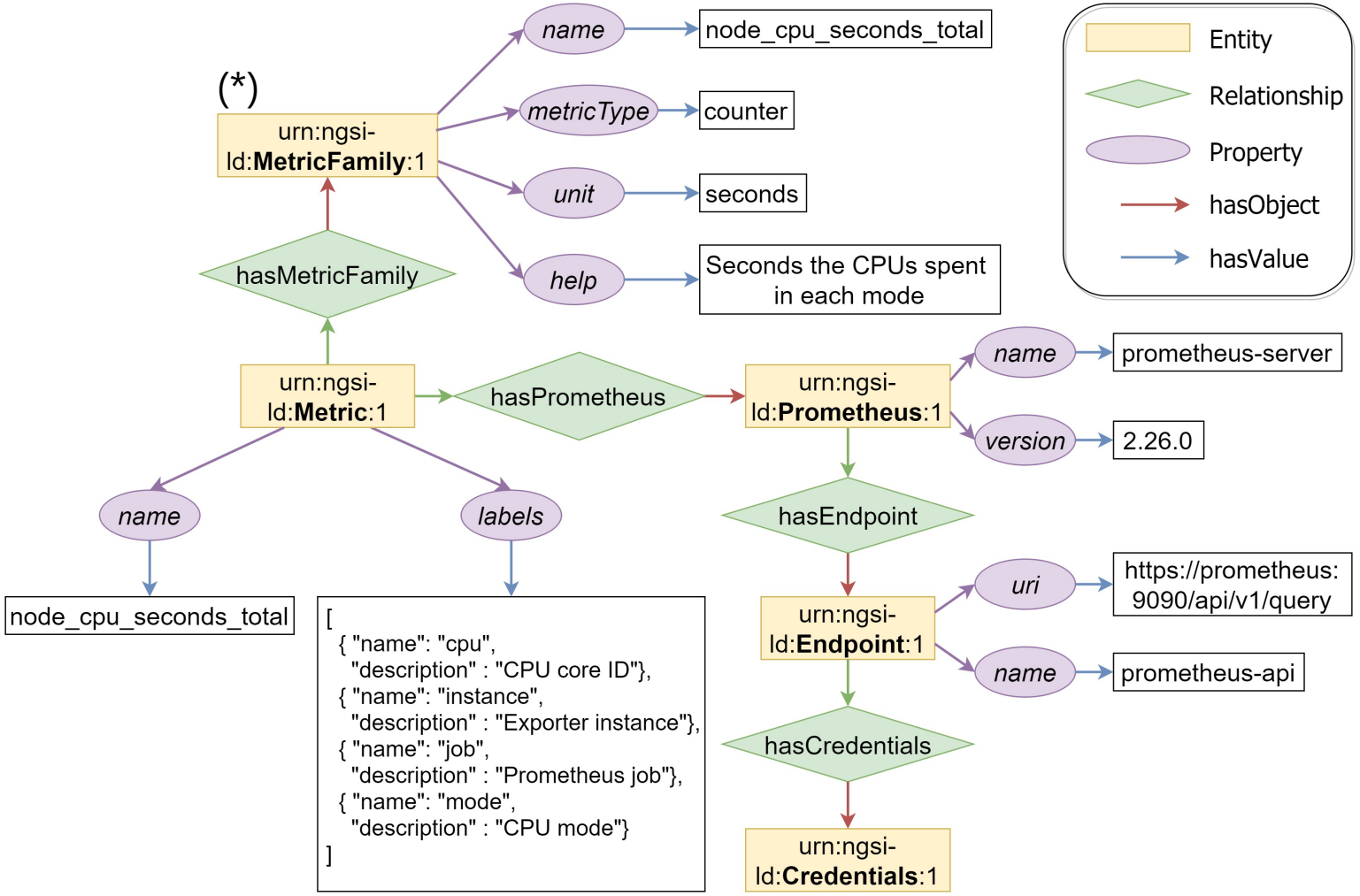
Context Components

- **Context Brokers** → Store and exchange context information
- **Context Sources** → Provide context information to the Context Broker (e.g., YANG-based devices)
- **Context Consumers** → Request and subscribe to context information from the Context Broker (e.g., database services)



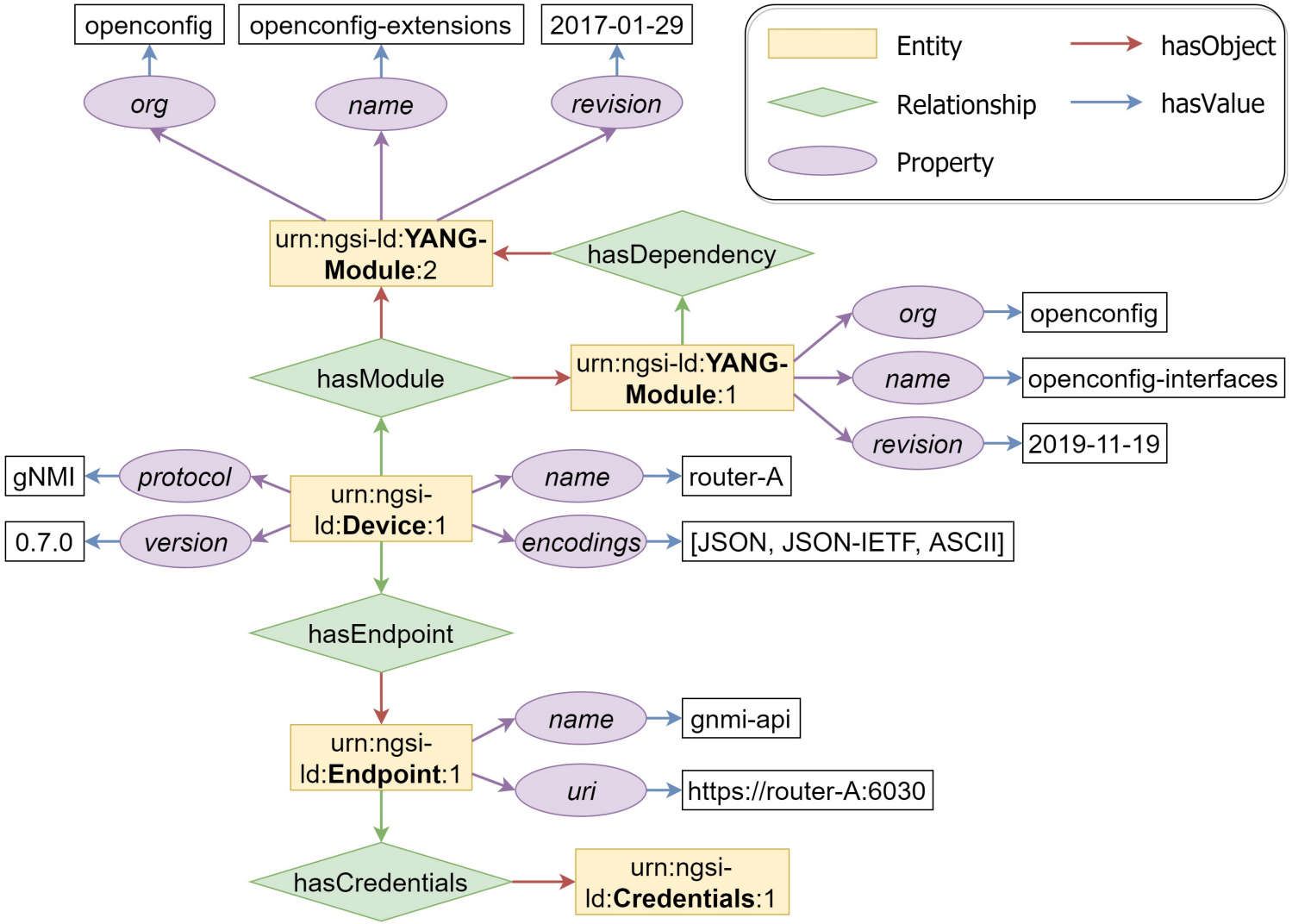
Context Modeling

Prometheus-based Data Source



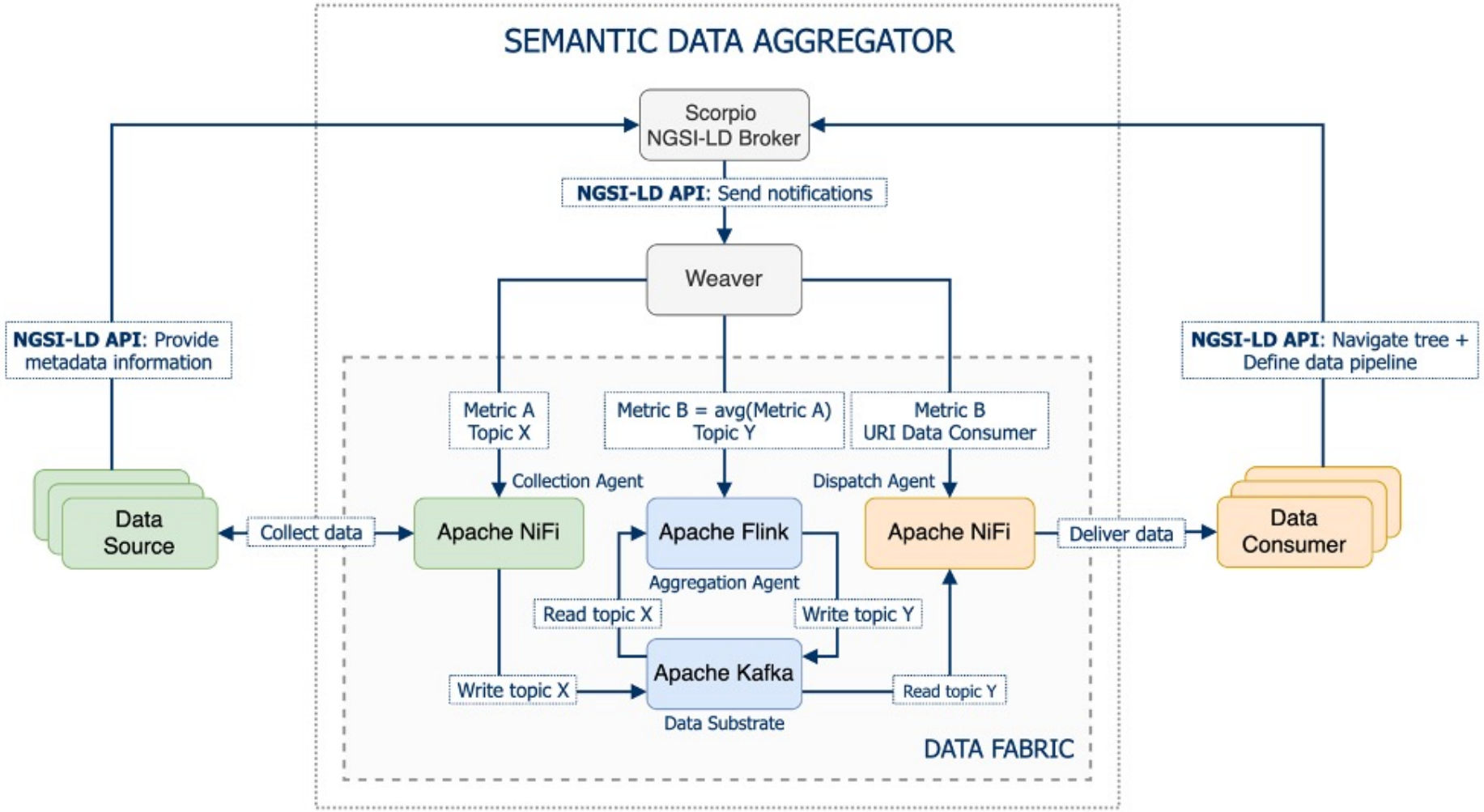
* *MetricFamily* NGSI-LD entity aligned with OpenMetrics initiative (https://openmetrics.io/)

Telemetry-based Data Source

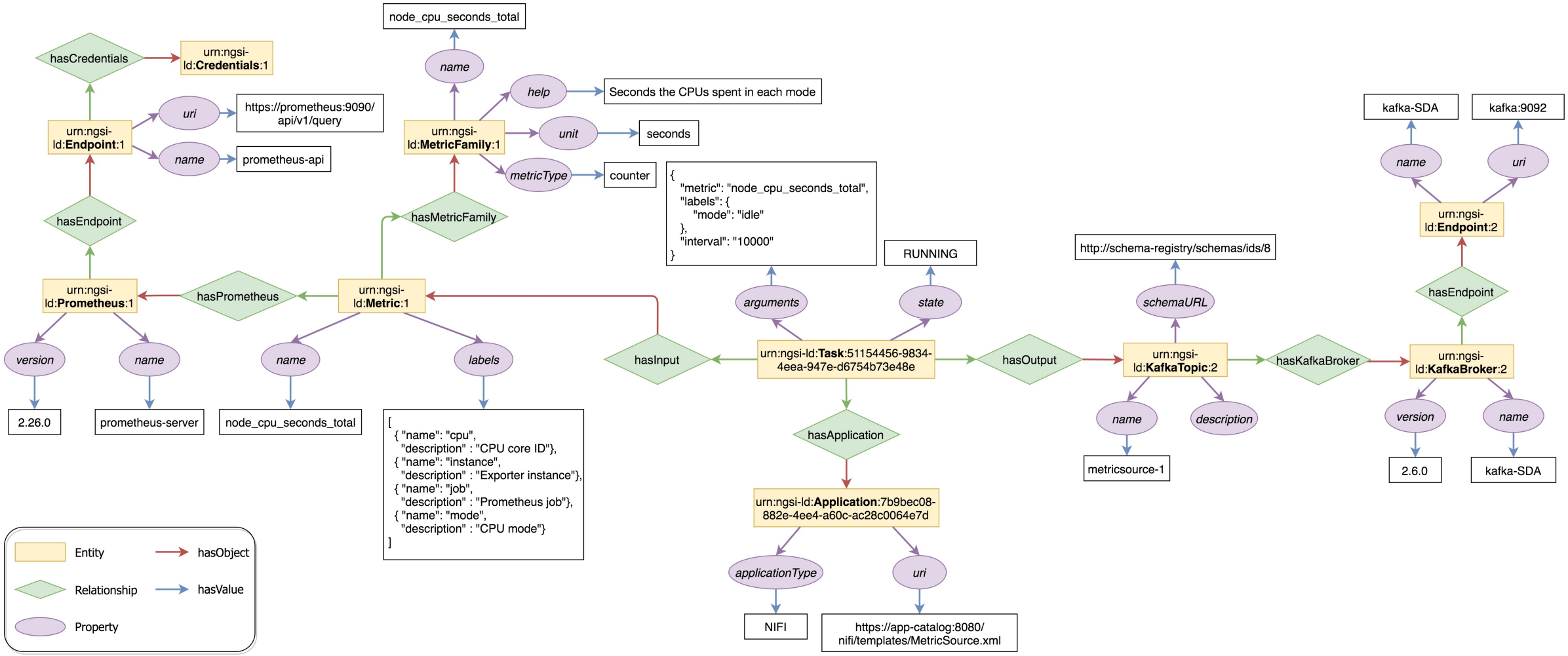


Semantic Data Aggregator (SDA) Framework

SDA Architecture Overview



Context Modeling of Data Pipelines



Real Use Case

Anomaly Detector (I)

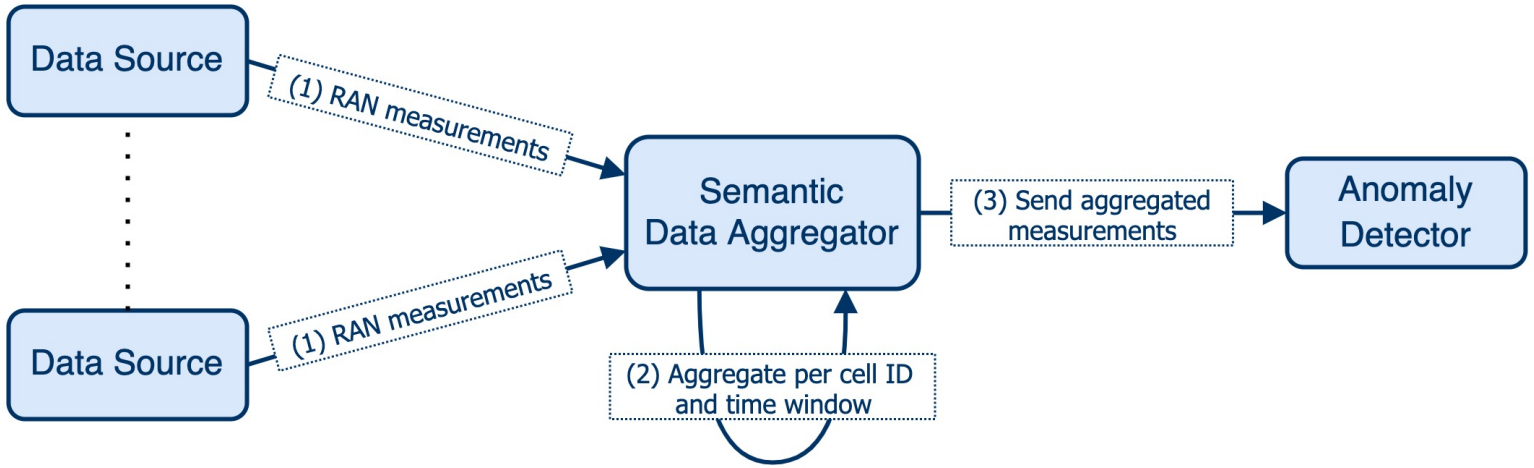
Module that analyzes the status of a RAN cell:

- Learns from data traffic patterns and mobility patterns
- Identifies and predicts anomalies based on RAN KPIs
- Exposes REST API for ingesting streams of events
- Provides a future notification/alert system

Field Name	Data Type	Description
ul_delay	Float	Uplink delay (ms)
dl_delay	Float	Downlink delay (ms)
lost_packets	Integer	# of lost packets, per service per user
rsrp	Float	RSRP (dB)
transfer_protocol	Boolean	TCP or UDP encoded [0,1]
urlx_cell	Integer	UE Bytes received from the cell
timestamp	Datetime	Measurement timestamp (datetime format - "yyyy'-'MM'-'dd' 'HH':'mm':'ss")
cell_id	Integer	RAN cell ID

Anomaly Detector (II)

- Context describes which data source provides which RAN KPI measurements
- SDA collects measurements and aggregates per cell ID and time window
- Aggregated data combined and transformed into the data model of the Anomaly Detector module
- SDA delivers data through the Anomaly Detector's REST API



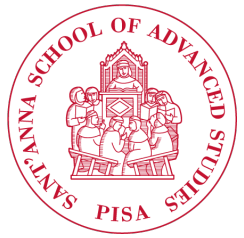
Conclusions

Summary

- Data-driven network management requires the integration of heterogeneous data sources and data consumers
- Context-aware management based on the ETSI CIM standard
  - Modeling of data sources, data consumers and data pipelines
- Development of monitoring framework for collecting and aggregating data
  - Separation between monitoring context and data planes

Next Steps

- Combination of context information from different levels:
  - Operations level → network functions, network services
  - Business level → network policies, intents, SLAs, owners
- Alignment with the SAIN architecture
- Auto discovery of context information
- Northbound API for interacting with the semantic data aggregator
- Closing the loop → Collection, processing, and application of configuration data



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 856709.