April 2023

DYNAMIC TELEMETRY PROFILE ENFORCEMENT IN A CONTROLLER NETWORK

Rajesh I V

Vinay Saini

Nagendra Kumar Nainar

Ram Mohan R

DYNAMIC TELEMETRY PROFILE ENFORCEMENT IN A CONTROLLER NETWORK

AUTHORS:
Rajesh I V
Vinay Saini
Nagendra Kumar Nainar
Ram Mohan R

ABSTRACT

Because telemetry processing can involve high resource usage, such processing is typically provided via a cloud infrastructure. However, there are drawbacks to current implementations involving such cloud infrastructure processing. For example, such processing typically follows standard processing patterns. Yet, with the increasing complexity of different network use cases, there are scenarios that would benefit from dynamic telemetry processing. Presented herein are techniques through which multiple device telemetry profiles can allow a cloud controller to dynamically match a telemetry profile to specific conditions for a tenant network. Each telemetry profile may include selections for data processing through priority and secured queues. Additionally, the cloud controller may have reverse telemetry policies to push reverse telemetry to the customer edge when original usage telemetry data is retrieved, processed, and/or transferred.

DETAILED DESCRIPTION

Telemetry processing is typically moved to a cloud infrastructure since it may require high resource usage. Individual tenant network controllers may be provided according to different deployment models, such as on-premise, hybrid, and/or distributed cloud, but most of the resource intensive telemetry processing happens in the cloud infrastructure. Many of the cloud service vendors provide minimal customization support for telemetry profiles (e.g., providing options like capturing maximum configuration, or optimal configuration, etc.,) and switching between telemetry profiles is typically in response to a manual trigger.

From the point of view of a cloud-based controller, telemetry data may be considered in two categories:

Category 1: Devices providing telemetry to the controller for anomaly detection, fault detection, capturing network metrics, etc.; and

Category 2: Controller Usage Telemetry in which the controller collects the usage patterns of features (e.g., frequency of usage, enablement of certain knobs and configuration issues etc.) as usage metrics. The controller vendors may use such data for improving the controller functionality and analytics.

For Category 1, the controller typically processes the telemetry data based on a telemetry profile that an enterprise creates upfront and then modifies the profile as needed. However, with the growing complexity of network use cases there is a need to dynamically determine the telemetry requirement and change the way telemetry data is processed in the data pipelines.

For instance, network circumstances (e.g., an emergency network problem at a particular site, a security attack, or a critical vulnerability detection in a software/hardware stack of edge devices or cloud infrastructure) may require switching the telemetry data collection and processing approach in a timely manner. This could mean a complete data set needs to be collected from a site, prioritizing the data from a site and streamline the data to more secured pipeline, or adjusting the priority the data in the pipeline. Re-configuring all the devices according to change in telemetry needs and streamlining the data processing to appropriate pipelines are complex tasks.

For Category 2, there is often a lack of deep observability on usage telemetry data. From a customer's point of view, there is always a fear of confidential data leakage and mishandling of data. Today, some vendors may pass insights back to customers after processing telemetry data, but this offers limited observability into the fulfillment of shared telemetry. In-line reverse telemetry support on collected data usage is typically a level of data observability that may not be provided.

This proposal describes a system to address telemetry data from both Category 1 and Category 2. Specifically, Device Telemetry profiles can be provided for Category 1

telemetry data collection and Reverse Telemetry profiles can be provided for Category 2 telemetry data collection.

Category 1: Device Telemetry profile:

Unlike the traditional approach of creating one configuration setting/profile for telemetry collection, we propose creating multiple custom profiles in controller portal. For instance, some example custom profiles could be:

Profile 1: Default profile. This profile may be applicable during normal network operations;

Profile 2: Site-based event profile. This profile may cause the telemetry system to process and prioritize data pertaining to a specific site during a specific emergency condition;

Profile 3: Time-based profile. This profile may cause the telemetry system to process critical data of devices during a specific time and discard others; and

Profile 4: Data sensitivity profile. This profile may cause the telemetry system to process sensitive data in more secured pipeline on detection of certain conditions.

As shown in Figure 1, below, each profile will have the following rules:

- **Switchover Rule** – This rule defines the condition and/or symptom detected by the controller to dynamically switch to the selected profile;
- **Data processing Rule** – This rule defines how to process and enrich telemetry data at the edge layer of the tenant network; and
- **Operational Rule** – This rule defines the conditions (e.g., time-bound, co-existence with other profiles, and/or priority over other profiles on multiple matching conditions) for the continued operation of the telemetry system under the selected profile. This rule also captures how the data needs to be processed in a cloud pipeline (e.g., more secured pipeline – Trusted Execution Environment (TEE) infrastructure, high priority queues, etc.).

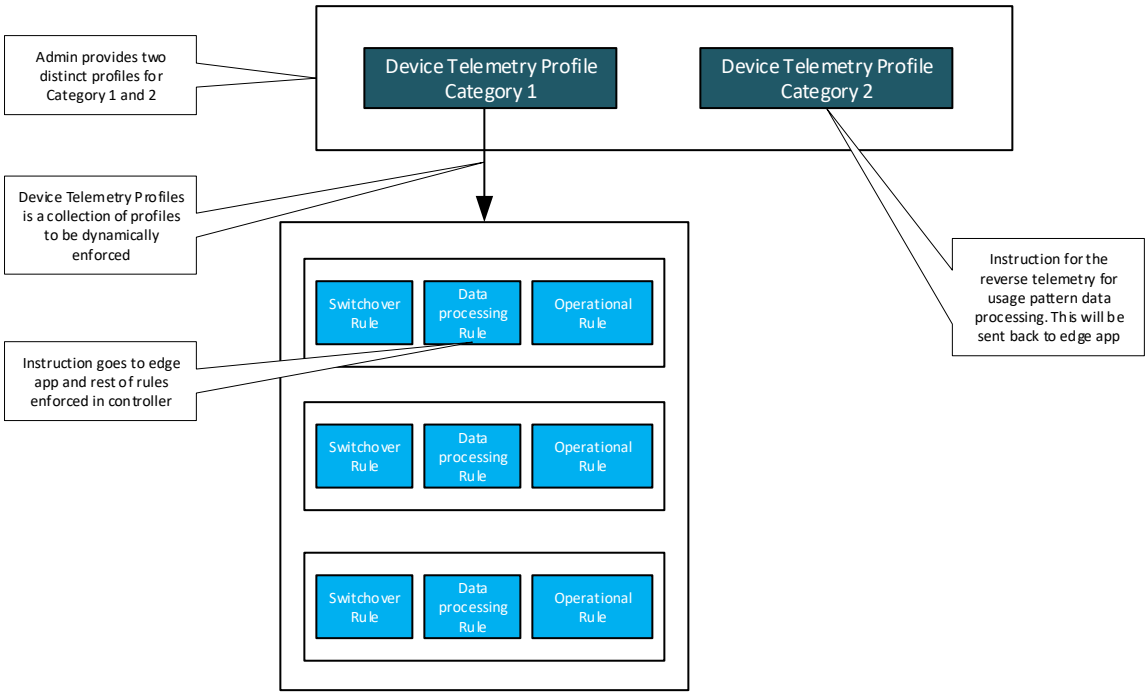

Figure 1 – Example Telemetry Profiles

Telemetry system infrastructure

As shown in Figure 2, below, the architecture for the telemetry system architecture separates the cloud-based controller from a Telemetry Edge Agent on the tenant network. The cloud-based controller includes a telemetry portal, a database of Device Telemetry profiles, processing pipelines, and a Telemetry Switch Service.

The telemetry portal enables an administrative user to access the cloud-based controller, for instance to define different Device Telemetry profiles for the telemetry system. The database stores the Device Telemetry profiles and enables the cloud-based controller to store all of the rules (e.g., switchover rules, data processing rules, and operational rules) associated with each Device Telemetry profile. The processing pipelines (e.g., the default pipeline, the priority pipeline, and the secured pipeline) process received telemetry data to generate insights into the operation of the tenant network.

The Telemetry Switch Service receives and monitors the telemetry data provided by the tenant network. When the switchover rule conditions associated with a Device Telemetry profile are met, the Telemetry Switch Service activates the appropriate Device Telemetry profile and pushes an instruction set down associated with the Device Telemetry

profile to the Telemetry Edge Agent. The Telemetry Switch Service manages the operational lifecycle (e.g., if the Device Telemetry profile specifies it is time-bound, then the Telemetry Switch Service automatically deactivates the profile when the time elapses). The Telemetry Edge Agent receives the instruction set from the Telemetry Switch Service and handles the device telemetry from the tenant network accordingly. Based on the instructions, the Telemetry Edge Agent may collect and send only the packets selected according to the Device Telemetry profile and drop rest of the telemetry data.

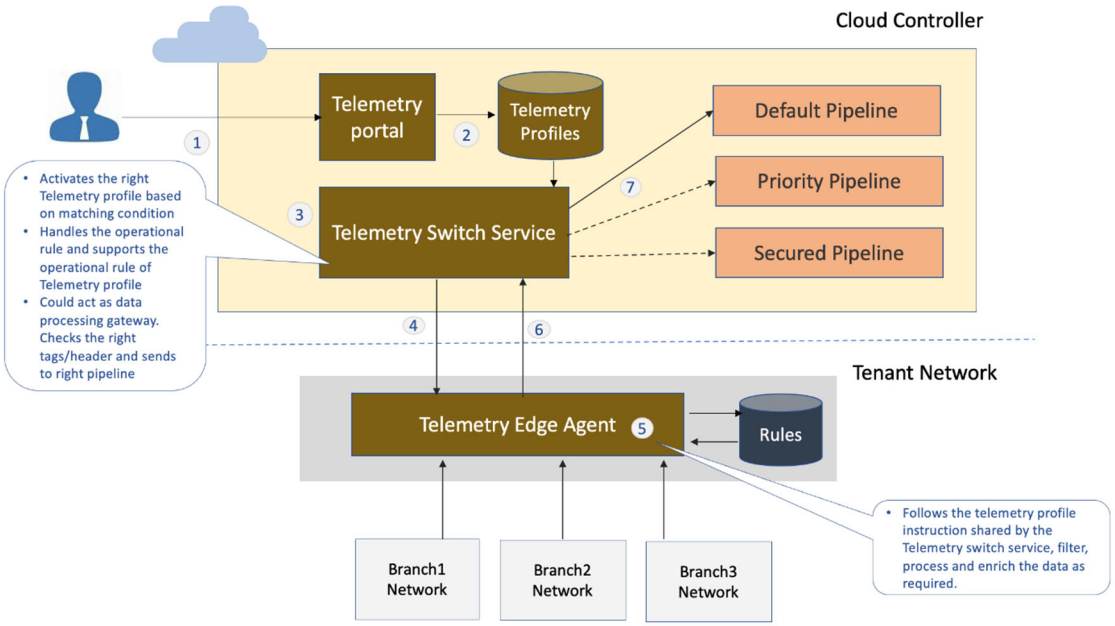

Figure 2 – Telemetry System Architecture and Flow

Figure 2 also shows an example flow of the telemetry system implementing and dynamically switching between multiple Device Telemetry profiles. At step 1, a user provides multiple Device Telemetry profiles to the cloud-based controller via the telemetry portal. Each device telemetry profile includes a switchover rule, a data processing rule, and an operation rule. At step 2, a database stores the Device Telemetry profiles in association with tenant information.

At step 3, the Telemetry Switch Service monitors the switchover rules associated with all of the Device Telemetry profiles, and activates a particular Device Telemetry

profile when the conditions match the corresponding switchover rule. At step 4, the Telemetry Switch Service configures the Telemetry Edge Agent with the data processing rule of matching Device Telemetry profile. At step 5, the Telemetry Edge Agent monitors the outgoing telemetry data and applies the data processing rule on the outgoing telemetry data. Accordingly, the Telemetry Edge Agent may filter and adds tags to annotate the data packets of the telemetry data. Annotating the data packets helps route the data packets to the appropriate pipeline in cloud based on the operational rule of the active Device Telemetry profile.

At step 6, the Telemetry Edge Agent sends the processed/annotated telemetry data packets to the cloud controller. At step 7, the Telemetry Switch Service handles the incoming telemetry data packets according to the operational rule of active Device Telemetry profile. The Telemetry Switch Service may act as data processing gateway as well, by determining the tags/headers on the telemetry data packets and sending the telemetry data packets to the appropriate pipeline. If the operational rule of the active Device Telemetry profile includes a time-bound limit, then the Telemetry Switch Service deactivates the Device Telemetry profile at the appropriate time.

Category 2: Reverse Telemetry:

The telemetry system may also be configured to send reverse telemetry data according to a Reverse Telemetry policy/profile. Reverse telemetry data provides the individual tenants observability into how the telemetry data provided from a tenant network is processed at the cloud-based controller. The reverse telemetry data may be sent to the Tenant Edge Agent at the customer edge of the tenant network whenever the original usage telemetry data is retrieved, processed, and/or transferred to provide the tenant insight into the use of the telemetry data at the cloud controller. As shown in Figure 2, the Telemetry Switch Service may additionally handle the reverse telemetry and provide the Telemetry Edge Agent with the appropriate reverse telemetry data. This approach is primarily used for observability concerns on data sent to cloud for usage telemetry.

In summary, the cloud-based telemetry system as proposed herein can provide for multiple Device Telemetry profiles that can be activated based on dynamic conditions of

the network matching the rules associated with a particular Device Telemetry profile. Additionally, the Device Telemetry profiles can provide a mechanism to specify data processing rules and operational rules for telemetry data packets. The data processing rules and operational rules can enable selective packet processing and annotation to ensure the telemetry data packets are routed through specific pipelines (e.g., high priority pipelines or highly secured pipelines) in the cloud based on the Device Telemetry profile. The Device Telemetry profiles can also provide a mechanism to activate specific profiles at a particular time, as well as priority rules for co-existing with other profiles that may also be activated by the current conditions. Furthermore, a Reverse Telemetry profile enables more observability by sending data in the reverse direction (i.e., from the cloud controller to the tenant network edge) when usage telemetry data is sent to cloud controller.