Workgroup:
Operations and Management Area Working Group
Internet-Draft:
draft-jeong-opsawg-intent-based-sdv-framework-02
Published: 24 June 2024
Intended Status: Informational
Expires: 26 December 2024

Authors: J. Jeong, Ed. Y. Shen
Sungkyunkwan University Sungkyunkwan University

An Intent-Based Management Framework for Software-Defined Vehicles in Intelligent Transportation Systems

Abstract

Software-Defined Vehicle (SDV) is a new player towards autonomous vehicles in Intelligent Transportation Systems (ITS). An SDV is constructed by a software platform like a cloud-native system like Kubernetes and has its internal network. To facilitate the easy and efficient configuration of networks in the SDV, an intent-based management is an appropriate direction. This document proposes a framework of intent-based management for networks, security, and applications in SDVs so that they can communicate with other SDVs and infrastructure nodes for safe driving and infotainment services in the road networks.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

The network management has been evolving dramatically from manual configuration to advanced automatic management. This evolution leads to the intent-based network (IBN) management and automation [RFC9315], which has been driven by several factors, including complexity of networks, scale, cost and efficiency, dynamic environments, service delivery, and security [Survey-IBN-CST-2023]. Apart from network management and automation, the automotive industry is also witnessing a fundamental transformation, particularly with the advent of software-defined vehicles (SDVs). SDVs leverage powerful onboard high-performance computers (HPCs) and a high-speed network backbone, typically Ethernet-based Internet Protocol (IP) network [Survey-IPVehNet-2021], to enable flexible and dynamic allocation of functions and resources. Shifting to SDVs is also a new paradigm in Intelligent Transportation Systems (ITS). The SDVs can interact with each other via Vehicle-to-Vehicle (V2V) communications and infrastructure via Vehicle-to-Infrastructure (V2I) communications (e.g., edge servers) for safe driving and infotainment services. Figure 1 shows an architecture of vehicular networks for SDVs that are grouped into multiple subnets. They can communicate with edge servers and vehicular cloud by IP Road-Side Unit (IP-RSUs, e.g., gNodeB in 5G [TS-23.501]).

```
                              Vehicular Cloud
               *******************************************
             *                                             *
            *              +------------------+             *
           *               | Cloud Controller |              *
           *               +------------------+              *
           *                         ^                       *
            *                        |                      *
             *                       v                     *
               *******************************************
                 ^ +------------+   ^ +------------+   ^ +------------+
                 | |Edge-Server1|   | |Edge-Server2|   | |Edge-Server3|
                 | +------------+   | +------------+   | +------------+
                 |   ^              |   ^              |   ^
                 |   |              |   |              |   |
                 v   V              v   V              v   V
               +---------+         +---------+        +---------+
               | IP-RSU1 |<------->| IP-RSU2 |<------>| IP-RSU3 |
               +---------+         +---------+        +---------+
                    ^                   ^                    ^
                    :                   :                    :
           +-----------------+ +-----------------+   +-----------------+
           |        : V2I    | |        : V2I    |   |       : V2I     |
           |        v        | |        v        |   |       v         |
+--------+ |   +--------+    | |   +--------+    |   |   +--------+    |
|  SDV1  |===> |  SDV2  |===>| |   |  SDV3  |===>|   |   |  SDV4  |===>|
+--------+<...>+--------+<........>+--------+    |   |   +--------+    |
           V2V     ^         V2V        ^        |   |        ^        |
           |       : V2V     | |        : V2V    |   |        : V2V    |
           |       v         | |        v        |   |        v        |
           |  +--------+     | |   +--------+    |   |    +--------+   |
           |  |  SDV5  |===> | |   |  SDV6  |===>|   |    |  SDV7  |==>|
           |  +--------+     | |   +--------+    |   |    +--------+   |
           +-----------------+ +-----------------+   +-----------------+
                 Subnet1              Subnet2              Subnet3
                (Prefix1)            (Prefix2)            (Prefix3)

        <----> Wired Link   <....> Wireless Link   ===> Moving Direction
```

Figure 1: Vehicular Networks for Software-Defined Vehicles

To facilitate the development of SDVs, a large number of automotive companies and original equipment manufacturers (OEMs) are developing the components of SDVs based on different open architectures, such as AUTOSAR [AUTOSAR-SDV] and Eclipse SDV [Eclipse-SDV]. An SDV can include many electronic control units (ECUs) and hundreds of sensors and actuators for in-vehicle functions and services, e.g., advanced driver-assistance systems (ADAS), automatic emergency braking (AEB), forward collision warning (FCW), and lane keeping assist (LKA) applications. They can also run multiple computing devices, operating systems, and a cloud-native platform (e.g., Kubernetes [Kubernetes]) to manage those ECUs and functions. The Connected Vehicle System Alliance (COVESA) [COVESA] has developed a common vehicle signal specification (VSS) to represent the vehicle data to be shared for both in-vehicle and vehicle-to-cloud networks. Figure 2 shows a vehicular platform for SDV having foundation hardwares, a virtualization engine (i.e., Hypervisor), different operating systems (OS), various applications and network functions (such as NF-1 to NF-x) along with their runtime and management agent.

```
+--------------------------------+  +---------------------------------+
|            Apps                |  |          Functions              |
| +------+  +------+  +-------+  |  | +------+  +------+     +------+ |
| | ADAS |  |  LKA |  |  AEB  |  |  | | NF-1 |  | NF-2 | ... | NF-x | |
| +------+  +------+  +-------+  |  | +------+  +------+     +------+ |
+--------------------------------+  +---------------------------------+
+-------------+  +--------------+  +-------------------+--------------+
|Critical Apps|  |Classical Apps|  | Container Runtime |  Mgmt Agent  |
+-------------+  +--------------+  +-------------------+--------------+
+-----------------+   +-------------------+   +-----------------------+
|                 |   |   Vehicle OS I    |   |     Vehicle OS II     |
|    Real-Time    |   +-------------------+   +-----------------------+
|       OS        |   +-----------------------------------------------+
|                 |   |                    Hypervisor                 |
+-----------------+   +-----------------------------------------------+
+---------------------------------------------------------------------+
|                    Vehicle Electric/Electronics                     |
|  +------------------+  +------------------+  +------------------+   |
|  |   Vehicle ECUs   |  |   Vehicle HPC    |  | Sensors/Actuators|   |
|  +------------------+  +------------------+  +------------------+   |
+---------------------------------------------------------------------+
```

Figure 2: A Vehicular Platform for SDV

To manage the ever-growing network functions and applications in SDVs, SDVs need an intent-based management framework for networks and security inside their in-vehicle networks. An intent is a declarative command to request a configuration for a network or security function [TS-28.312][TR-28.812]. It emphasizes more on "What" is needed (i.e., declarative command) to be accomplished than "How" it should be accomplished (i.e., imperative command). Since there are a huge number of vehicles produced by each automotive company, the networks and security for the SDV need to be remotely configured and monitored by a control center of each automotive company. The in-vehicle networks are based on Gigabit Ethernet and can be configured as multiple subnets including ECUs and infotainment devices. It requires huge overhead for an operator to configure and monitor networks and security for those in-vehicle networks.

This document proposes a framework of intent-based management for networks, security, and applications in SDVs that are Service Functions (SFs). Such SFs can be constructed and managed by Software-Defined Networking (SDN) [RFC7149], Network Functions Virtualization (NFV) [ETSI-NFV][ETSI-NFV-Release-2], and Cloud Native Computing Platform (e.g., Kubernetes [Kubernetes]). This framework automates the configuration and monitoring for the networks and security in each SDV through a vehicular cloud and the SDV's mobile network. An SDV User (i.e., administrator) for the management of SDVs can configure and monitor the networks and security through an intent. The intent from the SDV User is delivered to a Cloud Controller in charge of a vehicular cloud for SDVs. The Cloud Controller translates the intent into the corresponding high-level policy, and delivers the high-level policy to an SDV Controller in charge of an SDV. The SDV translates the high-level policy into the corresponding low-level policy and delivered it to an appropriate Network Function (NF) for a specific service (e.g., router, firewall, and navigator) in the SDV.

2. Terminology

This document uses the terminology described in [RFC8329], [I-D.ietf-i2nsf-applicability], [I-D.jeong-i2nsf-security-management-automation], [I-D.jeong-nmrg-ibn-network-management-automation], and [I-D.yang-i2nsf-security-policy-translation]. In addition, the following terms are defined below:

*Intent: A set of operational goals (that a network should meet) and outcomes (that a network is supposed to deliver) defined in a declarative manner without specifying how to achieve or implement them [RFC9315].

*Intent-Based Management (IBM): It enforces an intent from a user (or administrator) into a target system (e.g., SDV). An intent can be expressed as a Natural Language (e.g., English) and can be translated into a high-level policy by a Natural Language Processing (NLP) [USENIX-ATC-Lumi][BERT] [Deep-Learning]. In this document, the intent can be translated into the corresponding high-level policy by an intent translator [I-D.jeong-i2nsf-security-management-automation]. The high-level policy can also be translated into the corresponding low-level policy by a policy translator

[I-D.yang-i2nsf-security-policy-translation]. The low-level policy is dispatched to appropriate Service Functions (SFs). Through the monitoring of the SFs, the activity and performance of the SFs is monitored and analyzed. If needed, the rules of the high-level or low-level network policy are augmented or new rules are generated and configured to appropriate SFs.

3. Intent-Based Management Framework for Software-Defined Vehicles

This section introduces the intent-based management framework for SDVs. It first describes the life cycle of an intent-based system (IBS) for SDV management. Then, it discusses the V2V and V2I networking in the framework. Eventually, the components and interfaces of the framework are explained.

3.1. Life Cycle of an IBS for SDV Management

According to the life cycle design of IBN [RFC9315], Figure 3 shows the life cycle of an intent-based system (IBS) for SDV management. It divides the life cycle into three spaces, namely SDV User Space, Translation & IBS Space, and Network Operations (Ops) & Application (App) Space. Each space is further divided into two sections, fulfillment and assurance. The fulfillment section pipelines the steps (i.e., intent input, translation/refinement, learning/planning/rendering, and configuration/provisioning) toward the final SFs such as network functions (NFs) and applications in SDVs. The assurance section monitors final results of the intent fulfillment to validate and analyze the resulted NFs and applications for SDVs.

```
       SDV User      :            Translation/          : Network Ops/
        Space        :             IBS Space            :  App Space
Fulfill              :                                  :
       +----------+  :  +------------+   +------------+ : +-----------+
       |Recognize/|---->| Translate/ |-->|   Learn/   |-->| Configure/|
       | Generate |  :  |   Refine   |   |   Plan/    | : | Provision |
       | Intent   |<----|            |   |   Render   | : |           |
       +----------+  :  +------------+   +------------+ : +-----------+
            ^        :                         ^        :       |
............|..................................|................|.....
            |        :                    +----------+  :       v
            |        :                    | Validate |  :  +-----------+
            |        :                    +----^-----+<----| Monitor/  |
Assure      |        :                         |        :  | Observe   |
        +--------+   :  +----------+      +----------+<----|           |
        | Report |<-----| Abstract |<-----| Analyze/ |  :  +-----------+
        +--------+   :  +----------+      | Aggregate|  :
                     :                    +----------+  :
```

Figure 3: The Life Cycle of IBS for SDV Management

3.2. V2V and V2I Networking for SDVs

Benefited from V2V and V2I networking, SDVs can be managed and monitored by the vehicular cloud. Figure 4 shows an example of V2V communications between two SDVs having their internal SFs. An SDV has its own internal networks (called in-vehicle networks), which consist of multiple subnets connected with each other through routers. The SDV can communicate with other SDVs via the interface from an IP-based on-board unit (IP-OBU). IP-OBU is a network device in an SDV that has a basic processing ability and can be driven by a low-power CPU (e.g., ARM) with a 5G Vehicle-to-Everything (V2X) communication device [RFC9365]. By the IP-OBU interface, the internal SFs of the SDV can also communicate with that of other SDVs. In this way, the internal SFs can be flexibly managed and controlled through V2V networking.

```
                        (*)<........>(*)
     (2001:db8:1:1::/64) |            | (2001:db8:1:2::/64)
+------------------------|-----+  +---|-----------------------------+
|                        v     |  |   v                             |
| +---------+        +-------+ |  | +-------+         +---------+   |
| |Navigator|        |IP-OBU1| |  | |IP-OBU2|         |Navigator|   |
| +---------+        +-------+ |  | +-------+         +---------+   |
|     ^                  ^     |  |     ^                  ^        |
|     |                  |     |  |     |                  |        |
|     v                  v     |  |     v                  v        |
| ---------------------------- |  | ------------------------------- |
| 2001:db8:10:1::/64 ^         |  |     ^ 2001:db8:20:1::/64        |
|                    |         |  |     |                           |
|                    v         |  |     v                           |
| +---------+    +-------+     |  | +--------+ +-------+   +-------+|
| |Firewall |    |Router1|     |  | |Firewall| |Router1|...|Router2||
| +---------+    +-------+     |  | +--------+ +-------+   +-------+|
|     ^              ^         |  |     ^         ^           ^     |
|     |              |         |  |     |         |           |     |
|     v              v         |  |     v         v           v     |
| ---------------------------- |  | ------------------------------- |
|      2001:db8:10:2::/64      |  |       2001:db8:20:2::/64        |
+------------------------------+  +---------------------------------+
     SDV1 (Mobile Network1)                SDV2 (Mobile Network2)

   <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 4: V2V Networking

SDVs can receive software updates as well as the configuration of their networks and security from the vehicular cloud. As shown in Figure 1, SDVs as vehicles can communicate with each other via V2V and with infrastructure nodes such as IP-RSU via V2I, for example, gNodeB in 5G networks, respectively. Figure 5 illustrates the V2I networking with edge and cloud networks for SDVs. An Edge Network (EN) is a radio access network which has an IP-RSU for wireless communication with other SDVs having an IP-OBU and wired communication with other network devices (e.g., routers, IP-RSUs, and edge servers) [RFC9365]. The IP-RSU is a network device situated along the road as an infrastructure node. It has at least two distinct IP-enabled interfaces where one is for 5G V2X and the other is for the wired network connected to the vehicular cloud [RFC9365]. As shown in Figure 5, the IPv6 prefixes should be configured for both the in-vehicle network (also called mobile network) and EN. Also, for V2X IP networking, the wireless interfaces of IP-OBU and IP-RSU should be configured with appropriate IPv6 network prefixes and default gateways towards the infrastructure network connected to the vehicular cloud. An edge server in EN (e.g., Server1 inside EN1 shown in Figure 5) can help SDVs to perform their safe driving functions by processing environmental data collected by the SDVs and giving maneuver guidance to the SDVs.

```
                                                 +-----------------+
                        (*)<........>(*)  +----->| Vehicular Cloud |
     (2001:db8:1:1::/64) |            |   |      +-----------------+
+------------------------|-----+  +---|---|-------------------------+
|                        v     |  |   v   v                         |
| +---------+        +-------+ |  | +-------+         +---------+   |
| |Navigator|        |IP-OBU1| |  | |IP-RSU1|         |Navigator|   |
| +---------+        +-------+ |  | +-------+         +---------+   |
|     ^                  ^     |  |     ^                  ^        |
|     |                  |     |  |     |                  |        |
|     v                  v     |  |     v                  v        |
| ---------------------------- |  | ------------------------------- |
| 2001:db8:10:1::/64 ^         |  |     ^ 2001:db8:20:1::/64        |
|                    |         |  |     |                           |
|                    v         |  |     v                           |
| +---------+    +-------+     |  | +-------+ +-------+   +-------+ |
| |Firewall |    |Router1|     |  | |Router2| |Server1|...|ServerN| |
| +---------+    +-------+     |  | +-------+ +-------+   +-------+ |
|     ^              ^         |  |     ^         ^           ^     |
|     |              |         |  |     |         |           |     |
|     v              v         |  |     v         v           v     |
| ---------------------------- |  | ------------------------------- |
|      2001:db8:10:2::/64      |  |       2001:db8:20:2::/64        |
+------------------------------+  +---------------------------------+
     SDV1 (Mobile Network1)              EN1 (Fixed Network1)

   <----> Wired Link   <....> Wireless Link   (*) Antenna
```

Figure 5: V2I Networking with Edge and Cloud Networks

3.3. Intent-Based Management Framework for SDVs

For the automatic network configuration of SDVs, an intent-based management is required between the vehicular cloud and SDVs [I-D.jeong-nmrg-ibn-network-management-automation]. Figure 6 shows a framework of intent-based management for SDVs. The framework consists of a vehicular cloud and SDVs.

```
                        <Vehicular Cloud (VC)>
+---------------------------------------------------------------------+
| +------------------+                      +--------------------+    |
| |     SDV User     |          +---------->|    SDV Database    |    |
| +------------------+          |           +--------------------+    |
|          ^                    |                     ^               |
|          |                    | Database            | Database      |
|          |                    | Interface           | Interface     |
|          | Consumer-Facing    |                     V               |
|          | Interface (Intent) |           +--------------------+    |
|          |                    | +-------->|    Cloud Analyzer  |<-+ |
|          |                    | |         +--------------------+  | |
|          V                    | |Analytics                        | |
| +------------------+<---------+ |Interface                        | |
| | Cloud Controller |<-----------+         +--------------------+  | |
| +------------------+<-------------------->|Vendor's Mgmt System|  | |
|          ^         Registration Interface +--------------------+  | |
|          |                                          ^             | |
+----------|------------------------------------------|-------------|-+
           | Controller-Facing Interface   VMS-Facing |   Analyzer- |
           |     (High-level Policy)        Interface |   Facing    |
           |                                          |   Interface |
+----------|------------------------------------------|-------------|-+
|          |                                          |             | |
|          v                                          v             | |
| +------------------+     Registration     +--------------------+  | |
| |  SDV Controller  |<-------------------->|    SDV Vendor's    |  | |
| +------------------+      Interface       |    Mgmt System     |  | |
|          ^      ^                         +--------------------+  | |
|          |      |                                                 | |
|          |      |                                                 | |
|          |      |   Analytics Interface   +--------------------+  | |
|          |      +------------------------>|    SDV Analyzer    |<-+ |
|          |                                +--------------------+    |
|          | SF-Facing Interface                      ^               |
|          |  (Low-level Policy)                      |               |
|          |                                          |               |
|          |                                          |               |
|          |    +--------------+----------------------+---+           |
|          |    |              |   Monitoring Interface   |           |
|          v    v              v                          v           |
|   +---------------+  +---------------+        +---------------+     |
|   |     SF-1      |  |     SF-2      |........|     SF-n      |     |
|   |   (Router)    |  |  (Firewall)   |        |  (Navigator)  |     |
|   +---------------+  +---------------+        +---------------+     |
+---------------------------------------------------------------------+
                  <Software-Defined Vehicle (SDV)>
```

Figure 6: Intent-Based Management Framework for Software-Defined Vehicles

The vehicular cloud consists of SDV User (as network administrator), Cloud Controller (as an orchestrator for a vehicular cloud), SDV Database (as a main repository for SDV management and monitoring), and Cloud Analyzer (as a monitoring data analyzer for SDVs) such as Network Data Analytics Function (NWDAF) in 5G networks [TS-23.288] [TS-29.520].

- SDV User: It is the software (e.g., web-browser-based user interface) used by SDV administrators to deliver network intents to SDV controllers. In the 3GPP intent driven management service document, it is assumed that network intent is configured by the intent data model.

- Cloud Controller: It is a component that controls and manages other system components of the vehicular cloud. From a security point of view, a security service policy can be transmitted to the service function (SF) by converting the SDV User's security service intent into the corresponding security service policy and selecting an SF that provides an appropriate security service.

- Cloud Vendor's Management System: It is a component that provides images of virtualized SFs for vehicular cloud services and registers the SFs and access information with Cloud Controller.

- Cloud Analyzer: It gathers and evaluates monitoring data from SDV Analyzers to ensure the functionality and performance of SFs, e.g., the network data analytics function (NWDAF) in 5G networks.

- SDV Database: It is a database for managing SDVs, including network and security configuration information of SDVs, current location and navigation path of SDVs, etc.

An IBS in SDV is composed of SDV Controller (as a manager for an SDV), SDV Analyzer (as a monitoring data analyzer for an SDV) [I-D.jeong-nmrg-ibn-network-management-automation], Vendor's Management System (as a vendor system to provide cloud-native containers) [RFC8329][I-D.ietf-i2nsf-applicability], and Service Functions such as NFs (e.g., router, DNS server, firewall [I-D.jeong-nmrg-ibn-network-management-automation]) and applications (e.g., safe driver and navigator). The functions of each component is described as follows.

- SDV Controller: It is a component that controls and manages other components of the SDV framework. It translates the high-level policy received from the Cloud Controller into a low-level policy that the SF can understand. An SF to perform this low-level service policy is selected, and the policy is transmitted to the SF.

- SDV Vendor's Management System: It is a component that provides an image of a virtualized SF for SDV services to the SDV framework and registers the function and access information of the SF with SDV Controller.

- Service Function (SF): It is a component that refers to a virtual network function (VNF), cloud native network function (CNF), or physical network function (PNF) for a specific service. For security services, it provides security services such as firewalls, web filters, DDoS attack mitigators, and anti-viruses. In addition, networks and application services can also operate as SFs.

- SDV Analyzer: It is a component that collects monitoring data from SFs of SDVs and analyzes these data to confirm the activity and performance of SFs. SDV Analyzer acts as NWDAF in a 5G network. If there are problems (e.g., security attacks, traffic congestion, QoS degradation) in the SDV internal network, SDV Analyzer delivers either policy reconfiguration or feedback information to SDV Controller for security and network troubleshooting.

3.4. Interfaces in the SDV Management Framework

Together with the designed SDV management framework, in Figure 6, interfaces are also defined between a pair of system components in the vehicular cloud and SDV, respectively. These interfaces include

- Consumer-Facing Interface: It is an interface between SDV User and Cloud Controller for conveying intents.

- Controller-Facing Interface: It is an interface between Cloud Controller and SDV Controller for high-level policy delivery with translated intents.

- SF-Facing Interface: It is an interface between SDV Controller and SF for the delivery of a translated lower-level policy.

- Registration Interface: It is an interface used to transfer SF capabilities and access information for registration to either Cloud Controller or SDV Controller, or deliver SF queries for searching the requested SFs. This interface can be an interface between Cloud Controller and Cloud Vendor's Management System (Cloud VMS), or between SDV Controller and SDV Vendor's Management System (SDV VMS).

- Monitoring Interface: It is an interface between the SF and the SDV Analyzer used to collect the SF's monitoring data to identify SF-related security, system, and network issues.

- Analytics Interface: It is an interface for delivering policy reconfiguration or feedback as a result of analyzing SF monitoring data. This interface is an interface between SDV Analyzer and SDV Controller, between SDV Analyzer and Cloud Analyzer, or between Cloud Analyzer and Cloud Controller.

- Analyzer-Facing Interface: It is an interface between SDV Analyzer and Cloud Analyzer for the exchange of security, network, and system-related analysis of SFs.

- VMS-Facing Interface: It is an interface between Cloud VMS and SDV VMS to exchange SF container images with SF feature information.

- Database Interface: It is an interface for exchanging data in an SDV database. It is an interface between SDV Database and Cloud Controller, or between SDV Database and Cloud Analyzer.

The intent, high-level policy, and low-level policy can be either XML documents [RFC6020][RFC7950] or YAML documents [YAML]. They can be delivered to the destination components via NETCONF [RFC6241], RESTCONF [RFC8040], or REST API [REST].

As shown in Figure 6, the Intent-Based Management SDV Framework enforces an intent from an SDV User, which as a user (or administrator), into a target system such as SDV. The intent from the SDV User can be translated into the corresponding high-level policy by an intent translator in the Cloud Controller of the Vehicular Cloud [I-D.jeong-i2nsf-security-management-automation]. The high-level policy can also be translated into the corresponding low-level policy by a policy translator in the SDV Controller of the SDV [I-D.yang-i2nsf-security-policy-translation]. The low-level policy is dispatched from the SDV Controller to appropriate Service Functions (SFs) in the SDV, such as Router, Firewall, and Navigator, as shown in the figure. Through the monitoring of the SFs, the activity and performance of the SFs in the SDV is monitored and analyzed by the SDV Analyzer in the SDV. If needed, the rules of the high-level or low-level network policy can be augmented by the SDV Analyzer. Also, new rules can be automatically generated and configured to appropriate SFs by the SDV Analyzer.

Therefore, this document proposes a framework of intent-based management for networks in Software-Defined Vehicles. Through this intent-based management, the SFs in SDVs can be better managed and configured. Base on the proposed framework, both virtualized network functions and applications can be efficiently orchestrated for agile network resource re-configurations and flexible SDV application updates.

4. IANA Considerations

This document does not require any IANA actions.

5. Security Considerations

The same security considerations for the Interface to Network Security Functions (I2NSF) Framework [RFC8329] are applicable to the intent-based management framework this document.

6. References

6.1. Normative References

[RFC6020] Bjorklund, M., Ed., "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)", RFC 6020, DOI 10.17487/RFC6020, October 2010, <https://www.rfc-editor.org/info/rfc6020>.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011, <https://www.rfc-editor.org/info/rfc6241>.

[RFC7950] Bjorklund, M., Ed., "The YANG 1.1 Data Modeling Language", RFC 7950, DOI 10.17487/RFC7950, August 2016, <https://www.rfc-editor.org/info/rfc7950>.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017, <https://www.rfc-editor.org/info/rfc8040>.

[RFC8329] Lopez, D., Lopez, E., Dunbar, L., Strassner, J., and R. Kumar, "Framework for Interface to Network Security Functions", RFC 8329, DOI 10.17487/RFC8329, February 2018, <https://www.rfc-editor.org/info/rfc8329>.

[RFC9315] Clemm, A., Ciavaglia, L., Granville, L. Z., and J. Tantsura, "Intent-Based Networking - Concepts and Definitions", RFC 9315, DOI 10.17487/RFC9315, October 2022, <https://www.rfc-editor.org/info/rfc9315>.

[RFC9365] Jeong, J., Ed., "IPv6 Wireless Access in Vehicular Environments (IPWAVE): Problem Statement and Use Cases", RFC 9365, DOI 10.17487/RFC9365, March 2023, <https://www.rfc-editor.org/info/rfc9365>.

6.2. Informative References

[I-D.ietf-i2nsf-applicability] Jeong, J. P., Hyun, S., Ahn, T., Hares, S., and D. Lopez, "Applicability of Interfaces to Network Security Functions to Network-Based Security Services", Work in Progress, Internet-Draft, draft-ietf-i2nsf-applicability-18, 16 September 2019, <https://datatracker.ietf.org/doc/html/draft-ietf-i2nsf-applicability-18>.

[I-D.jeong-i2nsf-security-management-automation] Jeong, J. P., Lingga, P., Jung-Soo, J., Lopez, D., and S. Hares, "Security Management Automation of Cloud-Based Security Services in I2NSF Framework", Work in Progress, Internet-Draft, draft-jeong-i2nsf-security-management-automation-07, 7 February 2024, <https://datatracker.ietf.org/doc/html/draft-jeong-i2nsf-security-management-automation-07>.

[I-D.jeong-nmrg-ibn-network-management-automation] Jeong, J. P., Ahn, Y., Kim, Y., and J. Jung-Soo, "Intent-Based Network Management Automation in 5G Networks", Work in Progress, Internet-Draft, draft-jeong-nmrg-ibn-network-management-automation-04, 22 April 2024, <https://datatracker.ietf.org/doc/html/draft-jeong-nmrg-ibn-network-management-automation-04>.

[I-D.yang-i2nsf-security-policy-translation] Jeong, J. P., Lingga, P., and J. Yang, "Guidelines for Security Policy Translation in Interface to Network Security Functions", Work in Progress, Internet-Draft, draft-yang-i2nsf-security-policy-translation-16, 7 February 2024, <https://datatracker.ietf.org/doc/html/draft-yang-i2nsf-security-policy-translation-16>.

[YAML] Ingerson, B., Evans, C., and O. Ben-Kiki, "Yet Another Markup Language (YAML) 1.0", Available: https://yaml.org/spec/history/2001-05-26.html, October 2023.

[TS-23.501] "System Architecture for the 5G System (5GS)", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144, September 2023.

[TS-28.312] "Intent Driven Management Services for Mobile Networks", Available: https://portal.3gpp.org/desktopmodules/

Specifications/SpecificationDetails.aspx?specificationId=3554, September 2023.

[TR-28.812] "Study on Scenarios for Intent Driven Management Services for Mobile Networks", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3553, December 2020.

[TS-23.288] "Architecture Enhancements for 5G System (5GS) to Support Network Data Analytics Services", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579, September 2023.

[TS-29.520] "Network Data Analytics Services", Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3355, September 2023.

[RFC7149] Boucadair, M. and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment", RFC 7149, March 2014, <https://www.rfc-editor.org/rfc/rfc7149>.

[ETSI-NFV] "Network Functions Virtualisation (NFV); Architectural Framework", Available: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.02.01_60/gs_nfv002v010201p.pdf, December 2014.

[ETSI-NFV-Release-2] "Network Functions Virtualisation (NFV) Release 2; Management and Orchestration; Architectural Framework Specification", Available: https://www.etsi.org/deliver/etsi_gs/nfv/001_099/006/02.01.01_60/gs_nfv006v020101p.pdf, January 2021.

[REST] Fielding, R. and R. Taylor, "Principled Design of the Modern Web Architecture", ACM Transactions on Internet Technology, Vol. 2, Issue 2,, Available: https://dl.acm.org/doi/10.1145/514183.514185, May 2002.

[USENIX-ATC-Lumi]
Jacobs, A., Pfitscher, R., Ribeiro, R., Ferreira, R., Granville, L., Willinger, W., and S. Rao, "Hey, Lumi! Using Natural Language for Intent-Based Network Management", USENIX Annual Technical Conference, Available: https://www.usenix.org/conference/atc21/presentation/jacobs, July 2021.

[BERT] Devlin, J., Chang, M., Lee, K., and K. Toutanova, "BERT: Pre-training of Deep Bidirectional Transformers for

Language Understanding", NAACL-HLT Conference, Available: https://aclanthology.org/N19-1423.pdf, June 2019.

[Deep-Learning] Goodfellow, I., Bengio, Y., and A. Courville, "Deep Learning", Publisher: The MIT Press, Available: https://www.deeplearningbook.org/, November 2016.

[AUTOSAR-SDV] "AUTOSAR Adaptive Platform", Available: https://www.autosar.org/standards/adaptive-platform, March 2024.

[Eclipse-SDV] "Eclipse Software Defined Vehicle Working Group Charter", Available: https://www.eclipse.org/org/workinggroups/sdv-charter.php, March 2024.

[COVESA] "Connected Vehicle Systems Alliance", Available: https://covesa.global/, March 2024.

[Kubernetes] "Kubernetes: Cloud Native Computing Platform", Available: https://kubernetes.io/, March 2024.

[Survey-IBN-CST-2023] Leivadeas, A. and M. Falkner, "A Survey on Intent-Based Networking", Available: https://ieeexplore.ieee.org/document/9925251, March 2023.

[Survey-IPVehNet-2021] Jeong, J., Shen, Y., Oh, T., Cespedes, S., Benamar, N., Wetterwald, M., and J. Harri, "A comprehensive survey on vehicular networks for smart roads: A focus on IP-based approaches", Available: https://ieeexplore.ieee.org/document/9925251, June 2021.

Appendix A. Acknowledgments

This work was supported by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. RS-2024-00398199).

This work was supported in part by Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korea Ministry of Science and ICT (MSIT) (No. 2022-0-01015, Development of Candidate Element Technology for Intelligent 6G Mobile Core Network).

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korea government, Ministry of Science and ICT (MSIT) (No. 2023R1A2C2002990), and by Basic Science Research Program through the NRF of Korea funded by the Ministry of Education (No. 2022R1I1A1A01053915).

Appendix B. Contributors

This document is made by the group effort of OPWAWG, greatly benefiting from inputs and texts by Linda Dunbar (Futurewei), Yong-Geun Hong (Daejeon University), and Joo-Sang Youn (Dong-Eui University). The authors sincerely appreciate their contributions.

The following are coauthors of this document:

Yoseop Ahn
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4106
Email: ahnjs124@skku.edu
URI: http://iotlab.skku.edu/people-Ahn-Yoseop.php

Mose Gu
Department of Computer Science & Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4106
Email: rna0415@skku.edu
URI: http://iotlab.skku.edu/people-Moses-Gu.php

Authors' Addresses

Jaehoon Paul Jeong (editor)
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4957
Email: pauljeong@skku.edu
URI: http://iotlab.skku.edu/people-jaehoon-jeong.php

Yiwen Shen
Department of Computer Science and Engineering
Sungkyunkwan University
2066 Seobu-Ro, Jangan-Gu
Suwon
Gyeonggi-Do
16419
Republic of Korea

Phone: +82 31 299 4106
Email: chrisshen@skku.edu
URI: https://chrisshen.github.io