Autonomous Network Operation Based on User Requirements and Security Response Initiatives

KURODA Takayuki, AKABORI Satoshi, HOTCHI Ryosuke, SATODA Kozo

Abstract

Networks are becoming more and more complex with the advancement of virtualization technology, and the increasing burden of operating these networks is becoming an issue. However, conventional automation methods, in which instructions on monitoring and handling methods are specified by using templates, are susceptible to alterations in network requirements themselves and require additional work hours for adjustment. Against this background, the technology used in autonomous operation — by which the entire process from network construction to operation is automated based on information on user requirements (or intent) — is attracting attention. NEC started conducting the R&D of the technology used in autonomous operations in 2017 and has been making pioneering efforts since then. This paper provides an overview of NEC's technologies used in autonomous operations and its core automated design as well as an introduction to enhanced security support.

Keywords

network operation, autonomy, requirements, intention, security

1. Introduction

Problems, such as disruptions, with communication infrastructure are often reported and attract wide public attention. As business reforms through digitalization are being promoted in all industries, the prompt and stable provision of networks — which are the foundation of this transformation — has become an increasingly important issue. At the same time, network configurations are becoming more complex, and the burden on operations continues to increase because of the diversification of network needs and the advancement of virtualization technology. Thus, the R&D of technologies to streamline and automate operations is now being actively conducted[1)].

The basic process of network operation consists of three steps: monitoring, analysis, and correction[2)]. First, the network's condition is monitored. Then the monitored condition is analyzed. Finally, if there is any abnormality, it is corrected to restore it to the normal condition. Although it may seem that these tasks can be automated after the program is created, in reality, adjustments are often necessary because of changes in the configuration of the network itself. For example, if the number of servers increases in accordance with an increase in the number of users, the added servers also need to be subject to monitoring. This means that the threshold for determining anomalies will be raised, and additional tasks will be added to deal with anomalies. It is argued that it is hard to program for all these changes in advance, and the difficulty of automation lies in maintaining automatic operation.

As mentioned earlier, the details of the operations required for network management vary in accordance with the network's configuration. So, what is it that changes the configuration of the network? Generally speaking, when building a network, the requirements are first defined, and then based on these requirements, the design and operation methods are considered. When automating operations and maintaining automated operations, it is desirable to automatically generate configurations and operation methods based on the requirements. Intent-based and autonomous[3)] are keywords that have been recently used to describe this kind of approach. Since 2017, we at NEC have been leading the world in the R&D of technologies for autonomous operation based on user intent. In developing these technologies,

we are also focusing on maintaining the security of the target network.

In this paper, we take a look at the technology used in autonomous operation in section 2 and discuss an overview of automated design — which is the core of autonomous operation — as well as our efforts to address security issues in section 3. Then, we introduce an application example in section 4 and summarize our discussion in the conclusion in section 5.

2. Autonomous Operation Technology

NEC is currently undertaking the R&D of technology used in autonomous operation that automates the construction and maintenance of networks based on user requirements[4]. By specifying the requirements, users automatically generate configurations and operational plans tailored to the networks. If the content has no problems, the network operates automatically in accordance with the generated plans. Now let's take a look at an overview of the autonomous operation functions based on this technology.

2.1 Overview of the autonomous operation functions

An overview of the autonomous operation functions is shown in **Fig. 1**. The functions of autonomous operation are divided into two types: one for operational planning and the other for operational management. The operational planning function generates operational plans from requirements, whereas the operational management function carries out the construction and operation of a network based on operational plans.

Operational plans provide information about the details of monitoring, analysis, and correction. The plans include indicators to be monitored, appropriate configurations based on the values of the indicators, and operational procedures to be executed when the configuration is changed. **Fig. 2** shows a simplified example of an operational plan. Here the horizontal and vertical axes represent the indicators to be monitored. Appropriate configurations are defined for each value interval, and operational procedures for transitioning from one configuration to another are provided. The operational management function performs operations based on this information. It first monitors the network and then analyzes the results to determine the appropriate configuration according to the operational plan. If the resulting configuration differs from the current configuration, the function executes the procedures to transition from the current configuration to the appropriate configuration.

Automatic generation of requirement-based operational plans eliminates the need for adjusting operational plans in response to changing conditions, which has been a problem with conventional technology.

Autonomous operation has three types of requirements: functional, non-functional, and conditional (related to acceptable changes). **Fig. 3** shows an example of the requirements for a radio access network (RAN). Functional requirements describe the multiple items that are needed as well as the relationships between them. Included in the non-functional requirements for each item such as performance and availability are constraint conditions (e.g., requiring that the delay be 10 ms or less) and objective functions for optimization (e.g., recommending that the amount of resources used be as small as possible). The allowed changes are then given by specifying a value range (minimum and maximum values) for the aforementioned constraints.

To generate an operational plan from requirements, the operational planning function first divides the range

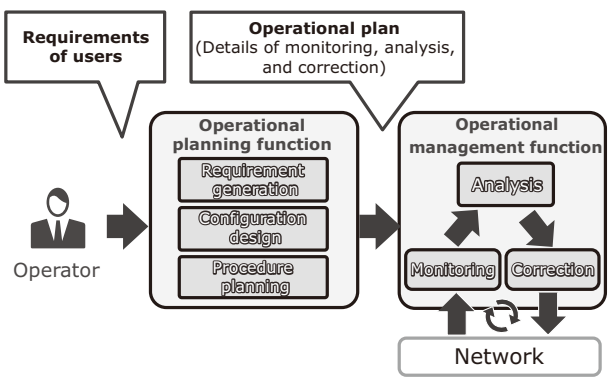

Fig. 1 Overview of autonomous operation functions.

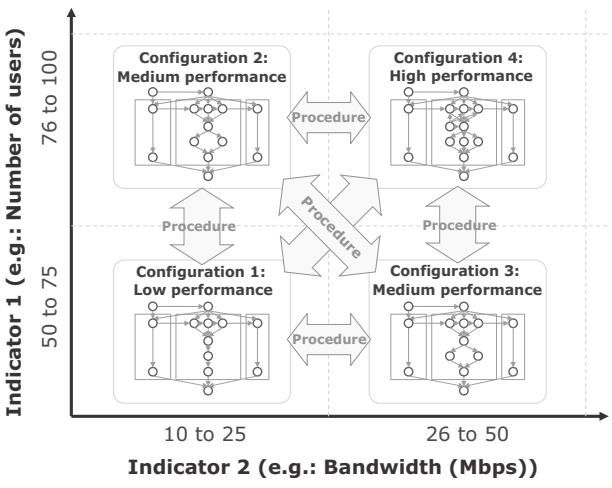

Fig. 2 Example of an operational plan.

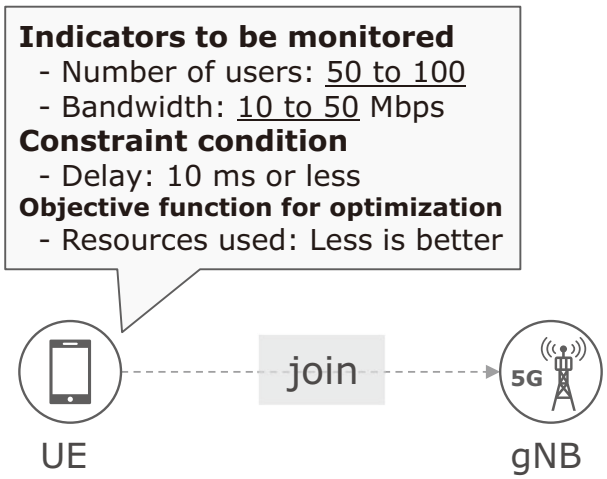

Fig. 3 Example of network requirements for RAN.

given as the allowed changes into an appropriate number of sections and then determines the values of the constraint conditions for each section, thereby generating requirements with clear values. Based on these requirements, this function designs the network configuration for each section[5] and finally generates migration procedures for each set of network configurations[6]. The items — for which the ranges are given as allowable changes — are elements that can trigger configuration changes during operation and are therefore the indicators to be monitored. For this reason, functions to monitor these indicators are also designed together with the network configuration.

Among the technologies that constitute the operational planning function, the core technology is the one that automatically designs the network configuration for each section. This technology used for automated design is discussed in section 3.

3. Overview of Automated Design and Security Measures

3.1 Automated design

The technology used for automated design is one that automatically designs specific network configurations in accordance with requirements. Among a vast number of candidate configurations for the network that may meet the requirements, this technology uses artificial intelligence (AI) to rapidly searches for a valid configuration. During the design process, step by step, the requirements become more and more concrete. At each step of this refinement process, various items — such as the server models to be used and the cloud infrastructure to be deployed at particular locations — are selected from several possible options. This process gradually narrows down the candidate configurations. If the selection is inappropriate, this process goes back to making the requirements more concrete and the selection is redone. The fewer times that this process is redone, then the faster the design can be completed. Therefore, the selections made at each step of the operation where the requirements are refined need to be determined as accurately as possible. As a result, the fulfillment of non-functional requirements — such as performance, availability, and security — is evaluated and utilized as a basis for decision making. In addition, AI and machine learning (ML) are utilized to increase the accuracy of decisions.

3.2 Addressing security requirements in automated design

As mentioned in section 3.1, when selecting a configuration during design, its security is evaluated. To evaluate security, the technology used in conventional automated design verifies whether or not there is an attack path. An attack path is a series of actions for a potential attacker to execute an attack. For example, to carry out an attack to destroy data, for example, the attacker would first attempt an unauthorized login, then acquire authorization, and finally execute a command to delete files. Here the attack path is composed of these three actions. If an attack path is found, it means that and attack can actually be carried out, so the configuration is determined as being insecure. In other words, checking whether or not there is an attack path is useful for security evaluation.

To determine the existence of an attack path, this technology uses threat models. Each threat model represents fragments of an attack path, for example, the requirement for authorization to execute a command to delete files. When designing a configuration plan, the threat models are connected with each other to attempt to generate attack paths, and then the existence of any attack paths are checked. In this way, the selection of a configuration plan that enables the existence of attack paths can be avoided, and a secure configuration plan can be created.

4. Application Example

Our development team in autonomous operation is actively working on applying this technology to 5G networks, specifically in applications that utilize the control units of 5G Core (5GC) networks and RANs as well as end-to-end networks. The following example describes an application of this technology in accordance with Open RAN (O-RAN)[7] specifications.

In O-RAN, operation and control are performed by a

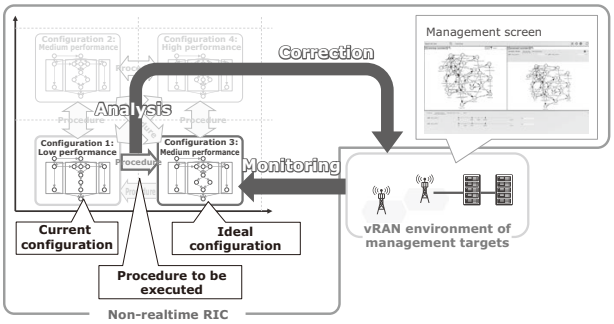

Fig. 4 Application example in the O-RAN domain.

component called the RAN intelligent controller (RIC). The RIC is divided into non-real time and near-real time components. The technology used in operation falls into the category of the non-real time RIC.

As an example of a specific operational flow, this technology monitors the number of users using a RAN belonging to a specific user group and adjusts the amount of resources allocated to the central unit (CU), which is a major functional module, in accordance with increases or decreases in the number of users. **Fig. 4** shows how operations are automated based on vRAN requirements.

A series of control actions follows the operational plan described in section 2, and the operational plan is automatically generated from the requirements. Therefore, even if the circumstances or operational conditions change, such as with the addition of new user groups or the installation of new equipment, the operational plan can still be automatically updated, enabling a quick transition to routine operations.

5. Conclusion

In this paper, we discuss autonomous operations mainly from a technical point of view. Adoption of autonomous operations is now a global trend, and we believe that it will continue to attract more and more attention in the future.

Going forward, we will continue our R&D with the aim of achieving complete automation of all networks by working on reducing the time required to generate operational plans, improving usability, and meeting the requirements for autonomous operation of the entire end-to-end network.

6. Acknowledgments

The results introduced in this paper were partially obtained from the commissioned research (No.04801) by National Institute of Information and Communications Technology (NICT) , Japan.

References

1) TM Forum: Autonomous Networks:Empowering Digital Transformation For Smart Societies and Industries, October 2020
https://www.tmforum.org/resources/whitepapers/autonomous-networks-empowering-digital-transformation-for-smart-societies-and-industries/
2) NTT: Efforts to Advance Network Operations by Use of AI and Machine Learning, December 2021 (Japanese)
https://hqsict.axies.jp/_media/sites/13/2021/12/211216_AXIES年次大会講演資料_TA1.pdf
3) ETSI: Intent driven management services for mobile networks, July 2022
4) Takayuki Kuroda: A proposal of automated network operation planning method based on user's intent: IEICE Technical Report (ICM), November 2022
5) Takayuki Kuroda, Yutaka Yakuwa, and Kazuki Tanabe: Network Design Automation Technology by AI/ML, The Journal of Electronics, Information and Communication Engineers, Vol.105 No.10, pp.1208–1214, October 2022 (Japanese)
6) Takayuki Kuroda, et al.: Adding Exchangeability of Deployment Agent to Template-based Provisioning, IEICE Technical Report, 115 (481), pp.151–158, March 2016
7) O-RAN ALLIANCE
https://www.o-ran.org/

Authors' Profiles

KURODA Takayuki
Principal Researcher
Secure System Platform Research Laboratories

AKABORI Satoshi
Assistant Manager
Secure System Platform Research Laboratories

HOTCHI Ryosuke
Secure System Platform Research Laboratories

SATODA Kozo
Director
Secure System Platform Research Laboratories

Information about the NEC Technical Journal

Thank you for reading the paper.
If you are interested in the NEC Technical Journal, you can also read other papers on our website.

Link to NEC Technical Journal website

Japanese

English

Vol.17 No.1 Special Issue on Open Network Technologies

– Network Technologies and Advanced Solutions at the Heart of an Open and Green Society

Remarks for Special Issue on Open Network Technologies
NEC's Technological Developments and Solutions for Open Networks

Vol.17 No.1
September 2023

Special Issue TOP

Papers for Special Issue

Open RAN and Supporting Virtualization Technologies
Innovations Brought by Open RAN
Reducing Energy Consumption in Mobile Networks
Self-configuring Smart Surfaces
Nuberu: Reliable RAN Virtualization in Shared Platforms
vrAIn: Deep Learning based Orchestration for Computing and Radio Resources in vRANs

Wireless Technologies for 5G/Beyond 5G
NEC's Energy Efficient Technologies Development for 5G and Beyond Base Stations toward Green Society
Millimeter-wave Beamforming IC and Antenna Modules with Bi-directional Transceiver Architecture
Radio-over-Fiber Systems with 1-bit Outphasing Modulation for 5G/6G Indoor Wireless Communication
28 GHz Multi-User Massive Distributed-MIMO with Spatial Division Multiplexing
28 GHz Over-the-Air Measurements Using an OTFS Multi-User Distributed MIMO System
Comprehensive Digital Predistortion for improving Nonlinear Affection and Transceivers Calibration to Maximize Spatial Multiplexing Performance in Massive MIMO with Sub6 GHz Band Active Antenna System
Black-Box Doherty Amplifier Design Method Without using Transistor Models
39 GHz 256 Element Hybrid Beam-forming Massive MIMO for 8 Multi-users Multiplexing

Initiatives in Open APN (Open Optical/All Optical)
NEC's Approach to APN Realization — Towards the Creation of Open Optical Networks
NEC's Approach to APN Realization — Features of APN Devices (WX Series)
NEC's Approach to APN Realization — Field Trials
Wavelength Conversion Technology Using Laser Sources with Silicon Photonics for All Photonics Network
Optical Device Technology Supporting NEC Open Networks — Optical Transmission Technology for 800G and Beyond

Initiatives in Core & Value Networks
Technologies Supporting Data Plane Control for a Carbon-Neutral Society
NEC's Network Slicing Supports People's Lives in the 5G Era
Application-Aware ICT Control Technology to Support DX Promotion with Active Use of Beyond 5G, IoT, and AI
Using Public Cloud for 5G Core Networks for Telecom Operators

Enhancing Network Services through Initiatives in Network Automation and Security
NEC's Approach to Full Automation of Network Operations in OSS
Autonomous Network Operation Based on User Requirements and Security Response Initiatives
Enhancing Information and Communications Networks Safety through Security Transparency Assurance Technology
Enhancing Supply Chain Management for Network Equipment and Its Operation

Network Utilization Solutions and Supporting Technologies
Positioning Solutions for Communication Service Providers
The Key to Unlocking the Full Potential of 5G with the Traffic Management Solution (TMS)
Introducing the UNIVERGE RV1200, All-in-one Integrated Compact Base Station, and Managed Services for Private 5G
Vertical Services Leveraging Private 5G to Support Industrial DX
Integrated Solution Combining Private 5G and LAN/RAN

Global 5G xHaul Transport Solutions
xHaul Solution Suite for Advanced Transport Networks
xHaul Transformation Services
xHaul Transport Automation Solutions
Fixed Wireless Transport Technologies in the 5G and Beyond 5G Eras
SDN/Automation for Beyond 5G
OAM Mode-Multiplexing Transmission System for High-Efficiency and High-Capacity Wireless Transmission

Toward Beyond 5G/6G
NEC's Vision and Initiatives towards the Beyond 5G Era

NEC Information

2022 C&C Prize Ceremony