An Intent-Driven Management Automation for 5G Mobile Networks

Yoseop Ahn* and Jaehoon (Paul) Jeong*
* Department of Computer Science & Engineering, Sungkyunkwan University, Suwon, Republic of Korea
Email: {ahnjs124, pauljeong}@skku.edu

***Abstract*—This paper introduces a Network Management System (NMS) for mobile network services in the area of 5G networks. It offers a structure authorized with Intent-Based Networking (IBN). Especially, the NMS supports network intent translator, closed-loop network control, and network audit system. It is a constructive framework with system factors supporting various features in NMS in terms of network management. The structure of the proposed NMS can make the network management be automatic and efficient in 5G mobile networks. Thus, it can perform effectively various services in the 5G mobile networks, such as the data gathering of Internet of Things (IoT) devices, the configuration and management of network slicing, and the Quality of Service (QoS) in 5G Vehicle-to-Everything (V2X).**

***Index Terms*—5G network, intent-based networking, network management, automation, interface.**

I. Introduction

Compared with 4G mobile networks, 5G mobile networks (also known as 5G networks) are the innovatory mobile networks concerning high speed, high-frequency bands, wide bandwidth, wide device connectivity, low energy usage, and intelligence. In particular, the ability to comprehend a user's intentions and enable comprehensive automation of network management depends significantly on the aspect of intelligence. The architecture of 5G networks draws from the experience of 4G networks while incorporating cutting-edge technologies like Network Functions Virtualization (NFV) [1] [2] and also Software-Defined Networking (SDN) [3], in addition to leveraging mmWave for minimal latency, blazing data speeds, and extensive network capacity [4].

The primary objective of 5G networks is to embrace intelligent networking. Intelligent networking plays a main role in equipping 5G networks together with Network Management System (NMS). It enables an autonomously driving network that boosts its operations and minimizes communication with humans (e.g., network users and administrators).

Implementing Intent-Based Networking (IBN) offers practical methods to enhance 5G networks with the NMS services [5] [6] [7]. The IBN concept introduces an closed-loop network management structure [5] that can dynamically suit the real-time conditions of an aimed network by gathering and processing the observing data from various Network Functions (NFs). These NFs encompass both Cloud-Native Network Functions (CNFs), Virtual Network Functions (VNFs), and Physical Network Functions (PNFs), which are relevant in edge and cloud computing environments. Within the 3rd Generation Partnership Project (3GPP), the Network Data Analytics Function (NWDAF) is established to analyze and gather VNFs and PNFs monitoring data within Cellular Communications [8] [9].

For the knowledgeable NMS services, this paper introduces a structural framework that unites the NWDAF and the IBN together to the 5G networks with Machine Learning (ML) and Artificial Intelligence (AI). The framework grants a network intent from either a user or a network operator to be translated to a network policy through a Network Intent Translator (NIT) [10]. A Natural Language Processing (NLP) can be used to implement an NIT [11]. The data model mapping between a network intent and a network policy needs to be functioned by a data model mapper for the intent translation [10]. The translated network policy can remotely configure NFs on top of CNFs, PNFs, or VNFs to enforce the requested intent in a goal network (e.g., 5G Networks). It also analyzes and accumulates the monitoring data from CNFs, PNFs, and VNFs so the network policy can be optimized and verified to fit the network intent requests. Note that this paper is based on our early IETF Internet Draft [12].

Within the contents of this paper, Network Management System (called NMS) addresses three key aspects, such as network intent translator, closed-loop network control, and network audit system. To facilitate these functionalities, this paper explains an architectural framework in detail, which has system components and interfaces. Notably, this framework is easily changing and extending its support to various NMS use cases within 5G networks. These use cases encompass data collection and analysis from Internet of Things (IoT) devices, enabling network slicing services, and enhancing Quality of Service (QoS) of 5G Vehicle-to-Everything (V2X) communications. In this paper, a specific example is illustrated as an IoT application in 5G networks, that is, the configuration, data collection, and data analysis for the IoT devices residing in 5G networks.

This paper's principal contributions can be enumerated as follows:

1) An Intent-Based Networking (IBN) network management automation in 5G networks. This IBN framework supports an easy network configuration with a high-level network intent, and supports a closed-loop network control for assurance and optimization of a requested network intent. (see Section III)

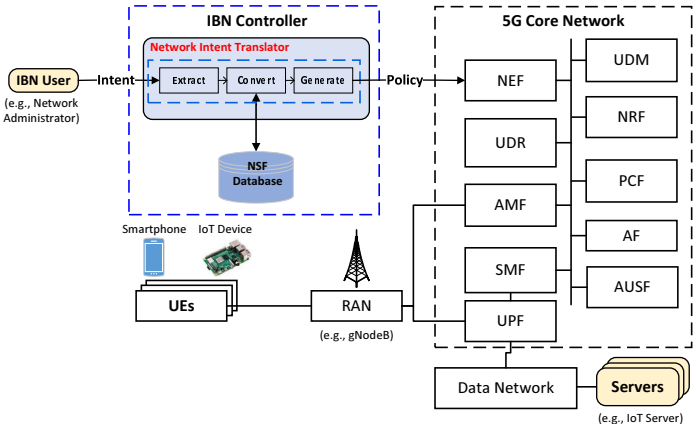

Fig. 1. Intent-Driven Management System for 5G Mobile Networks

2) A Network Intent Translator (NIT) for an easy network configuration. The NIT converts a high-level network intent into the corresponding low-level network policy. For the automatic intent translation, the NIT bridges smoothly an intent data model (called IBN Consumer-Facing Interface) with a network policy data model (called IBN NF-Facing Interface) by a data model mapper. (see Section IV)
3) A Network Audit System to remotely attestate the proposed NMS. This NAS finds vicious internal attacks such as supply chain attacks and insider attacks. All the IBN framework's elements report their activities to the NAS via Remote Attestation Interface. This NAS can identify malicious internal activities. (see Section V)

Thus, this paper proposes an Intent-Based Networking (IBN) network management system (NMS) within 5G networks. After building upon this foundational knowledge, this paper presents an IBN framework having Network Intent Translator (NIT), and Network Audit System (NAS). It highlights its potential to perform an effective role in the intelligent network management in the 5G networks. In addition, Fig. 1 shows the whole process of Intent-driven Network Management System in the 5G networks.

The remaining of this paper is structured as follows. Section II represents the new terms which are used in this paper. Section III explains the IBN-based framework for 5G networks which supports an intelligent network management. Section IV explains Network Intent Translator (NIT) to converts a network intent into the corresponding network policy. SectionV explains Network Audit System (NAS) which can identify vicious activities by either a supply chain attacker or an insider attacker. Section VII concludes this paper along with future work.

II. Terminology

The terminology which is used in [13], [14], and [15] is described in this paper. The following terminologies are defined below:

- **Intent:** An entity delivers a network intent to the IBN Controller. It is considered that a network intent is structured by the intent data model set in the 3GPP intent document [6].
- **Network Management System (NMS):** It involves the efficient enforcement of user or administrator-defined network intent within a target network system. This is achieved by translating these policies into detailed network policy rules through a network intent translator and then deploying them to the appropriate Network Functions (NFs). The NFs are continuously monitored and their activities and performance are analyzed. If necessary, adjustments are made to the network policy, including the generation and configuration of new network rules for the NFs.
- **Network Intent Translator (NIT):** It is the process of translating abstract network intent into a specific policy configuration that can be comprehended and implemented by Network Functions (NFs). These policies are tailored to suit various network services, ranging from data gathering for Internet of Things (IoT) devices to slice the network and also Quality of Service (QoS) provisioning in the communications of the Vehicle-to-Everything (V2X).
- **Closed-Loop Control System (CLCS):** The progression of a network service involves refining the network policy, which includes the adjustment of existing network rules and the incorporation of new rules, in response to identified network issues. These adjustments are informed by the comprehensive analysis of monitoring data collected from Network Functions (NFs).

III. Network Management Service

This part introduces an IBN-based framework for the 5G mobile networks. The foundation of this IBN based Framework is established upon the Interface to Network Security Functions (I2NSF) [13], [15]. As illustrated in Fig. 2, an IBN User can use the network functions by transmitting a network intent, which determines network goals and specifications that the IBN User intends to enforce through the Consumer-Facing Interface (CFI) to the IBN Controller.

A. Elements with IBN Framework for Network Management System

Listed below are the components of system within the IBN framework designed to be used in network management system in 5G networks.

- **IBN User**: This entity is responsible for conveying a network intent to IBN Controller. The process presumed that a network intent is constructed in the 3GPP intent document [6] by the intent data model.
- **IBN Controller:** This entity takes charge of controlling and managing various system elements within the IBN framework. It translates network intent into corresponding network policy and selects the suitable Network Functions (NFs) to carry out the network rules specified in the network policy.
- **Vendor's Management System (VMS):** This entity plays a crucial role by serving a virtualized NF image

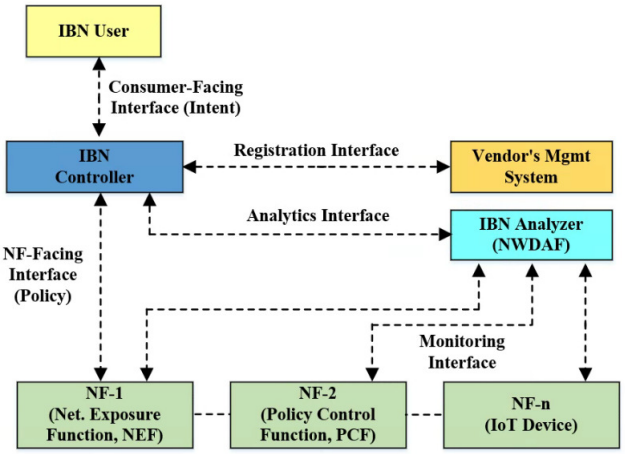

Fig. 2. IBN Framework for 5G Network Management Service

for a network service within the IBN framework. It also handles the NF's capabilities registration and access information by the IBN Controller.

- **Network Function (NF):** This entity takes on various functions, including Cloud-Native Network Function (CNF), Physical Network Function (called PNF), and Virtual Network Function (VNF). They are used for specific network services, such as IoT data aggregation, QoS provisioning, and network slicing in V2X communications.
- **IBN Analyzer:** This entity is the IBN Analyzer is tasked with the collection of monitoring data from NFs. It then employs advanced machine learning techniques and Deep Learning to analyze this data, evaluating the performance and activity of the NFs. In the context of 5G networks, the IBN Analyzer can also function as a Network Data Analytics Function (NWDAF) [TS-23.288][TS-29.520]. When any suspicious network issues emerge, such as traffic congestion or Quality of Service (QoS) degradation, the IBN Analyzer promptly generates a generation of network rules or a report of the augmentation, which is then communicated to the IBN Controller.

In IBN-based network services utilizing the IBN Analyzer, Closed-Loop Control System (CLCS) is a main IBN component for the IBN framework to analyzing and gathering the monitoring data from NFs. The precise details of the monitoring data analysis are out of the scope of this paper.

B. The IBN Framework Interfaces

These interfaces within the IBN framework can be modeled using YANG [16] or YAML [17], and network policies are transmitted via RESTCONF [18] or NETCONF [19]. REST API [20] support can also be provided for these interfaces according to 3GPP specifications.

- **Consumer-Facing Interface:** An interface transferring a network intent [21] between IBN User and IBN Controller.

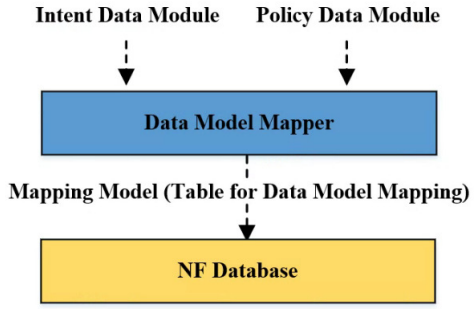

Fig. 3. Intent and Policy Data Models for Automatic Mapping

- **NF-Facing Interface:** An interface transferring a network policy [22] between an NF and IBN Controller (e.g., Network Exposure Function (NEF) of 5G Core Network).
- **Registration Interface:** An interface for the NF's capability registration between a VMS and IBN Controller and access information with the NF query or the IBN Controller for a required network policy [23].
- **Monitoring Interface:** An interface between an IBN Analyzer and NF to gather NF's monitoring data. It checks the performance and activity of an NF for a feasible network problem [24].
- **Analytics Interface:** An interface to send a report of the creation or the enhancement of IBN Controller's network rules between IBN Controller and IBN Analyzer. Then IBN Controller can apply the network rules report to its network intent management.

In IBN-based networking services with FSM, analytics Interface is IBN framework's main interface to send an network rules generation or analytics report of the augmentation to IBN Controller through the monitoring data analysis from NFs.

IV. Network Intent Translator

To improve the process of Network Intent Translation within an IBN Controller, it is important to implement a Network Intent Translator (NIT). This translator serves the role of converting a network intent (called intent) into its corresponding network policy (called policy). For the automation of NIT services, the IBN framework must seamlessly connect a policy data model and an intent data model in an automatic manner [10].

In Fig. 3, we can observe the policy data model and automatic mapping of intent for network policies. Automatic Data Model Mapper performs this task by taking a policy data module about the NF-Facing Interface and an intent data module about the Consumer-Facing Interface. After that, it creates a mapping table that links the data features of the intent data module with the related data features of the policy data module. Moreover, it creates a production rules set following a grammar structure to facilitate the structure of an XML or JSON file containing the rules for the network policy.

In Fig. 4, we can observe the procedure of network intent translation. Within the IBN Controller, the network intent translator consists of Policy Data Model Mapper, the Policy

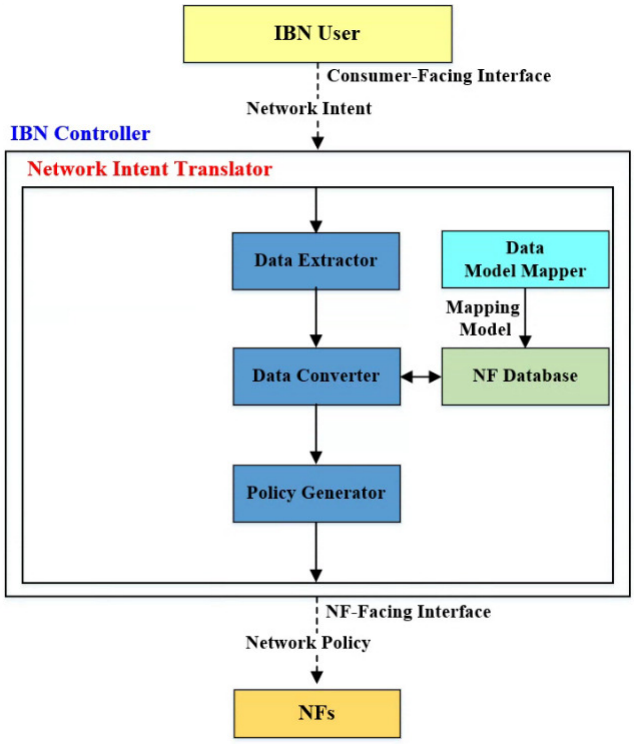

Fig. 4. The process of Network Intent Translation

Data Extractor, the Policy Data Converter, and the Policy Generator.

Data Model Mapper is responsible for mapping attributes and the network intent value to the corresponding features and the values in a policy of the network. Note that network intent values may involve a human language and need to be transformed into a suitable network policy value. Data Extractor's role is to extract the attribute values associated with a network intent which is provided by an User of IBN to the IBN Controller via the Consumer-Facing Interface [21]. Data Converter transforms the attribute values of the network intent into the corresponding network policy attribute values to generate the network policy [22]. Lastly, Policy Generator creates the related network policy transferred by the IBN Controller to an suitable NF via NF-Facing Interface [22].

V. Network Audit System

The IBN framework confides in NFs offered by VMS and presumes that NFs work for the network services properly [14]. Thus, it is susceptible to both a supply chain attack and an insider attack. To identify the vicious activity resulting from either a supply chain attack via a compromised VMS or an insider attack through a vicious VMS, the IBN framework necessitates a network audit system. This network audit system can facilitate the monitoring data generated in the IBN framework and the non-repudiation of configuration commands.

These are four main objectives in a network audit system:

- **Objective 1:** To verify the presense of a management system, a network policy, and its processes;

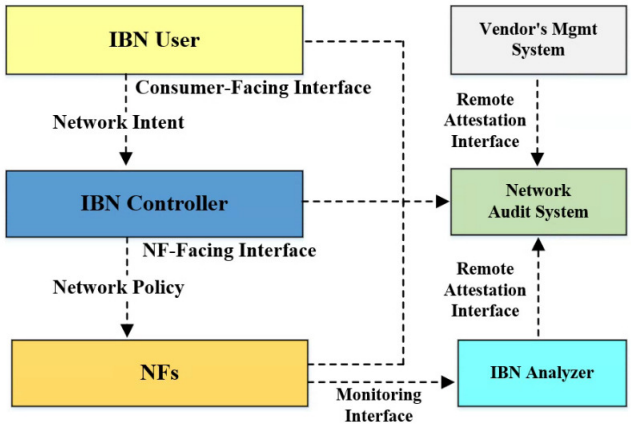

Fig. 5. Network Audit System for Activity Auditing

- **Objective 2:** To understand and validate the potential risks and weak points of either a supply chain attack or an insider attack;
- **Objective 3:** To assess administrative matters and existing network controls on operational;
- **Objective 4:** To offer corrective actions and recommendations to IBN Controller for security improvement and further network.

In Fig. 5, we can see the activity auditing process within the IBN framework using a network audit system. All the IBN framework components inform their behaviors (such as monitoring data and configuration commands), to Network Audit System transactions via the Remote Attestation Interface [25]. This network audit system can inspect the reported components of IBN activities to identify vicious behaviors such as a supply chain attack and an insider attack. Note that the system of network audit can be executed via methods like remote evidence [26] [25] or Blockchain [27]. The specific applications are beyond the confines of this paper.

To establish a set of essential controls aimed at mitigating the risks posed by the attack of an insider or a supply chain, the network audit system should regularly investigate the behaviors of all IBN framework elements, monitor the possible risks, and take appropriate actions since threats and vulnerabilities may be expanded in different environments as time progresses.

VI. IoT Device Data Aggregation Use Case

In this part, we describe a use case presenting the a policy establishment for the data collection from IoT devices for 5G networks within the IBN framework.

Fig. 6 illustrates the enforcement sequence about the data aggregation intent for an IoT device within the IBN Framework.

- IBN User sends a request of the Network Intent to IBN Controller.
- The IBN Controller interprets the request through the Network Intent Translator (NIT). Following Data Ex-

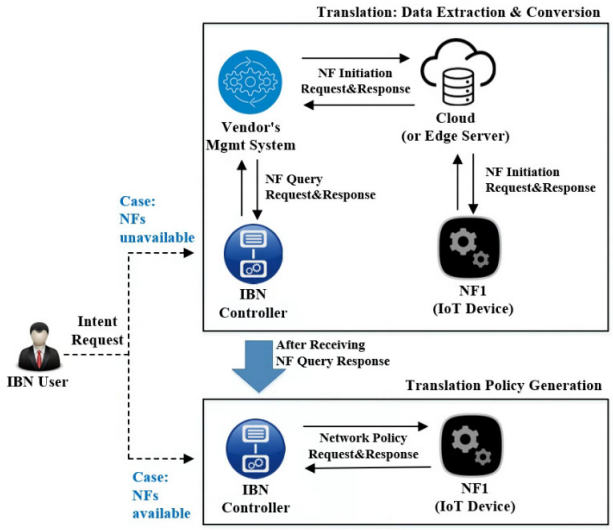

Fig. 6. Intent Enforcement of IoT Device Data Gathering within the IBN Framework

traction and Data Conversion steps, the NIT identifies suitable NFs for the request.

- If it is possible to use the NFs for the asked network policy, check the Policy Generation step in NIT. If it is not possible to use the NFs for the asked network policy, check the next step.
- The IBN Controller gives a Request of NF Query to the System of Vendor's Management (referred to as VMS) to identify a relevant NF for the required policy of the network.
- In the presence of a registered NF with VMS, this VMS dispatches an Request of NF Initialization to the Cloud (also called Edge Server) for the initialization of the NF.
- The Cloud (also called Edge Server) for the Request of NF Initialization to the proper NF for self-initialization.
- The NF undergoes initialization to execute tasks related to network policies within the 5G mobile networks.
- The NF gives a Response of NF Initialization to the Cloud (also called Edge Server) to signal its state to commence a task.
- The Cloud (also called Edge Server) for the Response of NF Initialization to VMS, signaling that the NF is prepared to initiate a work.
- VMS gives a Response of NF Query to the IBN Controller, indicating that the NF is prepared to execute tasks related to network access information.
- IBN Controller initiates the Policy Generation step within its NIT, incorporating the information of network access of the relevant NFs.
- IBN Controller gives a Request of Network Policy to the designated NF.
- The NF generates the configuration based on the provided Network Policy Request to execute the required task.
- The NF gives a Response of Network Policy to the IBN Controller to announce it's ready to execute the required work.

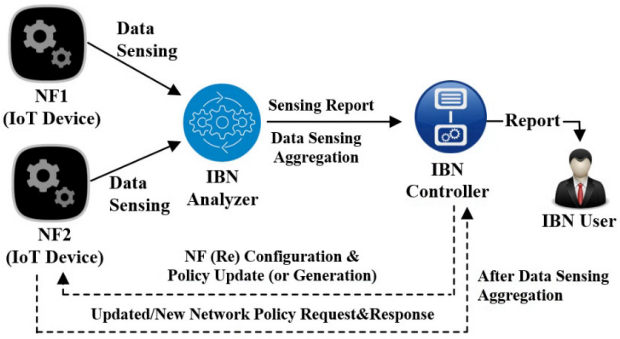

Fig. 7. Reporting of IoT Device Data Gathering within the IBN Framework

Fig. 7 outlines the process of reporting for IoT device data gathering in the IBN Framework, as detailed below:

- NF1 transmits Data Sensing to IBN Analyzer.
- NF2 transmits Data Sensing to IBN Analyzer.
- Analyzer of IBN creates Data Sensing Grouping and investigates the gathered sensing data using the techniques of Machine Learning (ML). Subsequently, it compiles a Sensing Report for the Controller of IBN.
- IBN Analyzer transmits a Sensing Report to the IBN Controller.
- IBN Controller reviews the Sensing Report for potential future action. If additional tasks are necessary, it either updates the operating network policy or creates the other new network policy.
- In cases where reporting is deemed necessary, the IBN Controller optionally gives the related report for the additional work to the IBN User.
- To initiate future action, the IBN Controller gives either a New Request of NF Policy or an Updated Request of NF Policy to the proper NFs.
- The relevant NFs configure the new NF Policy or adjust the Updated NF Policy within their respective systems.
- The appropriate NFs send a NEW NF Policy Response or an Updated NF Policy Response to the IBN Controller.

Therefore, this paper introduces the viability of the automation of intent-based network management within 5G networks.

VII. Conclusion

This paper proposes an Intent-Driven Management Automation for 5G Mobile Networks. For Network Management System (called NMS), the proposed system takes advantage of Intent-Based Networking (IBN). This system supports a closed-loop network control for the accurate enforcement of a network intent through the monitoring, analysis, optimization, and policy (re)generation. For a user's intent translation into a network policy, this paper proposes a Network Intent Translator (NIT). Also, this paper shows a use case such as data gathering of Internet of Things (IoT) devices through NMS. As future work, to fully support IBN, we will design and implement of NIT and NMS for the intent-based network

management in 5G networks. And we will create and deploy the practical solutions for translating network intent into network policies and automating network management processes within 5G networks. Within 5G network environments, we will conduct in-depth studies and experiments to explore and validate the effectiveness of NMS in the specific use cases.

ACKNOWLEDGMENTS

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government, Ministry of Science and ICT (MSIT) (No. 2023R1A2C2002990). This work was supported in part by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT)(No. 2022-0-01015, Development of Candidate Element Technology for Intelligent 6G Mobile Core Network). Note that Jaehoon (Paul) Jeong is the corresponding author.

REFERENCES

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

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

[3] M. Boucadair and C. Jacquenet, "Software-Defined Networking: A Perspective from within a Service Provider Environment," *RFC 7149*, March 2014. [Online]. Available: https://www.rfceditor.org/rfc/rfc7149

[4] "System Architecture for the 5G System (5GS)," September 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3554

[5] A. Clemm, L. Ciavaglia, L. Z. Granville, and J. Tantsura, "Intent-Based Networking - Concepts and Definitions," *RFC 8192*, October 2022. [Online]. Available: https://www.rfc-editor.org/info/rfc9315

[6] "Intent Driven Management Services for Mobile Networks," September 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3554

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

[8] "Architecture Enhancements for 5G System (5GS) to Support Network Data Analytics Services," September 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3579

[9] "Network Data Analytics Services," September 2022. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3355

[10] J. P. Jeong, P. Lingga, and J. Yang, "Guidelines for Security Policy Translation in Interface to Network Security Functions," Internet-Draft draft-yang-i2nsf-security-policy-translation-15, 24 July 2023, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-yang-i2nsf-securitypolicy-translation-15

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

[12] J. P. Jeong, Y. Ahn, Y. Kim, and J.-S. Park, "Intent-Based Network Management Automation in 5G Networks," *draft-jeong-nmrg-ibn-network-management-automation-03*, Nov. 2023. [Online]. Available: https://datatracker.ietf.org/doc/draft-jeong-nmrg-ibn-network-management-automation/

[13] L. Diego, L. Edward, D. Linda, S. John, and K. Rakesh, "Framework for Interface to Network Security Functions," *RFC 8329*, February 2018. [Online]. Available: https://www.rfc-editor.org/info/rfc8329

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

[15] J. P. Jeong, P. Lingga, P. Jung-Soo, D. Lopez, and S. Hares, "Security Management Automation of Cloud-Based Security Services in I2NSF Framework," Internet-Draft draft-jeong-i2nsf-security-management-automation-06, 24 July 2023, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-jeong-i2nsf-security-management-automation/06

[16] B. Martin, "YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF)," *RFC 6020*, october 2010. [Online]. Available: https://www.rfc-editor.org/info/rfc6020

[17] I. Brian, C. E. Clark, and O. Ben-Kiki, "Yet Another Markup Language (YAML) 1.0," October 2023. [Online]. Available: https://yaml.org/spec/history/2001-05-26.html

[18] A. Bierman, M. Bjorklund, and K. Watsen, "RESTCONF Protocol," *RFC 8040*, January 2017. [Online]. Available: https://datatracker.ietf.org/doc/rfc8040/

[19] R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, "Network Configuration Protocol (NETCONF)," *RFC 6241*, January 2011. [Online]. Available: https://datatracker.ietf.org/doc/rfc6241/

[20] R. T. Fielding and R. N. Taylor, "Principled Design of the Modern Web Architecture," *ACM Transactions on Internet Technology*, vol. 2, no. 2, May 2002. [Online]. Available: https://doi.org/10.1145/514183.514185

[21] J. P. Jeong, C. Chung, T.-J. Ahn, R. Kumar, and S. Hares, "I2NSF Consumer-Facing Interface YANG Data Model," Internet-Draft draft-ietf-i2nsf-consumer-facing-interface-dm-31, May 2023, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-i2nsf-consumer-facing-interface-dm/31/

[22] J. T. Kim, J. P. Jeong, P. Jung-Soo, S. Hares, and Q. Lin, "I2NSF Network Security Function-Facing Interface YANG Data Model," Internet-Draft draft-ietf-i2nsf-nsf-facing-interface-dm-29, June 2022, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-i2nsf-nsf-facing-interface-dm/29/

[23] S. Hyun, J. P. Jeong, T. Roh, S. Wi, and P. Jung-Soo, "I2NSF Registration Interface YANG Data Model for NSF Capability Registration," Internet-Draft draft-ietf-i2nsf-registration-interface-dm-26, May 2023, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-i2nsf-registration-interface-dm/26/

[24] J. P. Jeong, P. Lingga, S. Hares, L. Xia, and H. Birkholz, "I2NSF NSF Monitoring Interface YANG Data Model," Internet-Draft draft-ietf-i2nsf-nsf-monitoring-data-model-20, June 2022, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-i2nsf-nsf-monitoring-data-model/20/

[25] P. Yang, M. Chen, L. Su, D. Lopez, J. P. Jeong, and L. Dunbar, "I2NSF Remote Attestation Interface YANG Data Model," Internet-Draft draft-yang-i2nsf-remote-attestation-interface-dm-01, June 2022, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/draft-yang-i2nsf-remote-attestation-interface-dm/01/

[26] H. Birkholz, D. Thaler, M. Richardson, N. Smith, and W. Pan, "Remote ATtestation procedureS (RATS) Architecture," Internet-Draft draft-ietf-rats-architecture-22, January 2023, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-rats-architecture-22

[27] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," May 2009. [Online]. Available: https://bitcoin.org/bitcoin.pdf