사물인터넷융복합논문지 Vol. 12, No. 4, pp. 87-92, 2026 https://doi.org/10.20465/KIOTS.2026.12.4.087

대규모 사물인터넷 환경에서의 시그널링 폭주 분석 정보 및 활용 방안

성지훈[1], 경연웅[2*]
[1]전북대학교 컴퓨터인공지능학부 교수, [2]서울과학기술대학교 전자공학과 교수

Signalling Storm Analytics Information and Its Utilization in Massive IoT Environments

Jihoon Sung[1], Yeunwoong Kyung[2*]
[1]Professor, Department of Computer Science and Artificial Intelligence, Jeonbuk National University
[2]Professor, Department of Electronic Engineering, Seoul National University of Science and Technology

요 약 최근 스마트팩토리, 스마트시티 등 대규모 사물인터넷(Massive IoT) 서비스의 확산으로 인해 다수의 단말이 동시에 네트워크에 접속하는 환경이 증가하고 있다. 이러한 환경에서는 단말의 동시 접속 및 반복적인 재시도로 인해 시그널링 폭주(Signalling Storm)가 발생할 수 있으며, 이는 네트워크 성능 저하와 서비스 품질 저하를 초래할 수 있다. 본 논문에서는 3GPP 표준에서 정의된 시그널링 폭주 분석(Signalling Storm Analytics)의 동작 절차와 제공 정보를 분석하고, 이를 Massive IoT 환경에서 어떻게 활용할 수 있는지를 검토하였다. 이를 위해 스마트미터, 스마트팩토리 및 대규모 펌웨어 업데이트 환경을 대표적인 Massive IoT 시나리오로 고려하여 시그널링 폭주 분석 정보의 운영 활용 가능성을 고찰하였다. 본 연구는 표준에서 정의된 분석 정보를 실제 Massive IoT 시나리오와 연계하여 설명하고 구체적인 활용 예를 제시함으로써, 시그널링 폭주 분석 정보에 대한 이해를 돕고 활용 가능성을 구체화하였다는 점에서 의의를 가진다.

주제어 : 대규모 사물인터넷, 시그널링 폭주, 5G 코어 네트워크, 네트워크 데이터 분석 기능, 네트워크 안정성

Abstract As Massive Internet of Things (IoT) services, such as smart factories and smart cities, continue to expand, the number of devices simultaneously accessing networks is increasing. In such environments, repeated or synchronized device access behaviors may lead to signalling storms, resulting in network performance degradation and reduced service quality. This paper analyzes the operational procedures and information provided by Signalling Storm Analytics defined in 3GPP standards and examines how such information can be utilized in Massive IoT environments. To this end, smart metering, smart factory, and large-scale firmware update environments are considered representative Massive IoT scenarios to investigate the potential operational use of Signalling Storm Analytics information. By linking the analytics information defined in the standards to practical Massive IoT scenarios and presenting specific examples of its utilization, this study contributes to a better understanding of Signalling Storm Analytics information and clarifies its potential applications.

Key Words : Massive IoT, Signalling storm, 5G core network, Network data analytics function, network stability

본 연구는 2026년 과학기술정통신부 및 정보통신기획평가원의 SW중심대학사업 지원을 받아 수행되었음(2022-0-01067)
*교신저자 : 경연웅(ywkyung@seoultech.ac.kr)
접수일 2026년 06월 19일 수정일 2026년 08월 14일 심사완료일 2026년 08월 18일

1. 서론

최근 스마트팩토리, 스마트시티, 스마트빌딩 등 다양한 사물인터넷(Internet of Things, IoT) 서비스의 확산으로 인해 대규모 단말이 네트워크에 연결되는 환경이 증가하고 있다 [1]. 기존의 네트워크 서비스는 상대적으로 제한된 수의 단말을 대상으로 안정적인 연결성과 데이터 전송 성능을 제공하는 데 초점을 두었다. 반면, 대규모 사물인터넷(Massive IoT) 환경에서는 매우 많은 수의 단말이 소량의 데이터를 주기적으로 전송하는 특성을 가지며 [2], 이에 따라 대규모 단말 연결을 효율적으로 지원하기 위한 새로운 네트워크 요구사항이 등장하게 되었다 [3]. 이러한 Massive IoT 서비스 요구사항을 지원하기 위하여 이동통신 표준기구인 3GPP(3rd Generation Partnership Project)에서는 5G의 대표적인 서비스 유형 중 하나로 massive Machine-Type Communications (mMTC)를 정의하였다 [4]. 그러나 Massive IoT 환경에서는 단말 수 증가에 따른 네트워크 확장성 문제뿐만 아니라, 동기화된 접속 및 반복적인 재접속으로 인해 시그널링 트래픽이 집중되는 새로운 운영 이슈가 발생할 수 있다. 특히, 특정 시점에 다수의 단말이 동시에 접속 절차를 수행하는 경우 시그널링 폭주(Signalling Storm)가 발생할 수 있으며, 이는 네트워크 성능 저하 및 서비스 품질 저하를 초래할 수 있다.

기존의 시그널링 폭주 대응 연구는 시그널링 폭주 탐지 기법[5, 6], 시그널링 트래픽 분석 기법[7, 8] 및 시그널링 처리 효율화 기법[9, 10] 등을 중심으로 수행되어 왔다. 그러나 대부분의 연구는 탐지 및 완화 기법의 성능 향상에 초점을 두고 있으며, 실제 네트워크 운영 환경에서 이를 어떻게 적용하고 활용할 것인지에 대한 논의는 상대적으로 부족한 실정이다. 특히, 다양한 장비와 네트워크 기능(Network Function, NF)이 공존하는 실제 운영 환경에서는 개별적인 대응 기법뿐만 아니라 기존 운영 체계와의 연계 및 상호운용성을 고려한 접근 방식이 요구된다. 이러한 요구사항을 충족하기 위한 접근 방식 중 하나로 이동통신 국제 표준인 3GPP 기술을 활용할 수 있다. 3GPP에서는 NWDAF(Network Data Analytics Function)를 통해 다양한 네트워크 분석 기능을 정의하고 있으며, Signalling Storm Analytics 또한 그 중 하나이다 [11]. 또한 최근 3GPP에서는 비공용 네트워크(Non-Public Network, NPN)를 지원함으로써 산업 환경에서의 적용 가능성을 확대하고 있다 [12, 13]. 이에 따라, Signalling Storm Analytics와 같은 표준 기반 분석 기능의 실제 활용 방안에 대한 검토가 필요한 시점이다.

3GPP TS 23.288[11]에서는 시그널링 폭주 상황을 분석하기 위한 Signalling Storm Analytics를 규정하고 있다. Signalling Storm Analytics는 NF로부터 수집된 정보를 기반으로 시그널링 폭주 가능성을 분석하고, 관련 분석 정보를 제공함으로써 네트워크 운영 의사결정을 지원한다. 그러나 표준 문서는 분석 절차와 제공 정보 중심으로 기술되어 있어, Massive IoT 환경에서 해당 기능을 실제로 어떻게 활용할 수 있는지에 대한 설명은 제한적이다.

이에 본 논문에서는 3GPP TS 23.288에서 정의된 Signalling Storm Analytics의 동작 절차와 제공 정보를 분석하고, 이를 Massive IoT 환경에서 어떻게 활용할 수 있는지를 검토한다. 이를 위해 스마트미터, 스마트팩토리 및 대규모 펌웨어 업데이트 환경을 대표적인 Massive IoT 시나리오로 고려하여 시그널링 폭주 분석 정보의 운영 활용 가능성을 고찰한다. 본 연구는 표준에서 정의된 Signalling Storm Analytics의 기능과 정보를 실제 Massive IoT 시나리오와 연계하여 설명하고, 각 시나리오에서의 구체적인 활용 가능성을 검토하였다는 점에서 의의를 가진다.

2. 3GPP 시그널링 폭주 분석 기능

2.1 NWDAF 개요

NWDAF는 3GPP에서 정의한 네트워크 데이터 분석 기능을 제공하는 NF로서, 다른 NF(예: Access and Mobility management Function (AMF), Session Management Function(SMF), Policy Control Function (PCF))으로부터 수집한 정보를 기반으로 인공지능 기법을 활용하여 다양한 분석 정보를 생성하여 네트워크 운영 및 제어를 지원한다. NWDAF는 네트워크 상태 분석, 사용자 경험 분석, 이상 상황 탐지 등 다양한 분석 기능을 제공하며, 분석 결과는 분석을 요청한 다른 NF에 제공될 수 있다.

5G 코어 네트워크에서는 네트워크 데이터에 대한 분석 기능의 중요성이 증가함에 따라 NWDAF가 도입되었으며, 이후 다양한 분석 항목이 지속적으로 추가되어 왔다. 최근에는 NWDAF 기반 네트워크 분석 기술의 활용 범위와 적용 방안에 대한 연구도 활발히 진행되고 있다 [14, 15]. Signalling Storm Analytics는 이러한 NWDAF 기반 분석 기능 중 하나이다.

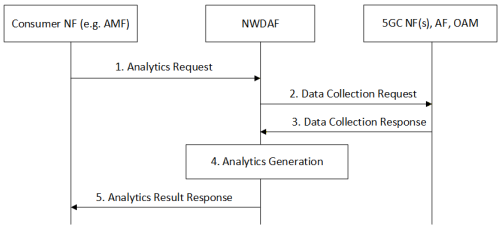
2.2 Signalling Storm Analytics 개요

Signalling Storm Analytics는 시그널링 폭주 발생 가능성을 분석하고 관련 정보를 제공한다. 시그널링 폭주는 특정 시점에 다수의 정상 단말이 동시에 접속 절차를 수행하거나 반복적인 재접속을 시도함에 따라 과도한 시그널링 트래픽이 발생하는 현상을 의미한다. 이러한 현상은 네트워크 자원의 비효율적인 사용을 초래할 뿐만 아니라 서비스 품질 저하로 이어질 수 있다.

3GPP TS 23.288에서는 Signalling Storm Analytics를 통해 시그널링 폭주와 관련된 분석 정보를 생성하고, 이를 요청한 NF에 제공할 수 있도록 규정하고 있다. 이를 통해 네트워크 운영자는 시그널링 폭주 상황을 조기에 인지하고 적절한 대응 방안을 수립할 수 있다.

2.3 Signalling Storm Analytics 절차

Signalling Storm Analytics는 일반적인 NWDAF 분석 요청 및 응답 절차를 기반으로 동작한다. 먼저, 분석 정보를 필요로 하는 NF는 NWDAF에 분석 요청을 전달한다. 이후 NWDAF는 관련 NF(예: AMF, SMF)로부터 필요한 정보를 수집하고 분석을 수행한다. 분석 결과가 생성되면 요청 NF에 분석 정보를 제공할 수 있다.



[Fig. 1] Signalling Storm Analytics procedure based on 3GPP TS 23.288.

Fig. 1은 TS 23.288에서 정의된 Signalling Storm Analytics 절차를 기반으로 재구성한 것이다. Signalling Storm Analytics 절차는 다음과 같이 구성된다.

1. Consumer NF(예: AMF)는 NWDAF에 Signalling Storm Analytics를 요청한다.
2. NWDAF는 분석에 필요한 정보 수집을 위해 관련 NF, AF(Application Function) 또는 OAM(Operation, Administration, and Maintenance)에 정보를 요청한다.
3. 요청을 수신한 NF, AF, 또는 OAM은 NWDAF에게 정보를 제공한다.
4. NWDAF는 수집된 정보를 기반으로 시그널링 폭주 관련 분석 정보를 생성한다.
5. NWDAF는 생성된 분석 결과를 Consumer NF에 제공한다.

2.4 Signalling Storm Analytics 제공 정보

3GPP TS 23.288에서는 앞 절에서 설명한 절차를 기반으로 Signalling Storm Analytics를 통해 시그널링 폭주 예측 결과와 관련된 다양한 분석 정보를 제공할 수 있도록 정의하고 있다. 제공되는 정보는 시그널링 폭주의 발생 가능성뿐만 아니라, 영향을 받는 NF, 발생 원인 및 영향 범위 등을 포함하며, 네트워크 운영자의 대응 의사결정을 지원하는 데 활용될 수 있다.

Table 1은 Massive IoT 환경에서의 활용 가능성을 고려하여 본 논문에서 주목한 주요 Signalling Storm Analytics 정보를 정리한 것이다.

〈Table 1〉 Key analytics information provided by Signalling Storm Analytics

Analytics Information	Description
Cause ID	Cause of signalling storm
Source UE / UE Group	Affected UE or UE group information
Target NF	Impacted NF
S-NSSAI	Affected network slice
DNN	Data network associated with the signalling storm
Confidence	Confidence level

Table 1에서 제시한 분석 정보는 시그널링 폭주 상황을 조기에 인지하고 적절한 대응 방안을 수립하기 위한 기초 자료로 활용될 수 있다. 특히 Cause ID와 UE Group 정보는 원인 식별에 활용될 수 있으며, S-NSSAI 및 DNN 정보는 영향을 받는 서비스 영역을 파악하는 데 활용될 수 있다. Confidence 정보는 분석 결과의 신뢰 수준을 판단하는 기준으로 활용될 수 있다. 한편, Target NF 정보는 시그널링 폭주로 인해 영향을 받을 수 있는 NF를 식별하는 데 활용될 수 있으며, 운영자는 이를 기반으로 자원 재할당 또는 정책 조정과 같은 대응 방안을 검토할 수 있다.

3. Massive IoT 환경에서의 활용 방안

3.1 Massive IoT 기반 시그널링 폭주 시나리오

Massive IoT 환경에서는 다수의 단말이 동일한 시점에 접속하거나 반복적인 재접속을 수행함에 따라 시그널링 폭주가 발생할 수 있다. 본 논문에서는 대표적인 Massive IoT 기반 시그널링 폭주 시나리오로 스마트미터, 스마트팩토리 및 대규모 펌웨어 업데이트 환경을 고려하였다.

첫째, 스마트미터 환경에서는 다수의 계량기가 동일한 보고 주기를 사용하여 데이터를 전송하는 경우 특정 시점에 접속 요청이 집중될 수 있다. 스마트미터는 일반적으로 동일한 설정값과 보고 주기를 사용하므로 특정 시점에 대규모 단말의 접속이 집중될 가능성이 높다. 이러한 특성은 시그널링 폭주 발생 가능성을 증가시키는 요인으로 작용할 수 있다.

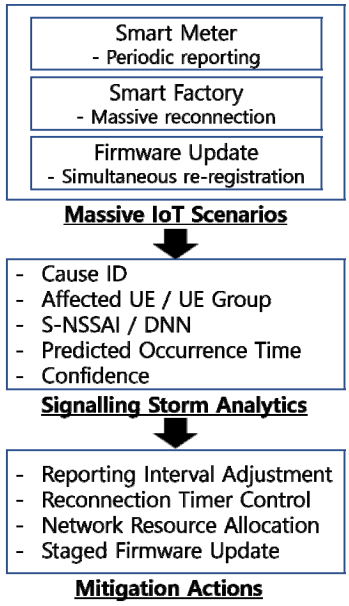
둘째, 스마트팩토리 환경에서는 네트워크 재부팅 및 장애 복구 이후 다수의 센서 및 제어 단말이 동시에 재접속을 시도함으로써 시그널링 부하가 증가할 수 있다. 특히 생산 설비와 연계된 센서 및 제어 단말은 장애 복구 이후 즉시 통신을 재개하려는 특성을 가지므로 순간적인 시그널링 집중 현상이 발생할 수 있다.

셋째, 대규모 펌웨어 업데이트 이후 다수의 단말이 동시에 재기동 및 재등록 절차를 수행하는 경우 일시적인 시그널링 폭주가 발생할 수 있다. 최근 보안 및 기능 개선을 위한 원격 업데이트가 널리 활용됨에 따라, 대규모 단말의 동시 재등록 문제는 중요한 운영 이슈로 부각되고 있다.

이러한 시나리오는 모두 정상 단말에 의해 발생할 수 있으며, 비정상 트래픽이나 공격 상황이 아니더라도 네트워크 운영에 영향을 줄 수 있다는 특징을 가진다. 따라서, 이러한 시그널링 폭주 상황에 대한 사전 예측 및 대응을 지원할 수 있는 Signalling Storm Analytics의 활용 방안을 검토할 필요가 있다.

3.2 Signalling Storm Analytics 활용 방안

앞서 설명한 시나리오에서는 시그널링 폭주 발생 이전에 관련 징후를 파악하고 적절한 대응을 수행하는 것이 중요하다. 2장에서 살펴본 바와 같이 Signalling Storm Analytics는 시그널링 폭주 발생 가능성, 영향을 받는 NF, 시그널링 폭주의 원인, 관련 UE 또는 UE 그룹 정보 등을 제공함으로써 이러한 운영 의사결정을 지원할 수 있다. Fig. 2는 Massive IoT 환경에서 Signalling Storm Analytics를 활용하여 시그널링 폭주 상황을 인지하고 대응하는 예를 나타낸다. Fig. 2에서와 같이 Massive IoT 환경에서 발생 가능한 다양한 시그널링 폭주 시나리오는 Signalling Storm Analytics를 통해 분석될 수 있다. 분석 결과로 제공되는 Cause ID, UE Group, S-NSSAI 및 Target NF 정보는 운영자가 적절한 대응 정책을 선택하는 데 활용될 수 있다.



[Fig. 2] Example Utilization of Signalling Storm Analytics in Massive IoT environments.

Table 2는 3GPP TS 23.288에서 정의된 Signalling Storm Analytics의 제공 정보를 기반으로, 본 연구에서 고려한 Massive IoT 시나리오별 정책 적용 조건, 대응 정책 및 기대 효과의 예를 정리한 것이다.

예를 들어, 스마트미터 환경에서는 특정 UE 그룹의 동시 접속으로 인해 시그널링 폭주 발생 가능성이 높은 것으로 예측되는 경우, Cause ID 및 관련 UE 그룹 정보를 활용하여 원인 및 대상 단말 그룹을 식별할 수 있다. 운영자는 이러한 분석 결과를 기반으로 해당 UE 그룹의 보고 주기 또는 접속 시점을 분산함으로써 특정 시점에 집중되는 접속 요청과 시그널링 부하를 완화할 수 있다.

또한 스마트팩토리 환경에서는 특정 NF 또는 중요 서비스 영역이 시그널링 폭주의 영향을 받을 것으로 분석되는 경우, Target NF, S-NSSAI 및 DNN 정보를 활용하여 영향을 받을 수 있는 NF와 서비스 영역을 식별할 수 있다. 운영자는 이러한 분석 결과를 기반으로 중요 생산 설비와 관련된 네트워크 자원을 우선적으로 할당하거나 관련 정책을 조정함으로써 시그널링 폭주가 중요 설비의 통신에 미치는 영향을 완화할 수 있다.

〈Table 2〉 Application Conditions, Response Policies, and Expected Effects Based on Signalling Storm Analytics

1. Smart Metering 1) Analytics Info.: - Cause ID, UE Group 2) Application Condition: - Potential signalling storm associated with simultaneous access by a UE group 3) Response Policy: - Reporting and access time dispersion 4) Expected Effect: - Mitigation of concentrated signalling traffic
2. Smart Factory 1) Analytics Info.: - Target NF, S-NSSAI, DNN 2) Application Condition: - Potential impact on a target NF or service 3) Response Policy: - Resource prioritization and policy adjustment 4) Expected Effect: - Mitigation of impact on critical communications
3. Large-scale Firmware Update 1) Analytics Info.: - Cause ID, UE Group 2) Application Condition: - Potential signalling storm associated with simultaneous re-registration by a UE group 3) Response Policy: - Staged update and re-registration time dispersion 4) Expected Effect: - Mitigation of concentrated re-registration and signalling traffic

대규모 펌웨어 업데이트 환경에서는 업데이트 대상 UE 그룹의 동시 재등록으로 인한 시그널링 폭주 가능성이 예상되는 경우, Cause ID 및 UE Group 등의 분석 정보를 기반으로 영향을 받을 수 있는 단말 그룹을 식별할 수 있다. 운영자는 이를 바탕으로 단계적 업데이트 정책을 적용하거나 단말의 재접속 시점을 분산시킴으로써 특정 시점에 집중되는 재등록 요청과 시그널링 부하를 완화할 수 있다.

또한, Confidence 정보는 분석 결과의 신뢰 수준을 판단하고 운영 정책의 적용 여부를 검토하기 위한 보조적인 정보로 활용될 수 있다.

이와 같이 Signalling Storm Analytics는 Massive IoT 환경에서 발생 가능한 시그널링 폭주 상황을 조기에 인지하고, 네트워크 운영자가 적절한 예방 및 완화 정책을 수립할 수 있도록 지원한다. 특히 정상 단말에 의해 발생하는 시그널링 폭주의 경우 사후 대응보다 사전 예측 기반 대응이 중요하다. 따라서, Signalling Storm Analytics는 Massive IoT 환경에서 발생 가능한 시그널링 폭주 상황을 사전에 인지하고, 이에 대한 운영 정책 수립을 지원하는 표준 기반 분석 정보로 활용될 수 있다.

4. 결론

본 논문에서는 3GPP TS 23.288에서 정의된 Signalling Storm Analytics의 동작 절차와 제공 정보를 분석하고, 해당 분석 정보를 Massive IoT 환경에서 어떻게 활용할 수 있는지를 검토하였다. 이를 위해 스마트미터, 스마트 팩토리 및 대규모 펌웨어 업데이트 환경을 대표적인 Massive IoT 시나리오로 고려하여 시그널링 폭주 분석 정보의 운영 활용 가능성을 고찰하였다.

검토 결과, Signalling Storm Analytics는 시그널링 폭주 발생 가능성, 영향 범위, 관련 UE 그룹 및 네트워크 정보 등을 제공함으로써 시그널링 폭주 상황을 조기에 인지하고 대응 정책 수립을 지원할 수 있는 것으로 나타났다. 또한, 제공되는 분석 정보를 활용하여 접속 시점 분산, 네트워크 자원 재할당 및 단계적 업데이트 정책과 같은 예방적 대응 방안을 적용할 수 있을 것으로 판단된다.

최근 3GPP 기반 NPN의 활용이 확대됨에 따라 Massive IoT 환경에서도 표준 기반 네트워크 분석 및 운영 기능의 중요성이 증가하고 있다. 본 연구에서 검토한 활용 방안은 스마트팩토리뿐만 아니라 스마트시티, 스마트빌딩 및 NPN 환경에도 적용 가능할 것으로 기대된다.

향후 연구에서는 본 연구에서 검토한 활용 방안의 실효성을 보다 구체적으로 검증하기 위해, 시그널링 메시지 발생량, 접속 성공률 및 처리 지연 등의 지표를 활용한 정량적 성능 평가를 수행할 예정이다. 또한 대응 정책을 적용하지 않은 경우 및 기존 백오프 방식과의 비교를 통해 각 대응 정책의 효과를 분석할 예정이다.

REFERENCES

[1] C.Choi, "A Study On IoT Data Consistency in IoT Environment," *Journal of Internet of Things and Convergence*, Vol.8, No.5, pp.127-132, 2022.

[2] Y.Kyung, T.Kim, and Y.Kim, "Retained Message Delivery Scheme utilizing Reinforcement Learning in MQTT-based IoT Networks," *Journal of Internet of Things and Convergence*, Vol.10, No.2, pp.131-135, 2024.

[3] S.Hong, "Research Study on Cognitive IoT Platform for Fog Computing in Industrial Internet of Things," *Journal of Internet of Things and Convergence*, Vol.10, No.1, pp.69-75, 2024.

[4] 3GPP TS 22.261, "Service Requirements for the 5G System," 3rd Generation Partnership Project.

[5] M.Q.Khan et al., "Modeling and Comprehensive Review of Signaling Storms in 3GPP-Based Mobile Broadband Networks: Causes, Solutions, and Countermeasures," *Computer Modeling in Engineering & Sciences*, Vol.142, No.1, pp.123-153, 2025.

[6] Y.Dong and J.Huang, "A Device-Class-Aware Token Bucket Algorithm with Dynamic Capacity Adjustment for 5G-IoT Signaling Storm Prevention in AMF," in Proceedings of the *6th International Conference on Neural Networks*, Information and Communication Engineering (NNICE), pp.997-1001, 2026.

[7] D.M.Manias, A.Chouman, and A.Shami, "An NWDAF Approach to 5G Core Network Signaling Traffic: Analysis and Characterization," in Proceedings of *IEEE Global Communications Conference (GLOBECOM)*, pp.6001-6006, 2022.

[8] E.Goshi, F.Mehmeti, T.F.La Porta, and W.Kellerer, "Modeling and Analysis of mMTC Traffic in 5G Core Networks," *IEEE Transactions on Network and Service Management*, Vol.22, No.1, pp.409-425, 2024.

[9] M.Kurata, A.Ikami, and M.Suzuki, "Geo-distributed and Dynamic Control Plane Management toward Green Mobile Networks," in Proceedings of *IFIP Networking Conference*, pp.347-355, 2025.

[10] M.Khaturia, N.Sharma, J.Choi, A.Nigam, and D.Kim, "Service-based Architecture Evolution: Towards Enhanced Signaling in Beyond 5G/6G Networks," in Proceedings of *IEEE Wireless Communications and Networking Conference (WCNC)*, pp.1-6, 2024.

[11] 3GPP TS 23.288, "Architecture Enhancements for 5G System (5GS) to Support Network Data Analytics Services," 3rd Generation Partnership Project.

[12] 3GPP TS 23.501, "System Architecture for the 5G System (5GS)," 3rd Generation Partnership Project.

[13] C.Arendt et al., "Towards Future Industrial Connectivity: Evaluation of Private 5G and Wi-Fi Networks in Professional Industrial Environments," in Proceedings of *IEEE 21st International Conference on Factory Communication Systems (WFCS)*, pp.1-8, 2025.

[14] T.F.Chen, C.Chen, and J.C.Chen, "A Machine Learning-Driven NWDAF Architecture for Intelligent 5G Core Networks," in Proceedings of *the 1st free5GC World Forum 2025*, pp.1-9, 2025.

[15] I.Hernández, D.Mejías, Z.Fernández, and V.Herranz, "Beyond NWDAF Services for Comprehensive 5G Network Analytics and Orchestration," in Proceedings of the *International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp.1-8, 2025.

성 지 훈(Jihoon Sung) [정회원]

- 2008년 2월 : 충남대학교 전기정보통신공학부(공학사)
- 2010년 1월 : 한국과학기술원 전기및전자공학과(공학석사)
- 2016년 8월 : 한국과학기술원 전기및전자공학과(공학박사)
- 2016년 9월 ~ 2020년 8월 : 삼성전자 무선사업부 책임연구원
- 2020년 9월 ~ 2025년 2월 : 한국전자통신연구원 표준연구본부 선임연구원
- 2025년 3월 ~ 현재 : 전북대학교 컴퓨터인공지능학부 교수

〈관심분야〉
사물인터넷, 5G/6G 이동통신, 네트워크 지능화

경 연 웅(Yeunwoong Kyung) [종신회원]

- 2011년 2월 : 고려대학교 전기전자전파공학부(공학사)
- 2016년 8월 : 고려대학교 전기전자전파공학부(공학박사)
- 2016년 9월 ~ 2020년 3월 : 삼성전자 무선사업부 책임연구원
- 2020년 3월 ~ 2022년 8월 : 한신대학교 컴퓨터공학부 교수
- 2022년 9월 ~ 2025년 2월 : 국립공주대학교 정보통신공학과 교수
- 2025년 3월 ~ 현재 : 서울과학기술대학교 전자공학과 교수

〈관심분야〉
사물인터넷, SDN, 5G/6G, 이동성, 모바일 서비스