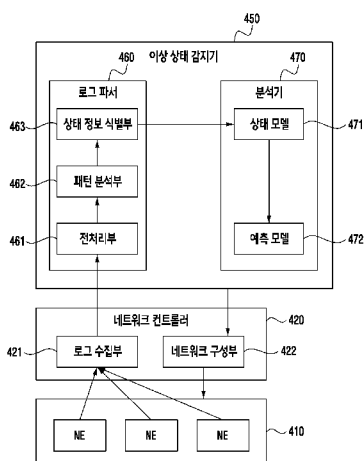




- | | | |
|--|--|---|
| (51) 국제특허분류:
<i>H04L 41/0695</i> (2022.01)
<i>H04L 41/147</i> (2022.01)
<i>G06F 18/26</i> (2023.01) | <i>G06F 18/15</i> (2023.01)
<i>G06F 9/448</i> (2018.01)
<i>G06N 3/0442</i> (2023.01) | (129 (KR). 유재형 (YOO, Jaehyoung): 37673 경상북도 포항시 남구 청암로 77 (KR). 김재곤 (KIM, Jaegon): 16677 경기도 수원시 영통구 삼성로 129 (KR). 홍원기 (HONG, Wonki): 37673 경상북도 포항시 남구 청암로 77 (KR). |
| (21) 국제출원번호: | PCT/KR2024/013947 | |
| (22) 국제출원일: | 2024 년 9 월 12 일 (12.09.2024) | (74) 대리인: 특허법인 광엔장 (KWANG AND JANG INTELLECTUAL PROPERTY LAW FIRM): 06300 서울특별시 강남구 논현로28길 40, 4층 (KR). |
| (25) 출원언어: | 한국어 | |
| (26) 공개언어: | 한국어 | |
| (30) 우선권정보:
10-2023-0152228 2023 년 11 월 6 일 (06.11.2023) KR
10-2023-0175982 2023 년 12 월 6 일 (06.12.2023) KR | | (81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW. |
| (71) 출원인: 삼성전자주식회사 (SAMSUNG ELECTRONICS CO., LTD.) [KR/KR]; 16677 경기도 수원시 영통구 삼성로 129 (KR). 포항공과대학교 산학협력단 (POSTECH RESEARCH AND BUSINESS DEVELOPMENT FOUNDATION) [KR/KR]; 37673 경상북도 포항시 남구 청암로 77 (KR). | | |
| (72) 발명자: 류승호 (RYU, Seungho): 16677 경기도 수원시 영통구 삼성로 129 (KR). 남석현 (NAM, Sukhuyn): 37673 경상북도 포항시 남구 청암로 77 (KR). 김태우 (KIM, Taewoo): 16677 경기도 수원시 영통구 삼성로 | | (84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, |

(54) Title: ELECTRONIC DEVICE AND METHOD FOR IDENTIFYING ANOMALY

(54) 발명의 명칭: 이상 상태를 식별하기 위한 전자 장치 및 방법



(57) Abstract: According to one embodiment of the present invention, an electronic device may comprise: a memory storing instructions; and a processor. The instructions, when executed individually or collectively by the at least one processor, may instruct the electronic device to: obtain log data related to an operation of at least one NE; obtain a log pattern; identify first state information and second state information; and identify an anomaly in the at least one NE.

(57) 요약서: 일 실시 예에 따르면, 전자 장치는, 인스트럭션들을 저장하는 메모리 및 프로세서를 포함할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 적어도 하나의 NE의 동작에 관한 로그 데이터를 획득하고, 로그 패턴을 획득하고, 제1 상태 정보 및 제2 상태 정보를 식별하고, 상기 적어도 하나의 NE의 이상 상태를 식별하도록, 야기할 수 있다.

- 420 ... Network controller
421 ... Log collection unit
422 ... Network configuration unit
450 ... Anomaly detector
460 ... Log parser
461 ... Preprocessing unit
462 ... Pattern analysis unit
463 ... State information identification unit
470 ... Analyzer
471 ... State model
472 ... Prediction model

TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, ME, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

공개:

— 국제조사보고서와 함께 (조약 제21조(3))

명세서

발명의 명칭: 이상 상태를 식별하기 위한 전자 장치 및 방법

기술분야

- [1] 본 개시(disclosure)는 이상 상태(anomaly)를 식별하기 위한 전자 장치 및 방법에 관한 것이다.

배경기술

- [2] 네트워크의 품질을 나타내기 위해 KPI(key performance indicator)가 정의될 수 있다. 무선 통신 시스템은, KPI에 관한 값을 통해 네트워크의 이상(anomaly)이 발생하였는지 여부를 판단할 수 있다. 무선 통신 시스템에서 KPI에 관한 값이 관리됨에 따라, 네트워크의 품질이 향상될 수 있다.
- [3] 상술한 정보는 본 개시에 대한 이해를 돕기 위한 목적으로 하는 배경 기술(related art)로 제공될 수 있다. 상술한 내용 중 어느 것도 본 개시와 관련된 종래 기술(prior art)로서 적용될 수 있는지에 대하여 어떠한 주장이나 결정이 제기되지 않는다.

발명의 상세한 설명

과제 해결 수단

- [4] 일 실시 예에 따르면, 전자 장치는, 인스트럭션들을 저장하고, 하나 이상의 저장 매체들을 포함하는 메모리, 및 처리 회로를 포함하는 적어도 하나의 프로세서를 포함할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 적어도 하나의 NE(network element)로부터, 상기 적어도 하나의 NE의 동작에 관한 로그 데이터를 획득하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 로그 데이터에 기반하여, 지정된 알고리즘을 통해 로그 패턴을 획득하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 로그 패턴에 기반하여, 제1 상태 정보 및 제2 상태 정보를 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제2 상태 정보가, 상기 제1 상태 정보를 이용하여 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제2 상태 정보가 상기 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 이상 상태를 식별하도록, 야기할 수 있다.
- [5] 일 실시 예에 따르면, 전자 장치에 의해 수행되는 방법은, 적어도 하나의 NE(network element)로부터, 상기 적어도 하나의 NE의 동작에 관한 로그 데이터

를 획득하는 동작을 포함할 수 있다. 상기 방법은, 상기 로그 데이터에 기반하여, 지정된 알고리즘을 통해 로그 패턴을 획득하는 동작을 포함할 수 있다. 상기 방법은, 상기 로그 패턴에 기반하여, 제1 상태 정보 및 제2 상태 정보를 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 제2 상태 정보가, 상기 제1 상태 정보를 이용하여 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 제2 상태 정보가 상기 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 이상 상태를 식별하는 동작을 포함할 수 있다.

도면의 간단한 설명

- [6] 도 1은 무선 통신 시스템을 도시한다.
- [7] 도 2는 NE(network element)의 동작에 관한 로그 데이터를 획득하기 위한 전자 장치를 포함하는 시스템을 도시한다.
- [8] 도 3은 SDN(software defined network) 아키텍처의 예를 도시한다.
- [9] 도 4는, 이상 상태 감지기(anomaly detector)의 구성을 도시한다.
- [10] 도 5는 이상 상태 감지기의 동작에 관한 흐름도를 도시한다.
- [11] 도 6은 로그 파서의 동작의 예를 도시한다.
- [12] 도 7은 상태 모델의 동작의 예를 도시한다.
- [13] 도 8은 예측 모델의 동작의 예를 도시한다.
- [14] 도 9는 이상 상태 감지기의 동작에 관한 흐름도를 도시한다.
- [15] 도 10은 전자 장치의 기능적 구성의 예를 도시한다.

발명의 실시를 위한 형태

- [16] 본 개시에서 사용되는 용어들은 단지 특정한 실시 예를 설명하기 위해 사용된 것으로, 다른 실시 예의 범위를 한정하려는 의도가 아닐 수 있다. 단수의 표현은 문맥상 명백하게 다르게 뜻하지 않는 한, 복수의 표현을 포함할 수 있다. 기술적이거나 과학적인 용어를 포함해서 여기서 사용되는 용어들은 본 개시에 기재된 기술 분야에서 통상의 지식을 가진 자에 의해 일반적으로 이해되는 것과 동일한 의미를 가질 수 있다. 본 개시에 사용된 용어들 중 일반적인 사전에 정의된 용어들은, 관련 기술의 문맥상 가지는 의미와 동일 또는 유사한 의미로 해석될 수 있으며, 본 개시에서 명백하게 정의되지 않는 한, 이상적이거나 과도하게 형식적인 의미로 해석되지 않는다. 경우에 따라서, 본 개시에서 정의된 용어일지라도 본 개시의 실시 예들을 배제하도록 해석될 수 없다.
- [17] 이하에서 설명되는 본 개시의 다양한 실시 예들에서는 하드웨어적인 접근 방법을 예시로서 설명한다. 하지만, 본 개시의 다양한 실시 예들에서는 하드웨어와 소프트웨어를 모두 사용하는 기술을 포함하고 있으므로, 본 개시의 다양한 실시 예들이 소프트웨어 기반의 접근 방법을 제외하는 것은 아니다.
- [18] 이하 설명에서 사용되는 신호를 지칭하는 용어(예: 신호, 정보, 심볼, 메시지, 시그널링, RS(reference signal), 데이터(data)), 자원을 지칭하는 용어(예: 심볼

(symbol), 슬롯(slot), 서브프레임(subframe), 무선 프레임(radio frame), 서브캐리어(subcarrier), RE(resource element), RB(resource block), BWP(bandwidth part), 기회(occasion)), 연산 상태를 위한 용어(예: 단계(step), 동작(operation), 절차(procedure)), 데이터를 지칭하는 용어(예: 패킷, 사용자 스트림, 정보(information), 비트(bit), 심볼(symbol), 코드워드(codeword)), 채널을 지칭하는 용어, 네트워크 객체(network entity)들을 지칭하는 용어, 장치의 구성 요소를 지칭하는 용어 등은 설명의 편의를 위해 예시된 것이다. 따라서, 본 개시가 후술되는 용어들에 한정되는 것은 아니며, 동등한 기술적 의미를 가지는 다른 용어가 사용될 수 있다.

[19] 또한, 본 개시에서, 특정 조건의 만족(satisfied), 충족(fulfilled) 여부를 판단하기 위해, 초과 또는 미만의 표현이 사용될 수 있으나, 이는 일 예를 표현하기 위한 기재일 뿐 이상 또는 이하의 기재를 배제하는 것이 아니다. '이상'으로 기재된 조건은 '초과', '이하'로 기재된 조건은 '미만', '이상 및 미만'으로 기재된 조건은 '초과 및 이하'로 대체될 수 있다. 또한, 이하, 'A' 내지 'B'는 A부터(A 포함) B까지의(B 포함) 요소들 중 적어도 하나를 의미한다. 이하, 'C' 및/또는 'D'는 'C' 또는 'D' 중 적어도 하나, 즉, {'C', 'D', 'C'와 'D'}를 포함하는 것을 의미한다.

[20] 본 개시는, 일부 통신 규격(예: 3GPP(3rd Generation Partnership Project), xRAN(extensible radio access network), O-RAN(open-radio access network)에서 사용되는 용어들을 이용하여 다양한 실시 예들을 설명하지만, 이는 설명을 위한 예시일 뿐이다. 본 개시의 다양한 실시 예들은, 다른 통신 시스템에서도, 용이하게 변형되어 적용될 수 있다.

[21] 도 1은 무선 통신 시스템을 도시한다.

[22] 도 1을 참고하면, 도 1은 무선 통신 시스템에서 무선 채널을 이용하는 노드(node)들의 일부로서, 기지국(110) 및 단말(120)을 예시한다. 도 1은 하나의 기지국만을 도시하나, 무선 통신 시스템은 기지국(110)과 동일 또는 유사한 다른 기지국을 더 포함할 수 있다.

[23] 기지국(110)은 단말(120)에게 무선 접속을 제공하는 네트워크 인프라스트럭처(infrastructure)이다. 기지국(110)은 신호를 송신할 수 있는 거리에 기초하여 정의되는 커버리지(coverage)를 가진다. 기지국(110)은 기지국(base station) 외에 '액세스 포인트(access point, AP)', '이노드비(eNodeB, eNB)', '5G 노드(5th generation node)', '지노드비(next generation nodeB, gNB)', '무선 포인트(wireless point)', '송수신 포인트(transmission/reception point, TRP)' 또는 이와 동등한 기술적 의미를 가지는 다른 용어로 지칭될 수 있다.

[24] 단말(120)은 사용자에 의해 사용되는 장치로서, 기지국(110)과 무선 채널을 통해 통신을 수행한다. 기지국(110)에서 단말(120)을 향하는 링크는 하향링크(downlink, DL), 단말(120)에서 기지국(110)을 향하는 링크는 상향링크(uplink, UL)라 지칭된다. 또한, 도 1에 도시되지 않았으나, 단말(120)과 다른 단말은 상호 간 무선 채널을 통해 통신을 수행할 수 있다. 이때, 단말(120) 및 다른 단말 간 링크(device-to-device link, D2D)는 사이드링크(sidelink)라 지칭되며, 사이드링크

는 PC5 인터페이스와 혼용될 수 있다. 다른 일부 실시 예들에서, 단말(120)은 사용자의 관여 없이 운영될 수 있다. 일 실시 예에 따라, 단말(120)은 기계 타입 통신(machine type communication, MTC)을 수행하는 장치로서, 사용자에게 의해 휴대되지 아니할 수 있다. 또한, 일 실시 예에 따라, 단말(120)은 NB(narrowband)-IoT(internet of things) 기기일 수 있다.

- [25] 단말(120)은 단말(terminal) 외 '사용자 장비(user equipment, UE)', '고객 맥내 장치'(customer premises equipment, CPE), '이동국(mobile station)', '가입자국(subscriber station)', '원격 단말(remote terminal)', '무선 단말(wireless terminal)', 전자 장치(electronic device)', 또는 '사용자 장치(user device)' 또는 이와 동등한 기술적 의미를 가지는 다른 용어로 지칭될 수 있다.
- [26] 웹 기반의 서비스가 증가함에 따라, 네트워크의 규모가 커지고, 네트워크 구성의 복잡도가 증가할 수 있다. 네트워크 구성의 복잡도가 증가함에 따라, 장애, 고장, 패킷 손실, 및/또는 지연(latency) 증가를 포함하는 다양한 문제들이 발생할 수 있다. 이러한 문제들을 해결하기 위해, 네트워크를 구성하는 NE(network element) (또는 네트워크 장비)들에 대한 심각한 고장이 발생하기 전, NE들에 대한 이상 상태(anomaly)를 식별하기 위한 방안이 요구될 수 있다.
- [27] NE들에 대한 이상 상태(anomaly)를 식별하기 위해서는, NE들 및 NE들과 관련된 시스템들의 자원 사용량, NE들 및 NE들과 관련된 시스템들의 상태 정보, 네트워크 트래픽 정보, 및/또는 로그 데이터 중 적어도 하나에 기반하여 네트워크의 상태가 실시간으로 모니터링되어야 한다. 네트워크 상태 및/또는 NE들의 상태를 실시간으로 모니터링하는 것은 많은 인적 자원 및 물적 자원이 필요할 수 있다. 따라서, 이하 명세서에서는, NE들에서 출력되는 로그 데이터(또는 NE들로부터 획득된 로그 데이터)에 기반하여, NE들의 동작에 관한 이상 상태를 식별하기 위한 기술적 특징이 설명될 것이다.
- [28] 일 실시 예에 따르면, 로그 데이터는 NE(또는 네트워크 장비)의 상태를 나타낼 수 있다. 다만, 로그 데이터는 NE(또는 네트워크 장비)의 제조사(또는 개발자)에 따라 다른 형식의 텍스트 데이터로 구성될 수 있다. 예를 들어, 로그 데이터는 비정형 데이터로 구성될 수 있다. 따라서, 지능(artificial intelligence)에 기반한 자연어 처리(natural language processing, NLP)를 이용하여 로그 데이터를 분석하기 위한 전자 장치의 동작이 이하에서 설명될 것이다.
- [29] 도 2는 NE(network element)의 동작에 관한 로그 데이터를 획득하기 위한 전자 장치를 포함하는 시스템을 도시한다.
- [30] 도 2를 참고하면, 전자 장치(210)는 복수의 NE(network element)들(230)의 동작에 관한 로그 데이터를 획득하기 위해 사용될 수 있다. 예를 들어, 복수의 NE들(230)은 NE(230-1) 및 NE(230-2)를 포함할 수 있다. 예를 들어, 복수의 NE들(230)은 라우터(router), DU(distributed unit) 및/또는 RU(radio unit)를 포함할 수 있다. 예를 들어, NE는 네트워크 장치(network device)로 참조될 수 있다.

- [31] 복수의 NE들(230) 각각은 동작에 대한 로그 데이터를 생성할 수 있다. 복수의 NE들(230) 각각은 동작에 대한 로그 데이터를 전자 장치(210)에게 전송할 수 있다. 예를 들어, 전자 장치(210)는 다양한 형식에 기반하여 생성된 로그 데이터를 수신할 수 있다. 전자 장치(210)는 로그 데이터를 모니터링 할 수 있다. 전자 장치(210)는 로그 데이터를 모니터링 하는 것에 기반하여, 복수의 NE들(230)에 대한 이상 상태(anomaly)를 식별(또는 결정)할 수 있다.
- [32] 이하에서 이상 상태(anomaly)는 비정상 상태(abnormal state)로 참조될 수 있다. 예를 들어, NE의 이상 상태를 식별한다는 것은, 비정상 상태의 NE를 식별하는 것으로 참조될 수 있다.
- [33] 일 실시 예에 따르면, 전자 장치(210)는 NE(예: NE(230-1), NE(230-2))의 센서를 통해 수집된 데이터 또는 NE 또는 전자 장치(210)에서 출력되는 데이터를 획득할 수 있다. 상기 획득된 데이터는 특정한 값의 형식으로 구성될 수 있다. 획득된 데이터의 정상 범위 및 비정상 범위에 대한 정보가 전자 장치(210)의 메모리에 저장된 상태일 수 있다. 전자 장치(210)는 획득된 데이터에 기반하여, NE가 이상 상태에 있는지 여부를 식별 또는 결정할 수 있다.
- [34] 일 실시 예에 따르면, 전자 장치(210)는 NE의 동작에 관한 비정형 데이터(unstructured data)를 획득할 수 있다. 비정형 데이터는 특정한 값의 형식이 아닐 수 있다. 전자 장치(210)는 획득된 비정형 데이터를 프로세싱할 수 있다. 전자 장치(210)는 프로세싱된 데이터에 기반하여, NE의 이상 상태를 식별(또는 판단)할 수 있다. 예를 들어, 전자 장치(210)는 2 가지의 기법들 중 적어도 하나를 이용하여, 비정형 데이터에 기반하여 NE의 이상 상태를 식별할 수 있다. 제1 기법에 따르면, 전자 장치(210)는 NE의 특정 작업(또는 동작)에 대한 결과에 기반하여, NE의 이상 상태를 식별할 수 있다. 제2 기법에 따르면, 전자 장치(210)는 NE의 동작에 관한 로그 데이터에 기반하여, NE의 이상 상태를 식별할 수 있다. 제2 기법은, 규칙 기반(rule-based)으로 동작 할 수 있다. 제2 기법에 따르면, 특정 로그가 발생하는 것에 기반하여, 알람이 발생될 수 있다.
- [35] 제1 기법에 따르면, 전자 장치(210)는 NE의 특정 작업(또는 동작)에 대한 결과에 기반하여, NE의 이상 상태를 식별할 수 있다. NE의 특정 작업(또는 동작)에 대한 결과는 복수의 카테고리들 중 하나로 구분될 수 있다. 따라서, 전자 장치(210)는 NE의 특정 작업(또는 동작)에 대한 결과가 복수의 카테고리들 중 하나에 포함되는지 여부를 판단하는 것에 기반하여, NE의 이상 상태를 판단할 수 있다. 전자 장치(210)는 순차적으로 수행되는 작업(또는 동작)들에 대한 결과가 복수의 카테고리들 중 하나에 포함되는지 여부를 판단하는 것에 기반하여, NE의 이상 상태를 판단할 수 있다.
- [36] 제2 기법에 따르면, 전자 장치(210)는 NE의 동작에 관한 로그 데이터에 기반하여, NE의 이상 상태를 식별할 수 있다. 로그 데이터는 비정형 데이터로 구성될 수 있다. 로그 데이터는 NE에 대한 제조사(또는 개발자, 사용자)가 출력이 필요하다고 판단한 정보들을 나타내는 텍스트를 포함할 수 있다. 제조사(또는 개발자, 사

용자) 또는 NE의 유형에 따라 로그 데이터는 다른 형식으로 구성될 수 있다. 따라서, 전자 장치(210)는 에러를 지시하는 로그 데이터가 지정된 내용을 포함하는 경우, NE가 비정상 상태임(또는 NE의 이상 상태(anomaly))을 식별할 수 있다. 실시 예에 따라, 전자 장치(210)는 로그 데이터 내에서 공통된 부분을 로그 키(log key)로 식별(또는 추출)할 수 있다. 전자 장치(210)는 로그 키에 기반하여, 로그 데이터의 의미를 분석할 수 있다. 전자 장치(210)는 로그 데이터의 의미에 따라, NE가 비정상 상태인지 여부를 판단할 수 있다. 실시 예에 따라, 전자 장치(210)는 시간 순으로 정렬된 로그 데이터를 이용하여 식별된 정상 로그 패턴을 통해 지정된 모델(예: 인공지능 모델)을 학습시킬 수 있다. 전자 장치(210)는 로그 데이터를 지정된 모델의 입력 데이터로 설정할 수 있다. 전자 장치(210)는 지정된 모델의 출력 데이터에 기반하여, NE가 비정상 상태인지 여부를 판단할 수 있다. 다만, 제2 기법에 따르면, 반복되는 단어가 로그 키로 설정되므로, 반복되는 단어에 대한 의미가 고려되지 않을 수 있다. 따라서, 실제 로그 데이터의 내용이 반영이 되지 않을 수도 있다.

- [37] 이하에서는, SDN(software defined network)에 기반하여 구성된 네트워크에서, 적어도 하나의 모델(예: 인공지능 모델)을 이용하여, NE의 이상 상태를 식별하기 위한 기술적 특징이 설명될 것이다. 먼저 도 3에서 SDN 아키텍처(architecture)가 설명될 것이다.
- [38] 도 3은 SDN(software defined network) 아키텍처의 예를 도시한다.
- [39] 도 3을 참고하면, SDN(300)는 애플리케이션 레이어(310), 제어 플레인 레이어(control plane layer)(320), 및/또는 데이터 플레인 레이어(data plane layer)(330)를 포함할 수 있다.
- [40] 애플리케이션 레이어(310)는, 라우팅(routing) 및/또는 로드 밸런스(load balance)를 포함하는 제어 동작을 위해 사용되는 하나 이상의 애플리케이션들을 포함할 수 있다. 애플리케이션은 SDN 컨트롤러에 의해 노출되는(exposed) 자원 셋(resource set)을 독점적으로 제어할 수 있다. 애플리케이션은 다른 애플리케이션을 호출(involve)하거나 다른 애플리케이션과 협력(collaborate)할 수 있다.
- [41] 제어 플레인 레이어(320)는 SDN 컨트롤러(321)를 포함할 수 있다. SDN 컨트롤러(321)는 전체 네트워크 자원들에 대한 제어를 위해 사용될 수 있다. SDN 컨트롤러(321)는 네트워크 정보를 획득하고, 획득된 정보를 애플리케이션에게 제공할 수 있다.
- [42] 데이터 플레인 레이어(330)는 적어도 하나의 NE(331)를 포함할 수 있다. 적어도 하나의 NE(331)는 적어도 하나의 물리 스위치(physical switch) 및/또는 적어도 하나의 가상 스위치(virtual switch)를 포함할 수 있다.
- [43] 제어 플레인 레이어(320) 및 애플리케이션 레이어(310) 사이의 인터페이스는 northbound API(application programming interface)로 참조될 수 있다. 제어 플레인 레이어(320) 및 데이터 플레인 레이어(330) 사이의 인터페이스는 southbound API로 참조될 수 있다. 예를 들어, 제어 플레인 레이어(320) 및 데이터 플레인 레이어

(330) 사이에서, 오픈 플로우 프로토콜(openflow protocol) 또는 OpFlex 프로토콜이 사용될 수 있다.

- [44] 기존의 NE(또는 네트워크 장비)들은 데이터 플레인 및 제어 플레인에 기반하여, 독립적으로 동작하는 것에 반해, SDN(300)에서는 NE의 데이터 플레인 및 제어 플레인이 분리될 수 있다. SDN 컨트롤러(321)는 NE의 제어 플레인의 동작을 수행할 수 있다. SDN(300)은 네트워크 제어를 위한 알고리즘에 기반하여 동작할 수 있다. 따라서, SDN(300)에서, 관리자의 개입 없이도 네트워크가 지정된 알고리즘에 기반하여 관리 및 제어될 수 있다. 또한 네트워크를 구성하는 적어도 하나의 NE(331)이 SDN 컨트롤러(321)를 통해 관리될 수 있다. 적어도 하나의 NE(331)은 SDN 컨트롤러(321)와 연동하여 동작하기 위해, REST(representational state transfer protocol), NETCONF(network configuration protocol), 또는 RESTCONF(representational state transfer configuration protocol) 중 적어도 하나를 지원할 수 있다. SDN 컨트롤러(321)는 REST, NETCONF, 또는 RESTCONF 중 적어도 하나를 이용하여 적어도 하나의 NE(331)를 제어할 수 있다.
- [45] 이하에서는, SDN(300)에서, 인공지능을 이용하여, 네트워크 관리를 수행하기 위한 기술적 특징이 설명될 것이다. 예를 들어, SDN 컨트롤러(321)를 통해 획득된 네트워크 정보(예: 로그 데이터)를 이용하여, 인공지능 모델을 통해 네트워크가 분석되고, 문제가 발생되는 경우, 인공지능 모델을 통해 발생한 문제를 해결할 수 있다. 예를 들어, SDN(300)에서, 인공지능 모델을 이용하여 NE의 이상 상태가 모니터링될 수 있다. SDN 컨트롤러(321)는 NE의 이상 상태가 발견되는 경우, 해당 NE를 격리하고, 네트워크 트래픽을 다른 NE를 통해서 전송하도록 제어할 수 있다.
- [46] 도 4는, 이상 상태 감지기(anomaly detector)의 구성을 도시한다. 이하 사용되는 '...부', '...기' 등의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어, 또는, 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.
- [47] 도 4를 참고하면, 적어도 하나의 NE(410)은 로그 데이터를 네트워크 컨트롤러(420)에게 전송할 수 있다. 네트워크 컨트롤러(420)는 적어도 하나의 NE(410)로부터 로그 데이터를 수신할 수 있다. 예를 들어, 네트워크 컨트롤러(420)는 도 3의 SDN 컨트롤러(321)에 상응할 수 있다.
- [48] 네트워크 컨트롤러(420)는 로그 수집부(421) 및 네트워크 구성부(422)를 포함할 수 있다. 로그 수집부(421)는 적어도 하나의 NE(410)로부터 로그 데이터를 수신하고, 수신된 로그 데이터를 이상 상태 감지기(450)에게 전송하도록 구성(configure)될 수 있다. 네트워크 구성부(422)는 적어도 하나의 NE(410)의 설정을 변경하거나, 적어도 하나의 NE(410)의 동작을 제어하도록 구성될 수 있다.

- [49] 이상 상태 감지기(450)는 로그 파서(log parser)(460) 및 분석기(analyzer)(470)를 포함할 수 있다. 적어도 하나의 NE(410)로부터 수집된 로그 데이터는, 네트워크 컨트롤러(420)를 통해 로그 파서(460)로 전달될 수 있다.
- [50] 로그 파서(460)은 전처리부(461), 패턴 분석부(462), 및/또는 상태 정보 식별부(463) 중 적어도 하나를 포함할 수 있다. 전처리부(461)는 로그 데이터를 전처리(preprocessing)하기 위해 사용될 수 있다. 패턴 분석부(462)는 로그 데이터에 기반하여, 로그 패턴을 획득(또는 식별)하기 위해 사용될 수 있다. 상태 정보 식별부(463)는 로그 패턴에 기반하여, 상태 정보를 식별하기 위해 사용될 수 있다. 예를 들어, 상태 정보는, 로그 데이터에 관한 이벤트 번호를 포함할 수 있다. 상태 정보 식별부(463)는 이벤트 분류부로 참조될 수 있다. 로그 파서(460)의 구체적인 동작은 도 6에서 후술될 것이다.
- [51] 분석기(470)는 로그 파서(460)로부터 상태 정보를 수신할 수 있다. 분석기(470)는 상태 정보에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다. 분석기(470)는 상태 모델(471) 및/또는 예측 모델(472) 중 적어도 하나를 포함할 수 있다.
- [52] 상태 모델(471)은 로그 패턴에 대한 상태 변화에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별하기 위해 사용될 수 있다. 상태 모델(471)은 유한 상태 기계(finite state automata)에 기반하여 구성될 수 있다. 상태 모델(471)의 구체적인 동작은 도 7에서 후술될 것이다.
- [53] 예측 모델(472)은 로그 패턴에 대한 예측된 상태에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별하기 위해 사용될 수 있다. 예측 모델(472)은 LSTM(long short term memory)에 기반하여 구성될 수 있다. 예측 모델(472)의 구체적인 동작은 도 8에서 후술될 것이다.
- [54] 일 실시 예에 따르면, 이상 상태 감지기(450)는 3 단계들을 통해 적어도 하나의 NE(410)의 이상 상태(anomaly)를 식별할 수 있다.
- [55] 첫 번째 단계에서, 이상 상태 감지기(450)는 로그 파서(460)을 이용하여, 로그 데이터에 기반하여 획득된 로그 패턴이, 정상 상태를 나타내는 복수의 로그 패턴들 중 하나에 상응하는지 여부를 식별하는 것에 기반하여, 적어도 하나의 NE(410)가 비정상 상태에 있는지 여부를 식별할 수 있다. 이상 상태 감지기(450)(또는 네트워크 컨트롤러(420))는 첫 번째 단계를 통해, 적어도 하나의 NE(410)의 이상 상태를 식별하는 것에 기반하여, 알림(notification)(또는 알람(alarm))을 제공할 수 있다. 이상 상태 감지기(450)는 첫 번째 단계를 통해, 적어도 하나의 NE(410)의 이상 상태가 아님을 식별하는 것에 기반하여, 두 번째 단계를 수행할 수 있다.
- [56] 두 번째 단계에서, 이상 상태 감지기(450)는 로그 파서(460)를 이용하여 획득된 상태 정보가 상태 모델(471)을 이용하여 획득된 상태 정보에 상응하는지 여부를 식별하는 것에 기반하여, 적어도 하나의 NE(410)가 비정상 상태에 있는지 여부를 식별할 수 있다. 이상 상태 감지기(450)(또는 네트워크 컨트롤러(420))는 두 번

제 단계를 통해, 적어도 하나의 NE(410)의 이상 상태를 식별하는 것에 기반하여, 알림(notification)(또는 알람(alarm))을 제공할 수 있다. 이상 상태 감지기(450)는 두 번째 단계를 통해, 적어도 하나의 NE(410)의 이상 상태가 아님을 식별하는 것에 기반하여, 세 번째 단계를 수행할 수 있다.

[57] 세 번째 단계에서, 이상 상태 감지기(450)는 로그 파서(460)를 이용하여 획득된 상태 정보가 예측 모델(472)을 이용하여 획득된 상태 정보에 상응하는지 여부를 식별하는 것에 기반하여, 적어도 하나의 NE(410) 비정상 상태에 있는지 여부를 식별할 수 있다. 이상 상태 감지기(450)(또는 네트워크 컨트롤러(420))는 세 번째 단계를 통해, 적어도 하나의 NE(410)의 이상 상태를 식별하는 것에 기반하여, 알림(notification)(또는 알람(alarm))을 제공할 수 있다.

[58] 일 실시 예에 따르면, 네트워크 컨트롤러(420)는 적어도 하나의 NE(410)의 이상 상태를 식별하는 것에 기반하여, 데이터 트래픽의 경로를 이상 상태가 발생한 NE를 우회하도록 변경할 수 있다.

[59] 도 5는 이상 상태 감지기의 동작에 관한 흐름도를 도시한다.

[60] 도 5를 참고하면, 동작 510에서, 이상 상태 감지기(450)(또는 이상 상태 감지기(450)를 위한 전자 장치)는 적어도 하나의 NE(410)의 동작에 관한 로그 데이터를 획득할 수 있다. 예를 들어, 이상 상태 감지기(450)는 네트워크 컨트롤러(420)를 통해, 적어도 하나의 NE(410)의 동작에 관한 로그 데이터를 획득할 수 있다. 이상 상태 감지기(450)는 적어도 하나의 NE(410)의 동작에 관한 로그 데이터를 모니터링할 수 있다.

[61] 동작 520에서, 이상 상태 감지기(450)는 지정된 알고리즘을 통해 로그 패턴을 획득할 수 있다. 예를 들어, 이상 상태 감지기(450)는 로그 데이터에 기반하여, 지정된 알고리즘을 통해 로그 패턴을 획득할 수 있다. 예를 들어, 이상 상태 감지기(450)는 로그 파서(460)를 이용하여 로그 패턴을 획득할 수 있다.

[62] 예를 들어, 이상 상태 감지기(450)는 지정된 알고리즘에 기반하여, 로그 데이터를 정규화(normalize)할 수 있다. 이상 상태 감지기(450)는 로그 데이터를 통해 상태 정보를 식별하기 위해, 로그 데이터를 정규화할 수 있다. 이상 상태 감지기(450)는 지정된 알고리즘을 통해 로그 데이터에서 불필요한 정보들을 제거할 수 있다. 이상 상태 감지기(450)는 로그 데이터에서 불필요한 정보들을 제거함으로써, 로그 데이터를 정규화할 수 있다. 이상 상태 감지기(450)는 로그 데이터를 정규화하는 것에 기반하여, 로그 패턴을 획득할 수 있다. 이상 상태 감지기(450)는 상태 정보를 식별하기 위해 로그 패턴을 획득할 수 있다.

[63] 동작 530에서, 이상 상태 감지기(450)는 제1 상태 정보 및 제2 상태 정보를 식별할 수 있다. 예를 들어, 이상 상태 감지기(450)는 로그 패턴에 기반하여, 제1 상태 정보 및 제2 상태 정보를 식별할 수 있다. 예를 들어, 로그 데이터는 지정된 시간 구간 내에서 획득된 로그 메시지(텍스트)들을 포함할 수 있다. 제1 상태 정보는 제1 시점에서의 적어도 하나의 NE(410)에 관한 상태를 나타낼 수 있다. 제2 상태 정보는 제1 시점 이후의 제2 시점에서의 적어도 하나의 NE(410)에 관한 상태를

나타낼 수 있다. 예를 들어, 제1 상태 정보는 적어도 하나의 NE(410)의 과거의 상태를 나타낼 수 있다. 제2 상태 정보는 적어도 하나의 NE(410)의 현재의 상태를 나타낼 수 있다. 예를 들어, 제1 상태 정보는 제1 이벤트 번호를 포함할 수 있다. 제2 상태 정보는 제2 이벤트 번호를 포함할 수 있다. 제1 이벤트 번호 및 제2 이벤트 번호 각각은 적어도 하나의 NE(410)의 상태를 지시하기 위한 값일 수 있다.

- [64] 일 실시 예에 따르면, 이상 상태 감지기(450)는 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는지 여부를 식별할 수 있다. 메모리에 저장된 복수의 로그 패턴들은 정상 상태를 나타낼 수 있다. 이상 상태 감지기(450)는 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는 경우, 로그 패턴에 기반하여, 제1 상태 정보 및 제2 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하지 않는 경우, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다.
- [65] 동작 540에서, 이상 상태 감지기(450)는 제2 상태 정보가 제1 상태 정보를 이용하여 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별할 수 있다.
- [66] 동작 550에서, 이상 상태 감지기(450)는 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다. 예를 들어, 이상 상태 감지기(450)는 제2 상태 정보가 제1 상태 정보를 이용하여 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다.
- [67] 예를 들어, 이상 상태 감지기(450)는 제1 상태 정보를 이용하여, 적어도 하나의 모델을 통해 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 과거의 상태를 나타내는 제1 상태 정보를 이용하여, 적어도 하나의 모델을 통해 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 식별된 상태 정보가 제2 상태 정보와 구별됨을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다.
- [68] 일 실시 예에 따르면, 적어도 하나의 모델은 상태 모델(471) 및 예측 모델(472)을 포함할 수 있다.
- [69] 예를 들어, 이상 상태 감지기(450)는 상태 모델(471)을 통해 제3 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 제1 상태 정보를 상태 모델(471)에 입력할 수 있다. 이상 상태 감지기(450)는 상태 모델(471)의 입력 데이터를 제1 상태 정보로 설정할 수 있다. 이상 상태 감지기(450)는 상태 모델(471)의 출력에 기반하여, 제3 상태 정보를 획득할 수 있다. 예를 들어, 상태 모델(471)은 정상 상태에서 제1 상태 정보로부터 변경(또는 전이) 가능한 상태 정보를, 제3 상태 정보로 식별할 수 있다. 이상 상태 감지기(450)는 제2 상태 정보가 제1 상태 정보로부터 변경 가능한 상태 정보가 아님을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다.
- [70] 예를 들어, 이상 상태 감지기(450)는 예측 모델(472)을 통해 제4 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 제1 상태 정보를 예측 모델(472)에 입력할 수 있다. 이상 상태 감지기(450)는 예측 모델(472)의 입력 데이터를 제1 상태 정보

로 설정할 수 있다. 이상 상태 감지기(450)는 예측 모델(472)의 출력에 기반하여, 제4 상태 정보를 획득할 수 있다. 예를 들어, 예측 모델(472)은 정상 상태에서 제1 상태 정보로부터 변경될 것으로 예측되는 상태 정보를, 제4 상태 정보로 식별할 수 있다. 일 예로, 이상 상태 감지기(450)는 예측 모델(472)의 출력에 기반하여, 복수의 상태들 각각에 대한 확률 데이터를 식별할 수 있다. 이상 상태 감지기(450)는 복수의 상태들 중 가장 높은 확률을 가지는 상태에 기반하여, 제4 상태 정보를 획득할 수 있다.

- [71] 이상 상태 감지기(450)는 제2 상태 정보가 예측된 상태를 나타내는 제4 상태 정보가 아님을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다.
- [72] 도 6은 로그 파서의 동작의 예를 도시한다.
- [73] 도 6을 참고하면, 이상 상태 감지기(450)는 로그 파서(460)를 이용하여, 적어도 하나의 NE(410)로부터 획득된 로그 데이터를 가공할 수 있다. 예를 들어, 로그 파서(460)는 전처리부(461), 패턴 분석부(462), 및/또는 상태 정보 식별부(463) 중 적어도 하나를 포함할 수 있다. 이상 상태 감지기(450)는 로그 파서(460)를 이용하여, 전처리 동작, 패턴 분석 동작, 및 상태 정보 식별 동작을 수행할 수 있다. 이상 상태 감지기(450)는 로그 파서(460)를 통해 로그 데이터를 로그 패턴으로 변경할 수 있다. 이상 상태 감지기(450)는 상기 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는지 여부를 식별할 수 있다. 메모리에 저장된 복수의 로그 패턴들은 정상 상태를 나타낼 수 있다. 이상 상태 감지기(450)는 상기 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하지 않음을 식별하는 것에 기반하여, 알림(또는 알람)을 제공할 수 있다.
- [74] 예를 들어, 이상 상태 감지기(450)는 로그 파서(460)의 전처리부(461)를 이용하여, 전처리 동작을 수행할 수 있다. 이상 상태 감지기(450)는 전처리부(461)를 이용하여, 로그 데이터의 정규화할 수 있다.
- [75] 일 예로, 전처리부(461)는 로그 데이터에 따른 로그 내용의 대문자를 소문자로 변경할 수 있다. 전처리부(461)는 지정된 규칙(rule)에 따라 로그 내용 중 숫자, 날짜, 파일 경로, 지역 명, 인터페이스 명, 및/또는 기호 중 적어도 하나를 제거할 수 있다. 제거되는 단어 중 일부는 의미를 가지는 토큰(token)으로 대체될 수 있다. 예를 들어, 로그 내용에 포함된 단어 중 일부는 하기의 표와 같이 변경될 수 있다.
- [76] [표1]

로그 내용	예시	토큰
숫자	1, 2, 3, ...	[number]
N 진수	2진수, 16 진수	[number]
날짜	Year, May, Monday, Friday	[date]
지역	'Jincheon', 'Hyehwa'	[loc]
파일 경로	/dic, /recent	[path]
인터페이스	HundGi0/3	[interface]

- [77] 표 1을 참고하면, 로그 내용에 포함된 단어들 중 일부는 표 1과 같은 규칙에 기반하여 토큰으로 치환될 수 있다. 예를 들어, 로그 내용에 포함된 숫자(number) (또는 아라비아 숫자(East Arabic numerals))는 [number] 토큰으로 치환될 수 있다. n 진법(radix n)의 값은 정규 표현식(regular expression)에 기반하여 변환되고, 변환된 숫자는 [number] 토큰으로 치환될 수 있다. 날짜 및 지역명은 학습용 데이터를 통해 획득된 사전을 통해 제거될 수 있다. 일 예로, 날짜는 [date] 토큰으로 치환될 수 있다. 지역명은 [loc] 토큰으로 치환될 수 있다. 파일 경로는 리눅스 기반의 파일 경로가 '/'로 시작하므로, '/'로 시작하는 단어를 [path] 토큰으로 치환될 수 있다. 인터페이스는 'interface' 단어 다음에 인터페이스의 이름이 따라오므로, 'interface' 단어 바로 뒤에 따라오는 단어는 [interface] 토큰으로 변경될 수 있다.
- [78] 로그 파서(460)의 전처리부(461)를 통한 전처리 동작은 토큰으로 변경되지 않은 모든 기호를 제거함으로써 완료될 수 있다. 전처리 동작은 표 1과 같은 지정된 규칙에 기반하여 수행될 수 있다. 따라서, 사용자(또는 관리자)는 실제 로그 데이터에 따라 규칙을 변경함으로써, 전처리 동작을 변경할 수 있다.
- [79] 예를 들어, 이상 상태 감지기(450)는 로그 파서(460)의 패턴 분석부(462)를 이용하여, 패턴 분석 동작을 수행할 수 있다. 이상 상태 감지기(450)는 전처리 동작이 수행된 후, 로그 파서(460)의 패턴 분석부(462)를 통해 패턴 분석 동작을 수행할 수 있다.
- [80] 일 예로, 패턴 분석부(462)는 단어 사전에 기반하여, 로그 패턴을 식별(또는 분석)할 수 있다. 단어 사전은 정상 상태의 로그 데이터를 통해서 미리 생성될 수 있다. 전처리 동작이 수행된 후의 학습용 데이터(예: 로그 데이터)에서 지정된 횟수(예: 3회) 이상 나타난 단어들로 단어 사전이 생성될 수 있다. 지정된 횟수(예: 3회) 이상 나타난 단어들로 단어 사전이 생성되므로, 프로세스 ID(identifier)와 같은 일시적으로 생성되는 단어들이 제거될 수 있다. 상기 지정된 횟수는 패턴 분석부(462)에 대한 설정 정보에 따라 변경될 수 있다.

- [81] 전처리 동작이 수행된 후 획득된 로그 내용 중 단어 사전에 없는 단어는 [UNK] (unknown) 토큰으로 변경될 수 있다. 패턴 분석 동작이 수행된 후 로그 데이터는 실질적으로 동일한 형태의 로그 패턴으로 변경(또는 압축)될 수 있다. 로그 내용(또는 로그 메시지)가 'Interface HundGi0/3, changed state to FREQ_LOCK'와 같이 구성된 경우, 전처리 동작 및 패턴 분석 동작이 수행된 후, 'interface [interface] changed state to freq lock'와 같이 구성된 로그 패턴으로 변경될 수 있다. 이 때, 인터페이스 이름만이 [interface] 토큰으로 변경될 수 있다. 상술한 예에 따르면, 인터페이스가 다른 경우에도 동일한 동작에 관한 로그 내용(또는 로그 메시지)는 하나의 로그 패턴으로 표현될 수 있다.
- [82] 예를 들어, 이상 상태 감지기(450)는 로그 파서(460)의 상태 정보 식별부(463)를 이용하여, 상태 정보 식별 동작을 수행할 수 있다. 이상 상태 감지기(450)는 패턴 분석이 수행된 후, 로그 파서(460)의 상태 정보 식별부(463)를 통해 상태 정보 식별 동작을 수행할 수 있다.
- [83] 상태 정보 식별부(463)는 로그 패턴에 기반하여, 상태 정보를 식별(또는 획득)할 수 있다. 상태 정보는 이벤트 번호(event number)를 포함할 수 있다. 이벤트 번호는 적어도 하나의 NE(410)의 상태를 지시하기 위한 값일 수 있다. 상태 정보 식별부(463)을 통해 이벤트 번호가 식별(또는 획득)된다는 점에서, 상태 정보 식별부(463)은 이벤트 분류부(event classification unit)으로 참조될 수 있다.
- [84] 상태 정보 식별부(463)는 로그 패턴에 기반하여, 상태 정보(예: 이벤트 번호)를 식별할 수 있다. 상태 정보 식별 동작에 기반하여, 동일 또는 유사한 로그 패턴들은 동일한 상태 정보(예: 이벤트 번호)로 식별(또는 분류)될 수 있다. 학습용 데이터에 기반하여 획득된 로그 패턴들은 상태 정보 식별 동작을 통해 상태 사전에 등록될 수 있다. 각 상태 정보에 따른 로그 패턴 목록이 메모리에 저장될 수 있다.
- [85] 상기 상태 사전을 구성하기 위한 동작은 최소 편집 거리(minimum edit distance) 알고리즘에 기반하여 수행될 수 있다. 최소 편집 거리 알고리즘은 두 문장의 유사도를 측정하기 위한 알고리즘일 수 있다. '단어 제거' 동작, '단어 추가' 동작, 및 '단어 변환' 동작을 각각 한 번의 수정으로 정의될 수 있다. 두 문장이 같아지기 위한 최소 수정 횟수를 통해 두 문장의 유사도가 측정될 수 있다.
- [86] 최소 편집 거리 알고리즘에 따르면, 코스트(cost)가 정의될 수 있다. 예를 들어, 유의어 및 반의어 사전을 이용하여, '단어 변환' 동작에 따라 기존 단어와 변환되는 단어의 관계가 유의어인 경우, 코스트가 제1 코스트(예: '0')으로 설정될 수 있다. 유의어 및 반의어 사전을 이용하여, '단어 변환' 동작에 따라 기존 단어와 변환되는 단어의 관계가 반의어인 경우, 코스트가 제2 코스트(예: '6')으로 설정될 수 있다. 실시 예에 따라, 제1 코스트 및 제2 코스트는 변경될 수 있다. 예를 들어, 제1 코스트 및 제2 코스트는 관리자(또는 사용자)에 의해 변경될 수 있다.
- [87] 두 로그 패턴들이 서로 반대되는 의미를 가지는 경우, '단어 변환' 동작에 대한 코스트를 더 증가시키기 위해, 반의어 사전이 사용될 수 있다. 'interface up' 및 'interface down'과 같이 두 로그 패턴들의 의미가 서로 반대되는 경우, 최소 편집

거리는 작으나 실제 의미는 반대이므로, 두 로그 패턴들은 서로 다른 상태 정보로 식별되어야 한다. 따라서, 상태 정보 식별부(463)는 반의어 사전을 이용하여, '단어 변환' 동작에 대한 코스트를 증가시킴으로써 반대의 의미를 가지는 두 로그 패턴들을 서로 다른 상태 정보로 식별할 수 있다. 실시 예에 따라, 반의어 사전은 WordNet과 같은 공개된 반의어 사전이 활용될 수 있다.

- [88] 상술한 최소 편집 거리 알고리즘에 기반하여, 두 로그 패턴들이 동일해지기 위한 코스트가 두 로그 패턴 길이의 평균의 절반보다 작은 경우, 두 로그 패턴의 절반 이하가 수정됨에 따라, 두 로그 패턴이 서로 같아질 수 있다. 따라서, 두 로그 패턴들은 동일한 상태 정보(예: 이벤트 번호)로 식별(또는 분류)될 수 있다. 상술한 예와 같이 두 로그 패턴 길이의 평균의 절반이 기준으로 설정된 이유는, 일정한 임계 값이 기준으로 설정되는 경우, 짧은 로그 패턴들은 의미와 관계없이 항상 같은 상태 정보로 식별될 수 있는 문제를 방지하기 위한 것이다.
- [89] 상술한 예를 통해, 최소 편집 거리 알고리즘에 기반하여, 학습용 데이터로부터 획득(또는 추출)된 복수의 로그 패턴들 각각이 상태 정보(예: 이벤트 번호)로 변경될 수 있다. 예를 들어, 코스트가 서로 다른 로그 패턴들은 서로 다른 상태 정보로 변경(또는 식별)될 수 있다. 예를 들어, 코스트가 서로 같은 로그 패턴들은 동일한 상태 정보로 변경(또는 식별)될 수 있다.
- [90] 상술한 복수의 로그 패턴들 각각은 메모리에 저장될 수 있다. 따라서, 이상 상태 감지기(450)는 로그 데이터에 기반하여 식별된 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는 것에 기반하여, 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 로그 데이터에 기반하여 식별된 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하지 않는 것에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다.
- [91] 상술한 실시 예에서는, 로그 데이터에 기반하여 상태 정보가 식별되는 예가 도시되었으나 이에 한정되는 것은 아니다. 로그 데이터는 시간에 따른 동작들에 대한 정보를 나타낼 수 있다. 따라서, 로그 데이터에 기반하여, 제1 상태 정보 및 제2 상태 정보가 식별될 수 있다.
- [92] 일 예로, 제1 상태 정보는 제1 시점에서의 적어도 하나의 NE(410)에 관한 상태를 나타낼 수 있다. 제2 상태 정보는 제1 시점 이후의 제2 시점에서의 적어도 하나의 NE(410)에 관한 상태를 나타낼 수 있다. 예를 들어, 제1 상태 정보는 적어도 하나의 NE(410)의 과거의 상태를 나타낼 수 있다. 제2 상태 정보는 적어도 하나의 NE(410)의 현재의 상태를 나타낼 수 있다. 예를 들어, 제1 상태 정보는 제1 이벤트 번호를 포함할 수 있다. 제2 상태 정보는 제2 이벤트 번호를 포함할 수 있다. 제1 이벤트 번호 및 제2 이벤트 번호 각각은 적어도 하나의 NE(410)의 상태를 지시하기 위한 값일 수 있다.
- [93] 도 7은 상태 모델의 동작의 예를 도시한다.
- [94] 도 7을 참고하면, 이상 상태 감지기(450)는 로그 파서(460)에 기반하여 상태 정보(예: 이벤트 번호)를 식별할 수 있다. 이상 상태 감지기(450)는 로그 파서(460)

를 이용하여 상태 정보를 순차적으로 식별(또는 출력)할 수 있다. 이상 상태 감지기(450)는 상태 모델(471)을 이용하여, 순차적으로 식별되는 상태 정보에 기반하여, 상태 변화가 정상적인 변화인지 여부를 식별할 수 있다. 예를 들어, 이상 상태 감지기(450)는 로그 파서(460)를 이용하여 제1 상태 정보 및 제2 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 제1 상태 정보를 상태 모델(471)에 입력할 수 있다. 이상 상태 감지기(450)는 상태 모델(471)의 출력에 기반하여, 제3 상태 정보를 획득할 수 있다. 이상 상태 감지기(450)는 제2 상태 정보가 제3 상태 정보와 구별됨을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다. 이상 상태 감지기(450)는 제2 상태 정보가 제3 상태 정보에 상응함을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 정상 상태를 식별할 수 있다.

[95] 일 실시 예에 따르면, 상태 모델(471)은 유한 상태 기계(finite state automata)에 기반하여 구성될 수 있다. 상태 모델(471)은 유한한 상태를 가지는 기계이며, 상태 모델(471)은 한 번에 하나의 상태를 가질 수 있다. 각 상태는 특정 사건에 따라 다른 상태로 전이(또는 변경)될 수 있다. 상태 모델(471)은 전이 상태 및 전이 상태를 유발하는 조건의 집합으로 구성될 수 있다.

[96] 상태 모델(471)은 상태 변화에 대한 집합을 포함할 수 있다. 예를 들어, 적어도 하나의 NE(410)가 정상적으로 동작하는 경우, q1 상태는 q139 상태로 변경될 가능성이 있다. q139 상태는 q175 상태로 변경될 가능성이 있다. q1 상태가 식별된 후, 로그 데이터에 기반하여, q139 상태가 식별되는 것에 기반하여, 이상 상태 감지기(450)는 적어도 하나의 NE(410)가 정상 상태임을 식별할 수 있다. q139 상태가 식별된 후, 로그 데이터에 기반하여, q175 상태가 식별되는 것에 기반하여, 이상 상태 감지기(450)는 적어도 하나의 NE(410)가 비정상 상태임을 식별할 수 있다. 반면, q139 상태가 식별된 후, 로그 데이터에 기반하여, q190 상태가 식별되는 것에 기반하여, 이상 상태 감지기(450)는 적어도 하나의 NE(410)가 비정상 상태임을 식별할 수 있다.

[97] 일 실시 예에 따르면, 상태 모델(471)에 포함되지 않은 상태 변화가 발생하는 경우에도, 2 번 이내의 상태 전이가 가능하다면, 적어도 하나의 NE(410)가 정상 상태로 식별될 수 있다. 예를 들어, q2 상태에서부터 q19 상태로 상태로의 전이는 상태 모델(471)에 포함되지 않으나, q2 상태에서부터 q19 상태로의 전이 및 q19 상태에서부터 q150 상태로의 전이가 가능한 경우, 적어도 하나의 NE(410)가 정상 상태로 식별될 수 있다.

[98] 도 8은 예측 모델의 동작의 예를 도시한다.

[99] 도 8을 참조하면, 이상 상태 감지기(450)는 로그 파서(460)에 기반하여 상태 정보(예: 이벤트 번호)를 식별할 수 있다. 이상 상태 감지기(450)는 로그 파서(460)를 이용하여 상태 정보를 순차적으로 식별(또는 출력)할 수 있다. 이상 상태 감지기(450)는 순차적으로 식별되는 상태 정보에 기반하여, 예측 모델(472)을 이용하여 예측되는 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 예측되는 상

태 정보에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다. 예를 들어, 이상 상태 감지기(450)는 로그 파서(460)를 이용하여 제1 상태 정보 및 제2 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 제1 상태 정보를 예측 모델(472)에 입력할 수 있다. 이상 상태 감지기(450)는 예측 모델(472)의 출력에 기반하여, 제4 상태 정보를 획득할 수 있다. 이상 상태 감지기(450)는 제2 상태 정보가 제4 상태 정보와 구별됨을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다. 이상 상태 감지기(450)는 제2 상태 정보가 제4 상태 정보에 상응함을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 정상 상태를 식별할 수 있다.

- [100] 일 실시 예에 따르면, 예측 모델(472)은 LSTM(long short term memory)에 기반하여 구성될 수 있다. 예측 모델(472)은 제1 레이어(801), 제2 레이어(802), 및 제3 레이어(803)를 포함할 수 있다.
- [101] 제1 레이어(801)의 입력은 n 개의 상태들로 구성될 수 있다. 이상 상태 감지기(450)는 예측 모델(472)에 연속된 n 개의 상태들을 입력할 수 있다. n 은 관리자(또는 사용자)에 의해 변경될 수 있다. 제1 레이어(801)는 LSTM 레이어로 참조될 수 있다. LSTM은 시계열 데이터 분석에 가장 적합한 것으로 알려진 기계학습 알고리즘의 하나일 수 있다. LSTM은 데이터를 순차적으로 입력 받은 경우 다음 결과(또는 흐름)의 예측에 대한 높은 성능을 가질 수 있다.
- [102] 제1 레이어(801)의 출력단에 제2 레이어(802)가 구성될 수 있다. 제2 레이어(802)는 FC(fully connected) 레이어로 참조될 수 있다. 복수의 상태들의 확률 데이터를 식별하기 위해, 제2 레이어(802)의 출력의 개수가 k 개로 설정될 수 있다. k 는 로그 파서(460)에서 식별된 상태 정보의 개수에 상응할 수 있다. 제2 레이어(802)의 출력으로 k 차원의 벡터가 생성될 수 있다. 제2 레이어(802)의 출력은 k 개의 상태들 각각이 발생될 확률을 나타낼 수 있다.
- [103] k 개의 상태들 각각이 발생될 확률의 전체 합을 1로 만들기 위해, 제3 레이어(803)가 제2 레이어(802)의 출력단에 구성될 수 있다. 제3 레이어(803)는 소프트맥스(softmax) 레이어로 참조될 수 있다. 이상 상태 감지기(450)는 예측 모델(472)을 이용하여, 가장 높은 확률을 가지는 상태에 기반하여, 예측되는 상태 정보를 획득할 수 있다.
- [104] 이상 상태 감지기(450)는 로그 데이터에 기반하여 식별된 상태 정보가 예측 모델(472)을 통해 예측되는 상태 정보에 상응함을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 정상 상태를 식별할 수 있다. 이상 상태 감지기(450)는 로그 데이터에 기반하여 식별된 상태 정보가 예측 모델(472)을 통해 예측되는 상태 정보와 구별됨을 식별하는 것에 기반하여, 적어도 하나의 NE(410)의 이상 상태를 식별할 수 있다.
- [105] 실시 예에 따라, 이상 상태 감지기(450)는 예측 모델(472)가 연속으로 지정된 횟수(예: 7회)만큼 이상 상태를 식별하는 것에 기반하여, 알림(또는 알람)을 제공할 수 있다.

- [106] 도 9는 이상 상태 감지기의 동작에 관한 흐름도를 도시한다.
- [107] 도 9를 참고하면, 동작 901에서, 이상 상태 감지기(450)(또는 이상 상태 감지기(450)를 위한 전자 장치)는 로그 데이터를 획득할 수 있다. 예를 들어, 이상 상태 감지기(450)는 적어도 하나의 NE(410)로부터 로그 데이터를 획득할 수 있다.
- [108] 동작 902에서, 이상 상태 감지기(450)는 로그 패턴을 식별할 수 있다. 예를 들어, 이상 상태 감지기(450)는 로그 데이터에 기반하여 로그 패턴을 식별할 수 있다. 이상 상태 감지기(450)는 지정된 알고리즘(또는 지정된 규칙)에 기반하여 로그 데이터를 정규화(normalize)할 수 있다. 이상 상태 감지기(450)는 로그 데이터를 정규화하는 것에 기반하여, 로그 패턴을 획득할 수 있다.
- [109] 동작 903에서, 이상 상태 감지기(450)는 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는지 여부를 식별할 수 있다. 이상 상태 감지기(450)는 로그 데이터에 기반하여 식별된 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는지 여부를 식별할 수 있다. 메모리에 저장된 복수의 로그 패턴들 각각은 정상 상태를 나타낼 수 있다.
- [110] 동작 904에서, 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는 경우, 이상 상태 감지기(450)는 제1 상태 정보 및 제2 상태 정보를 식별할 수 있다. 로그 패턴이 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응함을 식별하는 것에 기반하여, 이상 상태 감지기(450)는 제1 상태 정보 및 제2 상태 정보를 식별할 수 있다.
- [111] 예를 들어, 로그 데이터는 지정된 시간 구간 내에서 획득된 로그 메시지(텍스트)들을 포함할 수 있다. 제1 상태 정보는 제1 시점에서의 적어도 하나의 NE(410)에 관한 상태를 나타낼 수 있다. 제2 상태 정보는 제1 시점 이후의 제2 시점에서의 적어도 하나의 NE(410)에 관한 상태를 나타낼 수 있다. 예를 들어, 제1 상태 정보는 적어도 하나의 NE(410)의 과거의 상태를 나타낼 수 있다. 제2 상태 정보는 적어도 하나의 NE(410)의 현재의 상태를 나타낼 수 있다.
- [112] 예를 들어, 이상 상태 감지기(450)는 도 6에서 설명된 로그 파서(460)를 이용하여, 동작 902 내지 동작 904를 수행할 수 있다.
- [113] 동작 905에서, 이상 상태 감지기(450)는 제2 상태 정보가, 제1 상태 정보를 이용하여 상태 모델(471)을 통해 식별된 제3 상태 정보에 상응하는지 여부를 식별할 수 있다. 이상 상태 감지기(450)는 제1 상태 정보를 이용하여, 상태 모델(471)을 통해 제3 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 제2 상태 정보가 제3 상태 정보에 상응하는지 여부를 식별할 수 있다. 예를 들어, 상태 모델(471)은 유한 상태 기계(finite state automata)에 기반하여 구성될 수 있다. 제3 상태 정보는 제1 상태 정보로부터 전이되는 상태 정보를 의미할 수 있다.
- [114] 예를 들어, 이상 상태 감지기(450)는 도 7에서 설명된 상태 모델(471)을 이용하여, 동작 905를 수행할 수 있다.
- [115] 동작 906에서, 제2 상태 정보가 제3 상태 정보에 상응하는 경우, 이상 상태 감지기(450)는 제2 상태 정보가, 제1 상태 정보를 이용하여 예측 모델(472)을 통해 식

별된 제4 상태 정보에 상응하는지 여부를 식별할 수 있다. 예를 들어, 제2 상태 정보가 제3 상태 정보에 상응함을 식별하는 것에 기반하여, 이상 상태 감지기(450)는 제2 상태 정보가, 제1 상태 정보를 이용하여 예측 모델(472)을 통해 식별된 제4 상태 정보에 상응하는지 여부를 식별할 수 있다. 이상 상태 감지기(450)는 제1 상태 정보를 이용하여, 예측 모델(472)을 통해 제4 상태 정보를 식별할 수 있다. 이상 상태 감지기(450)는 제2 상태 정보가 제4 상태 정보에 상응하는지 여부를 식별할 수 있다. 예를 들어, 예측 모델(472)은 LSTM(long short term memory)에 기반하여 구성될 수 있다. 제4 상태 정보는 제1 상태 정보에 기반하여 예측되는 상태 정보를 의미할 수 있다.

- [116] 동작 907은 제2 상태 정보가 제4 상태 정보에 상응하는 경우, 적어도 하나의 NE(410)가 정상 상태임을 식별할 수 있다. 예를 들어, 이상 상태 감지기(450)는 제2 상태 정보가 제4 상태 정보에 상응함을 식별하는 것에 기반하여, 적어도 하나의 NE(410)가 정상 상태임을 식별할 수 있다. 이상 상태 감지기(450)는 동작 903의 조건, 동작 905의 조건, 및 동작 906의 조건이 모두 만족됨을 식별하는 것에 기반하여, 적어도 하나의 NE(410)가 정상 상태임을 식별할 수 있다.
- [117] 동작 908은, 동작 903의 조건, 동작 905의 조건, 및 동작 906의 조건 중 적어도 하나가 만족되지 않는 경우, 이상 상태 감지기(450)는 적어도 하나의 NE(410)가 비정상 상태(또는 적어도 하나의 NE(410)의 이상 상태(anomaly))임을 식별할 수 있다. 이상 상태 감지기(450)는 동작 903의 조건, 동작 905의 조건, 및 동작 906의 조건 중 적어도 하나가 만족되지 않음을 식별하는 것에 기반하여, 적어도 하나의 NE(410)가 비정상 상태임을 식별할 수 있다.
- [118] 동작 909는, 이상 상태 감지기(450)는 적어도 하나의 NE(410)가 비정상 상태임을 식별하는 것에 기반하여, 알람(또는 알람)을 제공할 수 있다. 실시 예에 따라, 이상 상태 감지기(450)는 네트워크 컨트롤러(420)에게 알람을 제공할 수 있다. 네트워크 컨트롤러(420)는 데이터 트래픽의 경로를 비정상 상태가 발생한 적어도 하나의 NE(410)를 우회하도록 변경할 수 있다.
- [119] 도 10은 전자 장치의 기능적 구성의 예를 도시한다.
- [120] 도 10을 참고하면, 전자 장치(1000)는 도 4 내지 도 9의 이상 상태 감지기(450)에 상응할 수 있다. 일 실시 예에 따르면, 전자 장치(1000)는 송수신기(1001), 프로세서(1003), 및 메모리(1005)를 포함할 수 있다.
- [121] 송수신기(1001)는, 유선 통신 환경에서, 신호를 송수신하기 위한 기능들을 수행할 수 있다. 송수신기(1001)는, 전송 매체(transmission medium)(예: 구리선, 광섬유)를 통해 장치와 장치 간의 직접적인 연결을 제어하기 위한, 유선 인터페이스를 포함할 수 있다. 예를 들어, 송수신기(1001)는 구리선을 통해 다른 장치에게 전기적 신호를 전달하거나, 전기적 신호와 광신호간 변환을 수행할 수 있다.
- [122] 송수신기(1001)는 무선 통신 환경에서, 신호를 송수신하기 위한 기능들을 수행할 수도 있다. 예를 들어, 송수신기(1001)는 시스템의 물리 계층 규격에 따라 기저대역 신호 및 비트열 간 변환 기능을 수행할 수 있다. 예를 들어, 데이터 송신 시,

송수신기(1001)는 송신 비트열을 부호화 및 변조함으로써 복소 심볼들(complex-valued symbols)을 생성한다. 또한, 데이터 수신 시, 송수신기(1001)는 기저대역 신호를 복조 및 복호화를 통해 수신 비트열을 복원한다. 또한, 송수신기(1001)는 다수의 송수신 경로(path)들을 포함할 수 있다.

[123] 송수신기(1001)는 상술한 바와 같이 신호를 송신 및 수신한다. 이에 따라, 송수신기(1001)의 전부 또는 일부는 '통신부', '송신부', '수신부' 또는 '송수신부'로 지칭될 수 있다. 또한, 이하 설명에서, 무선 채널을 통해 수행되는 송신 및 수신은 송수신기(1001)에 의해 상술한 바와 같은 처리가 수행되는 것을 포함하는 의미로 사용된다.

[124] 프로세서(1003)는 전자 장치(1000)의 전반적인 동작들을 제어한다. 프로세서(1003)는 제어부로 지칭될 수 있다. 예를 들어, 프로세서(1003)는 송수신기(1001)를 통해 신호를 송신 및 수신한다. 또한, 프로세서(1003)는 메모리(1005)에 데이터를 기록하고, 읽는다. 그리고, 프로세서(1003)는 통신 규격에서 요구하는 프로토콜 스택(protocol stack)의 기능들을 수행할 수 있다. 도 10에는 프로세서(1003)만 도시되었으나, 다른 구현 예에 따라, 전자 장치(1000)는, 둘 이상의 프로세서들을 포함할 수 있다.

[125] 본 개시에서, 프로세서(1003)의 동작들은 소프트웨어에 의해 실행되거나, FPGA(Field Programmable Gate Array) 또는 ASIC(application-specific integrated circuit)과 같은 하드웨어 구성요소들을 제어하는 것을 의미할 수 있다. 또한, 프로세서(1003)는 소프트웨어 구성요소들, 객체지향 소프트웨어 구성요소들, 클래스 구성요소들 및 태스크 구성요소들과 같은 구성요소들과, 프로세스들, 함수들, 속성들, 프로시저들, 서브루틴들, 프로그램 코드의 세그먼트들, 드라이버들, 펌웨어, 마이크로코드, 회로, 데이터, 데이터베이스, 데이터 구조들, 테이블들, 어레이들, 및 변수들 중 적어도 하나를 포함할 수 있다. 프로세서(1003)는 적어도 하나의 모듈을 포함할 수 있으며, 용어 "모듈"은 하드웨어, 소프트웨어 또는 펌웨어로 구성된 유닛을 포함한다. 예를 들어, 모듈은 로직, 논리 블록, 부품, 또는 회로 등의 용어와 상호 호환적으로 사용될 수 있다. 모듈은, 일체로 구성된 부품 또는 하나 또는 그 이상의 기능을 수행하는 최소 단위 또는 그 일부가 될 수 있다. 예를 들면, 모듈은 ASIC으로 구성될 수 있다.

[126] 예를 들어, 프로세서(1003)는 상술한 실시 예들에 따른 블록들(예: 도 4에 도시된 블록들) 중 적어도 일부 또는 전부를 포함할 수 있다. 프로세서(1003)는 상술한 실시 예들에 따른 블록들(예: 도 4에 도시된 블록들) 중 적어도 일부 또는 전부의 기능을 수행할 수 있다.

[127] 메모리(1005)는 전자 장치(1000)의 동작을 위한 기본 프로그램, 응용 프로그램, 설정 정보 등의 데이터를 저장한다. 메모리(1005)는 저장부로 지칭될 수 있다. 메모리(1005)는 휘발성 메모리, 비휘발성 메모리 또는 휘발성 메모리와 비휘발성 메모리의 조합으로 구성될 수 있다. 그리고, 메모리(1005)는 프로세서(1003)의 요청에 따라 저장된 데이터를 제공한다.

- [128] 일 실시 예에 따르면, 전자 장치는, 인스트럭션들을 저장하고, 하나 이상의 저장 매체들을 포함하는 메모리, 및 처리 회로를 포함하는 적어도 하나의 프로세서를 포함할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 적어도 하나의 NE(network element)로부터, 상기 적어도 하나의 NE의 동작에 관한 로그 데이터를 획득하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 로그 데이터에 기반하여, 지정된 알고리즘을 통해 로그 패턴을 획득하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 로그 패턴에 기반하여, 제1 상태 정보 및 제2 상태 정보를 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제2 상태 정보가, 상기 제1 상태 정보를 이용하여 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제2 상태 정보가 상기 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 이상 상태를 식별하도록, 야기할 수 있다.
- [129] 일 실시 예에 따르면, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 지정된 알고리즘에 기반하여, 상기 로그 데이터를 정규화(normalize)하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 로그 데이터를 정규화 하는 것에 기반하여, 상기 로그 패턴을 획득하도록, 야기할 수 있다.
- [130] 일 실시 예에 따르면, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 로그 패턴이 상기 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는지 여부를 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 로그 패턴이 상기 복수의 로그 패턴들 중 하나에 상응하는 경우, 상기 로그 패턴에 기반하여, 상기 제1 상태 정보 및 상기 제2 상태 정보를 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 로그 패턴이 상기 복수의 로그 패턴들 중 하나에 상응하지 않는 경우, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하도록, 야기할 수 있다.
- [131] 일 실시 예에 따르면, 상기 적어도 하나의 모델은, 상태 모델 및 예측 모델을 포함할 수 있다.

- [132] 일 실시 예에 따르면, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제2 상태 정보가, 상기 상태 모델을 통해 식별된 제3 상태 정보와 구별됨을 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제2 상태 정보가 상기 제3 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하도록, 야기할 수 있다.
- [133] 일 실시 예에 따르면, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제1 상태 정보를, 상기 상태 모델에 입력하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 상태 모델의 출력에 기반하여, 상기 제3 상태 정보를 획득하도록, 야기할 수 있다.
- [134] 일 실시 예에 따르면, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제2 상태 정보가 상기 제3 상태 정보에 상응함을 식별하는 것에 기반하여, 상기 제2 상태 정보가, 상기 예측 모델을 통해 식별된 제4 상태 정보와 구별됨을 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제2 상태 정보가 상기 제4 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하도록, 야기할 수 있다.
- [135] 일 실시 예에 따르면, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 제1 상태 정보를, 상기 예측 모델에 입력하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 예측 모델의 출력에 기반하여, 상기 제4 상태 정보를 획득하도록, 야기할 수 있다.
- [136] 일 실시 예에 따르면, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 예측 모델의 출력에 기반하여, 복수의 상태들 각각에 대한 확률 데이터를 식별하도록 야기할 수 있다. 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가, 상기 복수의 상태들 중 가장 높은 확률을 가지는 상태에 기반하여, 상기 제4 상태 정보를 획득하도록, 야기할 수 있다.
- [137] 일 실시 예에 따르면, 상기 상태 모델은, 유한 상태 기계(finite state automata)에 기반하여 구성될 수 있다. 상기 예측 모델은, LSTM(long short term memory)에 기반하여 구성될 수 있다.

- [138] 일 실시 예에 따르면, 전자 장치에 의해 수행되는 방법은, 적어도 하나의 NE(network element)로부터, 상기 적어도 하나의 NE의 동작에 관한 로그 데이터를 획득하는 동작을 포함할 수 있다. 상기 방법은, 상기 로그 데이터에 기반하여, 지정된 알고리즘을 통해 로그 패턴을 획득하는 동작을 포함할 수 있다. 상기 방법은, 상기 로그 패턴에 기반하여, 제1 상태 정보 및 제2 상태 정보를 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 제2 상태 정보가, 상기 제1 상태 정보를 이용하여 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 제2 상태 정보가 상기 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 이상 상태를 식별하는 동작을 포함할 수 있다.
- [139] 일 실시 예에 따르면, 상기 방법은, 상기 지정된 알고리즘에 기반하여, 상기 로그 데이터를 정규화(normalize)하는 동작을 포함할 수 있다. 상기 방법은, 상기 로그 데이터를 정규화 하는 것에 기반하여, 상기 로그 패턴을 획득하는 동작을 포함할 수 있다.
- [140] 일 실시 예에 따르면, 상기 방법은, 상기 로그 패턴이 상기 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는지 여부를 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 로그 패턴이 상기 복수의 로그 패턴들 중 하나에 상응하는 경우, 상기 로그 패턴에 기반하여, 상기 제1 상태 정보 및 상기 제2 상태 정보를 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 로그 패턴이 상기 복수의 로그 패턴들 중 하나에 상응하지 않는 경우, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하는 동작을 포함할 수 있다.
- [141] 일 실시 예에 따르면, 상기 적어도 하나의 모델은, 상태 모델 및 예측 모델을 포함할 수 있다.
- [142] 일 실시 예에 따르면, 상기 방법은, 상기 제2 상태 정보가, 상기 상태 모델을 통해 식별된 제3 상태 정보와 구별됨을 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 제2 상태 정보가 상기 제3 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하는 동작을 포함할 수 있다.
- [143] 일 실시 예에 따르면, 상기 방법은, 상기 제1 상태 정보를, 상기 상태 모델에 입력하는 동작을 포함할 수 있다. 상기 방법은, 상기 상태 모델의 출력에 기반하여, 상기 제3 상태 정보를 획득하는 동작을 포함할 수 있다.
- [144] 일 실시 예에 따르면, 상기 방법은, 상기 제2 상태 정보가 상기 제3 상태 정보에 상응함을 식별하는 것에 기반하여, 상기 제2 상태 정보가, 상기 예측 모델을 통해 식별된 제4 상태 정보와 구별됨을 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 제2 상태 정보가 상기 제4 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하는 동작을 포함할 수 있다.
- [145] 일 실시 예에 따르면, 상기 방법은, 상기 제1 상태 정보를, 상기 예측 모델에 입력하는 동작을 포함할 수 있다. 상기 방법은, 상기 예측 모델의 출력에 기반하여, 상기 제4 상태 정보를 획득하는 동작을 포함할 수 있다.

- [146] 일 실시 예에 따르면, 상기 방법은, 상기 예측 모델의 출력에 기반하여, 복수의 상태들 각각에 대한 확률 데이터를 식별하는 동작을 포함할 수 있다. 상기 방법은, 상기 복수의 상태들 중 가장 높은 확률을 가지는 상태에 기반하여, 상기 제4 상태 정보를 획득하는 동작을 포함할 수 있다.
- [147] 일 실시 예에 따르면, 상기 상태 모델은, 유한 상태 기계(finite state automata)에 기반하여 구성될 수 있다. 상기 예측 모델은, LSTM (long short term memory)에 기반하여 구성될 수 있다.
- [148] 상술한 실시 예에 따르면, 네트워크 장비(또는 NE)를 통해서 이상 상태가 실시간으로 식별(또는 탐지(detect))될 수 있다. 예를 들어, 로그 데이터에 기반하여, 유사한 로그 패턴이 분석됨으로써, 로그 데이터가 효과적으로 압축될 수 있다. 네트워크 장비가 정상 상태인 동안 로그 패턴을 학습시킴으로써, 네트워크 장비의 비정상 로그가 실시간으로 판단될 수 있다. 네트워크 장비의 이상 상태가 식별되는 경우, 네트워크 관리자에게 실제 이상 유무를 확인할 수 있도록 알림이 제공될 수 있다. 이에 따라, 이상 상태에 대한 알림이 먼저 제공되므로, 심각한 문제(critical problem)의 발생이 방지될 수 있다. 기존에는 네트워크 프로토콜에 대한 로그 내용 및 네트워크 장비의 특징이 반영된 로그 내용이 고려되지 않아 이상 상태가 식별되기 어려웠으나, 상술한 실시 예에 따르면, 네트워크 장비에서 출력되는 로그 데이터를 통해서 네트워크 장비의 상태가 학습되므로, 이상 상태가 정확히 탐지되는 효과가 있다.
- [149] 본 개시의 청구항 또는 명세서에 기재된 실시예들에 따른 방법들은 하드웨어, 소프트웨어, 또는 하드웨어와 소프트웨어의 조합의 형태로 구현될(implemented) 수 있다.
- [150] 소프트웨어로 구현하는 경우, 하나 이상의 프로그램들(소프트웨어 모듈들)을 저장하는 컴퓨터 판독 가능 저장 매체가 제공될 수 있다. 컴퓨터 판독 가능 저장 매체에 저장되는 하나 이상의 프로그램들은, 전자 장치(device) 내의 하나 이상의 프로세서들에 의해 실행 가능하도록 구성된다(configured for execution). 하나 이상의 프로그램들은, 전자 장치로 하여금 본 개시의 청구항 또는 명세서에 기재된 실시예들에 따른 방법들을 실행하게 하는 명령어(instructions)를 포함한다. 상기 하나 이상의 프로그램들은 컴퓨터 프로그램 제품(computer program product)에 포함되어 제공될 수 있다. 컴퓨터 프로그램 제품은 상품으로서 판매자 및 구매자 간에 거래될 수 있다. 컴퓨터 프로그램 제품은 기기로 읽을 수 있는 저장 매체(예: compact disc read only memory(CD-ROM))의 형태로 배포되거나, 또는 어플리케이션 스토어(예: 플레이 스토어™)를 통해 또는 두 개의 사용자 장치들(예: 스마트폰들) 간에 직접, 온라인으로 배포(예: 다운로드 또는 업로드)될 수 있다. 온라인 배포의 경우에, 컴퓨터 프로그램 제품의 적어도 일부는 제조사의 서버, 어플리케이션 스토어의 서버, 또는 중계 서버의 메모리와 같은 기기로 읽을 수 있는 저장 매체에 적어도 일시 저장되거나, 임시적으로 생성될 수 있다.

- [151] 이러한 프로그램(소프트웨어 모듈, 소프트웨어)은 랜덤 액세스 메모리 (random access memory), 플래시(flash) 메모리를 포함하는 불휘발성(non-volatile) 메모리, 롬(read only memory, ROM), 전기적 삭제가능 프로그램가능 롬(electrically erasable programmable read only memory, EEPROM), 자기 디스크 저장 장치 (magnetic disc storage device), 콤팩트 디스크 롬(compact disc-ROM, CD-ROM), 디지털 다목적 디스크(digital versatile discs, DVDs) 또는 다른 형태의 광학 저장 장치, 마그네틱 카세트(magnetic cassette)에 저장될 수 있다. 또는, 이들의 일부 또는 전부의 조합으로 구성된 메모리에 저장될 수 있다. 또한, 각각의 구성 메모리는 다수 개 포함될 수도 있다.
- [152] 또한, 프로그램은 인터넷(Internet), 인트라넷(Intranet), LAN(local area network), WAN(wide area network), 또는 SAN(storage area network)과 같은 통신 네트워크, 또는 이들의 조합으로 구성된 통신 네트워크를 통하여 접근(access)할 수 있는 부착 가능한(attachable) 저장 장치(storage device)에 저장될 수 있다. 이러한 저장 장치는 외부 포트를 통하여 본 개시의 실시예를 수행하는 장치에 접속할 수 있다. 또한, 통신 네트워크상의 별도의 저장장치가 본 개시의 실시예를 수행하는 장치에 접속할 수도 있다.
- [153] 상술한 본 개시의 구체적인 실시예들에서, 개시에 포함되는 구성 요소는 제시된 구체적인 실시예에 따라 단수 또는 복수로 표현되었다. 그러나, 단수 또는 복수의 표현은 설명의 편의를 위해 제시한 상황에 적합하게 선택된 것으로서, 본 개시가 단수 또는 복수의 구성 요소에 제한되는 것은 아니며, 복수로 표현된 구성 요소라 하더라도 단수로 구성되거나, 단수로 표현된 구성 요소라 하더라도 복수로 구성될 수 있다.
- [154] 실시예들에 따르면, 전술한 해당 구성요소들 중 하나 이상의 구성요소들 또는 동작들이 생략되거나, 또는 하나 이상의 다른 구성요소들 또는 동작들이 추가될 수 있다. 대체적으로 또는 추가적으로, 복수의 구성요소들(예: 모듈 또는 프로그램)은 하나의 구성요소로 통합될 수 있다. 이런 경우, 통합된 구성요소는 상기 복수의 구성요소들 각각의 구성요소의 하나 이상의 기능들을 상기 통합 이전에 상기 복수의 구성요소들 중 해당 구성요소에 의해 수행되는 것과 동일 또는 유사하게 수행할 수 있다. 실시예들에 따르면, 모듈, 프로그램 또는 다른 구성요소에 의해 수행되는 동작들은 순차적으로, 병렬적으로, 반복적으로, 또는 휴리스틱하게 실행되거나, 상기 동작들 중 하나 이상이 다른 순서로 실행되거나, 생략되거나, 또는 하나 이상의 다른 동작들이 추가될 수 있다.
- [155] 한편 본 개시의 상세한 설명에서는 구체적인 실시예에 관해 설명하였으나, 본 개시의 범위에서 벗어나지 않는 한도 내에서 여러 가지 변형이 가능함은 물론이다.

청구범위

- [청구항 1] 전자 장치에 있어서,
 인스트럭션들을 저장하고, 하나 이상의 저장 매체들을 포함하는 메모리;
 및
 처리 회로를 포함하는 적어도 하나의 프로세서를 포함하고,
 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로
 또는 집합적으로, 실행될 시, 상기 전자 장치가:
 적어도 하나의 NE(network element)로부터, 상기 적어도 하나의 NE의 동
 작에 관한 로그 데이터를 획득하고,
 상기 로그 데이터에 기반하여, 지정된 알고리즘을 통해 로그 패턴을 획득
 하고,
 상기 로그 패턴에 기반하여, 제1 상태 정보 및 제2 상태 정보를 식별하고,
 상기 제2 상태 정보가, 상기 제1 상태 정보를 이용하여 적어도 하나의 모
 델을 통해 식별된 상태 정보와 구별됨을 식별하고,
 상기 제2 상태 정보가 상기 적어도 하나의 모델을 통해 식별된 상태 정보
 와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 이상 상
 태를 식별하도록, 야기하는,
 전자 장치.
- [청구항 2] 제1 항에 있어서, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에
 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가:
 상기 지정된 알고리즘에 기반하여, 상기 로그 데이터를 정규화(normalize)
 하고,
 상기 로그 데이터를 정규화 하는 것에 기반하여, 상기 로그 패턴을 획득하
 도록, 더 야기하는,
 전자 장치.
- [청구항 3] 제1 항에 있어서, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에
 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가:
 상기 로그 패턴이 상기 메모리에 저장된 복수의 로그 패턴들 중 하나에 상
 응하는지 여부를 식별하고,
 상기 로그 패턴이 상기 복수의 로그 패턴들 중 하나에 대응하는 경우, 상
 기 로그 패턴에 기반하여, 상기 제1 상태 정보 및 상기 제2 상태 정보를 식
 별하고,
 상기 로그 패턴이 상기 복수의 로그 패턴들 중 하나에 대응하지 않는 경
 우, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하도록, 더 야기하는,
 전자 장치.
- [청구항 4] 제1 항에 있어서, 상기 적어도 하나의 모델은,
 상태 모델 및 예측 모델을 포함하는,

전자 장치.

- [청구항 5] 제4 항에 있어서, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가:
상기 제2 상태 정보가, 상기 상태 모델을 통해 식별된 제3 상태 정보와 구별됨을 식별하고,
상기 제2 상태 정보가 상기 제3 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하도록, 더 야기하는,

전자 장치.

- [청구항 6] 제5 항에 있어서, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가:
상기 제1 상태 정보를, 상기 상태 모델에 입력하고,
상기 상태 모델의 출력에 기반하여, 상기 제3 상태 정보를 획득하도록, 더 야기하는,

전자 장치.

- [청구항 7] 제5 항에 있어서, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가:
상기 제2 상태 정보가 상기 제3 상태 정보에 상응함을 식별하는 것에 기반하여, 상기 제2 상태 정보가, 상기 예측 모델을 통해 식별된 제4 상태 정보와 구별됨을 식별하고,
상기 제2 상태 정보가 상기 제4 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하도록, 더 야기하는,

전자 장치.

- [청구항 8] 제7 항에 있어서, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가:
상기 제1 상태 정보를, 상기 예측 모델에 입력하고,
상기 예측 모델의 출력에 기반하여, 상기 제4 상태 정보를 획득하도록, 더 야기하는,

전자 장치.

- [청구항 9] 제8 항에 있어서, 상기 인스트럭션들은, 상기 적어도 하나의 프로세서에 의해, 개별적으로 또는 집합적으로, 실행될 시, 상기 전자 장치가:
상기 예측 모델의 출력에 기반하여, 복수의 상태들 각각에 대한 확률 데이터를 식별하고,
상기 복수의 상태들 중 가장 높은 확률을 가지는 상태에 기반하여, 상기 제4 상태 정보를 획득하도록, 더 야기하는,

전자 장치.

- [청구항 10] 제4 항에 있어서, 상기 상태 모델은,

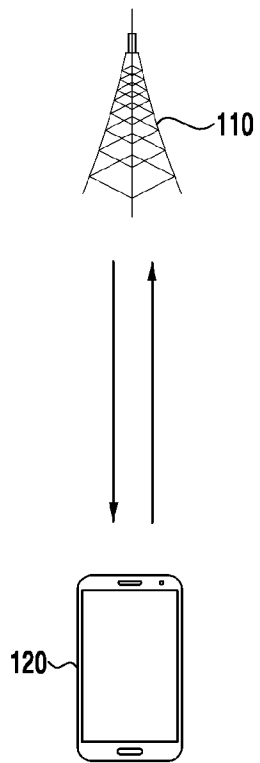
유한 상태 기계(finite state automata)에 기반하여 구성되고,
 상기 예측 모델은,
 LSTM (long short term memory)에 기반하여 구성되는,
 전자 장치.

- [청구항 11] 전자 장치에 의해 수행되는 방법에 있어서,
 적어도 하나의 NE(network element)로부터, 상기 적어도 하나의 NE의 동작에 관한 로그 데이터를 획득하는 동작;
 상기 로그 데이터에 기반하여, 지정된 알고리즘을 통해 로그 패턴을 획득하는 동작;
 상기 로그 패턴에 기반하여, 제1 상태 정보 및 제2 상태 정보를 식별하는 동작;
 상기 제2 상태 정보가, 상기 제1 상태 정보를 이용하여 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 동작; 및
 상기 제2 상태 정보가 상기 적어도 하나의 모델을 통해 식별된 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 이상 상태를 식별하는 동작을 포함하는,
 방법.
- [청구항 12] 제11 항에 있어서, 상기 방법은,
 상기 지정된 알고리즘에 기반하여, 상기 로그 데이터를 정규화(normalize)하는 동작; 및
 상기 로그 데이터를 정규화 하는 것에 기반하여, 상기 로그 패턴을 획득하는 동작을 더 포함하는,
 방법.
- [청구항 13] 제11 항에 있어서, 상기 방법은,
 상기 로그 패턴이 상기 메모리에 저장된 복수의 로그 패턴들 중 하나에 상응하는지 여부를 식별하는 동작;
 상기 로그 패턴이 상기 복수의 로그 패턴들 중 하나에 상응하는 경우, 상기 로그 패턴에 기반하여, 상기 제1 상태 정보 및 상기 제2 상태 정보를 식별하는 동작; 및
 상기 로그 패턴이 상기 복수의 로그 패턴들 중 하나에 상응하지 않는 경우, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하는 동작을 더 포함하는,
 방법.
- [청구항 14] 제11 항에 있어서, 상기 적어도 하나의 모델은,
 상태 모델 및 예측 모델을 포함하는,
 방법.
- [청구항 15] 제14 항에 있어서, 상기 방법은,

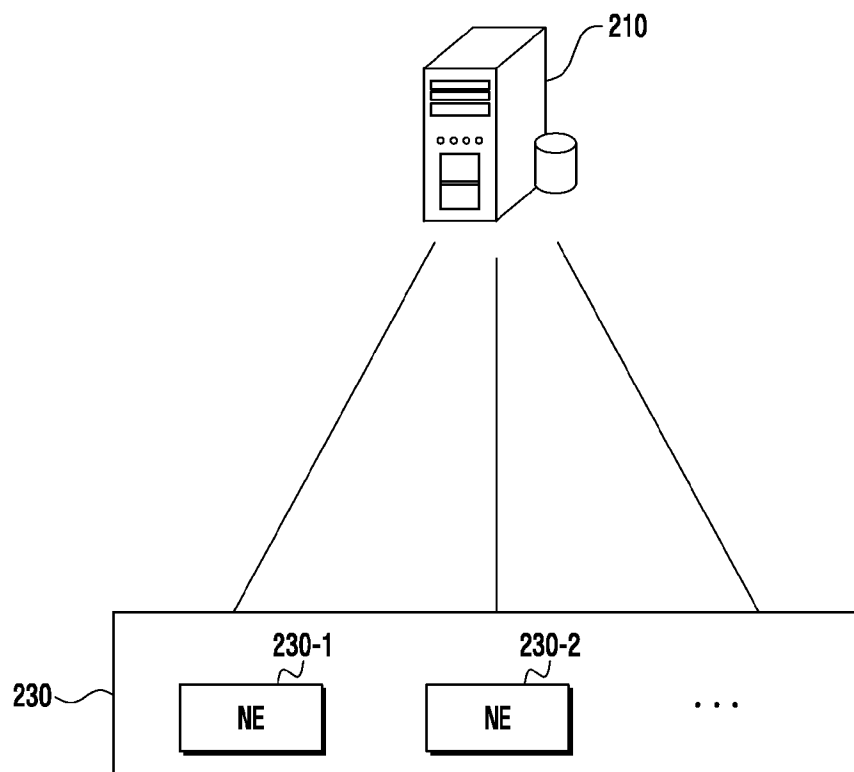
상기 제2 상태 정보가, 상기 상태 모델을 통해 식별된 제3 상태 정보와 구별됨을 식별하는 동작; 및

상기 제2 상태 정보가 상기 제3 상태 정보와 구별됨을 식별하는 것에 기반하여, 상기 적어도 하나의 NE의 상기 이상 상태를 식별하는 동작을 더 포함하는,
방법.

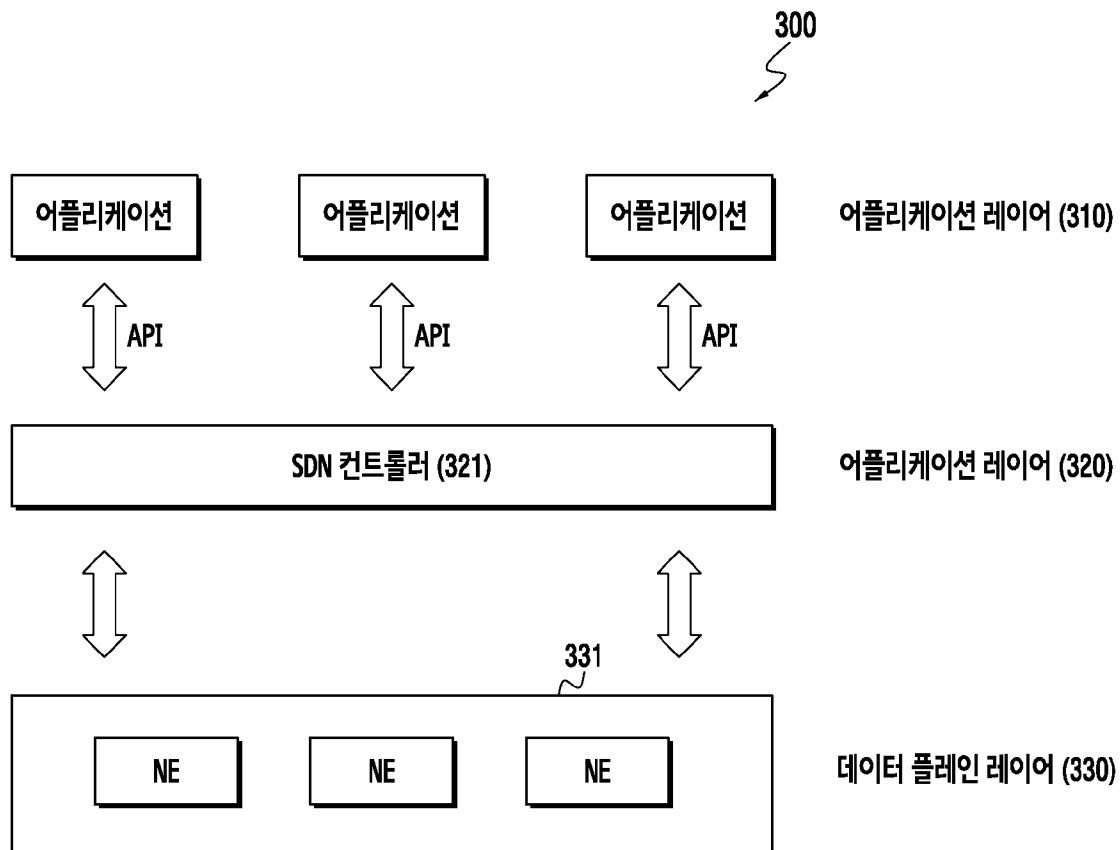
[도1]



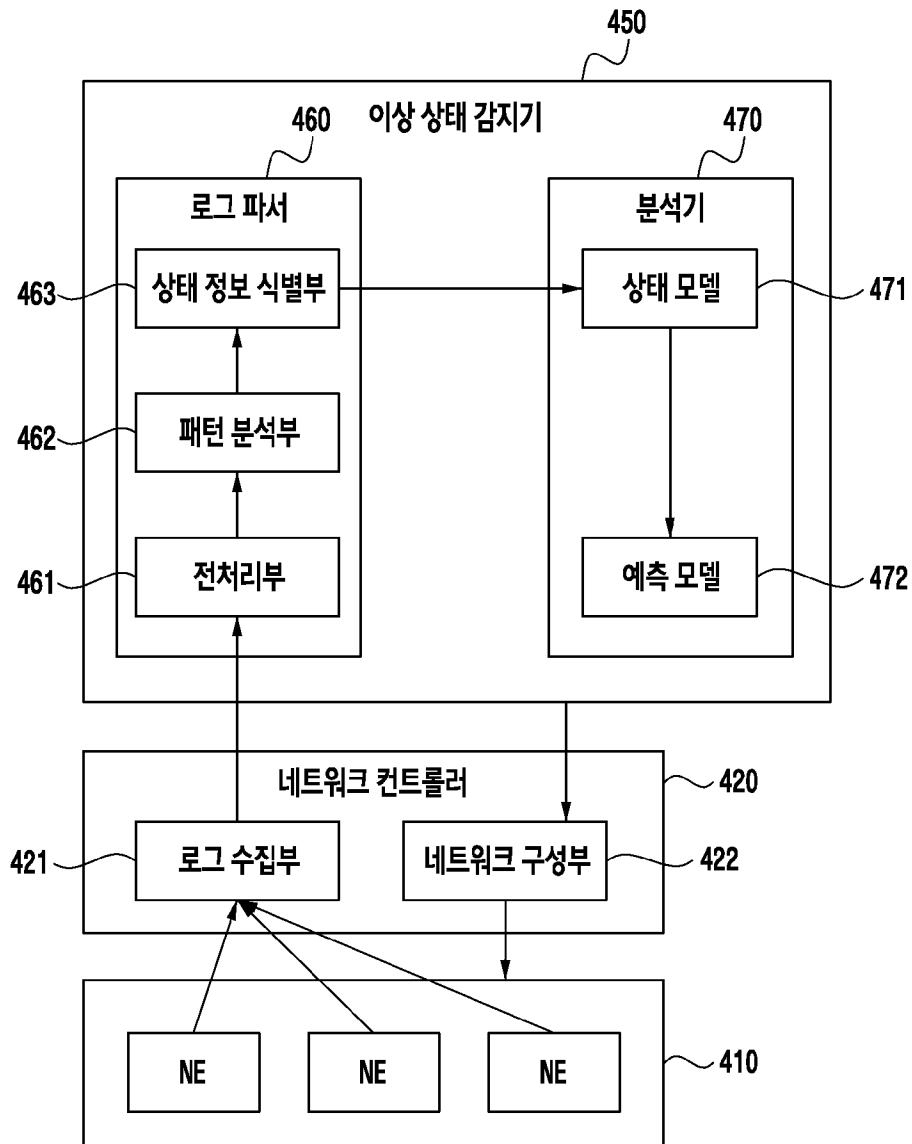
[도2]



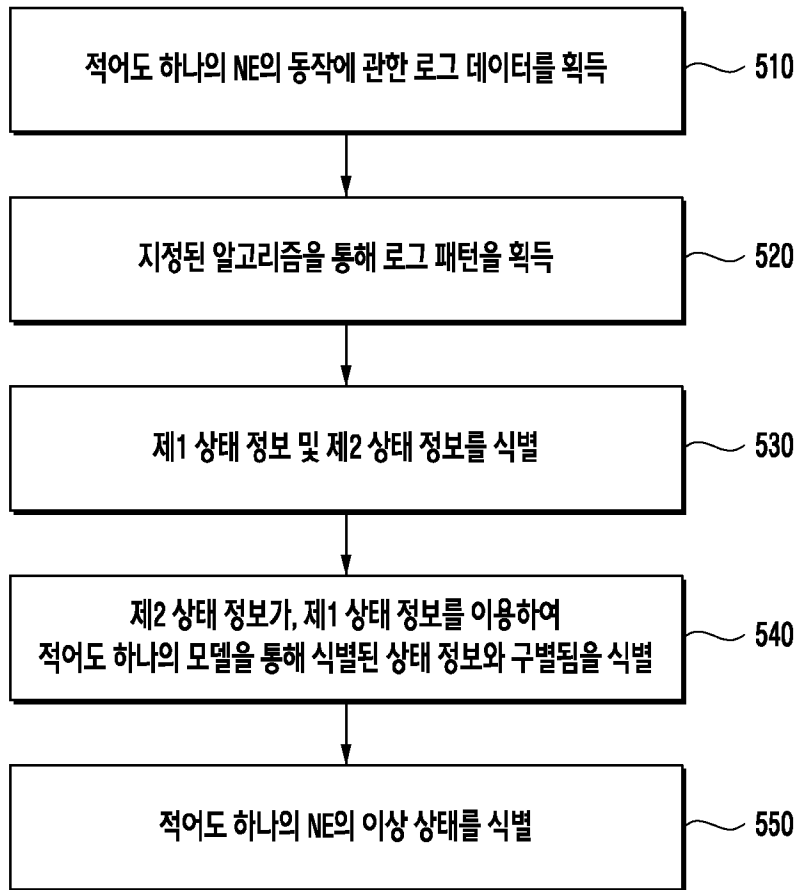
[도3]



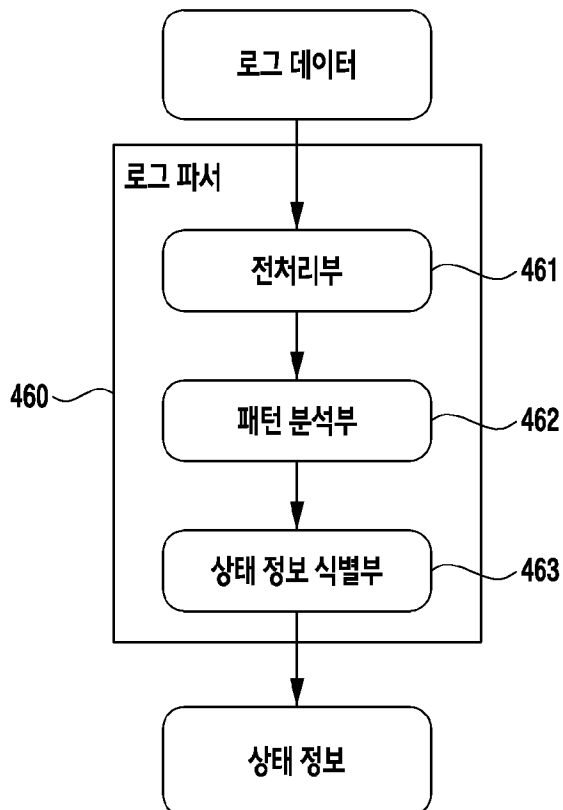
[도4]



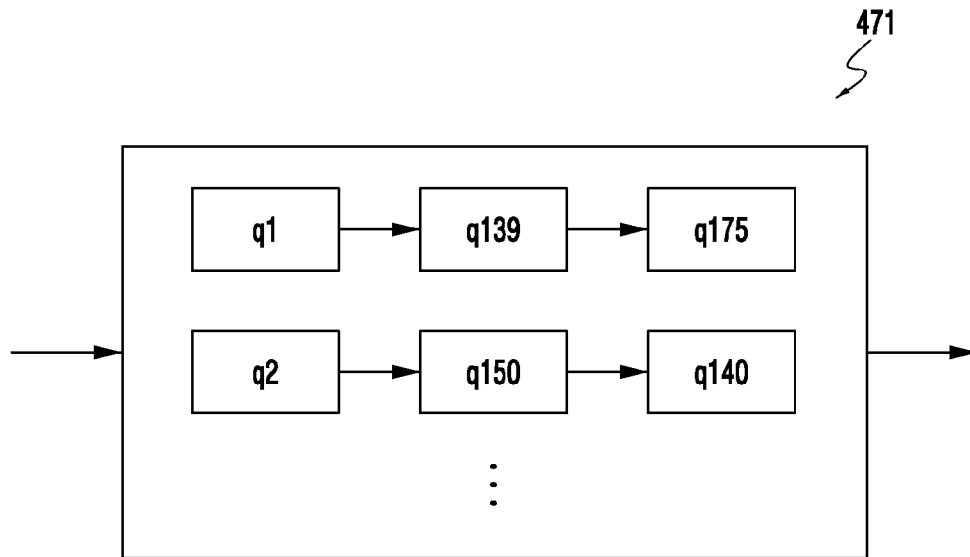
[도5]



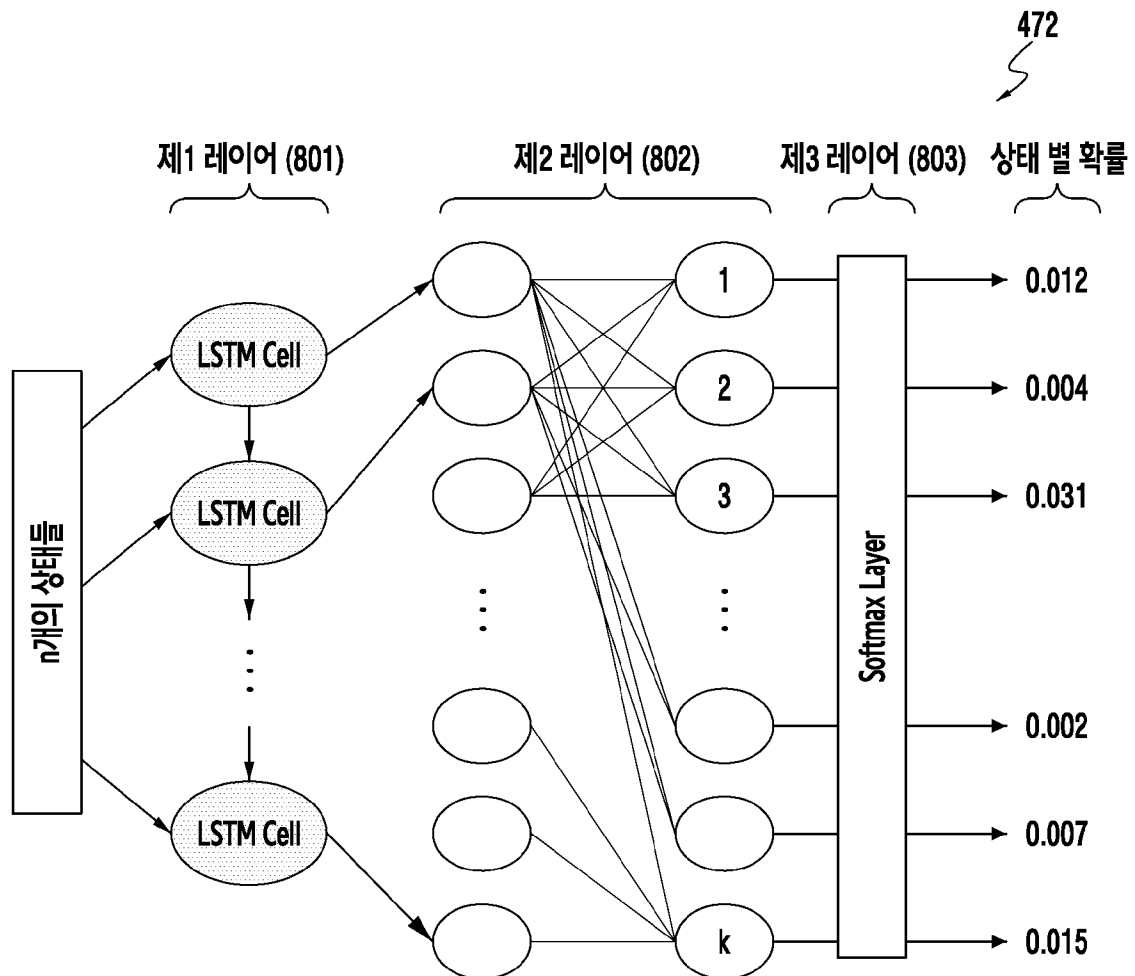
[도6]



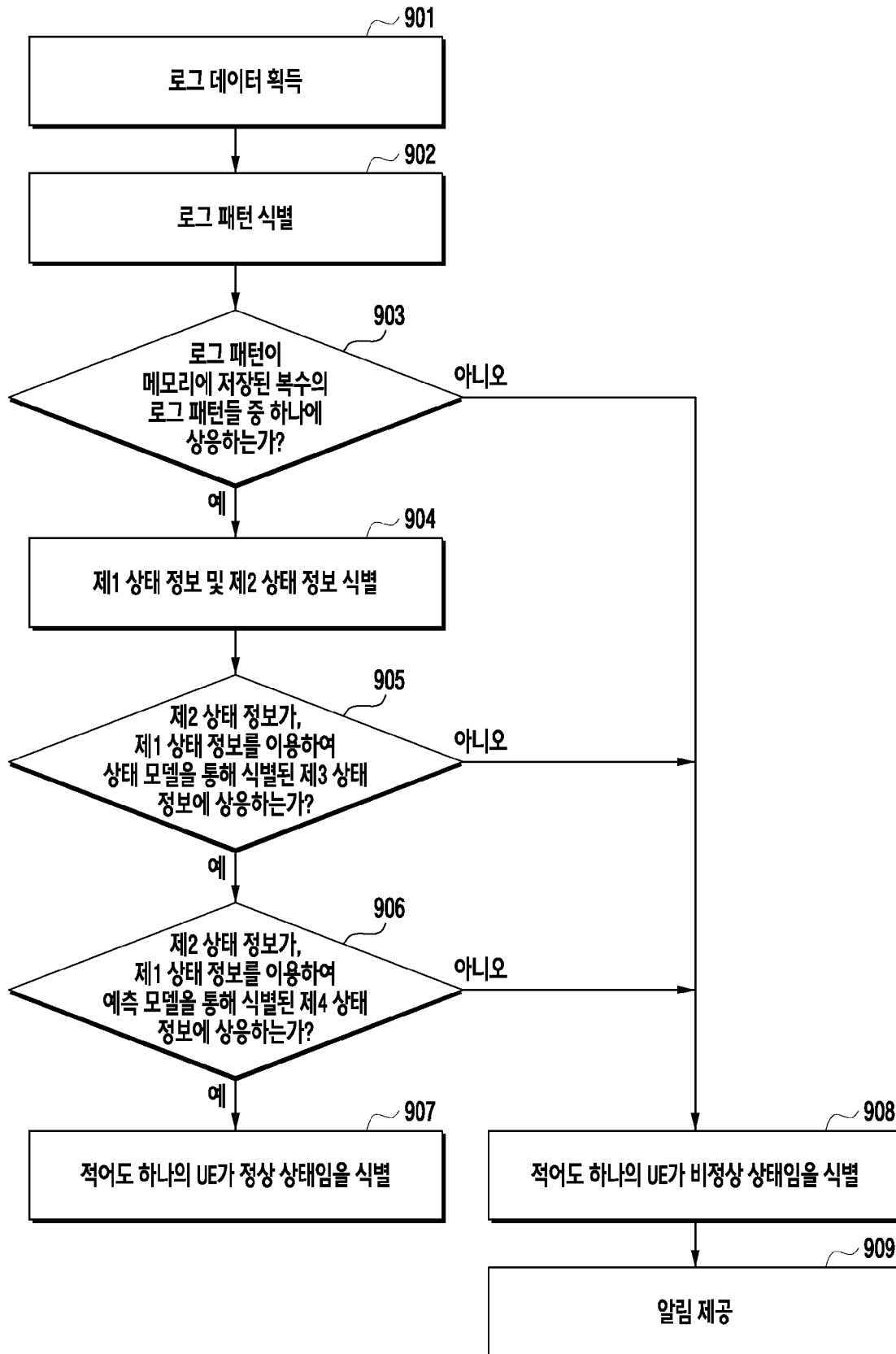
[도7]



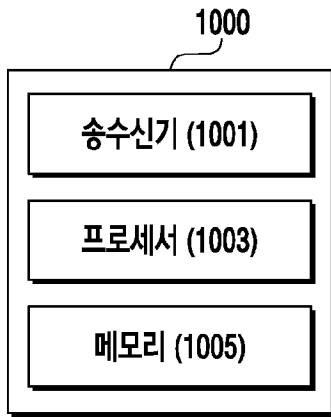
[도8]



[도9]



[도 10]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2024/013947

A. CLASSIFICATION OF SUBJECT MATTER**H04L 41/0695**(2022.01)i; **H04L 41/147**(2022.01)i; **G06F 18/26**(2023.01)i; **G06F 18/15**(2023.01)i; **G06F 9/448**(2018.01)i; **G06N 3/0442**(2023.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L 41/0695(2022.01); G06N 20/00(2019.01); H04L 12/24(2006.01); H04W 24/02(2009.01); H04W 24/08(2009.01); H04W 52/02(2009.01)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean utility models and applications for utility models: IPC as above
Japanese utility models and applications for utility models: IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (KIPO internal) & keywords: NE(network element), 로그 데이터(log data), 로그 패턴(log pattern), 상태 정보 (state information), 이상 상태(abnormal state)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2021-0028973 A1 (CIENA CORPORATION) 28 January 2021 (2021-01-28) See paragraphs [0081]-[0082], [0175] and [0182]; claim 7; and figures 4 and 23.	1-15
Y	CN 110224850 A (BEIJING BOCO INTER-TELECOM TECHNOLOGY CO., LTD.) 10 September 2019 (2019-09-10) See claims 1-4.	1-15
A	3GPP; TSG SA; Architecture enhancements for 5G System (5GS) to support network data analytics services (Release 18). 3GPP TS 23.288 V18.3.0. 19 September 2023. See sections 6.5 - 6.7.	1-15
A	KR 10-2020-0039295 A (SAMSUNG ELECTRONICS CO., LTD.) 16 April 2020 (2020-04-16) See paragraphs [0056]-[0073]; and figure 3.	1-15
A	KR 10-2020-0135867 A (CHINA ACADEMY OF TELECOMMUNICATIONS TECHNOLOGY) 03 December 2020 (2020-12-03) See paragraphs [0142]-[0169]; and figure 2.	1-15



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance
“D” document cited by the applicant in the international application
“E” earlier application or patent but published on or after the international filing date
“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
“O” document referring to an oral disclosure, use, exhibition or other means
“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

03 January 2025

Date of mailing of the international search report

06 January 2025

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon Building 4, 189 Cheongsaro, Seo-gu, Daejeon 35208

Facsimile No. +82-42-481-8578

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/KR2024/013947

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)		Publication date (day/month/year)
US	2021-0028973	A1	28 January 2021	US	11356320 B2	07 June 2022
CN	110224850	A	10 September 2019	None		
KR	10-2020-0039295	A	16 April 2020	CN	112840693 A	25 May 2021
				EP	3818744 A1	12 May 2021
				EP	3818744 A4	25 August 2021
				KR	10-2700547 B1	30 August 2024
				US	10986579 B2	20 April 2021
				US	11743823 B2	29 August 2023
				US	2020-0112921 A1	09 April 2020
				US	2021-0314868 A1	07 October 2021
				WO	2020-071874 A1	09 April 2020
KR	10-2020-0135867	A	03 December 2020	CN	110312279 A	08 October 2019
				CN	110312279 B	05 March 2021
				EP	3780702 A1	17 February 2021
				EP	3780702 A4	26 May 2021
				EP	3780702 B1	22 November 2023
				US	11700540 B2	11 July 2023
				US	2021-0022022 A1	21 January 2021
				WO	2019-184433 A1	03 October 2019

A. 발명이 속하는 기술분류(국제특허분류(IPC))

H04L 41/0695(2022.01)i; H04L 41/147(2022.01)i; G06F 18/26(2023.01)i; G06F 18/15(2023.01)i; G06F 9/448(2018.01)i; G06N 3/0442(2023.01)i

B. 조사된 분야

조사된 최소문헌(국제특허분류를 기재)

H04L 41/0695(2022.01); G06N 20/00(2019.01); H04L 12/24(2006.01); H04W 24/02(2009.01); H04W 24/08(2009.01); H04W 52/02(2009.01)

조사된 기술분야에 속하는 최소문헌 이외의 문헌

한국등록실용신안공보 및 한국공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

일본등록실용신안공보 및 일본공개실용신안공보: 조사된 최소문헌란에 기재된 IPC

국제조사에 이용된 전산 데이터베이스(데이터베이스의 명칭 및 검색어(해당하는 경우))

eKOMPASS(특허청 내부 검색시스템) & 키워드: NE(network element), 로그 데이터(log data), 로그 패턴(log pattern), 상태 정보(state information), 이상 상태(abnormal state)

C. 관련 문헌

카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항
Y	US 2021-0028973 A1 (CIENA CORPORATION) 2021.01.28 단락 [0081]-[0082], [0175], [0182]; 청구항 7; 및 도면 4, 23	1-15
Y	CN 110224850 A (BEIJING BOCO INTER-TELECOM TECHNOLOGY CO., LTD.) 2019.09.10 청구항 1-4	1-15
A	'3GPP; TSG SA; Architecture enhancements for 5G System (5GS) to support network data analytics services (Release 18)', 3GPP TS 23.288 V18.3.0, 2023.09.19 섹션 6.5 - 6.7	1-15
A	KR 10-2020-0039295 A (삼성전자주식회사) 2020.04.16 단락 [0056]-[0073]; 및 도면 3	1-15
A	KR 10-2020-0135867 A (차이나 아카데미 오브 텔레커뮤니케이션즈 테크놀로지) 2020.12.03 단락 [0142]-[0169]; 및 도면 2	1-15

☐ 추가 문헌이 C(계속)에 기재되어 있습니다.

☒ 대응특허에 관한 별지를 참조하십시오.

* 인용된 문헌의 특별 카테고리:

“A” 특별히 관련이 없는 것으로 보이는 일반적인 기술수준을 정의한 문헌

“D” 본 국제출원에서 출원인이 인용한 문헌

“E” 국제출원일보다 빠른 출원일 또는 우선일을 가지나 국제출원일 이후에 공개된 선출원 또는 특허 문헌

“L” 우선권 주장에 의문을 제기하는 문헌 또는 다른 인용문헌의 공개일 또는 다른 특별한 이유(이유를 명시)를 밝히기 위하여 인용된 문헌

“O” 구두 개시, 사용, 전시 또는 기타 수단을 언급하고 있는 문헌

“P” 우선일 이후에 공개되었으나 국제출원일 이전에 공개된 문헌

“T” 국제출원일 또는 우선일 후에 공개된 문헌으로, 출원과 상충하지 않으며 발명의 기초가 되는 원리나 이론을 이해하기 위해 인용된 문헌

“X” 특별한 관련이 있는 문헌. 해당 문헌 하나만으로 청구된 발명의 신규성 또는 진보성이 없는 것으로 본다.

“Y” 특별한 관련이 있는 문헌. 해당 문헌이 하나 이상의 다른 문헌과 조합하는 경우로 그 조합이 당업자에게 자명한 경우 청구된 발명은 진보성이 없는 것으로 본다.

“&” 동일한 대응특허문헌에 속하는 문헌

국제조사의 실제 완료일

2025년01월03일(03.01.2025)

국제조사보고서 발송일

2025년01월06일(06.01.2025)

ISA/KR의 명칭 및 우편주소

대한민국 특허청
(35208) 대전광역시 서구 청사로 189, 4동 (둔산동,
정부대전청사)

팩스 번호 +82-42-481-8578

심사관

양정록

전화번호 +82-42-481-5709

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
US 2021-0028973 A1	2021/01/28	US 11356320 B2	2022/06/07
CN 110224850 A	2019/09/10	없음	
KR 10-2020-0039295 A	2020/04/16	CN 112840693 A	2021/05/25
		EP 3818744 A1	2021/05/12
		EP 3818744 A4	2021/08/25
		KR 10-2700547 B1	2024/08/30
		US 10986579 B2	2021/04/20
		US 11743823 B2	2023/08/29
		US 2020-0112921 A1	2020/04/09
		US 2021-0314868 A1	2021/10/07
		WO 2020-071874 A1	2020/04/09
KR 10-2020-0135867 A	2020/12/03	CN 110312279 A	2019/10/08
		CN 110312279 B	2021/03/05
		EP 3780702 A1	2021/02/17
		EP 3780702 A4	2021/05/26
		EP 3780702 B1	2023/11/22
		US 11700540 B2	2023/07/11
		US 2021-0022022 A1	2021/01/21
		WO 2019-184433 A1	2019/10/03