

(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2016 년 12 월 8 일 (08.12.2016)



(10) 국제공개번호
WO 2016/195261 A1

- (51) 국제특허분류:
H04M 3/22 (2006.01)
- (21) 국제출원번호: PCT/KR2016/004805
- (22) 국제출원일: 2016 년 5 월 9 일 (09.05.2016)
- (25) 출원언어: 한국어
- (26) 공개언어: 한국어
- (30) 우선권정보:
10-2015-0077564 2015 년 6 월 1 일 (01.06.2015) KR
- (71) 출원인: 주식회사 케이티 (KT CORPORATION) [KR/KR]; 13606 경기도 성남시 분당구 불정로 90, Gyeonggi-do (KR).
- (72) 발명자: 백광현 (BAEK, Kwang-Hyun); 34049 대전시 유성구 엑스포로 448, 406 동 1604 호, Daejeon (KR). 김우태 (KIM, Woo-Tae); 34023 대전시 유성구 배울 2 로 42, 506 동 1001 호, Daejeon (KR). 안태진 (AHN, Tae-Jin); 34049 대전시 유성구 엑스포로 448, 506 동 701 호, Daejeon (KR).
- (74) 대리인: 유미특허법인 (YOU ME PATENT AND LAW FIRM); 06134 서울시 강남구 테헤란로 115, Seoul (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, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, 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, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

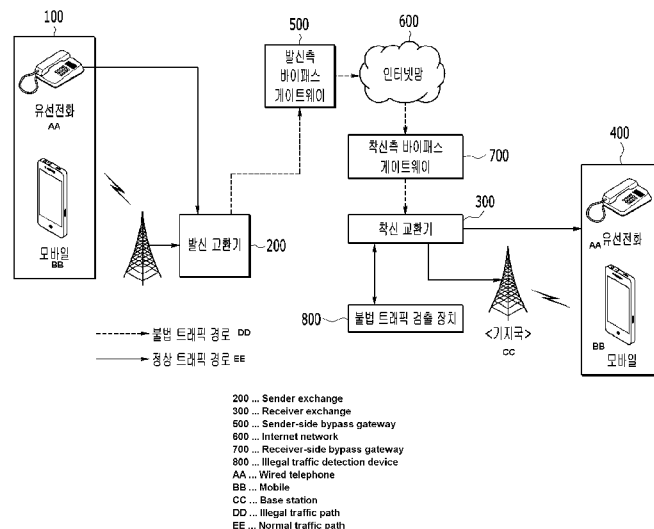
(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, 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 제 21 조(3))

(54) Title: ILLEGAL TRAFFIC DETECTION DEVICE AND METHOD

(54) 발명의 명칭 : 불법 트래픽 검출 장치 및 그 방법



(57) Abstract: Disclosed are an illegal traffic detection device and a method therefor. Here, an illegal traffic detection system comprises: a traffic collecting unit for collecting call traffic from an exchange, and parsing a call detail record (CDR) from the call traffic; a pattern detection unit for detecting, from the call traffic, whether pre-defined patterns appearing in illegal traffic occur for each type of pattern, on the basis of the call detail record; and an illegal traffic detection unit for determining whether the call traffic is illegal traffic, on the basis of the result of the pattern detection for each type of pattern, and transmitting the determination result to the exchange, wherein the illegal traffic is traffic that is fed into the exchange via an illegal traffic path instead of via a normal traffic path provided by a communication service provider.

(57) 요약서:

[다음 쪽 계속]

WO 2016/195261 A1



불법 트래픽 검출 장치 및 그 방법이 개시된다. 여기서, 불법 트래픽 검출 시스템은 교환기로부터 통화 트래픽을 수집하고, 상기 통화 트래픽으로부터 콜 상세 기록(CDR, Call Detail Record)을 파싱하는 트래픽 수집부, 상기 콜 상세 기록을 토대로 상기 통화 트래픽으로부터 기 정의된 불법 트래픽에서 나타나는 패턴의 유형별 발생 여부를 검출하는 패턴 검출부, 그리고 상기 유형별로 패턴의 검출 결과를 기초로 상기 통화 트래픽이 불법 트래픽인지 판단하고, 판단 결과를 상기 교환기로 전송하는 불법 트래픽 검출부를 포함하고, 상기 불법 트래픽은, 통신 사업자가 제공하는 정상 트래픽 경로를 거치지 않고 불법 트래픽 경로를 거쳐 상기 교환기로 유입된 것이다.

명세서

발명의 명칭: 불법 트래픽 검출 장치 및 그 방법

기술분야

- [1] 본 발명은 불법 트래픽 검출 장치 및 그 방법에 관한 것이다.

배경기술

- [2] CSCF(Communications Fraud Control Association)는 전세계 부정 통신 사용 피해 규모가 2013년 약43B\$ 손실이 발생했으며 이런 불법호 유형 톱(Top) 5중 우회 트래픽(Interconnect Bypass, SIM BOX)이 차지하는 비중이 약 9%라고 발표했다. 이처럼 불법호의 유형 및 그 발생 형태가 다양해지고 있는 현실이다.
- [3] 이렇게 통화를 우회하는 방식은 서비스 사업자의 수익을 감소 시킬 뿐만 아니라 서비스 품질 확보를 위한 여러 노력(장비 투자 및 회선 증설 등) 없이 공중 인터넷 네트워크를 활용 하므로써 회선의 트래픽 증가에 따른 이용 고객들에게 품질상의 문제를 야기 시키고 있음에도 이를 탐지하고 차단하는데 한계가 있는 현실이다.
- [4] 종래에 불법 국제 전화를 차단하기 위해 콜 상세 기록(CDR, Call Detail Record) 정보를 포함하는 통화 패턴과 기 정의된 이상 트래픽을 비교하여 이상 트래픽 여부를 판단한다는 구성은 존재한다. 하지만, 다양한 유형 및 무궁무진한 방법으로 불법 트래픽을 유발시키는 현재의 환경에서 단순히 CDR 정보만을 이용하는 경우, 개개의 불법 트래픽 유형을 탐지하는 데는 한계가 있다.

발명의 상세한 설명

기술적 과제

- [5] 따라서, 본 발명이 이루고자 하는 기술적 과제는 불법 트래픽의 유형별 또는 그 형태별 고유의 발생 패턴을 검출함으로써, 인터코넥트 바이패스(Interconnect Bypass)와 같이 이용 요금의 단가 차액을 주요 수입원으로 하는 통신 사업자를 우회하는 불법 트래픽을 검출하는 장치 및 그 방법을 제공하는 것이다.

과제 해결 수단

- [6] 본 발명의 하나의 특징에 따르면, 불법 트래픽 검출 장치는 교환기로부터 통화 트래픽을 수집하고, 상기 통화 트래픽으로부터 콜 상세 기록(CDR, Call Detail Record)을 파싱하는 트래픽 수집부, 상기 콜 상세 기록을 토대로 상기 통화 트래픽으로부터 기 정의된 불법 트래픽에서 나타나는 패턴의 유형별 발생 여부를 검출하는 패턴 검출부, 그리고 상기 유형별로 패턴의 검출 결과를 기초로 상기 통화 트래픽이 불법 트래픽인지 판단하고, 판단 결과를 상기 교환기로 전송하는 불법 트래픽 검출부를 포함하고, 상기 불법 트래픽은, 통신 사업자가 제공하는 정상 트래픽 경로를 거치지 않고 불법 트래픽 경로를 거쳐 상기 교환기로 유입된 것일 수 있다.
- [7] 상기 불법 트래픽 검출부는,

- [8] 상기 교환기로부터 수집한 통화 트래픽이 발신측 바이패스 게이트웨이, 인터넷망, 착신측 바이패스 게이트웨이로 이루어진 상기 불법 트래픽 경로로부터 수신된 것인지 판단할 수 있다.
- [9] 상기 불법 트래픽을 저장하는 데이터베이스를 더 포함하고,
- [10] 상기 트래픽 수집부는,
- [11] 상기 통화 트래픽을 수집한 경우, 상기 데이터베이스를 조회하여 상기 통화 트래픽이 상기 데이터베이스에 존재하는지 판단하고, 상기 데이터베이스에 존재하면 상기 통화 트래픽이 불법 트래픽임을 알리는 불법 트래픽 검출 정보를 상기 교환기로 전달하고,
- [12] 상기 트래픽 수집부는,
- [13] 상기 통화 트래픽이 상기 데이터베이스에 존재하지 않는 경우, 상기 콜 상세 기록을 생성하여 상기 패턴 검출부로 전달할 수 있다.
- [14] 상기 불법 트래픽 검출부는,
- [15] 상기 패턴 검출부가 검출한 패턴 별로 상기 패턴의 조합, 상기 패턴 별로 기 정의된 가중치 및 사용 빈도를 고려하여 최종적으로 상기 통화 트래픽이 불법 트래픽인지 판단할 수 있다.
- [16] 상기 패턴 검출부는,
- [17] 상기 콜 상세 기록을 토대로 상기 통화 트래픽의 발신 단말이 무선 단말이고, 지역적 이동 없이 통화를 발생시키는 패턴에 해당하는지 검출할 수 있다.
- [18] 상기 패턴 검출부는,
- [19] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 음성 통화만 사용하는 패턴에 해당하는지 검출할 수 있다.
- [20] 상기 패턴 검출부는,
- [21] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 전체 호 성공률 대비 발신 성공 호 비율이 임계치를 초과하는 패턴에 해당하는지 검출할 수 있다.
- [22] 상기 패턴 검출부는,
- [23] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 착신번호 수가 임계치를 초과하는 패턴에 해당하는지 검출할 수 있다.
- [24] 상기 패턴 검출부는,
- [25] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 전체 서비스 별 이용 횟수 대비 음성 통화 시도 횟수가 임계치를 초과하는 패턴에 해당하는지 검출할 수 있다.
- [26] 상기 패턴 검출부는,
- [27] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 기지국 내 음성 채널 할당 가입자수가 임계치를 초과하는 패턴에 해당하는지 검출할 수 있다.
- [28] 상기 패턴 검출부는,
- [29] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 야간 통화 발생 횟수가 임계치를 초과하는 패턴에 해당하는지 검출할 수 있다.
- [30] 상기 패턴 검출부는,

- [31] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 착신 성공호 평균 통화 유지 시간이 임계치 미만인 패턴에 해당하는지 검출할 수 있다.
- [32] 상기 패턴 검출부는,
- [33] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 가입자 망 내 이용율이 임계치를 초과하는 패턴에 해당하는지 검출할 수 있다.
- [34] 상기 패턴 검출부는,
- [35] 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 가입자의 통화량이 임계치를 초과하는 패턴에 해당하는지 검출할 수 있다.
- [36] 상기 패턴 검출부는,
- [37] 상기 콜 상세 기록을 토대로 상기 통화 트래픽의 품질이 임계치 미만인 패턴에 해당하는지 검출할 수 있다.
- [38] 상기 패턴 검출부는,
- [39] 상기 콜 상세 기록을 토대로 상기 통화 트래픽의 발신번호가 선불요금제 가입된 패턴에 해당하는지 검출할 수 있다.
- [40] 본 발명의 다른 특징에 따르면, 불법 트래픽 검출 방법은 교환기로부터 통화 트래픽을 수집하는 단계, 수집한 통화 트래픽이 기 정의된 불법 트래픽인지 판단하는 단계, 상기 수집한 통화 트래픽이 상기 불법 트래픽이 아닌 경우, 상기 수집한 통화 트래픽으로부터 콜 상세 기록(CDR, Call Detail Record)을 파싱하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽으로부터 기 정의된 불법 트래픽에서 나타나는 패턴의 유형별 발생 여부를 검출하는 단계, 상기 패턴 별로 상기 패턴의 조합, 상기 패턴 별로 기 정의된 가중치 및 사용 빈도를 고려하여 상기 수집한 통화 트래픽이 불법 트래픽인지 판단하는 단계, 그리고 상기 수집한 통화 트래픽이 불법 트래픽인지 아닌지를 나타내는 정보를 상기 교환기로 전송하는 단계를 포함하고,
- [41] 상기 불법 트래픽은, 통신 사업자가 제공하는 정상 트래픽 경로를 거치지 않고 발신측 바이패스 게이트웨이, 인터넷망, 착신측 바이패스 게이트웨이를 이루어진 불법 트래픽 경로를 거쳐 상기 교환기로 유입된 것일 수 있다.
- [42] 상기 패턴의 유형별 발생 여부를 검출하는 단계는,
- [43] 상기 콜 상세 기록을 토대로 상기 통화 트래픽의 발신 단말이 무선 단말이고, 지역적 이동 없이 통화를 발생시키는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 음성 통화만 사용하는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 전체 호 성공률 대비 발신 성공 호 비율이 임계치를 초과하는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 착신번호 수가 임계치를 초과하는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 전체 서비스 별 이용 횟수 대비 음성 통화 시도 횟수가 임계치를 초과하는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 기지국 내 음성 채널 할당 가입자수가

임계치를 초과하는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 야간 통화 발생 횟수가 임계치를 초과하는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 착신 성공호 평균 통화 유지 시간이 임계치 미만에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 가입자 망 내 이용율이 임계치를 초과하는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 가입자의 통화량이 임계치를 초과하는 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽의 품질이 임계치 미만인 패턴에 해당하는지 판단하는 단계, 상기 콜 상세 기록을 토대로 상기 통화 트래픽의 발신번호가 선불요금제 가입된 패턴에 해당하는지 판단하는 단계, 그리고 상기 패턴 중 적어도 하나 이상에 해당하는 경우, 상기 패턴을 판단한 결과 및 해당 통화 트래픽을 데이터베이스에 업데이트하는 단계를 포함할 수 있다.

발명의 효과

- [44] 본 발명의 실시예에 따르면, 통화로를 우회하는 불법 트래픽의 패턴을 분석 및 탐지함으로써, 불법 트래픽이 발생할 경우 즉시 탐지하고 차단 등의 조치를 실시할 수 있는 효과가 있다.

도면의 간단한 설명

- [45] 도 1은 본 발명의 실시예에 따른 불법 트래픽 검출을 위한 개략적인 네트워크 구성도이다.
- [46] 도 2는 본 발명의 실시예에 따른 불법 트래픽 검출 장치의 세부 구성을 나타낸 블록도이다.
- [47] 도 3은 본 발명의 실시예에 따른 불법 트래픽 검출 과정을 나타낸 흐름도이다.
- [48] 도 4 및 도 5는 본 발명의 실시예에 따른 패턴 검출 과정을 나타낸 순서도이다.

발명의 실시를 위한 최선의 형태

- [49] 아래에서는 첨부한 도면을 참고로 하여 본 발명의 실시예에 대하여 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자가 용이하게 실시할 수 있도록 상세히 설명한다. 그러나 본 발명은 여러가지 상이한 형태로 구현될 수 있으며 여기에서 설명하는 실시예에 한정되지 않는다. 그리고 도면에서 본 발명을 명확하게 설명하기 위해서 설명과 관계없는 부분은 생략하였으며, 명세서 전체를 통하여 유사한 부분에 대해서는 유사한 도면 부호를 붙였다.
- [50] 명세서 전체에서, 어떤 부분이 어떤 구성 요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성 요소를 제외하는 것이 아니라 다른 구성 요소를 더 포함할 수 있는 것을 의미한다.
- [51] 또한, 명세서에 기재된 "...부", "...모듈"의 용어는 적어도 하나의 기능이나 동작을 처리하는 단위를 의미하며, 이는 하드웨어나 소프트웨어 또는 하드웨어 및 소프트웨어의 결합으로 구현될 수 있다.

- [52] 이하, 도면을 참조로 하여 본 발명의 실시예에 따른 불법 트래픽 검출 장치 및 그 방법에 대하여 상세히 설명한다.
- [53] 도 1은 본 발명의 실시예에 따른 불법 트래픽 검출을 위한 개략적인 네트워크 구성도이다.
- [54] 도 1을 참조하면, 발신 단말(100)은 유선전화 또는 모바일을 포함할 수 있다. 발신 단말(100) 중 모바일은 기지국을 통해 발신 교환기(200)에 무선으로 접속하거나 또는 발신 단말(100) 중 유선 전화는 발신 교환기(200)에 유선으로 접속한다.
- [55] 발신 교환기(200)는 통신 사업자 망에 포함되고, 발신 단말(100)로부터 통화 연결 요청 신호를 수신하면, 착신자 위치 정보를 확인한 후, 확인한 위치 정보를 관리하는 착신 교환기(300)로 통화 연결 요청 신호를 전달한다.
- [56] 착신 교환기(300)는 통신 사업자 망에 포함되고, 발신 교환기(200)로부터 통화 연결 요청 신호가 전달되면, 해당하는 착신 단말(400)로 통화 연결 요청 신호를 전달한다.
- [57] 이때, 발신 교환기(200)와 착신 교환기(300)는 서로 다른 국가의 사업자망일 수 있다. 또한, 발신 교환기(200) 또는 착신 교환기(300)는 국제 전화 교환기일 수 있다.
- [58] 이때, 발신 단말(100) → 발신 교환기(200) → 착신 교환기(300) → 착신 단말(400)로 이루어진 경로는 통신 사업자 망에서 제공하는 정상 트래픽 경로에 해당된다. 정상 트래픽 경로는 정상적인 통신 사업자로서 정부의 사업 허가를 받고 사업 수행에 따른 세금 납세 뿐만 아니라 통화품질의 확보를 위한 비용 등이 수반되어 책정된 통신 요금을 납부하며 사용하는 경로이다.
- [59] 반면, 발신 단말(100)은 발신 교환기(200)를 거쳐 발신측 바이패스 게이트웨이(bypass gateway)(600)에 연결될 수 있다.
- [60] 발신측 바이패스 게이트웨이(600)는 인터넷망(700)을 통해 착신측 바이패스 게이트웨이(700)와 연결된다.
- [61] 발신 단말(100)이 통화 연결 요청 신호를 전송하면, 발신 교환기(200)가 통화 연결 요청 신호를 발신측 바이패스 게이트웨이(500)로 전달한다. 착신측 바이패스 게이트웨이(700)는 인터넷망(600)을 통해 통화 연결 요청 신호를 발신측 바이패스 게이트웨이(500)로부터 수신하여 해당하는 착신자가 위치한 착신 교환기(300)로 전달한다.
- [62] 여기서, 착신측 바이패스 게이트웨이(700)는 통화 연결 요청 신호, 즉, 해당 통화 트래픽을 국제 전화가 아닌 마치 착신자 측 자국내 로컬 통화로 변환하여 해당 트래픽은 착신자 국가내 이동통신 서비스 사업자의 착신 교환기(300)로 통화 트래픽을 전달한다. 그러면, 착신 교환기(300)는 착신측 바이패스 게이트웨이(700)로부터 수신된 통화 연결 요청 신호를 착신 단말(400)로 전달한다.
- [63] 착신측 바이패스 게이트웨이(700)는 주로 심 박스(SIM Box)라고 불리우는

다량의 심(SIM) 카드를 장착할 수 있도록 되어 마치 음성 전화 교환 장비처럼 동작 하므로써 착신자에게 연결해 주는 역할을 한다.

- [64] 이때, 발신 단말(100)이 무선인 경우, 기지국 → 발신 교환기(200) → 발신측 바이패스 게이트웨이(600) → 인터넷망(700) → 착신측 바이패스 게이트웨이(800)로 이루어진 경로는 불법 트래픽 경로에 해당된다. 여기서, 바이패스 트래픽이 구분되는 시점, 즉 정상 트래픽과 달리 바이패스 트래픽이 시작되는 지점은 발신 교환기(200)가 된다.
- [65] 또한, 발신 단말(100)이 유선 단말일 경우, 발신 단말(100) → 발신 교환기(200) → 발신측 바이패스 게이트웨이(600) → 인터넷망(700) → 착신측 바이패스 게이트웨이(800)로 이루어진 경로는 불법 트래픽 경로에 해당된다. 여기서, 바이패스 트래픽을 구분하는 시점은 발신 교환기(200)가 된다.
- [66] 이러한 불법 트래픽 경로는 인터코넥트 바이패스(Interconnect Bypass)와 같이 이용 요금의 단가 차액을 주요 수입원으로 하는 통신 사업자망을 우회하는 경로를 말한다.
- [67] 불법 트래픽 경로는 발신자 국가와 착신자 국가 사이를 일반 인터넷망(600)으로 연결하고 착신 국가에 별도의 무선 장비와의 연결을 위한 바이패스 게이트웨이(500, 700)를 설치하여 국제 구간은 상대적으로 값싼 일반 인터넷 회선을 사용하여 품질 저하 등의 문제를 내포하고 있을 뿐만 아니라 착신자 측에 설치된 무선 연결 장치인 바이패스 게이트웨이(700)를 통해 국제호가 아닌 국내호로 전환 하므로써 비정상 적인 통화 경로를 제공하는 형태이다. 즉, 통화로 우회 불법호 특히 심박스(SIM Box)는 정상적인 통신 서비스 사업자의 통화 경로가 아니라 별도의 통화 회선을 구성하여 그 요금의 차액을 수익으로 전환하는 불법 호를 유발한다.
- [68] 불법 트래픽 탐지 장치(800)는 전화 서비스 교환 장비(200, 300) 구간에서 통화 트래픽을 수집하여 불법 트래픽에서 발생하는 패턴들과 비교하여 불법 트래픽 여부를 판단하고 이를 통신 사업자에게 알려줄 뿐만 아니라 불법 트래픽 검출 결과를 제공한다.
- [69] 불법 트래픽 탐지 장치(800)는 착신 교환기(300)와 연결되어 착신 교환기(300)로부터 통화 트래픽을 수집한 후, 통화 트래픽이 불법 트래픽, 즉 불법 트래픽 경로를 거쳐 수신된 것인지 판단한다. 그리고 불법 트래픽 검출 정보를 착신 교환기(300)로 전달하여 호 차단 등의 정해진 처리를 수행하도록 한다.
- [70] 이러한 불법 트래픽 탐지 장치(800)의 구성은 도 2와 같이 구현될 수 있다.
- [71] 도 2는 본 발명의 실시예에 따른 불법 트래픽 검출 장치의 세부 구성을 나타낸 블록도이다.
- [72] 도 2를 참조하면, 불법 트래픽 탐지 장치(800)는 트래픽 수집부(801), 데이터베이스(803), 패턴 검출부(805) 및 불법 트래픽 검출부(807)를 포함한다.
- [73] 트래픽 수집부(801)는 교환기(300)로부터 통화 트래픽을 수집하고, 통화

트래픽으로부터 콜 상세 기록(CDR, Call Detail Record)을 파싱한다.

- [74] 여기서, 콜 상세 기록(CDR)은 통화 발신 가입자의 전화번호, 호출을 수신하는 전화번호, 콜의 시작시간, 통화시간, 통화요금 결제 전화번호, 기록을 작성하는 장비의 식별, 레코드 고유번호 식별번호, 유형(음성, SMS 등), 오류 상태, 콜의 종료 시간 등을 포함한다.
- [75] 트래픽 수집부(801)는 착신 교환기(300)로 유입되는 모든 트래픽을 수집한다. 착신 교환기(300)로 유입되는 트래픽중 시그널 트래픽 뿐만 아니라 미디어 트래픽 정보도 수집하여 유입된 트래픽의 CDR(Call Detail Record) 정보 및 미디어의 품질정보 분석을 위한 데이터 처리를 진행한다.
- [76] 트래픽 수집부(801)는 통화 트래픽을 수집한 경우, 데이터베이스(903)를 조회하여 통화 트래픽이 데이터베이스(803)에 존재하는지 판단한다. 즉, 데이터베이스(803)에 저장된 불법 트래픽에 해당하는지 판단한다. 데이터베이스(803)에 존재하면 통화 트래픽이 불법 트래픽임을 알리는 불법 트래픽 검출 정보를 교환기(300)로 전달한다.
- [77] 트래픽 수집부(801)는 수집된 통화 트래픽이 데이터베이스(803)에 존재하지 않는 경우, 콜 상세 기록(CDR)을 생성하여 패턴 검출부(905)로 전달한다.
- [78] 데이터베이스(803)는 불법 트래픽 정보 및 불법 트래픽에서 나타내는 패턴 정보를 저장한다. 이러한 데이터베이스(903)는 발신/착신번호, 우회트래픽 검출 이력, 표 1에 명시된 내역, 즉, [이동성 여부, 음성통화 only 여부, 발/착신 성공률 비율, 선불요금제 여부] 등으로 우회 트래픽 검출 이력은 블랙 리스트와 같이 과거 발생이력을 관리 및 재발생 여부 확인을 위한 용도이며, 나머지는 우회 트래픽 판단을 위한 데이터를 저장한다.
- [79] 패턴 검출부(805)는 트래픽 수집부(801)로부터 전달된 수집 정보를 바탕으로 통화로 우회 이상 트래픽이 발생했을 경우 나타나는 패턴의 유형별 발생 여부를 검출한다. 여기서, 패턴의 유형은 표 1과 같이 구현될 수 있다.

[80] [Table 1]

패턴 유형	패턴 탐지 방법
이동성 여부	기지국/대상 호처리 변경 여부
음성통화만 이용	음성통화외 사용여부(SMS, 데이터 등)
발신/착신 성공호 비율	$\frac{\text{발신성공호}}{\text{발신성공호}+\text{착신성공호}} > \text{임계치}$
착신 번호의 다양성	착신번호수 > 임계치
음성 서비스 비율	$\frac{\text{음성통화시도횟수}}{\text{각각의서비스별이용횟수}} > \text{임계치}$
기지국내 가입자수	기지국내 음성채널 할당 가입자수 > 임계치
야간 통화 발생수	야간 통화 발생수 > 임계치
착신 성공호 평균 통화 유지 시간	착신 성공호 평균 통화유지시간 > 임계치
가입자 망내 이용율	$\frac{\text{가입자망이용횟수}}{\text{타사망이용횟수}+\text{가입자망이용횟수}} > \text{임계치}$
많은 통화량(가입자 기준)	가입자 통화량(시도호) > 임계치
해당 기지국 통화량 폭주(기지국 기준)	기지국/대상 호처리 부하율/사용채널수(음성통화)>임계치
통화품질 저하 여부	지연(Delay), 지터(jitter), 패킷 손실(packet loss) > 임계치
발신번호 선불 요금제 사용 여부	발신번호의 선불 요금제 가입 여부

[81] 표 1에서 임계치는 각 패턴 별로 패턴의 특성에 맞게 서로 다른 값이다.

[82] 표 1을 참조하면, 패턴 검출부(805)는 트래픽 수집부(801)로부터 전달되는 콜 상세 기록(CDR)을 토대로 통화 트래픽으로부터 기 정의된 불법 트래픽에서 나타나는 패턴의 유형별 발생 여부를 검출한다.

[83] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽의 발신 단말이 무선 단말이고, 지역적 이동 없이 통화를 발생시키는 패턴에 해당하는지 검출한다.

[84] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 음성 통화만 사용하는 패턴에 해당하는지 검출한다.

[85] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 전체 호

성공률 대비 발신 성공 호 비율이 임계치를 초과하는 패턴에 해당하는지 검출한다.

- [86] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 착신번호 수가 임계치를 초과하는 패턴에 해당하는지 검출한다.
- [87] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 전체 서비스 별 이용 횟수 대비 음성 통화 시도 횟수가 임계치를 초과하는 패턴에 해당하는지 검출한다.
- [88] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 기지국 내 음성 채널 할당 가입자수가 임계치를 초과하는 패턴에 해당하는지 검출한다.
- [89] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 야간 통화 발생 횟수가 임계치를 초과하는 패턴에 해당하는지 검출한다.
- [90] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 착신 성공호 평균 통화 유지 시간이 임계치 미만에 해당하는지 검출한다.
- [91] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 가입자망 내 이용율이 임계치를 초과하는 패턴에 해당하는지 검출한다.
- [92] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽이 가입자의 통화량이 임계치를 초과하는 패턴에 해당하는지 검출한다.
- [93] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽의 품질이 임계치 미만인 패턴에 해당하는지 검출한다.
- [94] 또한, 패턴 검출부(805)는 콜 상세 기록(CDR)을 토대로 통화 트래픽의 발신번호가 선불요금제 가입된 패턴에 해당하는지 검출한다.
- [95] 불법 트래픽 검출부(807)는 패턴 검출부(805)로부터 검출된 패턴들의 정보를 바탕으로 오탐율을 최소화하여 통화로 우회 트래픽 여부를 판단한다. 이때, 불법 트래픽을 검출하기 위한 일실시예로 검출된 패턴들의 일정 조합으로 불법 트래픽을 검출할 수 있다. 이때, 패턴은 인터코넥트 바이패스(Interconnect Bypass) 트래픽을 판단하기 위한 고유하고도 특유한 파라미터 들로 구성된다.
- [96] 불법 트래픽 검출부(807)는 패턴 유형별로 패턴의 검출 결과를 기초로 통화 트래픽이 불법 트래픽인지 판단하고, 판단 결과를 교환기(300)로 전송한다.
- [97] 불법 트래픽 검출부(807)는 교환기(300)로부터 수집한 통화 트래픽이 발신측 바이패스 게이트웨이(500) → 인터넷망(600) → 착신측 바이패스 게이트웨이(700)로 이루어진 인터코넥트 바이패스(Interconnect Bypass)로 이루어진 불법 트래픽 경로로부터 수신된 것인지 판단한다.
- [98] 불법 트래픽 검출부(807)는 패턴 검출부(805)가 검출한 패턴 별로 패턴의 조합, 패턴 별로 기 정의된 가중치 및 사용 빈도를 고려하여 최종적으로 통화 트래픽이 불법 트래픽인지 판단할 수 있다.
- [99] 불법 트래픽 검출부(807)는 표 2와 같은 패턴 별 위험도 점수(가중치)를 조합하여 최종 위험도 점수를 산출하고, 최종 위험도 점수가 기 정의된 임계치를 초과하면 불법 트래픽으로 검출할 수 있다.

[100] 예를 들면, 1, 2단계 통합하여 최소 3개 이상 만족하며, 위험도 점수가 17점 이상시 불법 트래픽으로 검출할 수 있다.

[101] [Table 2]

패턴 유형	위험도	위험도 점수
이동성 여부	1단계	4
음성통화만 이용	2단계	3
발신/착신 성공호 비율	2단계	3
가입자망내 이용률	2단계	3
착신 번호의 다양성	3단계	2
음성 서비스 비율	3단계	2
기지국내 가입자수	3단계	2
야간 통화 발생수	3단계	2
착신 성공호 평균 통화 유지 시간	3단계	2
통화품질 저하여부	3단계	2
발신번호 선불요금제 사용 유무	3단계	2
많은 통화량(가입자 기준)	4단계	1
해당 기지국 통화량 폭주(기지국 기준)	4단계	1

[102] 그러면, 불법 트래픽 검출 과정 및 불법 트래픽 검출을 위한 패턴 검출 과정에 대해 이하 상세히 설명한다. 이때, 도 1 및 도 2의 구성과 연계하여 동일한 도면 부호를 사용한다.

[103] 도 3은 본 발명의 실시예에 따른 불법 트래픽 검출 과정을 나타낸 흐름도이다.

[104] 도 3을 참조하면, 트래픽 수집부(801)는 교환기(300)로부터 통화 트래픽을 수집한다(S101).

[105] 트래픽 수집부(801)는 불법 트래픽 패턴 발생 여부를 판단하기 위해 S101 단계에서 수집한 통화 트래픽에 대해 CDR 정보 및 미디어의 품질 정보 분석을 위한 데이터 처리를 수행한다(S103).

[106] 트래픽 수집부(801)는 S103 단계에서 처리된 CDR 정보가 데이터베이스(803)에 존재하는지 데이터베이스(803)를 조회(S105)하여 결과를 수신한다(S107).

[107] 트래픽 수집부(801)는 S101 단계에

[108] 트래픽 수집부(801)는 S101 단계에서 수집된 통화 트래픽이 데이터베이스(803)에 저장된 불법 트래픽에 해당하는지 판단한다(S109).

- [109] 이때, 불법 트래픽이 아니라면, S103 단계에서 처리된 데이터를 패턴 검출부(805)로 전달한다(S111).
- [110] 패턴 검출부(805)는 S111 단계에서 수신된 데이터(CDR 포함)를 토대로 통화 트래픽에 대한 패턴을 분석한다(S113). 그리고 분석 결과를 불법 트래픽 검출부(807)로 전달한다(S115).
- [111] 불법 트래픽 검출부(807)는 S115 단계에서 수신된 패턴 분석 정보를 토대로 S101 단계에서 수집한 통화 트래픽이 불법 트래픽인지 판단한다(S117). 그리고 판단 정보를 트래픽 수집부(801)로 전달한다(S119).
- [112] 트래픽 수집부(801)는 S119 단계에서 수신된 판단 정보를 토대로 통화 트래픽이 불법 트래픽인지 확인한다(S121).
- [113] 이때, S121 단계에서 불법 트래픽으로 확인되거나 또는 S109 단계에서 저장된 불법 트래픽으로 판단되면, 불법 트래픽 검출 정보를 교환기(300)로 전달(S123)하여 불법 트래픽 차단 및 관리에 활용되도록 한다. 즉, 데이터베이스(803)에서 관리하는 데이터와 유입된 트래픽이 수집되거나 불법 트래픽 패턴과 일치하는 트래픽이 수집되면, 불법 트래픽 검출 정보를 교환기(300)로 전달한다.
- [114] 또한, S113 단계 및 S117 단계에서 판단된 패턴 분석 정보 및 불법 트래픽 판단 정보는 데이터베이스(803)에 저장된다.
- [115] 한편, S113 단계를 상세히 설명하면, 도 4 및 도 5와 같다.
- [116] 도 4 및 도 5는 본 발명의 실시예에 따른 패턴 검출 과정을 나타낸 순서도이다.
- [117] 먼저, 도 4를 참조하면, 트래픽 수집부(901)가 수집한 트래픽으로부터 CDR을 파싱한다(S201).
- [118] 패턴 검출부(805)는 S201 단계에서 파싱된 CDR 정보를 토대로 발신 단말의 이동성 여부를 판단한다(S203). 즉, 착신측 바이패스 게이트웨이(Bypass Gateway)(600)에 사용되는 단말(SIM)이 무선 단말 임에도 불구하고 지역적 이동이 없이 지속적으로 통화를 발생시키는지 패턴인지 확인한다.
- [119] 이때, 이동성이 확인되지 않으면, 패턴 검출부(805)는 음성 통화만 이용하는 패턴인지 판단한다(S205). 즉, 음성 통화를 중계하는 바이패스 게이트웨이(500, 700)의 역할에 따른 패턴으로 음성 통화 이외에 문자메시지나 인터넷 사용 여부 등을 확인한다.
- [120] 이때, 음성 통화만 이용하는 패턴이 아닌 경우, 패턴 검출부(805)는 발신/착신 성공호의 비율을 확인한다(S207). 즉, 통화로 우회가 발생하는 방향에 따라 트래픽이 단일 방향으로 발생하는지 여부를 검출한다. 불법 트래픽의 경우, 주로 착신자 방향을 기준으로 발신호만 발생하는 패턴을 보이므로 이런 검출 패턴을 확인한다.
- [121] 이때, 단일 방향으로 발생하지 않은 경우, 패턴 검출부(805)는 착신번호의 다양성 여부를 확인한다(S209). 즉, 일반적인 사용자의 사용 패턴을 벗어나 다수의 번호로 발신하는지 여부를 검출 패턴으로 확인한다. 예를 들면,

착신번호의 수가 임계치를 초과하는 패턴인지 판단한다.

- [122] 이때, 착신번호가 다양하지 않은 경우, 패턴 검출부(805)는 음성 서비스 비율, 즉, 음성통화 시도 횟수가 임계치를 초과하는지 확인한다(S211). 즉, 음성통화 대비 문자 메시지나 기타 인터넷과 같은 데이터 서비스 이용율을 확인하여 전체 서비스 이용율 대비 음성 서비스 이용율이 임계치를 초과하는 패턴인지 판단한다.
- [123] 이때, 음성통화 시도 횟수가 임계치를 초과하지 않으면, 패턴 검출부(805)는 기지국내 가입자 수가 임계치를 초과하는지 판단한다(S213). 기지국내 가입자수는 일반적으로 착신측에 설치되는 착신측 바이패스 게이트웨이는 수십에서 수백 개에 이르는 다수개의 SIM 카드가 설치되어 운영 되므로 이를 검출 패턴으로 확인한다.
- [124] 다음, 도 5를 참조하면, S213 단계에서 가입자 수가 임계치를 초과하지 않으면, 패턴 검출부(805)는 야간통화 발생수가 임계치 이상인지 판단한다(S215). 통화로 우회 이상 트래픽은 착신자가 불특정 다수 인점을 감안 하여 일반 사용자에게 비해 야간 통화가 많이 발생됨을 검출 패턴으로 확인한다.
- [125] 이때, 야간 통화 발생수가 임계치 미만인 경우, 패턴 검출부(805)는 착신 성공호 평균 통화 유지시간이 임계치 미만인지 판단한다(S217). 통화로 우회 이상 트래픽은 대부분 단 방향으로 발생되며 이런 검출에 의한 탐지를 회피하고자 착신호를 발생 시킨다. 그래서 발신호 대비 착신호의 비율이 현저히 낮아 이를 평균 통화 시간을 확인 하므로써 그 비율을 비교해 검출 패턴을 확인한다.
- [126] 이때, 착신 성공호 평균 통화 유지시간이 임계치 이상인 경우, 패턴 검출부(805)는 가입자 망내 이용률이 임계치를 초과하는지 판단한다(S219). 불법 트래픽의 경우, 바이패스 게이트웨이(500, 700)가 로컬 전화를 발생 시킨다 하더라도 타사망으로의 통화료 대비 동일 통신 서비스 사업자내 통화료가 저렴하므로 동일 통신 서비스 사업자 망내 통화 비율이 현저히 높아지므로, 이러한 검출 패턴을 확인한다.
- [127] 이때, 가입자 망내 이용률이 임계치를 초과하지 않으면, 패턴 검출부(805)는 가입자의 통화량이 임계치를 초과하는지 판단한다(S221). 즉, 일반 사용자에게 비해 헤비 유저와 같이 통화 사용량이 현저히 많음을 감안해 이러한 검출 패턴을 확인한다.
- [128] 이때, 가입자의 통화량이 임계치를 초과하지 않으면, 패턴 검출부(805)는 기지국 통화량이 폭주 상태로 판단되는지 검출한다(S223). 기지국 통화량 수준은 주로 수십에서 수백 개의 SIM 카드를 동시에 사용하므로 해당 기지국 커버리지내 통화량이 주변 기지국의 통화량 대비 월등히 높다는 점을 감안해 검출 패턴으로 확인한다.
- [129] 이때, 기지국 통화량이 임계치를 초과하지 않으면, 패턴 검출부(805)는 통화 품질 저하 여부를 판단한다(S225). 통화품질 저하여부는 주로 발신지 국가와 착신지 국가 사이는 일반적으로 비용이 저렴한 인터넷 공중망을 사용하게 된다.

그러다 보니 트래픽량이 증가한 시간대에는 지연, 지터 및 패킷 손실율이 현저히 증가하게 되어 품질 저하가 발생된다. 이러한 품질 저하 현상을 검출 패턴으로 확인한다.

- [130] 통화 품질 저하 여부가 확인되지 않으면, 패턴 검출부(805)는 통화 발신번호가 선불 요금 가입인지 판단한다(S227). 우회 트래픽을 유발하는 심(SIM) 카드는 선불 요금제를 사용하므로써 가입 및 사용자의 정보 유출을 최소화 하려는 경향이 있어 이러한 검출 패턴을 확인한다.
- [131] 패턴 검출부(805)는 S203 단계 ~ S227 단계에서 판단된 패턴 검출 결과를 데이터베이스(803)에 각각 업데이트한다(S229). 그리고 패턴 검출 결과를 불법 트래픽 검출부(807)로 전달한다.
- [132] 그러면, 불법 트래픽 검출부(807)는 패턴 검출 결과를 기초하여 최종 불법 트래픽 검출 과정을 수행한다.
- [133] 이상에서 설명한 본 발명의 실시예는 장치 및 방법을 통해서만 구현이 되는 것은 아니며, 본 발명의 실시예의 구성에 대응하는 기능을 실현하는 프로그램 또는 그 프로그램이 기록된 기록 매체를 통해 구현될 수도 있다.
- [134] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

청구범위

[청구항 1]

교환기로부터 통화 트래픽을 수집하고, 상기 통화 트래픽으로부터 콜 상세 기록(CDR, Call Detail Record)을 파싱하는 트래픽 수집부, 상기 콜 상세 기록을 토대로 상기 통화 트래픽으로부터 기 정의된 불법 트래픽에서 나타나는 패턴의 유형별 발생 여부를 검출하는 패턴 검출부, 그리고

상기 유형별로 패턴의 검출 결과를 기초로 상기 통화 트래픽이 불법 트래픽인지 판단하고, 판단 결과를 상기 교환기로 전송하는 불법 트래픽 검출부를 포함하고,

상기 불법 트래픽은, 통신 사업자가 제공하는 정상 트래픽 경로를 거치지 않고 불법 트래픽 경로를 거쳐 상기 교환기로 유입된 것인 불법 트래픽 검출 장치.

[청구항 2]

제1항에 있어서,

상기 불법 트래픽 검출부는,

상기 교환기로부터 수집한 통화 트래픽이 발신측 바이패스 게이트웨이, 인터넷망, 착신측 바이패스 게이트웨이로 이루어진 상기 불법 트래픽 경로로부터 수신된 것인지 판단하는 불법 트래픽 검출 장치.

[청구항 3]

제1항에 있어서,

상기 불법 트래픽을 저장하는 데이터베이스를 더 포함하고,

상기 트래픽 수집부는,

상기 통화 트래픽을 수집한 경우, 상기 데이터베이스를 조회하여 상기 통화 트래픽이 상기 데이터베이스에 존재하는지 판단하고, 상기 데이터베이스에 존재하면 상기 통화 트래픽이 불법 트래픽임을 알리는 불법 트래픽 검출 정보를 상기 교환기로 전달하고,

상기 트래픽 수집부는,

상기 통화 트래픽이 상기 데이터베이스에 존재하지 않는 경우,

상기 콜 상세 기록을 생성하여 상기 패턴 검출부로 전달하는 불법 트래픽 검출 장치.

[청구항 4]

제3항에 있어서,

상기 불법 트래픽 검출부는,

상기 패턴 검출부가 검출한 패턴 별로 상기 패턴의 조합, 상기 패턴 별로 기 정의된 가중치 및 사용 빈도를 고려하여 최종적으로 상기 통화 트래픽이 불법 트래픽인지 판단하는 불법 트래픽 검출 장치.

[청구항 5]

제4항에 있어서,

상기 패턴 검출부는,

상기 콜 상세 기록을 토대로 상기 통화 트래픽의 발신 단말이 무선 단말이고, 지역적 이동 없이 통화를 발생시키는 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.

[청구항 6]

제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 음성 통화만 사용하는 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.

[청구항 7]

제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 전체 호 성공률 대비 발신 성공 호 비율이 임계치를 초과하는 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.

[청구항 8]

제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 착신번호 수가 임계치를 초과하는 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.

[청구항 9]

제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 전체 서비스 별 이용 횟수 대비 음성 통화 시도 횟수가 임계치를 초과하는 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.

[청구항 10]

제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 기지국 내 음성 채널 할당 가입자수가 임계치를 초과하는 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.

[청구항 11]

제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 야간 통화 발생 횟수가 임계치를 초과하는 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.

[청구항 12]

제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 착신 성공호 평균 통화 유지 시간이 임계치 미만인 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.

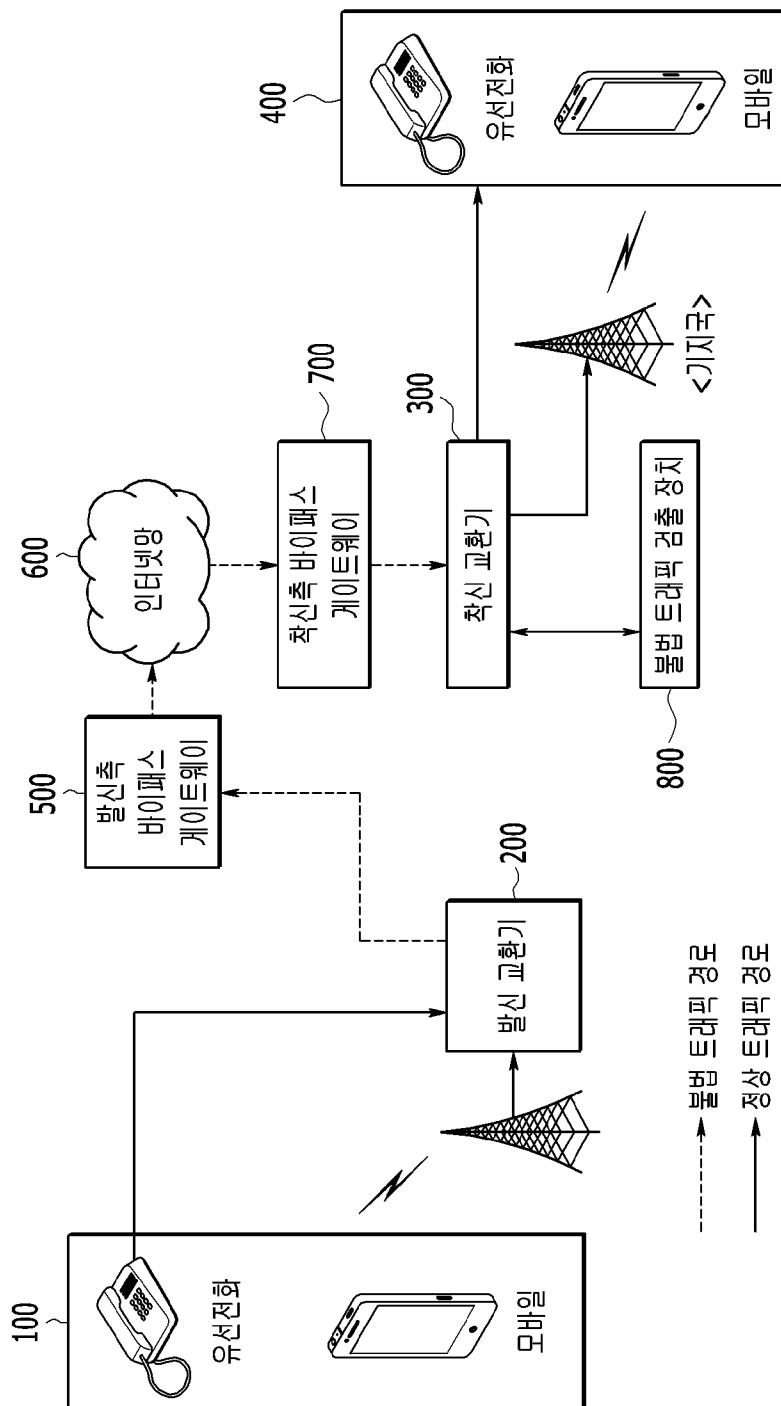
[청구항 13]

제4항에 있어서,

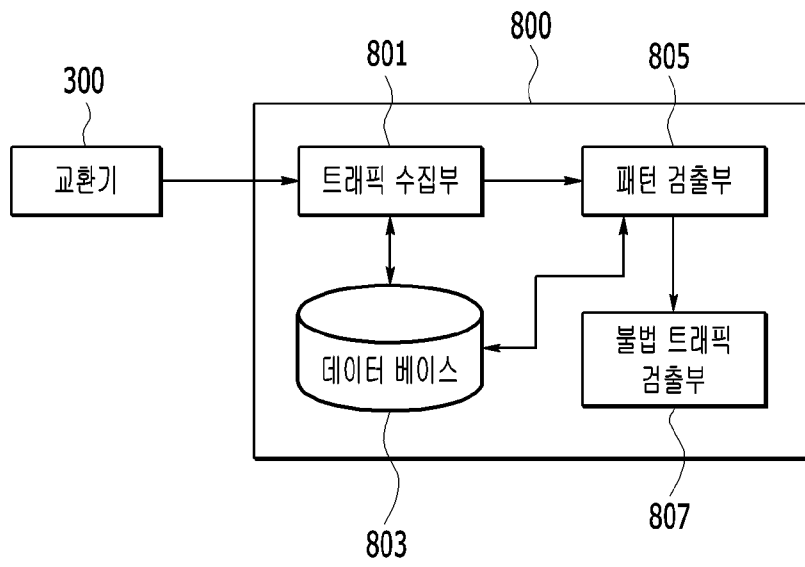
- 상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 가입자 망 내
이용율이 임계치를 초과하는 패턴에 해당하는지 검출하는 불법
트래픽 검출 장치.
- [청구항 14] 제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽이 가입자의
통화량이 임계치를 초과하는 패턴에 해당하는지 검출하는 불법
트래픽 검출 장치.
- [청구항 15] 제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽의 품질이 임계치
미만인 패턴에 해당하는지 검출하는 불법 트래픽 검출 장치.
- [청구항 16] 제4항에 있어서,
상기 패턴 검출부는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽의 발신번호가
선불요금제 가입된 패턴에 해당하는지 검출하는 불법 트래픽 검출
장치.
- [청구항 17] 교환기로부터 통화 트래픽을 수집하는 단계,
수집한 통화 트래픽이 기 정의된 불법 트래픽인지 판단하는 단계,
상기 수집한 통화 트래픽이 상기 불법 트래픽이 아닌 경우, 상기
수집한 통화 트래픽으로부터 콜 상세 기록(CDR, Call Detail
Record)을 파싱하는 단계,
상기 콜 상세 기록을 토대로 상기 통화 트래픽으로부터 기 정의된
불법 트래픽에서 나타나는 패턴의 유형별 발생 여부를 검출하는
단계,
상기 패턴 별로 상기 패턴의 조합, 상기 패턴 별로 기 정의된
가중치 및 사용 빈도를 고려하여 상기 수집한 통화 트래픽이 불법
트래픽인지 판단하는 단계, 그리고
상기 수집한 통화 트래픽이 불법 트래픽인지 아닌지를 나타내는
정보를 상기 교환기로 전송하는 단계를 포함하고,
상기 불법 트래픽은, 통신 사업자가 제공하는 정상 트래픽 경로를
거치지 않고 발신측 바이패스 게이트웨이, 인터넷망, 착신측
바이패스 게이트웨이로 이루어진 불법 트래픽 경로를 거쳐 상기
교환기로 유입된 것인 불법 트래픽 검출 방법.
- [청구항 18] 제17항에 있어서,
상기 패턴의 유형별 발생 여부를 검출하는 단계는,
상기 콜 상세 기록을 토대로 상기 통화 트래픽의 발신 단말이 무선

단말이고, 지역적 이동 없이 통화를 발생시키는 패턴에
 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 음성 통화만
 사용하는 패턴에 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 전체 호 성공률
 대비 발신 성공 호 비율이 임계치를 초과하는 패턴에 해당하는지
 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 착신번호 수가
 임계치를 초과하는 패턴에 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 전체 서비스 별
 이용 횟수 대비 음성 통화 시도 횟수가 임계치를 초과하는 패턴에
 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 기지국 내 음성
 채널 할당 가입자수가 임계치를 초과하는 패턴에 해당하는지
 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 야간 통화 발생
 횟수가 임계치를 초과하는 패턴에 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 착신 성공호 평균
 통화 유지 시간이 임계치 미만인 패턴에 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 가입자 망 내
 이용율이 임계치를 초과하는 패턴에 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽이 가입자의
 통화량이 임계치를 초과하는 패턴에 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽의 품질이 임계치
 미만인 패턴에 해당하는지 판단하는 단계,
 상기 콜 상세 기록을 토대로 상기 통화 트래픽의 발신번호가
 선불요금제 가입된 패턴에 해당하는지 판단하는 단계, 그리고
 상기 패턴 중 적어도 하나 이상에 해당하는 경우, 상기 패턴을
 판단한 결과 및 해당 통화 트래픽을 데이터베이스에 업데이트하는
 단계
 를 포함하는 불법 트래픽 검출 방법.

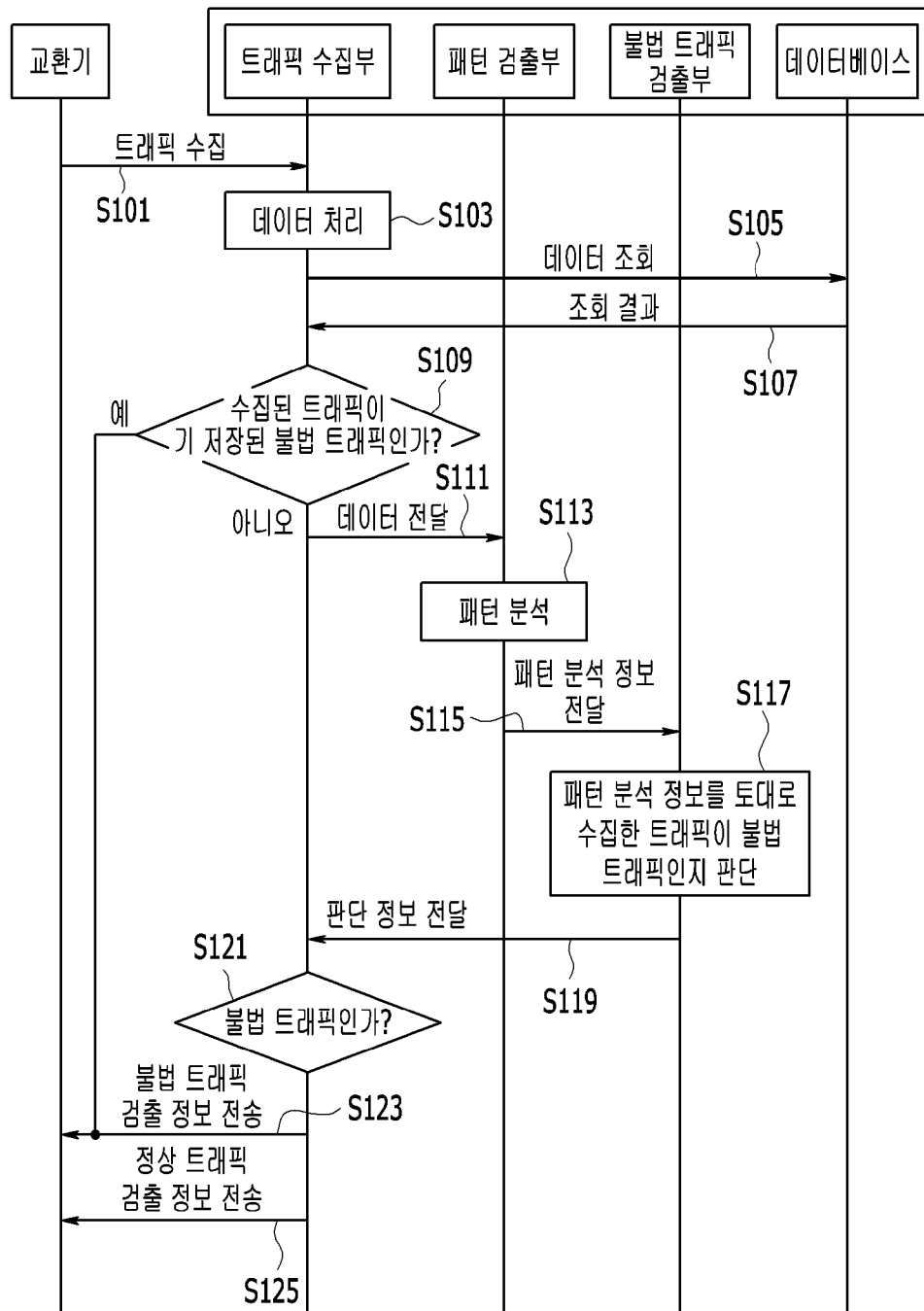
[Fig. 1]



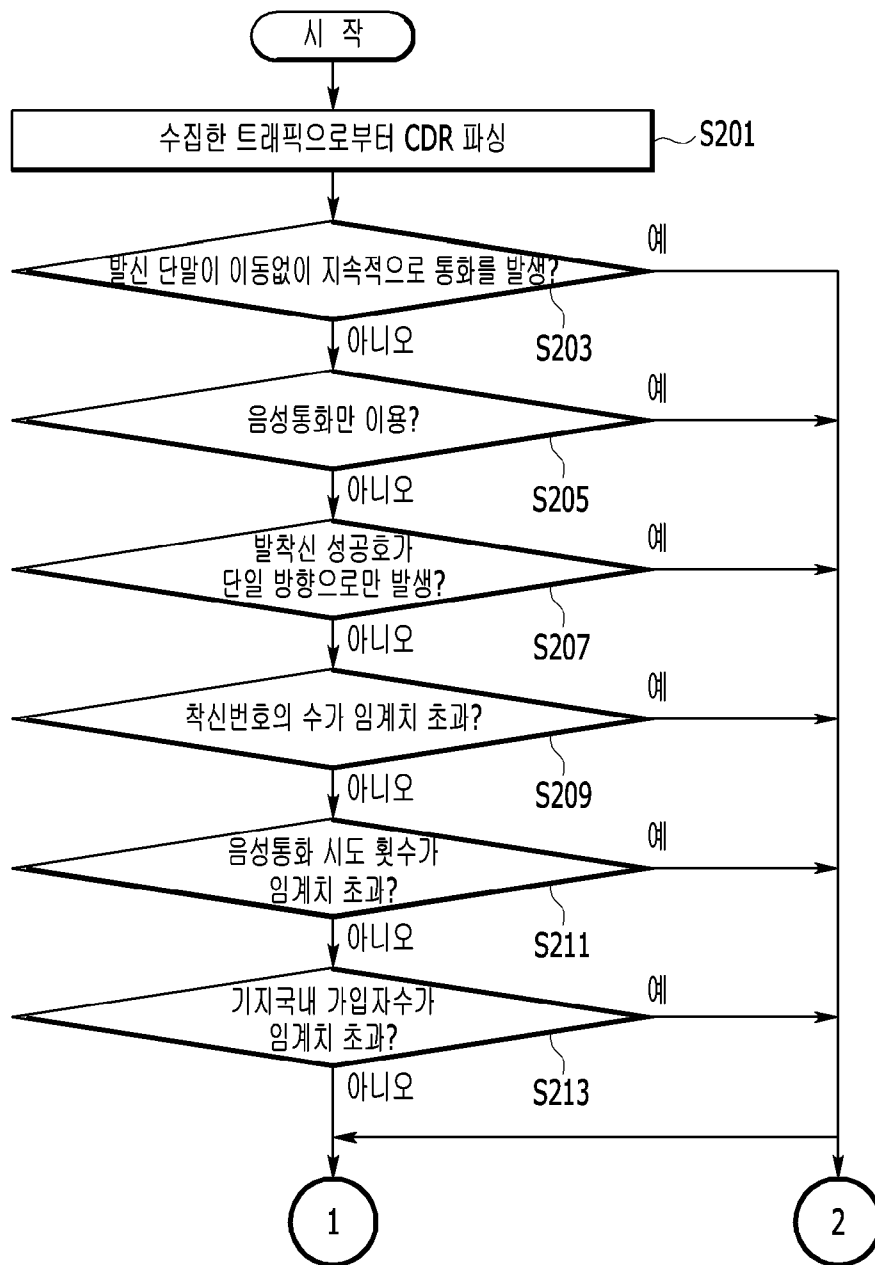
[Fig. 2]



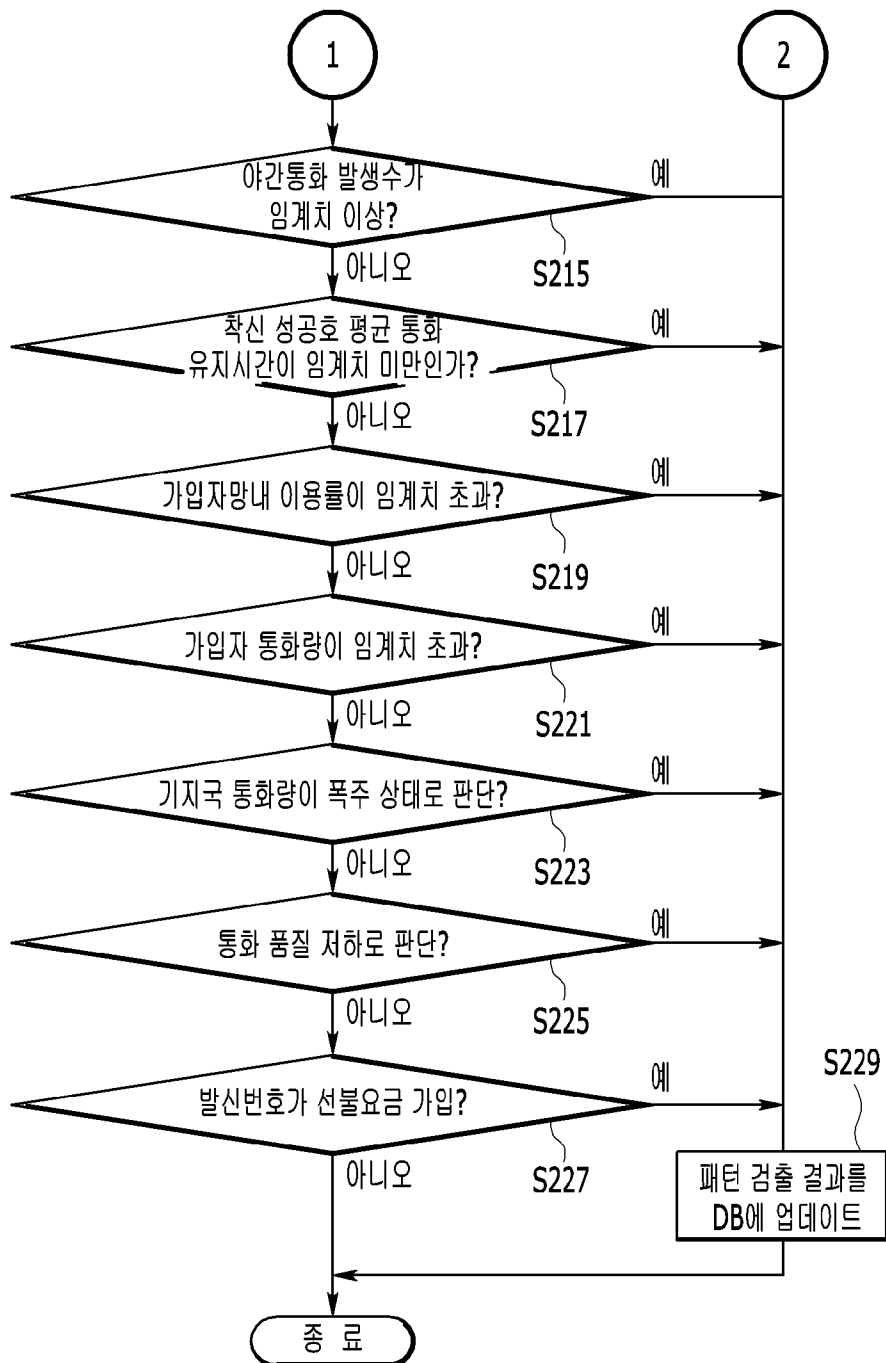
[Fig. 3]



[Fig. 4]



[Fig. 5]



INTERNATIONAL SEARCH REPORT

International application No.

PCT/KR2016/004805**A. CLASSIFICATION OF SUBJECT MATTER*****H04M 3/22(2006.01)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)

H04M 3/22; G06F 15/00; G06F 17/00; H04L 12/26; H04W 12/12; H04W 88/18; H04L 12/22; H04L 12/56

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: call, illegal traffic, call detail record (CDR), pattern, detection, bypass

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 10-1492733 B1 (FOUNDATION FOR RESEARCH AND BUSINESS, SEOUL NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY) 12 February 2015 See abstract, paragraphs [0033]-[0038] and figures 1-2.	1-2
A		3-18
Y	KR 10-2011-0079044 A (KT CORP.) 07 July 2011 See paragraphs [0017]-[0050] and figures 1-3.	1-2
A	KR 10-1281160 B1 (LG CNS CO., LTD.) 02 July 2013 See claim 1 and figures 1-3.	1-18
A	KR 10-2012-0071123 A (ELECTRONICS AND TELECOMMUNICATIONS RESEARCH INSTITUTE) 02 July 2012 See claims 1, 6 and figures 1-3.	1-18
A	JP 4413833 B2 (NIPPON TELEGR. & TELEPH. CORP.) 10 February 2010 See paragraphs [0024]-[0043] and figures 1-3.	1-18



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

"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

26 JULY 2016 (26.07.2016)

Date of mailing of the international search report

26 JULY 2016 (26.07.2016)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 189 Seonsa-ro, Daejeon 302-701,
Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Telephone No.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/KR2016/004805

Patent document cited in search report	Publication date	Patent family member	Publication date
KR 10-1492733 B1	12/02/2015	NONE	
KR 10-2011-0079044 A	07/07/2011	NONE	
KR 10-1281160 B1	02/07/2013	KR 10-2007-0079781 A	08/08/2007
KR 10-2012-0071123 A	02/07/2012	US 2012-0163212 A1	28/06/2012
JP 4413833 B2	10/02/2010	JP 2007-053430 A	01/03/2007

A. 발명이 속하는 기술분류(국제특허분류(IPC)) H04M 3/22(2006.01)i																							
B. 조사된 분야 조사된 최소문헌(국제특허분류를 기재) H04M 3/22; G06F 15/00; G06F 17/00; H04L 12/26; H04W 12/12; H04W 88/18; H04L 12/22; H04L 12/56 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: 통화, 불법 트래픽, 콜 상세 기록(CDR), 패턴, 검출, 우회																							
C. 관련 문헌 <table border="1"> <thead> <tr> <th>카테고리*</th> <th>인용문헌명 및 관련 구절(해당하는 경우)의 기재</th> <th>관련 청구항</th> </tr> </thead> <tbody> <tr> <td>Y</td> <td>KR 10-1492733 B1 (서울과학기술대학교 산학협력단) 2015.02.12 요약, 단락 [0033]-[0038] 및 도면 1-2 참조.</td> <td>1-2</td> </tr> <tr> <td>A</td> <td></td> <td>3-18</td> </tr> <tr> <td>Y</td> <td>KR 10-2011-0079044 A (주식회사 케이티) 2011.07.07 단락 [0017]-[0050] 및 도면 1-3 참조.</td> <td>1-2</td> </tr> <tr> <td>A</td> <td>KR 10-1281160 B1 (주식회사 엘지씨엔에스) 2013.07.02 청구항 1 및 도면 1-3 참조.</td> <td>1-18</td> </tr> <tr> <td>A</td> <td>KR 10-2012-0071123 A (한국전자통신연구원) 2012.07.02 청구항 1, 6 및 도면 1-3 참조.</td> <td>1-18</td> </tr> <tr> <td>A</td> <td>JP 4413833 B2 (NIPPON TELEGR & TELEPH CORP.) 2010.02.10 단락 [0024]-[0043] 및 도면 1-3 참조.</td> <td>1-18</td> </tr> </tbody> </table>			카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항	Y	KR 10-1492733 B1 (서울과학기술대학교 산학협력단) 2015.02.12 요약, 단락 [0033]-[0038] 및 도면 1-2 참조.	1-2	A		3-18	Y	KR 10-2011-0079044 A (주식회사 케이티) 2011.07.07 단락 [0017]-[0050] 및 도면 1-3 참조.	1-2	A	KR 10-1281160 B1 (주식회사 엘지씨엔에스) 2013.07.02 청구항 1 및 도면 1-3 참조.	1-18	A	KR 10-2012-0071123 A (한국전자통신연구원) 2012.07.02 청구항 1, 6 및 도면 1-3 참조.	1-18	A	JP 4413833 B2 (NIPPON TELEGR & TELEPH CORP.) 2010.02.10 단락 [0024]-[0043] 및 도면 1-3 참조.	1-18
카테고리*	인용문헌명 및 관련 구절(해당하는 경우)의 기재	관련 청구항																					
Y	KR 10-1492733 B1 (서울과학기술대학교 산학협력단) 2015.02.12 요약, 단락 [0033]-[0038] 및 도면 1-2 참조.	1-2																					
A		3-18																					
Y	KR 10-2011-0079044 A (주식회사 케이티) 2011.07.07 단락 [0017]-[0050] 및 도면 1-3 참조.	1-2																					
A	KR 10-1281160 B1 (주식회사 엘지씨엔에스) 2013.07.02 청구항 1 및 도면 1-3 참조.	1-18																					
A	KR 10-2012-0071123 A (한국전자통신연구원) 2012.07.02 청구항 1, 6 및 도면 1-3 참조.	1-18																					
A	JP 4413833 B2 (NIPPON TELEGR & TELEPH CORP.) 2010.02.10 단락 [0024]-[0043] 및 도면 1-3 참조.	1-18																					
☐ 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 “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 신구성 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 2016년 07월 26일 (26.07.2016)		국제조사보고서 발송일 2016년 07월 26일 (26.07.2016)																					
ISA/KR의 명칭 및 우편주소  대한민국 특허청 (35208) 대전광역시 서구 청사로 189, 4동 (둔산동, 정부대전청사) 팩스 번호 +82-42-481-8578		심사관 장기정 전화번호 +82-42-481-8364 																					

국제조사보고서
대응특허에 관한 정보

국제출원번호

PCT/KR2016/004805

국제조사보고서에서 인용된 특허문헌	공개일	대응특허문헌	공개일
KR 10-1492733 B1	2015/02/12	없음	
KR 10-2011-0079044 A	2011/07/07	없음	
KR 10-1281160 B1	2013/07/02	KR 10-2007-0079781 A	2007/08/08
KR 10-2012-0071123 A	2012/07/02	US 2012-0163212 A1	2012/06/28
JP 4413833 B2	2010/02/10	JP 2007-053430 A	2007/03/01