# 통신수사에서의 통화내역 분석과 SNA 기반 대포폰 탐지 알고리즘 연구

우병관, 김지온
한림대학교

byeongkwan.woo@hallym.ac.kr, jion972@hallym.ac.kr

# A Study on Call Detail Record Analysis and a Social Network Analysis-based Burner Phone Detection Algorithm for Crime Investigation

Woo Byeong Kwan, Kim Jion
Hallym Univ.

요 약

본 연구는 용의자가 대포폰으로 수사망을 피하는 문제에 대응하고자 사회연결망분석(SNA) 기반의 탐지 알고리즘을 제안한다. 용의자의 전화번호는 바뀌어도 관계망과 통화 패턴은 유지된다는 점에 착안하여, 1단계로 연결 중심성 분석을 통해 용의자의 핵심 관계망을 식별한다. 2단계에서는 구조적 등위성 분석으로 기존 용의자의 역할을 대체하는 대포폰 후보 번호를 탐색한다. 마지막으로 시계열 분석을 통해 통화 시간대 등 동적 활동 패턴의 유사성을 교차 검증하여 특정한다. 실제 사건 기반의 사례 연구를 통해 본 방법론이 수사 현장에서 적용 가능한 실용적 프레임워크임을 입증하였다.

## Ⅰ. 서 론

범죄 수사에서 용의자의 통신내역은 추적을 위한 핵심 단서 및 범죄를 입증하는 결정적인 증거로 활용된다. 그렇기 때문에 용의자들은 법집행기관의 추적을 피하기 위해 대포폰을 새로 개통하여 범죄를 실행하고 있으며, 이는 법집행기관의 수사에 큰 장애로 작용한다.

한편, 용의자는 대포폰을 개통하여 통화의 '수단'은 바꿀 수 있어도, 일상 생활이나 범행 실행과정에서 통화 상대방과 맺는 '관계' 또는 고유의 통화 '패턴'까지 완전히 바꾸기는 어렵다. 즉, 용의자의 전화번호만 변경될 뿐, 용의자가 맺고 있는 사회적 관계 네트워크는 그대로 유지되거나 유사한 형태로 계승된다는 것이다.

본 연구는 이러한 전제에 착안하여, 통신 네트워크의 구조적 속성과 사용자의 행동 패턴에 집중하는 새로운 대포폰 추적 알고리즘을 제안하였다. 알고리즘은 아래의 세 가지 핵심 질문에 답하는 과정으로 설계되었다.

- 용의자의 핵심 관계망은 누구로 구성되어 있는가?
- 이 관계망 내에서 용의자의 역할을 대체하는 번호는 무엇인가?
- 그 번호가 용의자의 행동 습관까지 모방하는가?

이러한 다층적 접근을 통해, 본 연구는 실제 대포폰을 높은 정확도로 특정하는 실용적이고 정교한 방법론을 제공하고자 한다.

## Ⅱ. 관련 개념 및 연구

1. 통신수사와 통신사실확인자료

'통신수사'는 범죄 수사에서 범인이 사용하는 다양한 통신수단을 조사하여 필요한 증거를 확보하는 방법을 의미[1]하며, 실무적으로 통신수사는 이러한 증거 자료를 수집·분석하여 범인을 특정하고 검거하는 수사 기법으로 정의할 수 있다.

통신수사를 통해 확보할 수 있는 증거로는 통신자료(가입자 정보), 통신사실확인자료(통화내역, 발신 기지국 위치정보 등), 감청자료 등이 있는데, 본 연구는 통화내역에 SNA 알고리즘을 적용하여 대포폰을 탐지하는 알고리즘을 제안한다는 점에서 여러 유형의 증거 자료 중 통신사실확인자료를 대상자료로 삼고 있다.

2. 사회연결망분석

사회연결망분석(이하 SNA)이란 사람들의 사회적 행위를 그들이 맺은 관계로 구성된 연결망의 특성으로 설명하려는 시도[2], 사회 구성원 간의 관계에 분석의 초점을 맞추어 이들 관계의 패턴으로부터 의미있는 시사점을 도출하는 방법론[3]을 말한다. 즉, 분석 대상 고유의 '속성'이 아니라 분석 대상이 맺고 있는 '관계'에 주목하여, 전화통화 내역, SNS 전송, 송금 내역 등 주요 범죄정보를 분석하는 것이다.

경찰은 그간 SNA를 활용하여 범인의 검거·특정, 공범 식별, 범죄혐의 증명이 가능함을 확인[4]하고, SNA 중 중심성(Centrality), 등위성(Equivalence), 고유벡터(Eigenvector) 등 알고리즘을 조합하여 범죄 데이터를 분석할 수 있음을 보이는 등[5][6] 연구를 진행하였으며, 학계에서도 사이버금융범죄 수사를 위해 2-mode 범죄 데이터를 1-mode로 변환 후 SNA를 적용하는 연구가 있었다[7].

## Ⅲ. SNA 기반 대포폰 탐지 알고리즘 제안

대포폰 탐지 알고리즘은 아래와 같이 4단계로 구성하였다.

1. (1단계) 네트워크 모델링

경찰이 압수수색영장을 통해 확보한 통화내역 데이터 중 '전화번호'를 노드(Node)로, 두 전화번호 간 통화 기록을 엣지(Edge)로 정의하고, 발신전화에서 착신전화로 방향성을 갖도록 모델링한다. 두 전화번호 간 통화 횟수를 가중치로 설정하되, 시간정보를 반영한 타임라인 분석을 수행하는 경우에는 엣지에 시간정보를 입력하고, 별도의 가중치를 부여하지는 않는다.

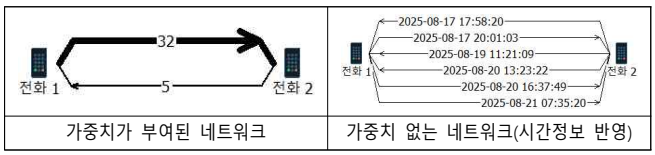


그림 1 네트워크 모델링 유형

2. (2단계) 핵심 네트워크 식별(연결 중심성 분석)

용의자는 통신 수단을 변경하더라도 기존에 맺고 있던 핵심적인 사회 관계망은 유지하는 경향이 있을 수 있으므로, 특정 노드가 네트워크 내 다른 노드들과 얼마나 많은 직접적 연결을 갖는지를 측정하

는 연결 중심성(Degree Centrality) 분석을 통해 용의자의 핵심 관계망을 식별한다.

이를 통해 먼저 용의자의 기존 번호와 가장 많이 통화한 집단, 즉 주요 의심 다수통화자를 추출하고 수사 맥락 상 중요한 의미를 갖는 대상자를 선별하여 분석의 기준인 '핵심 관계망'으로 삼고, 이들 '핵심 관계망' 번호와 많이 통화한 다수통화자를 추출하여 구조적 등위성 및 시계열 분석을 위한 대상을 특정한다.

3. (3단계) 용의자 등위 노드 탐색(구조적 등위성 분석)

용의자가 기존에 사용하던 번호를 해지하면, 해당 노드가 차지하던 네트워크 내의 구조적 위치는 공백으로 남게 되는데, 새로 개통한 대포폰은 이 공백을 대체하며 위의 핵심 네트워크 및 과거 용의자와 유사한 연결 형태를 형성한다. 이 때 특정 노드들이 네트워크 내 다른 노드들과 맺는 관계 형태의 유사성을 측정하는 기법인 구조적 등위성(Structural Equivalence)을 적용하여 유의미한 노드, 즉 네트워크 안에서 용의자의 위치를 대체하는 노드를 탐색한다. 용의자의 기존 번호가 핵심 관계망과 형성했던 연결 형태와 가장 유사한 형태를 나타내는 번호가 용의자의 대포폰일 가능성이 높기 때문이다.

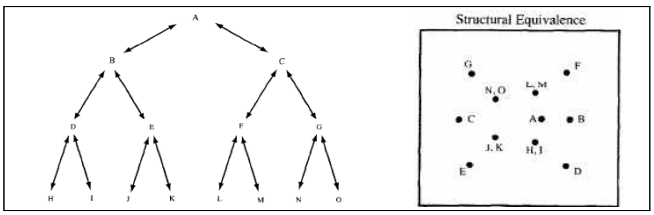


그림 2 구조적 등위성(Structural Equivalence) [8]

4. (4단계) 시계열 분석을 통한 검증

구조적 등위성 분석만으로는 통화 대상자가 우연히 겹친 제3자를 용의자로 오인할 가능성이 존재한다. 이러한 오류를 최소화하고, 억울한 수사대상자를 만들지 않기 위해서 통화의 패턴까지 유사한지 검증하는 절차가 필요하다. 타임라인 분석을 통해 용의자가 기존에 사용하던 휴대전화의 통화 기록과, 위에서 특정한 대포폰 번호 후보군의 통화 기록을 시계열적으로 비교하여, 주 통화 시간대, 평균 통화 시간, 통화 주기 등 동적 활동 패턴의 유사도를 분석한다. 이처럼 구조적 역할의 등위성뿐만 아니라 행동 패턴의 유사성까지 검증함으로써, 실제 대포폰을 특정할 확률을 높이고 분석 결과의 신뢰성을 확보한다.

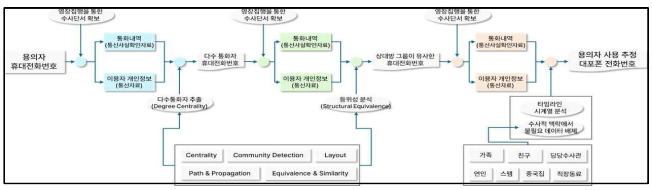

그림 3 대포폰 탐지를 위한 알고리즘

## Ⅳ. 사례 연구를 통한 방법론 적용 및 타당성 검증

본 연구를 통해 제안한 알고리즘이 수사 과정에 적용할 수 있는지 방법론 타당성을 검증하기 위해 정량적 데이터셋을 통한 성능 평가 대신 실제 사건 기반의 사례 연구를 적용하였다.

수사관은 살인 혐의로 지명수배가 된 용의자의 대포폰을 특정하기 위하여 용의자가 기존에 사용하던 휴대전화번호의 통화내역에 연결중심성 분석을 적용, 부인, 내연녀, 친구 등 통화량이 많은 3명을 도출하였다. 다음으로, 부인, 내연녀, 친구 휴대전화번호 통화내역에 연결중심성 분석을 적용하여 통화량이 많은 대상을 추출하고 등위성 분석을 통해 용의자 기존 휴대전화번호와 네트워크 안에서 구조적으로 같은 위치에 있는 전화번호 3개를 특정하였다. 그 중 하나는 담당수사관의 번호였고, 다른 하나는 범행 이전에 개통된 전화번호로 범죄와 관련성이 낮아 대포폰 후보군에서 제외되었으며, 새롭게 발견된 나머지 하나를 대포폰으로 추정하게 되었다. 이후 시계열 분석을 통해 내연녀가 담당수사관과 전화를 주고받은 직후 대포폰 추정 번호로 전화를 거는 패턴이 확인되었으며, 이와 같은 교차 검증을 바탕으로 수배자의 대포폰을 특정하게 되었다.

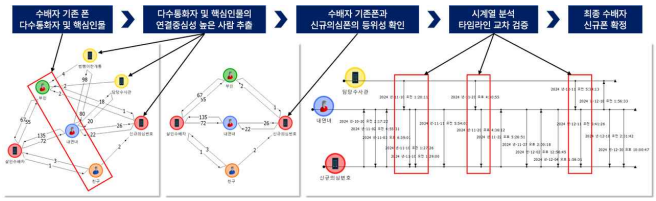


그림 4 실제 수사사례 적용 결과

## Ⅴ. 결론

본 연구를 통해 통신수사 과정에서 사회 연결망 분석(SNA)을 적용하여 조직적으로 사용되는 대포폰을 효과적으로 탐지하는 알고리즘을 제안하였다. 위의 사례 분석을 통해, 제안하는 4단계 알고리즘이 복잡한 통신 데이터 속에서 논리적 흐름에 따라 대포폰 후보를 효과적으로 압축하고 특정할 수 있는 체계적인 분석 프레임워크를 제공함을 보였다. 통화내역을 네트워크로 모델링하고 커뮤니티 탐지 및 중심성 분석을 통해 대포폰 사용 집단의 구조적 특징을 식별함으로써, 기존 분석 기법의 한계를 보완하고 수사 효율성을 높일 수 있는 가능성을 제시했다는 점에서 실무적 의의가 있다.

다만, 본 연구는 두 가지 한계가 있다. 첫째로, 사회적 관계를 반드시 정량적으로만 분석할 수는 없다는 점이다. 통화 횟수가 적더라도 가족, 친인척, 업무상 관계 등 수사적 맥락에서 중요한 전화번호가 있는데, 가중치가 낮거나 연결중심성 지표가 낮아 핵심 네트워크에서 제외되는 경우가 발생할 수 있다. 둘째로, 사례 연구를 통해 제안 모델의 실효성을 확인하였지만, 여러 사건, 대규모 데이터에 대한 일반화 가능성이나 탐지 정확도(Precision), 재현율(Recall)과 같은 정량적 지표를 제시하지는 못했다.

향후 수사적 맥락을 반영한 가상의 데이터를 생성하여 정확도를 검증하고, 시간의 흐름에 따른 네트워크 변화를 동적으로 분석하는 동적 네트워크 분석(Dynamic Network Analysis) 기법을 도입하여 더욱 고도화된 탐지 모델을 개발할 계획이다.

## ACKNOWLEDGMENT

이 논문은 2025년도 경찰청의 재원으로 과학치안진흥센터 사이버범죄 수사단서 통합분석 및 추론시스템 개발 사업사업의 지원을 받아 수행된 연구임(No. RS-2025-02218280)

## 참 고 문 헌

[1] 박노섭 · 이동희 · 이윤 · 장윤식, "범죄수사학", 경찰대학 출판부, 2013

[2] Yong Hak Kim and Young Jin Kim, "Social Network Analysis", PAKYOUNGSA, 2024

[3] Kee Young Kwahk, "Social Network Analysis", CRBooks, 2017

[4] 김지온. "사회연결망 분석원리의 범죄 수사상 활용방안에 관한 연구", 디지털포렌식연구, 13(2), pp. 89-109.

[5] Byeongkwan Woo and Ji On Kim and Ro-seop Park, "A Study on the Intelligent Using Methodology of Crime Scene Investigation Data", Journal of Data Forensics Research, 1(1), pp. 63-87

[6] 김지온 and 우병관. "사이버 범죄 탐지 및 분석기술에 대한 탐색적 연구", 한국치안행정논집, 19(3), pp. 57-76.

[7] 김현철 and 윤지원. "소셜네트워크 분석을 통한 사이버금융범죄 수사 활용사례(2-모드 중심으로)" 디지털포렌식연구, 14(4), pp. 449-465.

[8] Burt, R. S. "Detecting role equivalence". Social networks, 12(1), pp. 83-97.