스팸 메시지 발생 빈도 및 패턴 분석에 관한 연구*

서수연[01], 허민석[1], 황재호[1], 장지원[2], 신지호[3], 민무홍[2]

[1]성균관대학교 실감미디어공학과

[2]성균관대학교 컴퓨터교육과

[3]성균관대학교 과학수사학과

sooyon1119@g.skku.edu, alexhur3535@g.skku.edu, ashiereki@g.skku.edu, jiwon6424@g.skku.edu, sing0021@g.skku.edu, iceo@g.skku.edu

A Study on the Frequency and Pattern Analysis of Spam Messages

Sooyon Seo[01], Minseok Hur[1], Jaeho Hwang[1], Jiwon Jang[2], Jiho Shin[3], Moohong Min[2]

[1]Department of Immersive Media Engineering, Sungkyunkwan University

[2]Department of Computer Education, Sungkyunkwan University

[3]Department of Forensics, Sungkyunkwan University

요 약

스팸 메시지는 사용자들에게 불편과 위협을 안겨주는 문제로, 특히 사용자의 개인정보를 탈취하거나 악의적인 목적을 달성하기 위한 수단으로 자주 이용된다. 이러한 문제에 대처하기 위해서는 대량의 스팸 메시지 데이터를 분석하여 그 패턴을 파악하는 것이 필수적이다. 따라서 본 연구에서는 한 달여간 스마트폰으로 신고한 스팸 문자 데이터를 분석하여 신고 날짜, 시간대, 유형별 발생 패턴과 언어적 특징을 분석하였다. 이를 통해 스팸 메시지의 특성을 파악하고 보안 정책 개선을 위한 기초 자료를 제공해, 보다 효과적인 대응 방안을 모색할 수 있을 것으로 기대한다.

1. 서 론

스팸 메시지는 현대 사회에서 널리 퍼져 있는 문제로써 법적, 사회적, 경제적 등 다방면에 걸쳐 영향을 미치고 있다. 이는 사용자에게 불편만 야기할 뿐 아니라, 불법도박과 같은 범죄에 노출시켜 도박 중독, 경제적 손실, 가정파탄 등의 문제를 초래하며[1], 반대로 범죄 조직은 이를 통해 수익을 창출하며 사회에 혼란을 가져온다[2]. 이렇듯 스팸 메시지는 종종 범죄와 연결되어 있으며, 정보의 홍수 속에서 사용자들의 개인정보를 탈취하거나 악의적인 목적을 달성하기 위한 수단으로 이용된다.

빅데이터[3] 분석의 중요성은 이러한 스팸 메시지 문제에 대처하기 위해서는 필수적이다. 대량의 스팸 메시지 데이터를 분석함으로써, 스팸 메시지의 유형, 발생 빈도, 그리고 패턴을 이해할 수 있다. 이는 효과적인 스팸 필터링 알고리즘의 개발과 사용자 보호에 중요한 역할을 한다.

본 논문은 이러한 배경을 바탕으로, 스팸 메시지 데이터를 분석하여 그 사회적 문제를 이해하고 대응하는 데 그 목적이 있다[4]. 특히, 우리는 스팸 메시지의 발생 날짜 및 시간대, 그리고 유형별 분포를 조사하여 스팸 메시지의 특성을 파악하고자 한다. 또한 추가적으로 스팸 메시지의 언어적 특징을 분석하여, 우리는 보다 효과적인 스팸 필터링 시스템의 개선과 사용자 보호에 기여할 수 있을 것으로 기대한다.

2. 배 경

2.1 스팸 메시지

스팸 메시지는 일반적으로 사용자가 원치 않는 정보나 광고를 포함한 전자 메일, 문자 메시지, 소셜 미디어 메시지 등을 말한다. 이런 메시지들은 대개 대량으로, 수신자의 동의 없이 전송된다. 이들은 보통 상업적인 목적을 갖고 있으며, 광고성 메시지, 사기 및 불법 행위, 악성 코드 전파 등 다양한 형태를 띠고 있다[5]. 특히, 불법 도박 사이트와 같이 합법적인 광고 채널을 사용하기 어려운 경우 링크나 정보를 전달해 고객을 유인하기 위해 대량으로 스팸 메시지를 발송한다[6]. 이들은 단순 문자열을 비교하거나 스팸 전화번호를 차단하는 기존의 자동 스팸 필터링 시스템을 우회하기 위해 점차 비정상적인 형태로 발전하고 있다[7]. 이러한 스팸 메시지는 개인 정보 보호 및 보안, 그리고 사용자 경험 측면에서 큰 사회적 문제로

* 이 성과는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임(No. RS-2022-00166729)임.

그리고 과학기술정보통신부 및 정보통신기획평가원의 메타버스 융합대학원의 연구 결과로 수행되었음"(IITP-2024-RS-2023-00254129)

여겨지고 있기 때문에, 이에 대한 효과적인 대응이 필요하며, 스팸 필터링 시스템에도 개선이 이루어져야 한다.

2.2 한국인터넷진흥원(KISA)

KISA는 대한민국의 인터넷 진흥, 인터넷 정보보호 및 그와 관련한 국내외 협력 업무를 수행하는 준정부기관이다. KISA는 불법스팸대응센터를 통해 이용자로부터 스팸 신고를 접수하고, 스팸 발신자에 대한 조사 및 제재를 통해 불법 스팸을 근절하고 있다.

3. 실험방법

3.1 데이터

본 연구는 스마트폰 사용자가 신고한 스팸 문자 데이터를 KISA로부터 제공받아 진행하였다. 신고된 스팸 메시지는 KISA의 자체 분류 시스템에 의해 불법 도박, 성인, 금융상품, 선거 및 여론조사, 결제 및 인증 코드, 사적 대화, 교육, 오프라인 광고, 주식 및 투자, 대출, 통신가입, 불법 의약품, 온라인 서비스 광고, 스미싱 의심, 도박 의심, 대리운전, 병원 및 의약품, 구인광고, 게임, 종교, 유흥업소, 확인불가, 기타 총 23개의 유형으로 분류되어 있다.

각 스팸 데이터는 최초/최종 신고일시, 최초/최종 수신 일시, 유형 정보, 그리고 메시지 본문으로 구성되어 있다. 데이터 예시는 아래 표 1과 같다.

표 1 스팸 데이터 예시

1	[(KISA:SOL)]202402270152[(KISA)]202403151957[(KISA)]202402270152[(KISA)]202402271506[(KISA)]불법 도박[(KISA)]【공지안내】드디어 우리계열에서에!볼!루!션이 가능합니다!편하실때 오셔서 즐겨보세요!▶ kkn2024.＊＊＊
2	[(KISA:SOL)]202402270924[(KISA)]202403031155[(KISA)]202402270917[(KISA)]202402270918[(KISA)]주식 및 투자[(KISA)]단독 입수한 특별정보입니다.어제 17%돌파 VIP방 잠시 엽니다https://han.gl/ZTd01코드:7777

본 연구에서는 최초 수신 일시를 기준으로 분석을 진행하였고, 2024년 2월 27일부터 2024년 3월 20일까지 약 한 달간 신고된 119,285건의 스팸 데이터를 분석하였다.

3.2 스팸 메시지 데이터 발생 패턴 분석 시스템

본 연구에서는 데이터 분석 시스템을 파이썬으로 구현하여 실험하였다. 해당 시스템이 작동하는 방식은 다음과 같다.

먼저, 스팸 데이터가 있는 CSV 파일을 읽어와 각 행을 순회하며, "KISA:SOL"로 시작하는 부분을 정규식으로 찾아 스팸 데이터를 확인한다. 그 데이터가 스팸인 경우, 날짜와 시간을 추출하고 이와 함께 요일 정보를 추가 및 저장한다. 그리고 텍스트 내에서 스팸 유형에 해당하는 단어를 찾아 저장한다. 이후, 추출한 정보를 결합하여 데이터프레임으로 변환하고, 날짜별, 요일별, 유형별, 시간대별로 그룹화하여 스팸 개수를 센 다음, 해당 결과를 출력한다.

3.3 스팸 메시지 본문 분석

스팸 메시지의 발생 패턴 분석을 통해 판별된 상위 5개 유형의 스팸 메시지의 본문을 분석하였다. 수집된 스팸 메시지를 읽으며 기존의 비스팸 메시지와는 어떤 구별되는 특징이 있는지 등을 살펴보았다. 각 메시지에서 빈번하게 등장하는 키워드나 구문, 어조, 문법적 오류, 링크 분석, 요청 사항 등 스팸 메시지가 어떤 언어적 특징을 갖고 있는지 식별하여 기록하였다.

4. 결 과

4.1 스팸 메시지 데이터 발생 패턴

날짜별, 요일별, 시간대별 스팸 메시지 개수 분석 결과를 표 2에 정리하였다.

표 2 분류 기준별 스팸 메시지 개수 분석 결과 (단위: 개)

기준	min	Max	mean	median
날짜	1,848 (3/03)	6,915 (3/20)	5,186.3	5,804
요일	6,898 (Sun)	26,532 (Tue)	17,040.7	17,652
시간	53 (5시)	14,089 (11시)	4,970.2	2,547

분석 결과, 월요일부터 금요일까지는 스팸이 많이 발생하는 경향이 있었다. 특히 화요일이 가장 많은 스팸이 발생한 날로, 26,532건(22.2%)이 있었다. 반면에 주말인 토요일과 일요일에는 스팸이 상대적으로 적게 발생한 것으로 나타났다.

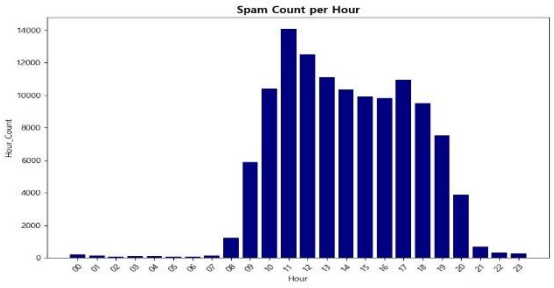

그림 1 시간대별 스팸 메시지 개수

또한 시간대별로 살펴보면, 오전 10시에서 오후 5시 사이에 가장 많은 스팸이 발생한 것으로 나타났다. 특히 오전 11시와 오후 12시에 수신된 건수가 총 26,594건(22.3%)으로 스팸 발생이 두드러지게 많았다. 이후 시간대는 점차 스팸 발생 건수가 줄어드는 모습을 볼 수 있었다.

추가적으로, 각 유형별 스팸 발생 빈도는, 가장 많은 스팸이 불법 도박과 주식 및 투자와 관련되어 있었다. 분석한 기간 내 불법 도박은 48,637건(40.8%), 주식 및 투자는 22,251건(18.7%) 발송된 것을 확인하였다. 반면에 유흥업소와 관련된 스팸은 매우 적은 수준으로, 단 2건만 존재하였다.

이러한 분석을 통해, 특정 날짜, 유형, 요일 및 시간대에 스팸이 집중적으로 발생한다는 점을 파악하였다. 따라서 본 연구에서 고안한 분석 시스템을 통해 스팸 메시지의 발생 패턴 및 특징을 파악할 수 있음을 알 수 있다. 이러한 정보는 스팸 필터링 시스템이나 보안 조치를 강화하는 데 도움이 될 것이다.

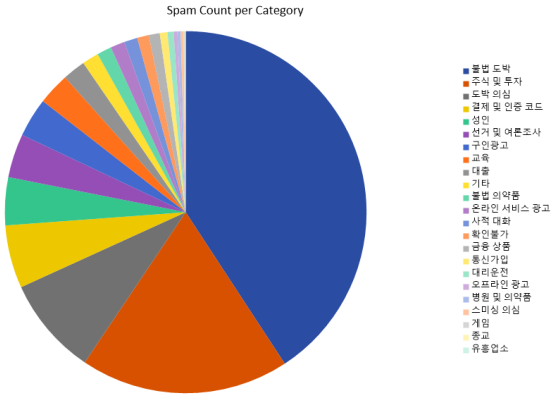

그림 2 스팸 메시지 유형별 비율

4.2 스팸 메시지 언어적 특징

스팸 메시지의 분석 결과, 불법 도박, 주식 및 투자, 도박 관련 내용, 결제 및 인증 코드, 그리고 성인 콘텐츠가 가장 빈번하게 포함된다는 사실을 확인하였다. 이러한 유형의 메시지들은 특정한 양식과 특징을 공유하며, 다음과 같은 패턴들을 보인다.

먼저, 문법이나 철자에 대한 비정상적인 사용이 두드러지게 나타난다. "빠워볼 작업비대면수슈료25퍼시작….(후략)", "월꿉날까지 기다려주는 대.:/츌빠르게….(후략)"과 같이 띄어쓰기가 일정하지 않거나, 의도적으로 철자 오류를 도입하여 자동 필터링을 우회하려는 경향이 보인다. 또한, 문장부호를 임의로 배치하여 일반적인 문장 구조를 혼동시키는 것도 흔히 발견된다.

다음으로, 메시지에는 링크나 연락처가 자주 포함되어 있다. "꽃길주소.comkkka:FFREF", "a7h.pe.kr", "ccggg.club"과 같이 수상한 도메인이나 텍스트로 이루어져 있어 일반적인 사용자에게는 신뢰하기 어려운 형태를 띤다. 특히, 해외 연락처를 사용하거나 손쉽게 채팅방을 개설 및 삭제가 가능한 카카오톡 오픈 채팅방 링크나 아이디를 통한 연락 방법이 주로 사용되며, 이는 추적이 어렵다는 문제가 있다.

마지막으로, 안전성과 신뢰를 강조하는 어조가 많이 사용된다. 이러한 메시지들은 감정적으로 호소하거나, 제품이나 서비스에 대한 부가적인 보장이나 확약을 제시함으로써 사용자들의 불안감을 경감시키고 구매를 유도한다. 이는 피해자의 판단력을 흐리게 하고 신뢰를 형성하는 데 기여한다.

이러한 특징들은 스팸 메시지의 유형을 파악하고 대응하기 위한 중요한 지표를 제공한다. 향후 보다 효과적인 스팸 필터링 및 예방 정책 개발 시 이러한 특징들을 고려하는 것이 필요하다.

5. 고 찰

우선, 본 연구를 통해 스팸 메시지의 발생 패턴 및 언어적 특징을 이해할 수 있다. 연구에서는 스팸 메시지의 발생 패턴을 날짜별, 요일별, 시간대별로 상세하게 분석하였다. 본 연구에서 고안한 분석 시스템을 통해, 추후에도 스팸 발생 패턴을 파악하고 그 변화를 쉽게 감지할 수 있을 것이다.

다음으로, 본 연구에서는 스팸 메시지의 텍스트를 분석하여 언어적 특징 및 패턴을 발견하였다. 이러한 패턴은 불법 도박, 주식 및 투자, 성인 콘텐츠 등과 관련이 있으며, 메시지의 문법적 오류, 수상한 링크 및 연락처, 그리고 안전성과 신뢰를 강조하는 어조 등이 주목되었다.

그러나, 본 연구에서는 특정 기간의 스팸 데이터만을 대상으로 분석하였다는 한계가 존재한다. 스팸 메시지는 계속해서 변하고 발전하기 때문에, 실시간으로 데이터를 수집하고 분석하여 신속하게 대응하는 방법을 연구하는 것이 중요하다. 또한, 언어적 특징 분석 시 자동화된 시스템을 구축한다면 보다 정확하고 효율적인 분석이 가능할 것이다. 자연어 처리 기술을 활용하여 스팸 메시지의 문법적 오류나 특이한 문장 구조, 스팸 패턴을 탐지하는 시스템을 개발하고, 머신러닝 및 딥러닝 기술을 활용해 스팸 메시지를 자동으로 분류하는 모델을 학습시킨다면, 실시간으로 스팸 메시지를 모니터링 하고, 즉각적으로 대응할 수 있는 종합 시스템을 구축할 수 있을 것이다.

마지막으로, 본 연구 결과를 이용해, 사용자의 스팸 신고 패턴이나 스팸 메시지의 변화에 따른 보안 정책에 대한 연구를 제안한다. 데이터 분석에 그치지 않고, 여러 정책과 조치를 통해 보다 신속하고 효과적인 스팸 대응 방안을 마련할 수 있다면, 스팸으로부터 사용자를 보호하는 데 더욱 효과적일 것으로 기대한다.

참고문헌

[1] Yeonho Lee et al., "Illegal Gambling Participation and Its Determinants," in *Journal of Social Science*, Vol. 57, No.1, 101-131, 2018.

[2] 김동하, "北, 불법 도박사이트 수천개 제작…한국 범죄조직에 팔았다," *조선일보*, 2024.

[3] I. Emmanuel and C. Stanier, "Defining Big Data," in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies (BDAW '16),* Article 5, 1-6, 2016.

[4] 박선우, "빅데이터 시대와 데이터 융합," *in ICT & Media Policy*, Vol. 30, No. 1, 1-24, 2018.

[5] S Aditya Chaturvedi and Lalit Purohit, "Spam Message Detection: A Review," in *International Journal of Computing and Digital Systems*, Vol. 12, No. 1, 2022.

[6] Beom-Oh Lee, "A Study on the Major Types of Cyber gambling, Punishment Laws and Countermeasures," in *Legal Theory & Practice Review*, Vol. 8, No. 4, 277-298, 2020.

[7] Ji-hye Kim and Ok-ran Jeong, "Knowledge Graph-based Korean New Words Detection Mechanism for Spam Filtering," in *Journal of Internet Computing and Services*, Vol. 21, No.1, 79-85, 2020.