네트워크 트래픽 패턴 변화에 대한 행위 탐지 규칙 업데이트 시스템 설계

박지태, 신창의*, 유경민, 김주성, 김명섭
고려대학교, 국방기술품질원*
{pjj5846, rudals2710, jsung0514, tmskim}@korea.ac.kr, *superego99@dtaq.re.kr

A Behavior Detection Rule Update System for the Changes in Network Traffic Patterns

Jee-Tae Park, Chang-Yui Shin*, Gyeong-Min Yu, Ju-Sung Kim, Myung-Sup Kim
Korea University, *Defense Agency for Technology and Quality

요 약

네트워크 내에서 발생하는 응용 트래픽에 대한 연구는 효율적인 네트워크 관리를 목적으로 오래전부터 다양하게 수행되어 왔다. 여러 연구들 중에서 사용자 행위 탐지 연구는 네트워크 모니터링, 관리, 보안 측면에서 관리자에게 유용한 정보를 제공하기 때문에 많은 연구가 수행되었다. 본 연구의 선행 연구에서는 SaaS 응용을 대상으로 정확한 사용자 행위 탐지를 위해 규칙 기반 탐지 방법을 제안하였다. 규칙 기반의 사용자 행위 탐지 방법은 트래픽 분석을 활용하여 사전에 각 행위 별 공통 특징을 추출하고, 추출된 특징을 규칙으로 정의하며, 정의 된 규칙을 기반으로 행위를 탐지하는 방법으로 정확도 측면에서 높은 성능을 보인다. 하지만, 네트워크 환경이 점차적으로 복잡해면서, 대상 응용의 기능 및 서비스 추가, 보안 업데이트 등의 이유로 응용의 버전이 업데이트 될 경우, 사전에 정의한 공통 특징이 변하는 경우가 발생하며, 이러한 경우에 사전에 정의한 규칙 기반의 탐지 방법의 성능은 크게 저하된다. 따라서 본 논문에서는 응용 버전 업데이트와 같은 트래픽 패턴 변화 상황에서도 대처 할 수 있는 규칙 업데이트 시스템을 제안한다.

Ⅰ. 서 론

네트워크 기술의 급격한 발전에 따라 다양한 응용 서비스가 발생하고 있으며, 발생하는 트래픽 양도 점차적으로 증가하고 있다. 특히 퍼스널 디바이스 사용의 증가와 모바일 및 클라우드 기반의 서비스 확대에 따라 이러한 추세는 점차적으로 가속화 될 것으로 보인다. 발생하는 대규모 트래과 네트워크 자원을 효율적으로 관리하고, 사용하는 응용에 대한 원활한 서비스 제공을 위해 응용 트래픽에 대한 연구는 오래전부터 수행되어 왔다. 응용 트래픽에 대한 연구는 다양하게 수행되어 왔으며, 대표적으로 어플리케이션, 서비스, 프로토콜 등의 범주에서 수행되는 트래픽 클래스 분류 연구와 대상 응용의 특성 혹은 연구 목적에 따라 특정 응용 및 서비스를 탐지, 식별하는 연구 등이 가장 활발하게 수행되어 왔다[1]. 여러 연구들 중 응용에 대한 사용자 행위 탐지 연구는 네트워크 모니터링, 관리 및 보안 측면에서 관리자에게 많은 정보를 제공 할 수 있기 때문에 중요하다[2,4]. 예를 들어 네트워크 보안 측면에서 공격자는 사전에 공격 대상 응용의 취약점을 분석하고, IDS에 탐지되지 않기 위해 정상 사용자인 것처럼 위장하는 경향이 있다. 네트워크 보안 관제 시스템은 사용자 행위에 대한 지속적인 모니터링 및 분석을 통해 이러한 위장된 악성 행위에 대해 신속하고 정확하게 탐지해야 한다[2, 3].

본 연구의 선행 연구에서는 사용자 행위 탐지를 위해 규칙 기반의 탐지 방법을 제안하였다. 규칙 기반의 사용자 행위 탐지 방법은 사전에 대상 응용에 대한 트래픽을 분석을 통해 각 행위 별로 도출되는 공통 특징을 추출하여 규칙으로 정의하고, 정의된 규칙을 기반으로 대상 응용에 대한 사용자 행위를 탐지한다. 선행 연구에서 제안한 방법은 각 행위 별로 발생하는 공통적인 특징을 기반으로 행위를 탐지하기 때문에 높은 성능을 보이며, 실제로 Office 365, Adobe Creative Cloud를 대상으로 사용자 행위 탐지 실험을 수행하여 검증하였다.

하지만 점차적으로 복잡해지고 고도화되는 네트워크 환경에 따라 대상 응용의 보안 기능 강화, 새로운 기능 및 서비스 추가 등의 이유로 응용의 버전 업데이트가 빈번하게 발생하며, 수행되는 업데이트에 따라 대상 응용에서 발생한 트래픽의 패턴이 바뀌게 될 수 있다. 이 경우에는 업데이트 전에 정의한 공통 특징과 업데이트 후 달라진 공통 특징이 일치하지 않기 때문에 탐지 성능이 크게 저하되는 문제점이 있다. 따라서 본 연구에서는 응용 버전 업데이트 등의 상황에서 트래픽 패턴이 달라지더라도 유동적으로 대처 할 수 있는 규칙 업데이트 시스템을 제안한다.

본 논문의 구성은 본 장의 서론에 이어 2장 관련 연구에서 기존의 사용자 행위 탐지 연구에 대해 기술하고, 3장 본론에서 제안하는 규칙 업데이트 시스템 구조에 대해 설명한다. 마지막으로 4장에서 결론 및 향후 연구에 대해 기술한 후 마친다.

Ⅱ. 관련 연구

사용자 행위 탐지 연구는 네트워크 관리, 유지를 목적으로 다양하게 수행되어 왔다. 사용자 행위는 연구 목적, 응용 특성에 따라 다양하게 정의될 수 있기 때문에 같은 응용에라도 정의 된 행위가 달라질 수 있다. 본 논문에서는 수행된 여러 연구 중 대표적인 연구를 표1에 정리하였다.

[2]에서는 메시지 및 파일 전송을 목적으로 하는 카카오톡을 대상 응용으로 선정하였다. 카카오톡의 메신저 형태 특성을 반영하여 메시지 수신, 발신, 친구 추가 등의 11가지 행위를 정의하고, 각 행위를 높은 정확도로 분류한다. [2]의 연구는 네트워크 보안 측면에서 대상 응용이 암호화 트래

본 논문은 2020년도 산업통상자원부 및 한국산업기술평가관리원(KEIT) 연구비 지원에 의한 연구 (No. 20008902, IT비용 최소화를 위한 5채널 탐지기술 기반 SaaS SW Management Platform(SMP) 개발)이며, 2021년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 결과입니다. (2021RIS-004)

픽을 사용하더라도 사용자 행위 추론을 통해 악성 행위를 수행 할 수 있다는 점을 강조한다. [3]에서는 SNS 형태의 Instagram 응용을 대상으로 로그인, 포스팅 등의 9가지의 행위를 정의하여 분류한다. [3]에서는 네트워크 보안 분야에서 악성 행위 탐지를 목적으로 사용자 행위 탐지 연구를 수행한다. 본 연구의 선행 연구인 [4]에서는 문서 작업에 주로 사용되는 Office 365를 대상으로 응용 시작, 로그인 등의 6가지의 행위를 정의한다. [4]에서는 클라우드 기반 서비스 응용의 특성을 고려하여 효율적인 지출 관리를 목적으로 사용자 행위 탐지 연구를 수행한다. 본 논문에서는 [4]의 선행 연구에서 응용 버전 업데이트로 발생 할 수 있는 문제점을 제시하고, 이를 해결하기 위해 사용자 행위 탐지 규칙 업데이트 시스템을 제안한다.

표 1 사용자 행위 탐지 관련 연구

응용	연구 목적	형태	행위 예시
KakaoTalk[2]	네트워크 보안	메신저	Receive a message, Send a message 등
Instagram[3]	네트워크 보안	SNS	Enter, Login, Posting, 등
Office 365[4]	지출 관리	문서 작업	응용 시작, 로그인, 로그아웃 등

Ⅲ. 본론

본 장에서는 제안하는 규칙 업데이트 시스템의 구조와 동작 과정에 대해 설명하며, 전체 시스템 구조는 그림 1에 나타나있다. 선행 연구에서 수행된 규칙 기반의 사용자 행위 탐지 시스템 전체 구조는 크게 규칙 생성과 행위 탐지 과정으로 구분된다.

규칙 생성 과정에서는 하나의 호스트에서 수집된 대상 응용에 대한 트래픽을 입력으로 헤더, 통계, SNI 정보 등을 활용하여 공통 특징을 추출하고, 규칙을 생성하는 과정이다. 2장 관련 연구에서 설명했듯이 사용자 행위는 목적과 응용 특성에 다양하게 정의될 수 있으며, 일반적으로 하나의 응용에서 여러 가지 사용자 행위를 정의한다. 대상 응용에 대한 행위 탐지를 위한 규칙은 사전에 정의한 행위 별로 생성이 되기 때문에 하나의 응용에서 여러 개의 행위 규칙(Action Rule)이 생성된다. 규칙 생성 과정에서는 생성 된 여러 개의 행위 규칙을 하나의 규칙으로 취합하여 최종적으로 응용 규칙(Application Rule)을 생성하게 된다.

행위 탐지 과정은 여러 호스트가 있는 실제 네트워크 환경에서 적용되며, 사전에 생성된 행위 탐지 규칙과 여러 호스트에서 수집된 트래픽을 입력으로 대상 응용에 대한 행위 탐지를 수행한다. 패킷 미러링을 통해 실시간으로 여러 호스트에서 발생한 패킷을 수집하고, 전처리 과정을 거친 후에 생성된 규칙과 함께 행위 탐지 시스템에 입력으로 들어간다. 행위 탐지 시스템에서는 입력된 트래픽에서 사전에 정의한 각 행위 별 공통 특징이 나타나는지 확인하고, 나타날 경우에 해당 트래픽의 발생 시간, 호스트, 대상 응용, 응용 행위 순으로 결과를 도출한다.

제안하는 규칙 업데이트 시스템은 기존의 규칙 생성 과정과 동일하게 사용하며, 규칙 유효성 검사(Rule Validity Check)와 규칙 재생성(Rule Generation) 과정으로 구성되어 있다. 규칙 유효성 검사는 규칙의 성능을 평가하여 대상 응용의 행위 탐지 규칙의 유효성을 검사하는 과정이다. 규칙 기반의 행위 탐지 시스템의 탐지 성능을 평가하기 위하여 API 기반의 사용자 행위 탐지를 함께 적용한다. API 기반의 사용자 행위 탐지는 네트워크 트래픽을 사용하지 않고 사용자의 응용 사용에 따라 생성되는 API 로그를 기준으로 행위를 탐지한다. 규칙 기반의 행위 탐지 시스템의 탐지 결과와 API 기반의 사용자 행위 탐지 결과를 비교하여 정탐지, 미탐지, 오탐지를 판단하고, 이를 기준으로 Recall, Precision, F-measure 값을 계산한다. 계산된 F-measure 값이 사전에 정의한 Threshold보다 낮아질 경우 규칙 업데이트가 필요한 상황으로 판단하고, 규칙 재생성 과정이 수행된다. 이 때, 너무 낮은 Threshold는 규칙 업데이트가 필요한 상황에도 규칙 재생성 과정을 수행하지 않을 수 있으며, 너무 높은 Threshold는 규칙 재생성 과정을 과도하게 수행할 수 있기 때문에 적절한 Threshold 선정이 필요하다.

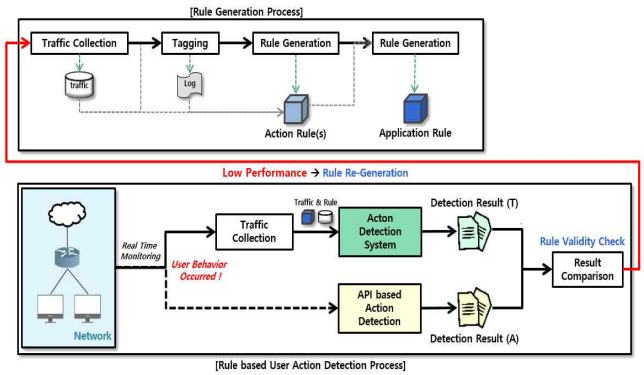

그림 1. 규칙 업데이트 시스템 구조

Ⅲ. 결론

본 논문에서는 사용자 행위 탐지 연구의 필요성과 이전에 수행되었던 여러 연구를 소개하며, 선행 연구에서 제안한 규칙 기반의 사용자 행위 탐지 연구에서 응용의 업데이트에 따른 트래픽 패턴 변화에 따라 발생 할 수 있는 성능 저하 상황을 문제점으로 제시한다. 제시한 문제점을 해결하기 위해 트래픽의 패턴이 변할 경우에 대처 할 수 있는 규칙 업데이트 시스템을 제안한다. 규칙 업데이트 시스템은 규칙 유효성 검사와 규칙 재생성 과정으로 구성되며, 규칙 유효성 검사 과정에서는 탐지 성능을 기준으로 규칙 업데이트 필요한 상황을 판단하고, 규칙 재생성 과정에서 판단된 상황에 따라 규칙을 생성한다. 제안하는 시스템은 응용 버전 업데이트와 같이 여러 상황에서 발생 할 수 있는 트래픽 패턴 변화에도 규칙 기반의 행위 탐지 방법을 유동적으로 적용 할 수 있다는 장점이 있다.

향후 연구로는 설계한 규칙 업데이트 시스템을 구현하고, 선행 연구를 포함한 여러 가지 응용을 대상으로 적용 할 예정이다. 또한 적절한 Threshold를 선정하기 위해 다양한 실험을 진행 할 예정이다.

참 고 문 헌

[1] 박준상, 박진완, 윤성호, 오영성, 김명섭. "응용 레벨 트래픽 분류를 위한 시그니쳐 생성 시스템 및 검증 네트워크의 개발." 한국정보처리학회 학술대회논문집 16(1), 2009, pp. 1288-1291

[2] K. Park and H. Kim. “Encryption Is Not Enough: Inferring user activities on Kakaotalk with traffic analysis” International Workshop on Information Security Applications, 2015, pp. 254-265, Springer, Cham,

[3] H. Wu, Q. Wu, G. Cheng and S. Guo, "Instagram User Behavior Identification Based on Multidimensional Features," IEEE INFOCOM 2020 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2020, pp. 1111-1116

[4] J. -T. Park, U. -J. Baek, M. -S. Kim, M. -S. Lee and C. -Y. Shin, "Rule-based User Behavior Detection System for SaaS Application," 2022 23rd Asia-Pacific Network Operations and Management Symposium (APNOMS), 2022. pp.1-4