네트워크 트래픽 패턴 변화에 즉각적인 대응을 위한 실시간 시그니쳐 업데이트 시스템에 관한 연구

심규석, 이수강, 구영훈, 이성호, 김명섭
고려대학교

{kusuk007, sukanglee, gyh0808, secma66, tmskim}@korea.ac.kr

A Study on the Real-time Signature Update System for Immediate Response to Changing Network Traffic Pattern

Kyu-Seok Shim, Su-Kang Lee, Young-Hoon Goo, Sung-Ho Lee, Myung-Sup Kim
Korea Univ.

요 약

오늘날 네트워크 환경이 증가하며 응용 및 서비스 별로 발생시키는 트래픽 패턴에 다양한 종류가 생성됨에 따라 응용 및 서비스 별로 분류할 수 있는 빈번한 시그니쳐 업데이트의 중요성이 증가하고 있다. 그러나, 시그니쳐를 생성하는 작업은 트래픽 패턴 변화를 관리자가 인지 해야할 뿐만 아니라 인지한 후에 새롭게 시그니쳐를 추출하는 작업은 시간과 비용을 매우 많이 소비하는 작업이다. 따라서 본 논문은 네트워크 트래픽 패턴 변화에 즉각적으로 대응할 수 있도록 실시간으로 시그니쳐를 업데이트가 가능한 시스템을 제안한다. 본 시스템은 실시간으로 수집되는 네트워크 트래픽을 TMA 를 이용하여 각 프로세서별로 정답지 트래픽으로 분류한 뒤, 기존 시그니쳐로 트래픽을 분석하여 분류되지 않은 트래픽을 다시 분류하고, 분류되지 않은 트래픽을 이용하여 시그니쳐를 자동으로 생성한다. 자동으로 생성된 시그니쳐는 해당 응용을 제외한 다른 응용의 트래픽을 이용하여 시그니쳐의 정확도를 측정하여 다른 응용에서 분석되지 않은 시그니쳐만을 선별한다. 본 시스템은 시간이 지남에 따라 업데이트된 시그니쳐가 각 응용의 분석률 상승 및 오탐률 감소된 결과를 통해 타당성을 증명하였다.

Ⅰ. 서 론

오늘날 네트워크 환경은 증대되고 있고, 그에 따라 네트워크를 이용하는 응용의 종류도 증가하고 있다. 이러한 다양한 응용은 각자 다른 패턴을 트래픽을 발생시킨다. 또한 각 응용은 개발자에 의해 사용자에게 고품질의 서비스를 제공하기 위해 지속적으로 트래픽 패턴을 변화시킨다. 네트워크 관리자는 이러한 트래픽 패턴을 이용하여 관리 네트워크 내의 트래픽을 분류하여 QoS 조절 및 모니터링을 한다. 시그니쳐는 트래픽을 각 응용 별로 분류할 수 있는 각 응용만의 고유한 트래픽 패턴을 의미한다.

시그니쳐는 트래픽의 특징 별로 다양한 형태로 존재한다. 본 논문에서는 트래픽의 페이로드 내 고유한 문자열로 트래픽을 분류할 수 있는 페이로드 시그니쳐를 사용한다[1]. 페이로드 시그니쳐는 매우 높은 정확도와 분석률로 분류할 수 있는 장점이 있지만, 시그니쳐 추출과정이 매우 복잡하고, 시간이 오래 걸리는 단점을 가지고 있다.

따라서 시그니쳐 자동 생성 시스템은 활발히 연구되고 있다. 그러나 추출을 목적으로 한 응용의 트래픽은 사용자가 수집하여 시스템의 입력데이터로 해야하기 때문에 트래픽 패턴의 변화를 사용자가 직접 인지하고, 해당 응용의 트래픽을 수집하여 시그니쳐 추출을 하는 것은 매우 어려운 작업이다.

본 논문은 실시간으로 트래픽 패턴 변화에 대응하기 위해 하루 단위로 시그니쳐를 업데이트하는 시스템을 제안한다. 본 시스템은 TMA 를 이용하여 실시간으로 정답지 트래픽을 분류하고, 응용 별로 분류된 트래픽을 해당 응용의 시그니쳐로 분석하여 분석되지 않은 트래픽을 분류한다. 본 과정에서 분석에 사용되지 않는 시그니쳐는 불필요한 시그니쳐로 판단하여 삭제된다. 분류된 트래픽은 시그니쳐 자동 생성 시스템에서 시그니쳐 추출을 위해 사용되고, 추출된 시그니쳐와 기존 시그니쳐는 해당 응용이 아닌 다른 응용의 트래픽을 분류함으로써 정확도를 판단한다[2].

본 논문은 서론에 이어, 2 장에서 본 시스템에 대한 각 역할별 프로세스를 언급한 뒤 3 장에서 본 시스템을 사용하여 추출된 시그니쳐로 실험을 통해 본 시스템의 타당성을 증명한다. 마지막으로 4 장에서 결론 및 향후 연구에 대해 언급한 뒤 본 논문을 마친다.

Ⅱ. 본론

본 장에서는 실시간 시그니쳐 업데이트 시스템에 대해 언급한다. 실시간 시그니쳐 업데이트 시스템은 그림 1 과

2016 년 한국과학기술정보연구원 연구과제(첨단연구망기반 협업플랫폼 서비스 및 글로벌 연동, K-16-L01-C02-S03)과 2015 년도 정부(교육부)의 재원으로 한국연구재단의 지원(No.2015R1D1A3A01018057)으로 수행되었습니다.

같이 정답지 트래픽 생성부, 시그니쳐 관리부, 시그니쳐 생성부, 시그니쳐 검증부로 총 4 개의 파트로 나누어져서 시스템이 수행된다. 4 개의 파트가 하루 단위로 수행되면서 관리자는 정확한 가장 최신의 시그니쳐를 유지할 수 있다.

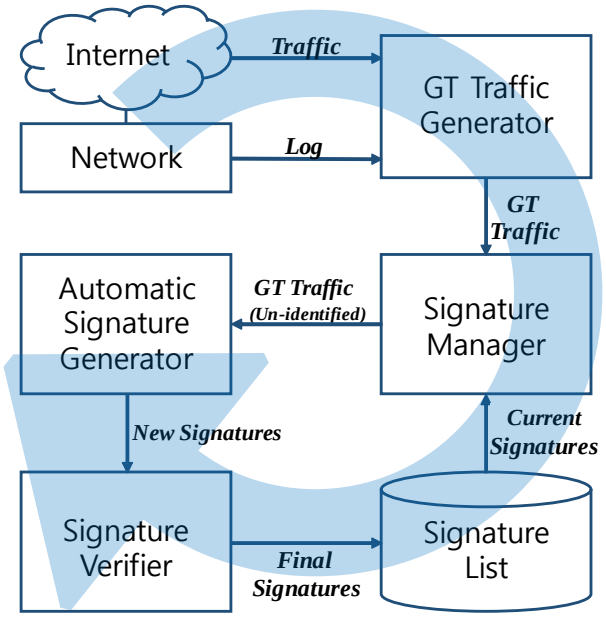

Figure 1. 실시간 시그니쳐 업데이트 시스템

먼저, 실시간 정답지 트래픽 생성부는 TMA 를 사용하여 정답지 트래픽을 분류한다. 본 시스템은 하루 단위로 그 전날 트래픽을 각 프로세스 이름별로 분류하는 역할을 한다. 두번째는 각 프로세스 별로 분류된 정답지 트래픽을 기존 사용자가 가지고 있던 각 프로세스 시그니쳐로 분석한다. 본 과정에서 분석에 사용되지 않은 시그니쳐는 불필요한 시그니쳐로 판단하여 삭제되고, 분류가 되지 않은 트래픽만 출력한다. 출력된 트래픽은 시그니쳐 생성 시스템으로 입력되어 새로운 시그니쳐를 추출한다. 분석에 사용된 시그니쳐와 새롭게 추출된 시그니쳐는 시그니쳐 검증부에서 해당 응용을 제외한 나머지 응용의 트래픽을 분석하여 False-Positive 수치 즉, 오탐률을 측정한다[3]. 각 시그니쳐별로 오탐률을 측정하면서 오탐할 수 있는 시그니쳐는 본 단계에서 삭제된다.

Ⅲ. 실험

본 시스템의 성능을 측정하기 위해 총 4 일 동안 시그니쳐 업데이트 시스템을 수행했다. 가장 많이 사용되는 응용 4 가지를 대상으로 실험을 진행하였다. 응용 4 가지는 AfreecaTV, Kakaotalk, Facebook, 그리고 Torrent 를 선정하였다. 따라서 기존 시그니쳐를 포함한 총 5 종류의 시그니쳐가 추출되었고, 해당 시그니쳐들로 시그니쳐 추출에 사용되지 않은 트래픽을 분석하였다. 분석결과는 표 1 에서와 같이 분석률과 오탐률을 나타낸다.

기존 시그니쳐로 현재 발생하고 있는 트래픽을 분석했을 때 분석률이 매우 낮을 뿐만 아니라 오탐률 또한 매우 높은 것을 확인하였다. 그러나, 업데이트 횟수가 많아질 수 록 분석률은 상승하고 오탐률은 감소하는 것을 확인하였다. 표 1 의 단위는 플로우의 분석률과 바이트의 분석률을 나타낸다.

Table 1. 실시간 시그니쳐 업데이트 시스템 수행 횟수 별 분석률 및 오탐률

S \ T		Afreeca		Kakaotalk		Facebook		Torrent	
		F	B	F	B	F	B	F	B
AF	O	0.2	9.6	0	0	0.1	2.3	1.3	19.5
	1	50.3	96.6	0	0.1	0.4	5.2	1.9	0.1
	2	49.6	96.5	0	0.1	0.2	4.9	1.9	0.1
	3	53.5	97.2	0	0	0.5	4.9	1.9	0.1
	4	51.6	97.5	0	0	7.2	0.2	0	0
KA	O	0.3	0.1	0.1	0	0	0	0.2	1.7
	1	0	0	58.6	13	0	0	0	0
	2	0	0	78	27	0	0	0	0
	3	0	0	79.1	33.8	0	0	0	0
	4	0	0	80.5	66.9	0	0	0	0
FA	O	0.1	0.8	0.1	0.2	0	0	0.4	0.1
	1	0.3	0.5	0.1	0.1	35.5	98.5	0	0
	2	0.1	0.2	0.9	0.2	35.2	95.9	0	0
	3	2.0	0.5	0	0	53.8	91.2	0	0
	4	2.2	0.4	0	0	46.5	94.4	0	0
TO	O	21.1	44.1	0	0.1	3.8	22.6	24.6	76.9
	1	0	0	0	0	0	0	15.6	82
	2	0	0	0	0	0	0	15.6	82
	3	0	0	0	0	0	0	15.6	82
	4	0	0	0	0	0	0	19	88.9

Ⅳ. 결론 및 향후 연구

본 논문은 트래픽 수집, 시그니쳐 관리, 시그니쳐 생성 그리고 시그니쳐 검증의 과정을 실시간으로 수행할 수 있는 실시간 시그니쳐 업데이트 시스템을 제안하였다. 본 시스템은 실험을 통해 정확하고, 가장 최신의 시그니쳐를 유지할 수 있는 것을 증명하였다.

향후 트래픽 수집과정에서 TMA 로 분류하지 못하는 응용 및 서비스에 대해 분류할 수 있는 방법을 적용하여 모든 응용 및 서비스의 시그니쳐를 유지할 수 있는 방법을 연구할 계획이다.

참 고 문 헌

[1]Jun-Sang Park, Sung-Ho Yoon, Myung-Sup Kim, "Performance Improvement of the Payload Signature based Traffic Classification System using Application Traffic Temporal Locality," Proc. of the Asia-Pacific Network Operations and Management Symposium (APNOMS) 2013, Hiroshima, Japan, Sep. 25-27, 2013, pp.1-6.

[2]심규석, 윤성호, 이수강, 김성민, 정우석, 김명섭, "네트워크 트래픽 분석을 위한 Snort Content 규칙 자동 생성", Vol.40, No.04, April, 2015, pp666-677.