대용량 네트워크에서의 플로우 모니터링 시스템 구현

권우창, 박병연*
한국과학기술정보연구원, *한국과학기술정보연구원
wckwon@kisti.re.kr, *bypark@kisti.re.kr

Implementation of a flow monitoring system in a high bandwidth network

Kwon Woo Chang, Park Byeong Yeon*
KISTI., *KISTI

요 약

과학기술연구에 대한 데이터기반의 연구들은 증가하는 추세이며, 이러한 연구에 밑바탕이 되는 네트워크 대역폭은 나날이 증가하고 있다. 이러한 추세에 맞춰 대용량 네트워크에 흐르는 트래픽에 대한 수집 및 분석에 대한 요구도 들어가고 있다. 본 논문은 대용량 네트워크에 흐르는 트래픽을 플로우 기반으로 분석하기 위해 수집, 저장 및 가시화를 할 수 있는 모니터링 시스템에 대해서 제안한다

Ⅰ. 서 론

최근 전세계 과학기술연구의 추세는 대형실험장비 및 빅데이터에 대한 분석을 위한 대용량의 트래픽이 발생하고 있다. 이러한 대용량의 트래픽이 흐르는 네트워크에서는 백본 트래픽에 대한 수집 및 분석이 반드시 필요하며, 이에 대한 요구가 늘어가고 있다.

본 논문에서는 이러한 요구사항을 해결하기 위해 국가과학기술연구망(KREONET)[1]의 글로벌과학기술협업연구망(GLORIAD-KR)[2]에 흐르는 10Gbps급 네트워크 트래픽에 대한 수집, 저장 및 분석된 정보를 3D 가시화를 통해 효율적인 국제망 모니터링 환경을 구축하는 것을 목표로 하는 네트워크 플로우[3] 모니터링 시스템에 대해 기술한다.

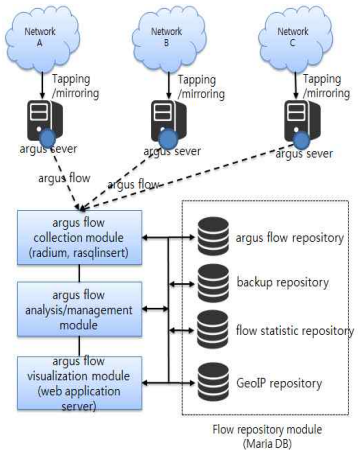
Ⅱ. 본론

국가연구망인 KREONET 및 GLORIAD-KR에 적용할 수 있는 10Gbps급의 대용량 네트워크에서 흐르는 네트워크 트래픽에 대한 플로우 정보를 샘플링(중요도 및 우선순위가 높은 정보들만 추출) 없이 전체 플로우 정보를 제어하는 것은 시스템의 많은 부하가 걸리며, 이러한 문제를 해결할 수 있는 수집/저장/분석하는 기술의 확보가 필요한 상황이다.

이러한 플로우 정보를 수집하기 위해서 Argus[4]라는 오픈소스 도구를 이용하였다. Argus는 네트워크의 성능에 대한 분석부터 프로토콜 데이터 수집까지 다양한 기능을 수행하여, 중앙 집중식 네트워크 관리 시스템을 구축하는데 있어 많은 장점을 갖고 있다. 본 시스템에서는 네트워크 트래픽에 대한 플로우 정보를 샘플링하여 수집하고 저장하는 용도로 사용하였으며 이러한 기능들을 이용한 본 시스템의 큰 4가지 기능은 다음과 같다.

1. netflow 스키마 기반 플로우 정보 수집 및 분석 모듈: 대용량 네트워크인 국제과학기술연구망의 네트워크 운영, 성능 측정 및 보안관제를 하기 위한 오픈소스 기반 플로우 정보 수집 및 분석 도구인 argus를 이용하여 netflow 정보 수집/갱신/삭제하는 기능을 구현한다.

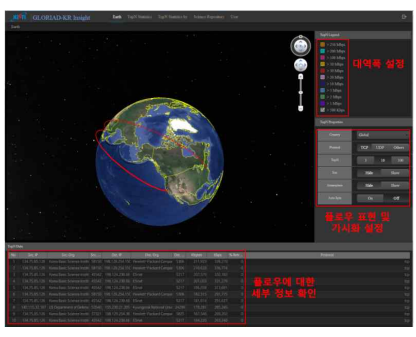
2. 웹 기반 플로우 정보 3D 기반 가시화 모듈: 수집된 netflow 정보를 웹 기반의 3D GUI에 가시화하는 것을 목표로 사용자를 위한 웹 기반 GUI 및 대시보드와 netflow 정보를 가시화할 수 있는 기능을 구현한다.



(그림1) 플로우 모니터링 서비스 구조도

3. 3D 가시화를 위한 지리정보 mash-up 모듈: netflow 정보와 IP기반 사용자 위치 정보를 조합하여 위치기반 3D 가시화에 사용할 수 있는 가공하는 기능과 위치기반 사용자 위치 정보 DB를 구축할 수 있는 자동화 도구를 구현한다.

4. 네트워크 플로우 리포팅 모듈: 본 시스템에서 얻어진 대용량의 플로우 정보의 효율적인 운용 및 분석을 위해 수집된 플로우 정보를 최적화하여 시간별, 사용자별 통계 데이터로 제공하는 기능을 구현한다.

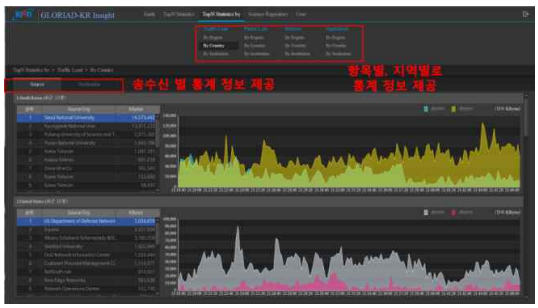


(그림2) Top N 노드 조회

수집된 네트워크 플로우에 대한 정보를 사용자 및 관리자가 효과적으로 모니터링 하기 위해서는 효율적인 사용자 인터페이스가 필요하다. 본 시스템은 사용자의 접근성 및 확장성을 고려하여 그림 2처럼 웹 인터페이스로 가시화 도구를 구현하였으며, 전 세계의 네트워크 flow를 한눈에 표현하기 위해 Google 사의 Google Earth 3D API를 이용하였다.

(그림3) 시간별 통계 정보 조회

그림 3은 시간별 통계 정보조회 기능은 10분, 1시간, 1일, 1달, 1년의 주기이며 각각의 네트워크 트래픽에 따라 차트 및 표를 이용하여 상세한 정보를 제공하며, 보다 체계적인 정보를 제공하기 위해 데이터의 정렬 및 추가 기능에 대한 부분을 구현하였다.



(그림4) 분류별 통계 정보 조회

그림 4는 사용자가 원하는 항목별로 통계정보를 제공하기 위한 페이지이다. 사용자는 네트워크 트래픽에 대한 통계를 원하는 요소별로 조회할 수 있다. 지역별(대륙, 국가, 기관), 패킷로스 통계, 프로토콜별 등 다양한 요소별로 통계정보를 조회할 수 있으며, 각각의 요소에 대해 출발지 및 도착지별로도 통계정보를 조회할 수 있다.

Ⅲ. 결론

본 시스템의 구축을 통해 국가과학기술연구망(KREONET) 및 글로벌과학기술협업연구망(GLORIAD-KR)에 흐르는 네트워크 플로우를 수집하여 효율적인 관리가 가능하였다. 또한 다양한 통계정보를 제공하는 서비스와, 사용자 편의성을 증가시키기 위한 웹 인터페이스 3D 가시화 도구를 통해 관리의 효율성을 제고할 수 있었다.
그리고 본 연구에서는 10Gbps 급의 대용량 네트워크에서 네트워크 트래픽에 대한 netflow를 수집하여 네트워크를 모니터링하는 방안을 제시하였다. 향후에는 점차 대용량화 되는 40Gbps 및 100Gbps 대용량 네트워크 관리시장에서도 대응할 수 있는 요소기술에 대한 연구가 필요하다.

ACKNOWLEDGMENT

본 연구는 2020년도 한국과학기술정보연구원(KISTI) 주요사업 과제로 수행한 것입니다.

참 고 문 헌

[1] Davies R. W." The Data Encryption standard in perspective,"Computer Security and the Data Encryption Standard, pp. 129-132.

[2] Miles E. Smid, "From DES to AES," 2000, (http//www.nist.gov/aes).

[3] Shamir, A. "On the security of DES," Advances in Cryptology, Proc.Crypto '85, pp. 280-285, Aug. 1985.

[4] NIST, "Announcing the Advanced Encryption Standard(AES),"FIPS PUB ZZZ, 2001, (http://www.nist.gov/aes).

[5] Daemen, J., and Rijmen, V. "AES Proposal: Rijndael, Version2.," Submission to NIST, March 1999.