클래스기반 KREONET 트래픽분석시스템 설계 및 구현

김승해
한구과학기술정보연구원
shkim@kisti.re.kr

Design and implementation of class-based KREONET traffic analysis system

Seunghae Kim
KREONET Center, Korea Institute of Science and Technology Information

요 약

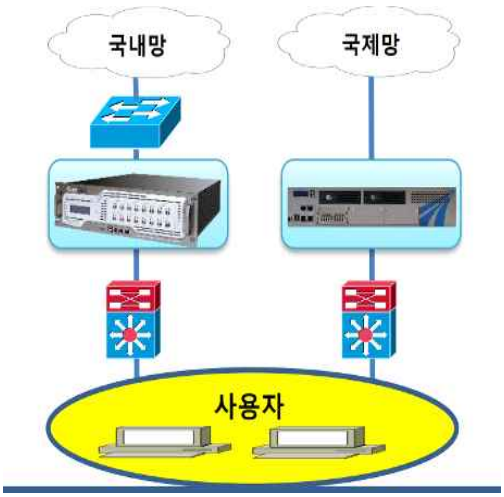
본 논문은 국가과학기술연구망 회원기관의 과학연구 및 범용 트래픽이 유통되는 국내 인터넷 교환노드와 국제 인터넷 게이트웨이 구간에 실시간으로 트래픽분석이 가능한 시스템을 설계하고 구현하였다. 또한 구현된 시스템을 통해 Class별 트래픽분석을 시행하여 현재의 트래픽 문제점과 개선 방안에 대한 고찰을 하였다. 본 시스템을 통해 클래스별 트래픽 분류 및 모니터링은 망운영 관점에서 매우 중요한 요소이며 안정적인 과학연구 트래픽의 유통을 보장할 수 있다.

Ⅰ. 서 론

국가 과학기술연구망(KREONET)[1]은 국가적인 과학기술분야의 대용량 데이터전송과 정보공유 그리고 실시간 글로벌 협업연구가 가능하도록 백본 인프라 제공하는 것을 목적으로 한다. 연구자나 첨단 연구그룹이 지속적으로 연구망서비스를 받기 위해서는 고대역폭의 백본인프라는 필수적인 요소이다. 하지만 한정된 예산과 회선 자원으로 고비용의 인터넷교환노드와 광백본인프라 고도화를 지속적으로 시행하기에는 매우 어려운 실정이다. 이에 따라 기존의 인프라를 좀더 효율적으로 운영하고 관리하기 위한 시스템 도입이 절실하였다. 서비스 품질시스템(QoS)[2]는 네트워크 또는 첨단응용연구 어플리케이션과 같은 특정 서비스의 전체 성능, 특히 사용자가 네트워크 성능에 대한 품질을 보장하거나 또는 트래픽의 추이 측정 및 분석을 하는 시스템이다. 서비스 품질을 정량적으로 측정하기 위해, 패킷 손실, 전송률, 처리량, 전송 지연, 가용성과 지터 등과 같은 네트워크 서비스의 여러 관련 측면 등이 고려된다. 불특정 사용자 과다점유, 비업무 트래픽 과다점유, 웹컨텐츠의 대용량화, 세션 및 웜 등의 보안 공격발생과 한정된 회선 등이 트래픽 관리를 어렵게 하는 요소들이다. 이러한 이유로 많은 네트워크 운영자들은 현재의 트래픽 추이와 트래픽의 특성을 분석하여 효율적인 제어정책을 개발하고, 실시간으로 트래픽 제어와 관리가 가능한 시스템이 필요하였다. 네트워크 트래픽 분류는 네트워크에 존재하는 네트워크 응용 프로그램 또는 프로토콜을 식별하는 프로세스이다. 지난 20여 년 동안 네트워크 트래픽 분류는 매우 중요하였다. 많은 논문에서는 네트워크 애플리케이션을 분류하는 많은 방법을 제안했습니다.[3][4] 포트 기반 기술, 페이로드 기반 기술 및 기계 학습 (ML)[5] 기술 등 이 소개되었다. 본 논문에서는 200여 개 과학기술연구망 회원기관의 과학연구와 범용인터넷 트래픽이 유통되는 국내 인터넷교환노드와 국제 인터넷 게이트웨이 구간에 실시간으로 트래픽분석이 가능한 시스템을 설계하고 구현하였다. 또한 구현된 시스템을 통해 Class별 트래픽분석을 시행하여 현재의 트래픽 문제점과 개선방안에 대한 고찰을 하고자 한다.

Ⅱ. 시스템 설계 및 구현

본 KREONET 트래픽분석시스템은 KREONET 회선 대역폭 안에서 발생하는 트래픽에 대한 명확한 실체 파악과 비정상 트래픽에 대한 분석 및 제어를 통하여 한정된 회선 대역폭 안에서의 최대 효율 사용을 목적으로 설계하였다. 특히 기본적인 정책기반 트래픽 특성 분석과 클래스별 QoS[3]를 통한 제어가 가능하도록 설계하였다. 일시적인 고용량 어플리케이션 활용에 따른 병목현상이나 사용자 체감속도 저하를 막고 위기관리가 가능한 시스템으로 설계하였다. 그림 1과 같이 KREONET 연구 회선을 사용하는 사용자 기준으로 트래픽 집선구간 국내망(8Gbps), 국제망(2Gbps) 회선구간에 각 1대 QoS 구성하였다. 본 구성은 Auto Bypass 활용으로 QoS 장비 이슈 상황 시에 즉각 Bypass 되어 회선 구간 영향 최소화 방안을 적용하였다.



(그림 1) KREONET 트래픽분석시스템 구성도

Ⅲ. 트래픽 추이 및 분석

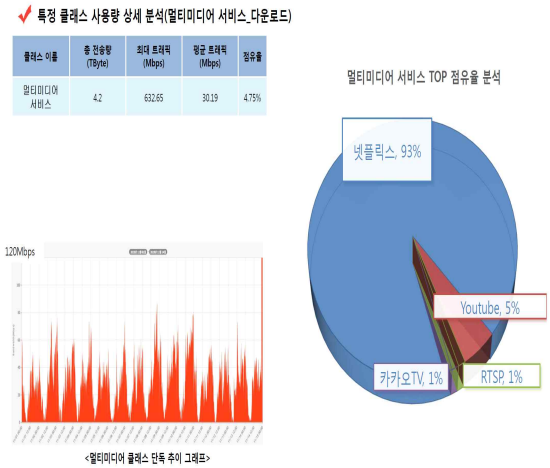
본 논문에서 구현된 시스템을 활용하여 2019년 11월 1일부터 14일까지 약 14일간 KREONET의 인터넷교환노드(8G)구간의 유입트랙픽을 분석하였다. 이를 토대로 그림2는 클래스별 다운로드 트래픽 통계자료로써, 클래스별로 사용 통계를 확인이 가능하다. 클래스란 사용자가 특정 조합을 필터로 담고 있는 그룹으로 특정 트래픽이나 어플리케이션을 그룹화할 수 있다. 본 통계분석을 보면 각 회선별 Peak 전송량(단위: Mbps)이 높은 서비스 그룹이 빨간색으로 표현되어있다. Peak 전송량이란 분석기간중 가장 사용량이 많았던 1분 평균값 표현으로써, Peak 전송량이 높다는 것은 언제든 순간적인 과점유 트래픽발생으로 대역폭을 모두 사용하여 병목현상 발생 및 네트워크 서비스 장애를 유발시킬 가능성이 높다. 이런 클래스는 중요도에 따라 대역폭을 제어(대역폭제한, 사용자 한명당 대역폭 제한 등)하여 발생할 수 있는 이슈를 사전 방지하는 것을 고려해볼 수 있다. 본 분석에서는 네트워크그룹(NTP) (43.9%)와 웹그룹 클래스(33.8%)가 가장 많은 트래픽을 유발하고 있으며, 멀티미디어서비스(4.6%), Update서비스(1.4%), 파일전송서비스(1.8%), P2P(1%)를 점유하고 있음을 알 수 있다. 특히 빨간색 표시 클래스에 대해서는 향후 대역폭 제한 또는 IP당 대역폭 적용을 검토해볼 필요가 있음을 알 수 있다.

클래스별 통계 리스트 (단위 : Mbps) (단위 : Mbps)

범례	CLASS 이름	총전송량(bytes)	Peak 전송량	Peak 시간	초당전송량	비율
	전체	296,814,135,015,386	4,813.76	11-13 09:40~09:49	1,963.06	
	미등록클래스	101,446,982,196	40.04	11-01 15:50~15:59	0.67	0.03%
	웹그룹	100,435,682,103,447	2,940.47	11-13 09:10~09:19	664.26	33.84%
	HTTP_WEB	70,377,418,060,499	2,404.68	11-12 14:00~14:09	465.46	23.71%
	HTTP_DOWN	28,909,437,102,555	1,549.27	11-13 09:10~09:19	191.20	9.74%
	HTTP_APP	49,513,688,590	46.62	11-07 17:30~17:39	0.33	0.02%
	HTTP_MAIL	53,918,500,510	134.86	11-14 17:30~17:39	0.36	0.02%
	증권	0	0.00	00:00	0.00	0.00%
	SNS	1,041,156,844,640	56.22	11-01 13:50~13:59	6.89	0.35%
	PHOTO	14,746,989	1.55	11-11 15:50~15:59	0.00	0.00%
	P2P서비스	3,220,517,257,059	482.21	11-12 00:20~00:29	21.30	1.09%
	웹하드그룹	316,419,028,776	312.25	11-06 16:00~16:09	2.09	0.11%
	파일전송서비스	5,410,868,634,979	904.37	11-06 13:20~13:29	35.79	1.82%
	게임서비스	616,026,422,311	767.73	11-05 21:20~21:29	4.07	0.21%
	메신저서비스	28,072,041,796	31.61	11-11 10:30~10:39	0.19	0.01%
	멀티미디어서비스	13,696,227,640,075	567.62	11-03 23:50~23:59	90.58	4.61%
	UPDATE서비스	4,241,475,422,027	647.39	11-04 09:30~09:39	28.05	1.43%
	VoIP	196,906,412,910	35.25	11-06 21:00~21:09	1.30	0.07%
	인터넷품질측정서비스	977,191,680	81.53	11-12 14:40~14:49	0.01	0.00%
	네트워크그룹	130,499,473,177,924	1,385.34	11-06 21:10~21:19	863.09	43.97%
	DB_터미널	9,381,333,765,534	677.13	11-05 18:00~18:09	62.05	3.16%
	TCP_Nego	692,010,130,432	196.87	11-04 01:00~01:09	4.58	0.23%
	메일	1,731,057,099,327	387.11	11-06 02:00~02:09	11.45	0.58%
	은행_보안프로그램	111,910,794,420	23.49	11-04 14:40~14:49	0.74	0.04%
	Other_UDP	7,048,583,707,319	437.18	11-11 14:50~14:59	46.62	2.37%
	Other_TCP	17,914,788,233,693	991.10	11-04 09:20~09:29	118.48	6.04%

(그림 2) 국내 Inbound 트래픽 추이 및 통계분석

그림 3은 KREONET 트래픽 분석시스템을 통해 추출한 특정클래스 사용량의 상세분석이다. 특별히 멀티미디어서비스 클래스에 대한 사용량 분석을 보여주고 있다. 본 시스템으로 측정 당시에 전체 서비스 클래스중 멀티미디어 서비스가 차지하는 비중은 약 4.75%였으며 어플리케이션은 넷플릭스(93%), Youtube(5%), 카카오TV(1%), RTSP(1%)의 상세 추세를 보여주고 있다. 이와 같이 본 시스템을 활용하여 클래스별로 통계리스트를 분류하여 특정 IP나 특정 트래픽 쏠림현상을 사전에 예방할 수 있다. 이와 더불어 향후 축적된 연구망의 빅데이터에 기반한 기계학습을 통해 트래픽추이 및 예방관리가 가능한 운영시스템으로 진화 가능성이 향상되었다.



(그림 3) 멀티미디어서비스 클래스 사용량 분석 결과

Ⅳ. 결과 및 고찰

본 시스템은 KREONET 회선 대역폭 안에서 발생중인 트래픽을 실시간으로 분석하여 클래스별 제어 및 향후 고도화를 위한 기초자료로 활용이 가능하다. 현재의 시스템상의 결과를 분석해보면 비중요 및 비정상 트래픽이 다소 발생하여 고가의 회선을 점유함을 파악할 수 있다. 국내 인터넷교환노드의 경우 대역폭 제한 설정과 사용자 체감서비스에 대한 대역폭 보장설정이 필요할 것으로 판단된다. 국제회선의 경우 대역폭이 모두 소진됨에 따른 병목구간이 다소 예측된다. 특히 국제망 게이트웨이의 2개 라인중 1개 라인이 가용성 측면에서 떨어지는 것을 발견할 수 있었다. 비중요 트래픽이나 비정상 트래픽은 점검후 제어를 시도하거나 회원기관의 협조를 통해 제한이 가능하다. 본 시스템을 통해 클래스별 트래픽 분류 및 모니터링은 망운영관점에서 매우 중요한 요소이며 안정적인 트래픽의 유통을 보장할 수 있다. 향후 본 시스템을 통해 축적된 빅데이터를 기반으로 주요 서비스별 트래픽제어 및 효율적인 서비스 운영관리, 효율적인 트래픽 관리, 실시간 현황분석을 통한 네트워크 품질을 향상함으로써 연구망 서비스품질 향상 및 백본고도화에 대한 정책설계에 기여할 것으로 기대한다.

참 고 문 헌

[1] Homepage, http://www.kreonet.net.

[2] Y. Snir, Y. Ramberg, et. Al, “Policy Quality of Service (QoS) Information Model,” RFC3644, Nov. 2003..

[3] T. Nguyen and G. Armitage, "A Survey of Techniques for Internet Traffic Classification using Machine Learning", IEEE Surveys and Tutorials, vol. 10, no. 4, pp. 56-76, 2008.

[4] J. Korhonen, H. Tschofenig, et. Al, “Traffic Classification and Quality of Service(QoS) Attributes for Diameter,” RFC5777, Feb. 2010.

[5] M. Shafiq, et. Al, “Network Traffic Classification techniques and comparative analysis using Machine Learning algorithms”, 2016 2nd ICCC, Oct, 2016