한국전력 데이터통신망 트래픽 분석 시스템 개발

오도은[0] 박명혜 성기혁 이진기 조선구
한전 전력연구원 정보통신그룹
{hifive[0], pmh, ghsung, jklee, csk9306}@kepri.re.kr

Network Traffic Analysis System for KEPCO's Data Telecommunication Network

Do-Eun Oh[0] Myoung-Hye Park Gi-Hyeok Sung Jin-Kee Lee Sun-Ku Cho
Information & Telecommunication Group, KEPRI

요 약

최근 업무 전산화로 인한 분산 컴퓨팅 환경이 확대되고 네트워크 기반의 응용 서비스들이 다양하게 개발됨에 따라 네트워크 트래픽은 증가 일로에 있으며 어느 호스트에서 어떤 형태의 트래픽이 얼마만큼 유발되는지를 알아내는 일은 한정된 네트워크 자원을 효율적으로 활용하는데 매우 중요한 일이 되었다. 하지만, 현재의 네트워크관리시스템들은 트래픽 모니터링에 따른 통계값 제공 등의 단순 평면적인 정보만을 제공할 뿐, 네트워크를 정밀 분석하고 그에 따른 대책을 마련하기에는 미약하다. 따라서 효율적인 네트워크 자원 활용을 위하여 네트워크 트래픽을 자세히 분석하며, 네트워크 계층별, 지역별, 호스트별 및 응용 서비스별로 트래픽을 측정 및 분석할 수 있는 시스템의 개발이 필요하다.

본 논문은 한국전력 데이터통신망을 대상으로 네트워크 트래픽의 발원지로부터 목적지까지의 백본 및 LAN 구간에서의 트래픽을 플로우별로 수집, 분석할 수 있는 트래픽 분석 시스템을 설계 및 구현하였다. 본 시스템은 트래픽 측정을 위해 백본에서는 Netflow 기능을 이용하며, LAN 구간에서는 패킷 캡처 방식의 Probe를 이용한다. 이 때 기존의 패킷 캡처 방식의 기능을 개선하여 이를 플로우화 함으로써 LAN 구간에서도 동일한 인터페이스를 통하여 네트워크 트래픽을 분석할 수 있게 하였다.

1. 서 론

현재 한국전력 통신망은 전력의 안정적인 공급을 위한 송변전자동화망, 배전자동화망 등의 전력 수급용 전용 통신망과 사내 업무 지원을 위한 데이터통신망, IBM 온라인망, 사내 방송망 등 다양한 종류의 통신망이 구축, 운용되고 있으며, 이들 통신망을 이용한 다양한 종류의 통신서비스를 제공하고 있다. 이 가운데 사내 업무 전산화에 따른 네트워크 기반의 각종 응용 서비스들을 제공하고 있는 데이터통신망은 인터넷의 폭발적인 증가와 함께 최근의 업무 환경이 클라이언트/서버 모델의 분산 컴퓨팅 환경으로 변화함에 따라 네트워크 트래픽이 증가 일로에 있다. 이에 따라 어느 곳에서, 어떤 형태의, 얼마나 많은 트래픽이 유발되고 소모되는지를 알아내는 일은 한정된 네트워크 자원을 효율적으로 활용하기 위한 네트워크 관리자들에게 당면한 중요한 과제가 되었다. 하지만, 현재의 네트워크관리시스템들은 트래픽 모니터링에 따른 단순 평면적인 통계 자료 만을 제공할 뿐, 네트워크를 정밀 분석하고 그에 따른 대책을 마련하기에는 미약하다.

본 논문은 효율적인 네트워크 자원 활용을 위하여 네트워크 트래픽을 자세히 분석하며, 네트워크 계층별, 지역별, 호스트별 및 응용 서비스별로 트래픽을 측정 및 분석할 수 있는 시스템을 설계 및 구현하였다. 이 시스템은 한국전력 데이터통신망을 대상으로 백본에서 LAN 구간에 이르기까지 네트워크 트래픽의 발원지로부터 목적지까지의 트래픽을 플로우별로 수집하여 종합 분석할 수 있다.

2. 관련 연구

본 장에서는 플로우의 개념을 알아보고 기존에 소개된 Netflow 기반 트래픽 측정 도구들의 특성과 장단점을 비교 한다.

2.1 플로우

플로우는 송신자에서 수신자로의 단방향성 패킷의 흐름으로 정의되는 것으로, 플로우의 구분은 IP 주소와 Port 번호로 이루어진다.[1]

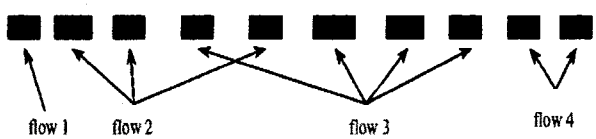


그림 1. 플로우(flow)

2.2 Netflow 기반 트래픽 측정 도구

2.2.1 FlowScan

Netflow 정보를 바탕으로 원하는 기간만큼의 프로토콜별, 응용 서비스별 네트워크 사용에 대한 시간 축 상의 그래프를 그려낸다. 또한 Custom graph, Top AS usage, Top user, Raw flow dump 등 대부분의 유용한 분석이 가능한 것이 장점이다. 하지만 시각화된 정보 이외의 통계 데이터를 얻기 힘들다.

2.2.2 Cflowd

Netflow로부터 얻은 플로우 정보를 수집하여 Arts++ 형태의 파일로 저장한다. 기본적으로 수집부분만 담당하며, 분석은 Arts utility를 이용해 몇 가지 정해진 통계 정보를 텍스트 형태로 얻어낼 수 있다.

2.2.3 MADAS

MIRNET-STARTAP 사이의 트래픽 측정을 위해 러시아에서 개발한 트래픽 측정 도구로 실시간 그래프 기능과 쿼리 인터페이스가 가능한 이상적인 도구이다. MADAS는 국가간 트래픽 측정에 초점이 맞추어져 있다. 이는 다른 측정 도구에는 없는 특이한 기능인데 AS를 바탕으로 국가간 트래픽을 분석해 낸다는 점에서 백본망에 어울리는 기능이라 할 수 있다. 쿼리의 결과가 그래프로 나타내지는 장점이 있긴 하지만, 응용 서비스별 분석이 불가능 한 점은 취약한 부분이다.

2.2.4 Flowtools

Cflowd & ARTS와 비슷한 기능을 한다. Netflow로부터 정보를 모아 미리 정해진 20가지의 통계 정보를 얻어낼 수 있다. CGI를 사용해 웹에서 쿼리가 가능하지만 기본적으로 커맨드 기반의 프로그램이다.

2.2.5 NetFlow FlowCollector

CISCO에서 개발한 상업용 Netflow 기반 트래픽 측정 도구이다. Netflow 트래픽을 export device로부터 수집하고 가공하여 저장하는 역할을 한다. 저장된 데이터는 Netflow DataAnalyzer와 같은 다른 Netflow 응용프로그램에 의해 사용될 수 있다. Thread와 Filter라는 기능에 의한 집합에 의해 사용자가 원하는 정보를 정확하고 간결하게 저 용량으로 저장할 수 있고, 플로우를 다양한 방법으로 집합할 수 있다. 또한 호스트, 라우터, AS, 프로토콜, 포트 등 다양한 방법으로 데이터를 집합해서 저장할 수 있다. 그러나 상용 트래픽 측정 도구로 매우 고가이며, Raw data 분석이 용이하지 못한 단점이 있다.

2.2.6 NetFlow DataAnalyzer

CISCO에서 개발한 상업용 NetFlow 기반 트래픽 측정 도구로 Netflow FlowColletor에 의해 수집, 집합, 저장된 Netflow 데이터를 받아와서 시각화한다. Netflow FlowCollector에게서 데이터를 받아오는 형식이므로 Netflow FlowCollector에서 어떻게 설정을 해서 데이터를 수집했는지가 중요하다. 여러 가지 집합으로 데이터를 볼 수 있게 하며 Time Slider, AS Drilling Down, Search 등의 특수한 기능도 제공 한다. 그래프에서 시간축으로 전체 트래픽이 표시가 안 되고, 웹이 지원이 안되며 느리다는 단점이 있다.[2]

3. 시스템 구성

한국전력 데이터통신망은 크게 본사와 전국 주요 거점 사업소를 연결하는 백본망과 각 거점사업소에 연결된 LAN으로 구성되어 있다. 본 시스템은 트래픽 측정을 위해 백본망에서는 Netflow 기능을 이용하며, LAN 구간에서는 패킷 캡처 방식의 Probe를 이용한다. 이 때 기존의 패킷 캡처 방식의 기능을 개선하여 이를 플로우화 함으로써 LAN 구간에서도 동일한 인터페이스를 통하여 네트워크 트래픽을 분석할 수 있게 하였다.

3.1 백본망 트래픽 분석

백본망의 트래픽 측정을 위해 Netflow 기능을 이용하며, 기존의 Netflow 기반 트래픽 측정 도구들 가운데 쿼리 인터페이스와 시각화 기능을 동시에 가지고 있는 도구가 존재하지 않으므로 본 시스템은 두 가지 기능을 모두 가지도록 기존의 Cflowd를 개선하였다. 이 때 Cflowd의 텍스트 기반 저장 형태를 데이터베이스 저장 형태로 변경함으로써 그래픽을 포함한 웹 기반의 사용자 환경을 구축할 수 있게 하였다. 이는 또한 실시간 트래픽 분석이 가능하다는 장점을 가진다.

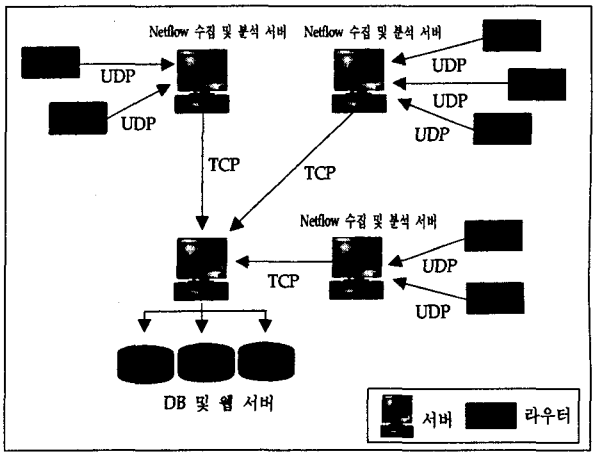
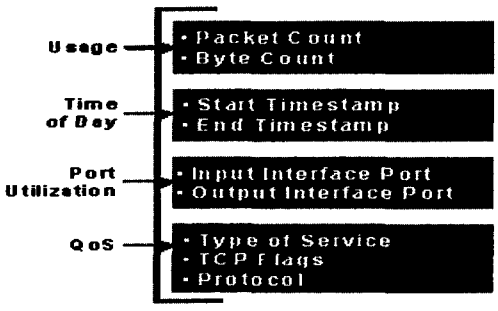


그림 2. Netflow 기반 트래픽 분석 시스템 구성도

Netflow 기반 트래픽 분석에서는 다음 7가지 기준으로 패킷을 플로우로 분류하고 이에 대한 정보를 저장한다.

- Source Address
- Destination Address
- Source Port
- Destination Port
- Layer 3 Protocol
- Type Of Service(TOS) Byte
- Input Interface



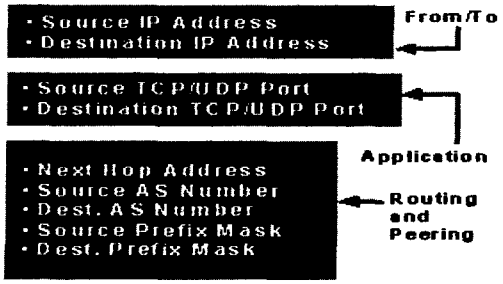


그림 3. Netflow 기반 트래픽 분석 정보

그림 2와 그림 3은 Netflow 기반 트래픽 분석 시스템 구성도와 Netflow 기반 트래픽 분석 정보를 보여준다.

3.2 LAN 구간 트래픽 분석

LAN 구간에서는 패킷 캡처 방식의 Probe를 이용하였으며, 이 때 기존의 패킷 캡처 방식의 기능을 개선하여 이를 플로우화 함으로써 LAN 구간에서도 동일한 인터페이스를 통하여 네트워크 트래픽을 분석할 수 있게 하였다. 그림 4는 Probe 기반 트래픽 분석 시스템 구성도를 보여준다.

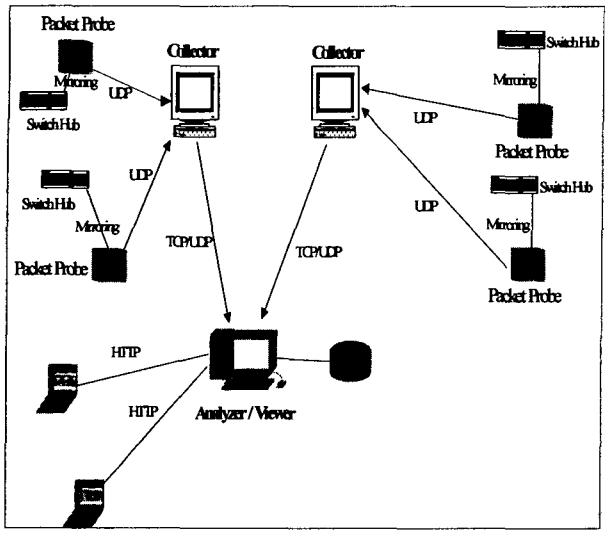


그림 4. Probe 기반 트래픽 분석 시스템 구성도

Probe 기반 트래픽 분석에서는 다음 5가지 기준으로 패킷을 플로우로 발생시켜 정보를 저장한다.

- Source Address
- Destination Address
- Source Port
- Destination Port
- Layer 3 Protocol

그림 5는 Probe 기반 트래픽 분석 정보를 보여준다.

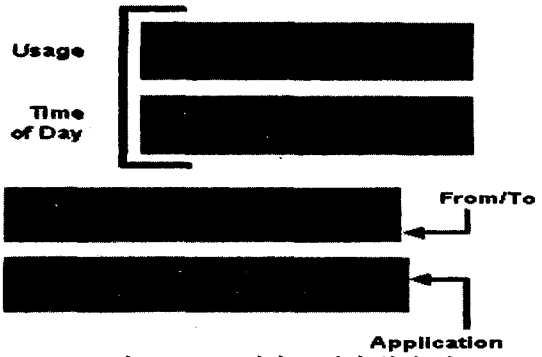


그림 5. Probe 기반 트래픽 분석 정보

3.3 구현

그림 6은 포트별 트래픽 분석 결과를 파이 그래프 형태로 보여준다.

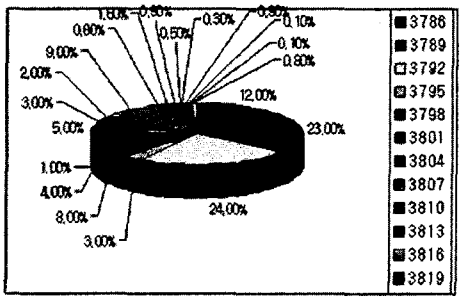


그림 6. 포트별 트래픽 분석 결과

4. 결론

네트워크 기반의 다양한 응용 프로그램 개발에 따른 급속한 네트워크 트래픽 증가로 네트워크 트래픽 유발량과 네트워크 계층별, 지역별, 호스트별 및 응용 서비스별 트래픽 정보 분석은 한정된 네트워크 자원을 효율적으로 활용하는데 매우 중요한 일이 되었다.

본 논문은 한국전력 데이터통신망을 대상으로 효율적인 네트워크 자원 활용을 위한 네트워크 트래픽 분석 시스템 개발하였다. 본 논문은 Netflow 기반 트래픽 측정 도구들에 대해 정리하고 궁극적으로 네트워크 트래픽 분석 시스템 구성 및 개발에 대해 소개하였다.

5. 참고문헌

[1] 전력연구원, "트래픽 측정 및 분석 기술", TM.01PJ16.P2002.274, 2002. 5

[2] KAIST, "Passive Measurement Tool의 분석과 적용", 중간보고서, 2001. 9

[3] 정재훈, 이순윤, 김용진, 인터넷 트래픽 측정방법 및 시스템, 전자통신동향분석 제16권 제5호 2001년 10월

[4] Netflow, http://www.cisco.com/

[5] Cflowd, http://www.caida.org/