트래픽 분산 그래프 기반의 비정상 트래픽 탐지

정태열 O,1, Le Quoc Do[2], 홍원기 [1,2]

포항공과대학교 [1]컴퓨터공학과, [2]정보전자융합공학부

{dreamerty, lequocdo, jwkhong}@postech.ac.kr

요 약

네트워크의 안정적인 관리를 위해서 비정상 트래픽을 초기에 탐지하고 대응하는 것은 매우 중요하다. 하지만 네트워크에서 발생하는 트래픽의 양이 점점 증가하고 네트워크 공격 방법이 날로 다양해지면서 기존의 비정상 트래픽 탐지 방법들은 많은 한계를 보이고 있다. 이에 따라 본 논문에서는 트래픽 분산 그래프라는 그래프 모델을 기반으로 인터넷 트래픽에서 호스트들 사이의 커뮤니케이션 패턴을 표현하고 이를 활용하여 비정상 트래픽 탐지 뿐만 아니라 해당 비정상 트래픽을 유발한 네트워크 공격의 종류를 판단할 수 있는 방법을 제안하고 이를 실제 DDoS Trace 에 적용하여 그 타당성을 검증한다.

1. 서론

인터넷의 규모가 지속적으로 커지면서 비정상 트래픽을 탐지하고 대응하기 위해 네트워크 관리자의 입장에서 보안의 중요성이 날로 커지고 있다. 비정상 트래픽은 서비스 거부 공격(DoS), 포트 스캔, 인터넷 웜 같은 다양한 원인에 의해 발생할 수 있는데 이러한 비정상 트래픽들은 네트워크의 정상적인 기능에 심각한 영향을 초래한다. 따라서 비정상 트래픽 탐지는 네트워크 보안 인프라에서 뺄 수 없는 중요한 요소이다. 하지만 실질적으로 비정상 트래픽을 유발하는 위협들을 탐지하고 판별하는 것은 쉬운 일이 아니다. 현재까지 사용되어 온 비정상 트래픽 탐지 기법들은 주로 기계 학습, 데이터 마이닝, 통계적 분석에 기반한 것이었지만 이러한 방법들은 인터넷 트래픽을 분석하는데 많은 시간이 소모되거나 종종 잘못된 알람을 생성하기 때문에 이를 보완할 수 있는 새로운 접근 방법이 필요하다. 지난 10 년 동안 Complex network 의 개념은 컴퓨터 공학, 사회학, 생물학 등 다양한 분야에서 연구되어 왔는데 이들 학문 분야들은 네트워크가 형성하고 있는 구조적인 특성들을 분석하는데 주력해 왔다. 본 연구에서는 이와 비슷한 관점을 인터넷 트래픽에 적용하여 비정상 트래픽 탐지에 활용하고자 한다.

본 논문에서 비정상 트래픽은 Traffic Dispersion Graph (TDG), 트래픽 분산 그래프 라는 그래프 모델을 사용해 탐지되는데 트래픽 분산 그래프로부터 네트워크의 특성을 표현할 수 있는 변수들을 추출하고 이를 활용해 네트워크 내에 비정상 트래픽 존재 유무를 결정 짓는다 [1]. 변수 추출은 정적 변수와 동적 변수 두 가지로 이루어진다. 정적 변수는 그래프가 특성 시점에서 가지는 정적인 특성을 나타내고 동적 변수는 시간에 따라 변화하는 그래프의 정도를 표현한다. 비정상 트래픽이 탐지 되었다면 부분 그래프 매칭 알고리즘을 사용해 비정상 트래픽을 유발한 공격 종류를 판단한다. 본 연구에서는 DDoS 공격을 당할 당시의 CAIDA Trace[2]에 나타나는 비정상 그래프가 POSTECH Trace 에 존재함을 확인함으로써 부분 그래프가 공격 종류를 판단하는 데 활용될 수 있음을 보였다.

2. 관련 연구

Iliofotou 는 네트워크 노드들의 커뮤니케이션 패턴을 표현할 수 있는 Traffic Dispersion Graph(TDG) 즉 트래픽 분산 그래프를 소개하고 네트워크 트래픽을 트래픽 분산 그래프를 기반으로 분석하여 서로 다른 어플리케이션을 분류하는데 사용하였다 [3]. 본 논문에서는 트래픽 분산 그래프를 네트워크 트래픽을 표현하기 위한 그래프 모델로 사용하여 비정상 트래픽을 탐지하였다.

많은 논문들에서 그래프 매칭 알고리즘을 사용하여 네트워크에서 공격 패턴을 탐지하려는 시도들이 연구되어왔다 [4, 5]. 하지만 이 논문들에서는 그래프 매칭 알고리즘을 전체 네트워크 트래픽에 바로 적용하기 때문에 계산 시간이 너무 많이 소모된다는 문제점이 존재한다. 본 논문에서는 비정상 트래픽이 탐지되었을 경우에만 그래프 매칭 알고리즘을 적용하기 때문에 계산해야 할 트래픽의 양을 대폭 감소시켰다.

그래프 기반으로 네트워크 트래픽을 분석 하기

본 연구는 한국연구재단을 통해 교육과학기술부의 세계수준의 연구중심대학육성사업(WCU)으로 부터의 지원 (R31-2010-000-10100-0) 및 2011 년도 정부(교육과학기술부)의 재원으로 한국연구재단-차세대정보컴퓨팅기술개발사업의 지원 (No. 2011-0020518)을 받아 수행되었습니다.

위해 다양한 정적 변수들이 사용될 수 있는데 특히 Node degree 값으로부터 상당히 많은 정보들을 얻을 수 있다. 트래픽 분산 그래프 모델에서는 In-node 와 Out-node 를 구분할 수 있기 때문에 한 노드가 얼마나 많은 노드들과 커뮤니케이션 하는지, 그리고 그 커뮤니케이션 방향은 어떻게 되는지를 Node degree 를 통해 확인할 수 있다. 본 논문에서는 그래프의 최대 Node degree 를 나타내는 Kmax 값을 비정상 트래픽 탐지를 위한 정적 변수로 사용하였다.

시간에 따라 변화하는 두 그래프의 차이를 추적할 수 있는 동적 변수들도 네트워크 트래픽 분석에 유용하게 활용될 수 있다. 그 중 dK-2 동적 변수는 두 그래프의 Joint Degree Distribution 을 나타내는데 이는 두 그래프의 연관 정도를 양적으로 표현하기 위한 변수이다 [6, 7]. 본 논문에서는 매 분마다 변화하는 dK-2 값 사이의 Euclidean Distance 값을 의미하는 dK-2 Distance 를 비정상 트래픽과 정상 트래픽을 구분하기 위해 동적 변수로 사용하였다.

3. 비정상 트래픽 탐지 및 공격 종류 판별

3 장에서는 본 논문에서 제안하는 그래프 기반의 비정상 트래픽 탐지 방법 및 공격 종류 판별에 대해 구체적으로 살펴보고자 한다. 여기서 비정상 트래픽은 DoS/DDoS 공격, 인터넷 웜, 네트워크 스캐닝 등 공격자의 악의적인 의도에 의해 발생하는 트래픽으로 한정하고 이를 탐지하기 위한 방법에 대해 논의 한다.

제안하는 비정상 트래픽 탐지 시스템은 그림 1 에서 볼 수 있는 것과 같이 크게 두가지 모듈로 구성되어 있다. 첫 번째는 인터넷 트래픽이 정상인지 비정상 인지를 판단하는 것이고 두 번째는 앞서 인터넷 트래픽이 비정상으로 판단 되었다면 해당 비정상 트래픽을 유발한 공격의 종류를 판별하는 과정이다. 비정상 트래픽 탐지 모듈은 인터넷 트래픽 모니터링 시스템으로부터 플로우 정보를 받아서 플로우 정보로부터 트래픽 분산 그래프를 얻는다. 비정상 트래픽 탐지 모듈은 트래픽 분산 그래프에서 정적 및 동적 변수를 분석해 현재 인터넷 트래픽이 비정상 유무를 판단하는 역할을 한다. 공격 종류 판별 모듈은 다양한 원인에 의해 발생할 수 있는 비정상 트래픽이 어떠한 종류의 공격에 의해 생겨난 것인지를 판단하는 모듈이다.

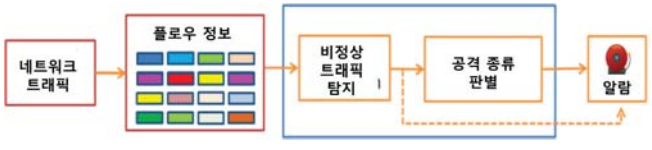

그림 1. 전체 시스템의 구조

3.1 비정상 트래픽 탐지

비정상 트래픽 탐지 단계에서 네트워크 트래픽은 매 분 마다 샘플링 되고 그에 상응하는 트래픽 분산 그래프 가 매 분마다 얻어진다. 시스템은 매 분마다 생성되는 트래픽 분산 그래프에서 그래프 변수들을 계산하고 그 값들에 근거하여 트래픽의 비정상 여부를 결정한다. 이러한 비정상 트래픽 탐지 단계는 그림 2 와 같이 크게 4 단계로 이루어져 있다.

- 1 단계 : 네트워크 트래픽을 샘플링하고 플로우 정보를 얻는다.
- 2 단계 : 플로우 정보로부터 매 분마다의 트래픽 분산 그래프를 얻는다.
- 3 단계 : 트래픽 분산 그래프에서 인접 행렬 정보를 계산하고 그로부터 정적 및 동적 그래프 변수 값을 계산한다.
- 4 단계 : 트래픽 분산 그래프에서 얻은 그래프 변수 값들을 비정상 트래픽을 결정짓는 Threshold 값과 비교한다. 만약 그래프 변수 값들이 Threshold 값보다 크다면 비정상 트래픽으로, Threshold 값보다 작다면 정상 트래픽으로 간주한다.

NG-MON 시스템 [8]은 네트워크 트래픽을 모니터링하고 그로부터 플로우 정보를 생성하여 데이터베이스에 저장하기 위해 사용되었다. 데이터베이스에 저장 된 플로우 정보는 DOT 포맷의 형태로 변형되어 트래픽 분산 그래프를 그리는데 사용된다 [9]. DOT 포멧으로 플로우 정보를 표현한 후 비정상 트래픽 탐지에 사용되는 그래프 변수 값들을 계산하기 위해 그래프의 인접행렬 값들을 계산한다.

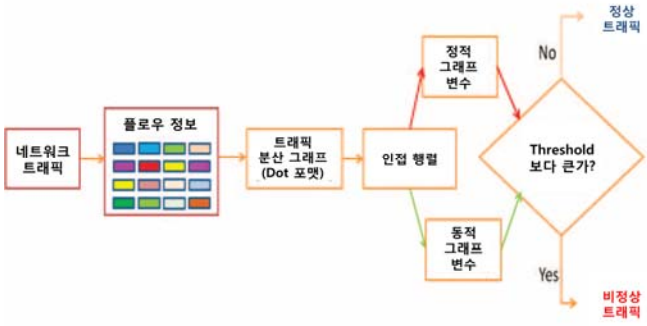

그림 2. 비정상 트래픽 탐지 과정

비정상 트래픽을 판단하기 위한 Threshold 값은 POSTECH 네트워크에서 장기간 모니터링 한 트래픽을 기준으로 설정하였다. 연속적인 트래픽 분산 그래프 G_i 와 G_{i+1} 의 dK-2 Distance 값을 얻기 위해

Joint Degree Distribution 알고리즘 [10]이 사용되었고 이를 두 개의 연속적인 트래픽 분산그래프의 인접 행렬에 적용한다. 이후 두 Joint Degree Distribution $JDD(G_i)$ 와 $JDD(G_{i+1})$ 사이의 Euclidean Distance 가 계산된다. 네트워크 트래픽의 시각화를 위해 Graphviz Library 를 사용하여 노드들의 커뮤니케이션을 형상화 하였다 [11].

3.2 공격 종류 판별

네트워크에서 비정상 트래픽은 DoS/DDoS 나 인터넷 웜 같은 다양한 이유에 의해 발생할 수 있다. 공격 종류 판단 모듈은 앞서 비정상 트래픽 탐지 과정에서 비정상으로 탐지된 트래픽이 어떤 공격에 의해 발생한 것인지를 판단한다. 기존에 잘 알려진 네트워크 공격들의 공격 패턴을 파악하고 그것을 공격 종류 판단에 사용하기 위해서 그림 3 와 같은 과정이 필요하다. 본 연구에서는 그림 4 와 같이 DDoS CAIDA Trace 로부터 DDoS 공격 패턴을 추출하고 이를 DDoS 공격 판단을 위한 비교 대상으로 사용하였다. DDoS 외에도 다양한 네트워크 공격들의 커뮤니케이션 패턴을 정의하여 공격 종류 판단에 사용할 수 있다. 본 논문에서 비정상 트래픽에 포함된 공격의 종류를 탐지하는 과정은 부분 그래프 매칭 알고리즘을 사용하여 기존에 알고 있던 공격 패턴이 비정상 트래픽 TDG 내에 포함되어 있는지를 판단함으로써 이루어진다. 부분 그래프 매칭을 위해서 다른 부분 그래프 매칭 알고리즘에 비해 가장 좋은 효율을 보이는 VF2 알고리즘이 사용되었다 [12, 13].

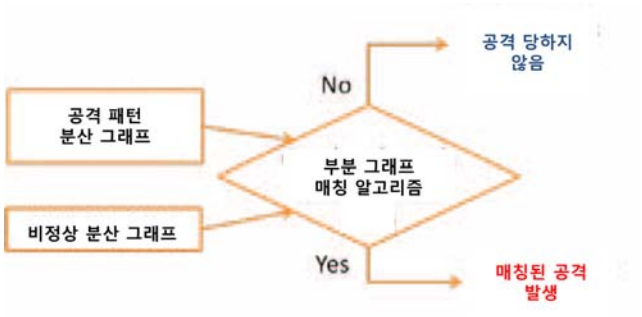

그림 3. 공격 종류 탐지 과정

기존 연구에서는 공격 패턴을 전체 네트워크 트래픽에 직접 매칭시켜 공격이 존재하는지 판단했지만, 본 논문에서는 먼저 비정상 트래픽을 판별한 후 VF2 알고리즘을 적용하기 때문에 대용량의 트래픽에 대해서도 훨씬 빠른 계산이 가능하다.

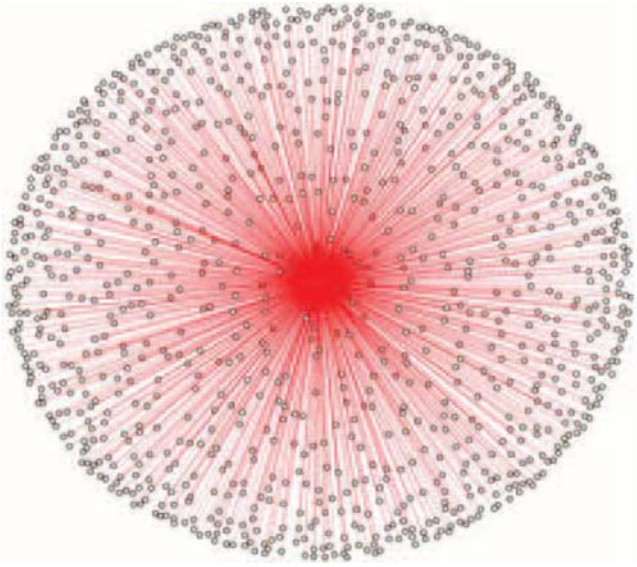

그림 4. CAIDA Trace 의 DDoS 공격 패턴

4. 결과 및 검증

제안한 시스템이 정상적으로 비정상 트래픽을 탐지할 수 있는지 검증하기 위해 2009 년 7 월 7 일 저장된 POSTECH Trace 가 사용되었다. 당시 POSTECH 네트워크 내에는 DDoS 공격에 이용된 다수의 좀비 PC 들이 존재했었고 POSTECH Trace 에는 DDoS 공격에 참여한 좀비 PC 들의 트래픽이 포함되어 있다. 검증을 위해 POSTECH Trace 는 1 분 단위로 샘플링 되었고 매 분마다 그에 해당하는 트래픽 분산 그래프를 얻었다.

그림 5 와 그림 6 은 비정상 트래픽 탐지를 위해 Kmax 와 dK-2 Distance 값을 사용하여 1 시간 동안의 POSTECH 트래픽을 분석한 결과이다. 2 분, 22 분, 23 분의 시각에 Kmax 값과 dK-2 Distance 값이 급변하는 것으로 보아 해당 시각에 비정상 트래픽이 발생했던 것을 확인할 수 있다. 그림 7 에서 볼 수 있는 것처럼 발생한 패킷의 수를 이용하는 기본적인 통계기반 분석의 경우 비정상 트래픽과 정상 트래픽의 차이가 크지 않아 판단에 어려움이 따른다. 그에 반해 그림 5, 그림 6 에서는 비정상 트래픽과 정상 트래픽의 구별이 확실하게 드러난다. 이후 비정상 트래픽을 유발한 공격 종류의 판별을 위해 비정상 트래픽이 탐지된 2 분, 22 분, 23 분의 트래픽 분산 그래프에 대해서 그래프 매칭 알고리즘을 적용하였다. 그 결과 POSTECH Trace 에서 DDoS CAIDA Trace 에서 발견된 공격 패턴과 일치하는 패턴이 발견되었고, 해당하는 시각의 플로우 정보를 역추적하여 그 당시 DDoS 공격이 Internet Relay Chat(IRC) TCP 포트 6667 번을 사용하는 봇넷에 의한 DDoS 공격이었음을 확인할 수 있었다.

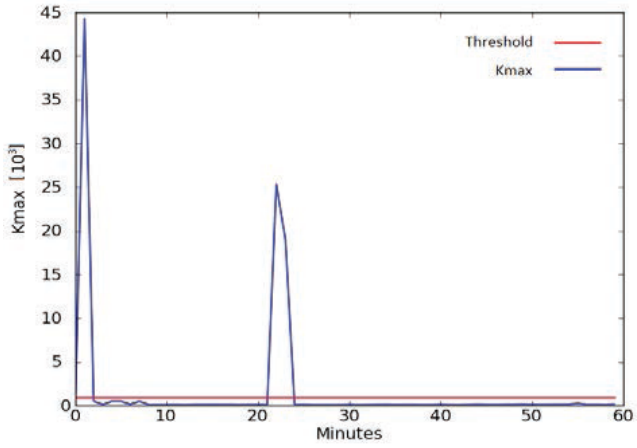

그림 5. POSTECH Trace 의 Kmax 값 변화

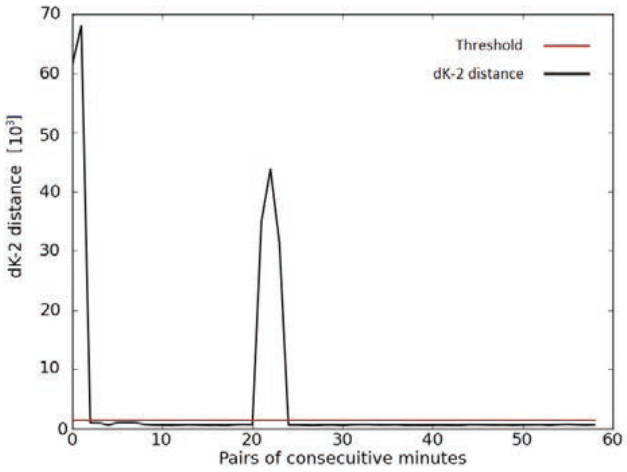

그림 6. POSTECH Trace 의 dK-2 값 변화

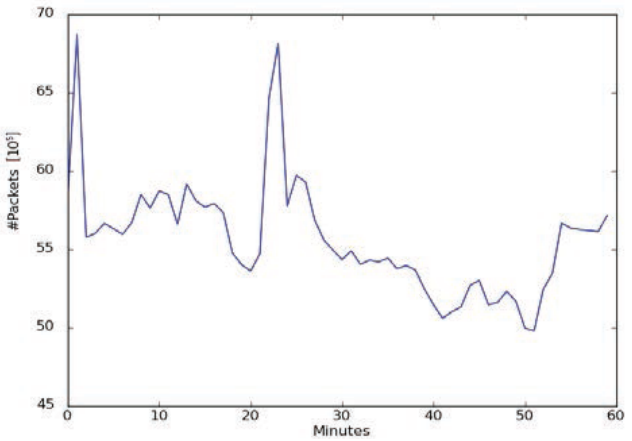

그림 7. POSTECH Trace 의 패킷수 변화

5. 결론

본 논문에서는 그래프 이론을 기반으로 네트워크 상에서 발생하는 비정상 트래픽을 탐지하는 방법을 소개하였다. 제안한 방법은 네트워크 트래픽을 트래픽 분산 그래프의 형태로 나타내고 그 그래프를 통해 비정상적인 커뮤니케이션 패턴을 파악하여 비정상 트래픽을 탐지한다. 또한 제안하는 방법의 타당성을 검증하고 평가하기 위해 실제 DDoS 공격 트래픽을 포함하고 있는 2009 년 7.7 DDoS POSTECH Trace 를 사용하여 비정상 트래픽을 탐지 할 수 있음을 보였다. 이후 부분 그래프 매칭 알고리즘을 적용하여 DDoS CAIDA Trace 가 포함하고 있는 DDoS 공격 그래프 패턴이 POSTECH Trace 에 포함되어 있음을 보임으로써 7.7 POSTECH Trace 가 DDoS 공격 트래픽을 포함하고 있음을 확인 할 수 있었다. 향후 연구에서는 DDoS 트래픽 뿐만 아니라 다양한 네트워크 공격 또는 네트워크 상의 문제로 인해 야기되는 비정상 트래픽을 분석하여 그들이 트래픽 분산 그래프 상에서 보이는 특성들을 연구할 예정이다. 또한 시스템의 심도 있는 검증을 위해 더 많은 비정상 트래픽 Trace 들을 확보하고 기존의 비정상 트래픽 탐지 시스템들과의 성능을 비교 및 평가할 계획이다.

6. 참고 문헌

[1] Iliofotou, M., Pappu, P., Faloutsos, M., Mitzenmacher, M. Singh, S. and Varghese, G. Network monitoring using traffic dispersion graphs (tdgs). In Proceedings of the 7th ACM SIGCOMM conference on Internet measurement (IMC '07). ACM, New York, NY, USA, 2007, 315-320.

[2] Hick, P., Aben, E., Claffy, K. and Polterock, J.2007. The CAIDA DDoS Attack 2007 Dataset. http://www.caida.org/data/passive/ddos-20070804dataset.xml (accessed on 2011-05-10).

[3] Iliofotou, M., Faloutsos, M. and Mitzenmacher, M. 2009. Exploiting dynamicity in graph-based traffic analysis: techniques and applications. In Proceedings of the 5th international conference on Emerging networking experiments and technologies (CoNEXT '09). ACM, New York, NY, USA, 2009, 241-252.

[4] Godiyal, A., Garland, M. and John, C.H. 2010. Enhancing network traffic visualization by graph pattern analysis, https://agora.cs.illinois.edu/download/attachments/18744303/NetflowPatternGraph.pdf?version=1&modificationDate=1238354953000.

[5] Cordella, L.P., Foggia, P., Sansone, C. and Vento, M. 2004. A (Sub)Graph isomorphism algorithm for matching large graphs. IEEE Trans. Pattern Anal. Mach. Intell. 26, 10 (October 2004), 1367-1372.

[6] Sala, A., Cao, L., Wilson, C., Zablit, R., Zheng, H. and Zhao, B. 2010. Measurement-calibrated graph models for social network experiments. In WWW, 2010, pages 861-870.

[7] Mahadevan, P., Hubble, C., Krioukov, D., Huffaker, B., Vahdat, A. 2007. Orbis: rescaling degree correlations to generate annotated Internet topologies. SIGCOMM Computer Communications Review, 2007, 325-336.

[8] Hong, J.W. 2004. Internet traffic monitoring and analysis using NG-MON. POSTECH, Advanced Communication Technology. The 6th International Conference, 2004, Volume: 1, page(s): 100- 120.
[9] Gansner, E., Koutsofios, E. and North, S. Drawing graphs with dot.
[10] Whitney, D. 2008. Basic Network Metrics. Lecture note.
http://ocw.mit.edu/courses/engineering-systems-division/esd-342-network-representations-of-complex-engineeringsystems-spring-2010/readings/MITESD_342S10_ntwk_metrics.pdf
[11] Graphviz – graph visualization software.
http://www.graphviz.org/
[12] Foggia, P., Sansone, C. and Vento, M. 2001. A Performance Comparison of Five Algorithms for Graph Isomorphism Proc. 3rd IAPR TC-15 Workshop on Graph-based Representations in Pattern Recognition, 2001.
[13] Voss, S. and Subhlok, J. 2010. Performance of general graph isomorphism algorithms. Technical Report UH-CS-09-07, University of Houston, 2010.