네트워크 자원 모니터링을 통한 내부 감염호스트 탐지 시스템의 설계 및 구현

유기성, 이행곤, 김주석, 이원혁

한국과학기술정보연구원

A Design and Implementation of the system for detecting infected host using resource monitoring in local area

Yu Ki-Sung, Lee Haeng-Gon, Kim Ju-Seok, Lee Won-Hyuk

Korea Institute of Science and Technology Information

요 약

최근 웜이나 바이러스, DDoS(Distributed Denial of Service)와 같은 네트워크 침해사고가 빈번히 발생되고 있어 이를 해결하기 위한 여러 가지 방안이 연구 중이다. 하지만 대개의 경우 외부의 침입탐지에 대한 대책만이 이루어지고 있어, 실제로 내부 호스트에서 감염되어 발생시키는 트래픽에 대해서는 원인 진단이 어려운 실정이다. 따라서 네트워크 장애의 원인이 되는 단말 호스트를 찾아내어 장애처리를 하는 것이 정상적인 네트워크 환경구축을 위하여 필요하다. 본 논문에서는 네트워크 자원 모니터링과 트래픽 분석을 통하여 이상 트래픽에 대한 징후를 사전에 탐지하고, 최종 단말 호스트의 위치까지 추적 가능한 시스템을 설계 및 구현하고자 한다.

I. 서론

네트워크 백본 및 엑세스망이 고속화되면서 네트워크 환경이 복잡한 구성을 가지게 되었으나, 이에 대한 관리는 미흡한 실정이다. 최근 웜이나 바이러스에 의한 네트워크 장애가 빈번히 발생되고 있는데, 주요 요인이 외부에서의 공격에 의한 것보다도 내부 호스트에서 유출되는 비정상적인 트래픽에 의한 것이 많다. 즉 웜이나 바이러스에 감염된 내부 호스트가 네트워크에 장애를 일으키는 주요 원인이 되는 것이다. 그러나 현재 학교나 연구소와 같이 중소규모의 네트워크를 운영하는 곳에서는 네트워크 관제뿐만 아니라 보안 시스템이 제대로 갖춰지지 않고, 전문 인력의 수도 많이 부족한 실정이다. 따라서 웜이나 바이러스에 의한 피해 발생시에 감염 호스트의 근원지를 찾는데 어려움이 있고, 네트워크 정상화에 많은 시간과 노력이 소요된다. 네트워크 장애시 내부 사용자들의 불편은 물론이고, 대외적으로 서비스 불가에 대한 불만이 증가할 것이며, 이는 대외 인지도나 신뢰성에도 영향을 초래하여, 비용으로도 따질 수 없는 치명적인 일이 될 것이다.

지난 1.25대란에 발생한 MS-SQL취약점을 이용한 웜바이러스 공격에서 보는바와 같이 이상 트래픽을 발생하는 시스템이 한 네트워크 뿐만 아니라 전 세계적으로 얼만큼 타격을 입힐 수 있는지 알 수 있을 것이다.

다음 [표1]은 지난 8월경 웜에 걸린 호스트들에 의하여 내부 망이 중단현상을 보였을 때의 패킷을 모니터링한 결과이다. 위에서 보는 바와 같이 IP주소가 무작위로 생성되고, 포트번호는 순차적으로 증가하면서 패킷이 생성되고 있다. 이러한 웜에 의한 트래픽 증가로 인하여 상위의 스위치가 다운되었으며, 원인이 되는 호스트들을 감지하기까지 많은 노력과 시간이 소요되었다. 또한 수초

동안 수천 개의 패킷을 무작위로 전송하고 다시 대기상태가 되므로, 이상징후의 정확한 위치 파악은 더욱 어려움이 있었다.

표 1: 웜으로 인한 패킷생성의 예.

System:8	TCP	sslee:2588	167.46.177.243:microsoft-ds	SYN_SENT
System:8	TCP	sslee:2589	143.47.24.156:microsoft-ds	SYN_SENT
System:8	TCP	sslee:2594	194.88.171.109:microsoft-ds	SYN_SENT
System:8	TCP	sslee:2595	56.70.180.155:microsoft-ds	SYN_SENT
System:8	TCP	sslee:2596	204.137.200.122:microsoft-ds	SYN_SENT
.....		.....	.....	.....
.....		.....	.....	.....

따라서 네트워크 상에서 어느 사용자가 얼만큼의 대역폭을 사용하며 트래픽을 유발하는지 실시간적인 모니터링을 통하여 이상징후 발견시 신속하게 탐지해야 한다. 하지만 네트워크의 규모가 대규모일경우에 모든 구간에서의 트래픽을 실시간적으로 파악하기에는 분석 시스템의 성능 등을 고려할 때 매우 어려운 일이다. 특히 내부 사용자들의 호스트에서 발생하는 웜이나 바이러스와 같은 이상 트래픽으로 인하여 상위의 스위치나 라우터가 마비될 경우 그 원인을 찾기는 더욱 어려워진다.

따라서 본 논문에서는 하위의 스위치들에 대한 노드 부하를 모니터링하여 이상 트래픽에 대한 이상징후를 사전에 탐지하고, 이상 트래픽 징후 발견시 대상 스위치의 포트별 트래픽까지도 모니터링하여 최종 단말호스트까지 위치를 추적하고자 한다.

II. 본문

외부공격자에 의한 네크워크 침해는 인입지점의 특정 시스템의 관리나 복구로 트러블슈팅이 가능하나, 내부의 감염된 PC는 신속하게 그 위치를 찾아내고 원인을 제거하기 전에는 계속 네트워크에 영향을 미친다. 따라서 본 논문에서는 내부 스위치에 대한 계층적인 관리와 자동적인 트래픽 분석을 통하여 비정상적인 트래픽을 탐지하고 위치까지 파악하는 ATDS(Abnormal Traffic Detection System)를 설계 및 구현하여 안정적으로 네트워크 운영 및 관리를 수행하도록 하고자 한다.

본 논문에서 제안하는 ATDS 알고리즘은 내부사용자들의 웜이나 바이러스에 의한 감염으로 인한 네트워크 자원낭비와 더 나아가 네트워크 중단현상을 보다 신속하게 탐지하여 대처하기 위한 방법이다. 네트워크 자원의 노드 부하율(CPU, MEMORY)을 파악하여 각각의 자원별 포트에 대한 트래픽의 이용률과 패킷의 유출입량(bps,pps)을 동시에 측정한다. 어느 네트워크에서 트래픽이 많이 사용되는지를 자동으로 감지하여 이상징후시에 원인 파악의 자료로 사용하며 여러 가지 문제들을 실시간으로 데이터베이스에 저장하고 통계를 파악하여 장애관리에 사용할 수 있다. 또한 실측 데이타를 바탕으로 각 네트워크의 성능과 사용량을 분석하여 네트워크 동향을 예측하고, 이를 바탕으로 네트워크 계획수립 및 증설의 자료로 활용할 수 있을 것이다.

1. ATDS시스템의 설계

ATDS는 [그림 1]과 같이 관리 네트워크상에서 동작하며 하위 스위치까지의 모든 네트워크 노드를 등록하고 관리를 수행한다. 또한 SNMP를 기반으로 private과 public으로 정의된 OID(Object Identifier)들을 이용하여 네트워크 노드의 부하를 상시 체크하며, 이상시 ATDS알고리즘을 사용하여 웜이나 바이러스에 감염된 단말 노드를 검색하는 과정을 거친다.

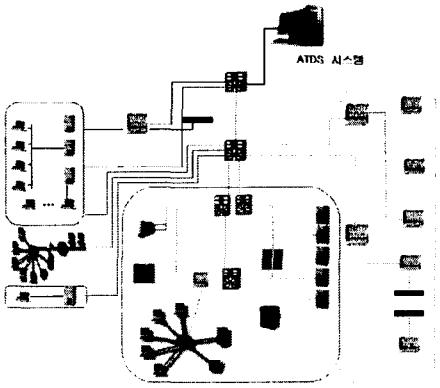

그림 1: 시스템 전체 구성도.

1) ATDS의 노드 분석항목

본 시스템에서는 네트워크 노드의 상태를 장비 부하률과 트래픽 사용량으로 구분지어 검사하며 이를 위해 실시간으로 폴링을 수행한다. 이와 같은 분석항목은 다음 [표 2]와 같다. Traffic Status를 나타내는 항목은 public MIB으로서 인터페이스별 상태를 나타내고, Node Status를 나타내는 항목은 private MIB으로서 스위치의 특성에 맞는 적절한 OID로 사용하여야 한다.

표 2: 노드 분석항목.

항 목	사용 Object ID	의 미	비고
이용률	1.3.6.1.2.1.2.2.1.10 1.3.6.1.2.1.2.2.1.16	스위치나 라우터의 입출력 패킷량을 분석하여 실제 이용률을 계산	Traffic Status
입력 패킷량	1.3.6.1.2.1.2.2.1.11 1.3.6.1.2.1.2.2.1.12	인터페이스로 입력되는 패킷량을 단위시간으로 표현	
출력 패킷량	1.3.6.1.2.1.2.2.1.17 1.3.6.1.2.1.2.2.1.18	인터페이스로 출력되는 패킷량을 단위시간으로 표현	
입력바이트량	1.3.6.1.2.1.2.2.1.10	단위시간당 입력 바이트량을 출력	
출력바이트량	1.3.6.1.2.1.2.2.1.16	단위시간당 출력 바이트량을 출력	
CPU량	1.3.6.1.4.1.1991.1.1.2.1.50	Foundry 스위치 CPU의 5초간 수집통계	Node Status
메모리	1.3.6.1.4.1.1991.1.1.2.1.53 1.3.6.1.4.1.1991.1.1.2.1.55	Foundry 스위치 Memory의 사용량 (percentage,Mbytes)	

* Node Status는 Found Switch private OID임

2) ATDS의 동작 흐름도

본 시스템의 전체 동작 흐름도는 [그림 2]와 같으며 네트워크 노드의 상태를 실시간으로 감지하기 위한 1차 폴링 엔진과 이상징후 감지시에 ATDS알고리즘을 통하여 세부 분석을 위한 2차 폴링 엔진으로 구성된다. 1차 폴링 엔진은 타이머에 의하여 지속적으로 상태 폴링을 수행하여, 전체 네트워크에 영향을 미치기 전에 미리 문제 발생의 소지를 갖는 호스트에 대한 탐지와 조치를 수행하는 것이 가능하다.

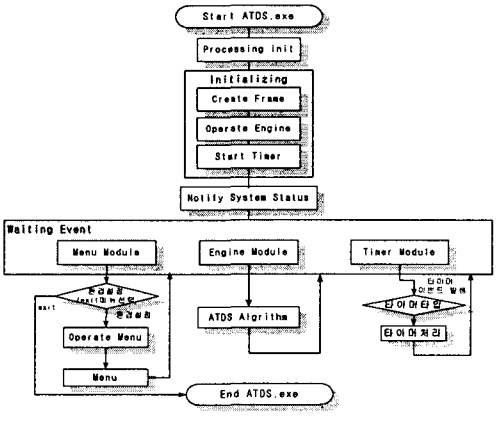

그림 2: 동작흐름도.

3) ATDS 알고리즘

1차 폴링 엔진에 의하여 네트워크 노드가 정해진 임계값을 초과하면 ATDS알고리즘을 수행하는데 그 동작 과정은 [그림 3]과 같다. 2차 폴링 엔진이 동작하면 최하위 스위치까지 recursive search를 통하여 탐지하고, 최하위 스위치에서 각 포트의 사용량을 폴링한다. 포트별 사용량을 비교하여 임계값을 초과하는 포트를 찾아내어 웜이나 바이러스의 감염여부를 확인한다.

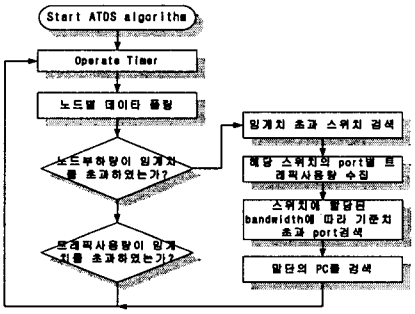

그림 3: ATDS 알고리즘.

2. ATDS시스템의 구현

1) 1차 네트워크 노드 폴링

다음은 1차 폴링 엔진에 의하여 네트워크 노드의 부하상태를 모니터링하는 화면을 나타낸다. [그림 4]에서와 같이 좌측에는 그래프를 통하여 부하상태를 직관적으로 알아볼 수 있고, 임계값 초과시에는 오른쪽 로그화면에 상태를 나타낸다. 이러한 데이터는 비쥬얼한 화면뿐만 아니라 로그로 남아 차후에 객관적인 통계에도 이용할 수 있으며, 실측데이터를 숫자로 표현하여 노드간 정확한 비교도 가능하다.

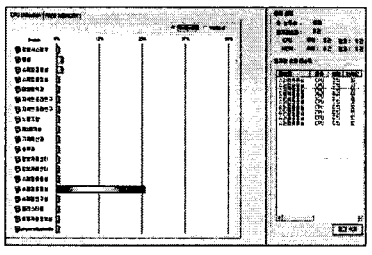

그림 4: 1차 노드 부하탐지(Graphic).

2) 2차 단말 스위치 포트 모니터링

1차 폴링 엔진에 의하여 이상 징후가 발견된 스위치에 대하여 모든 포트에 대한 트래픽을 수집하기 위하여 ATDS 알고리즘을 수행한다. [그림 5]는 스위치의 한 포트에 대한 실시간 트래픽 현황을 보여주는 화면이다. 이런 방법으로 내부적으로 모든 포트에 대한 트래픽을 수집하여 주어진 대역폭에 비하여 많은 사용량을 사용하는 포트를 탐지하여 보고한다.

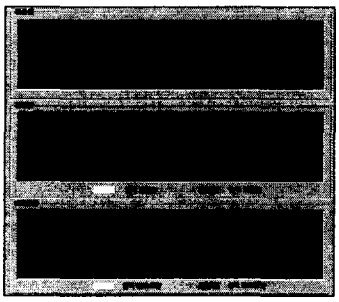

그림 5: 2차 트래픽 모니터링.

3) 3차 단말 호스트의 세부 트래픽 분석

ATDS 알고리즘에 의하여 찾아진 단말 호스트에 대하여 실제 웜이나 바이러스가 걸린 것이지 판단하기 위하여 상용툴을 사용하여 분석을 수행하였다. 이 툴을 이용하여 분석한 결과 [그림 6]에서 보는 바와 같이 ATDS 시스템에서 검색된 시스템에서 다수의 패킷이 발생되는 것을 알 수 있다. 따라서 웜으로 의심되는 단말 호스트에서 발생한 수많은 패킷으로 인하여 특정 포트의 사용량이 증가하고, 이를 처리하기 위한 노드 부하량이 증가하였음을 확인할 수 있었다.

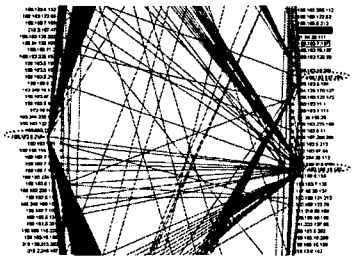

그림 6: 패킷 상세 분석
(EtherPeek툴 사용)

III. 결론

현재 대부분의 네트워크 침해사고 방지를 위한 시스템은 내부의 자원에 대하여 외부의 공격에 대해서 탐지하는 데에 치중이 되어 있다. 따라서 실제 내부 호스트가 웜이나 바이러스에 감염되어서 트래픽을 유발하는 것에는 탐지가 어렵고, 비정상 트래픽으로 인한 네트워크 장애에 대한 근본적인 원인을 찾기가 어렵다. 따라서 본 ATDS는 실시간으로 네트워크 노드의 부하율을 측정함과 동시에 트래픽 사용량을 조회하여 문제가 되는 단말 호스트의 탐지 및 위치 추적까지 가능하므로 근본적인 원인 해결에 도움을 줄 수 있다.

하지만 네트워크 자원의 부하률과 트래픽의 증가만으로 웜이나 바이러스에 의한 트래픽이라고 단정하기는 어려운 면이 있으므로 신뢰성 있는 탐지 시스템을 위하여 트래픽의 실질적인 유형분석에 대한 연구를 더욱 세분화되어 수행해 나갈 것이다.

참고문헌

[1] J. Nevil Brownlee, "Internet Traffic Measurement", A background paper for the ICAIS seminar, march 1999

[2] 정태명, "인터넷 침해사고 원인과 대책", 한국정보처리학회 논문지, pp.22-26, 2003년 3월

[3] David J. Marchette, "Computer Intrusion Detection and Network Monitoring:A Statistical Viewpoint", Springer-Verlag New York, 2001

[4] C.Hare and K. Siyan, "Internet Firewalls and Network Security", 2nd edition, New Riders Publishing, 1996

[5] 남영우, 이장세, 지승도, "네트워크 정보 시스템의 취약성 분석과 Survivability", 한국정보보호학회, 2002년 11월

[6] Felix Lau, et al., "Distributed Denial of Service Attacks", Systems, Man, and Cybernetics, 2000 IEEE International Conference Vol3, pp2275-2280, 2000