IPv6 환경에서의 유해 트래픽 분석

Harmful Traffic Analysis on the IPv6 Environment

구향옥, 백순화*, 오창석
충북대학교, 백석대학*

Koo Hyang-Ohk, Baek Soon-Hwa*,
Oh Chang-Suk
Chungbuk National University, Baeksuk University*

요약

홈네트워크와 인터넷이 결합된 IPv6환경이 도래 되어도 각종 바이러스와 웜 공격 등으로 인해 입는 피해들도 계속 증가할 것이다. 본 논문에서는 TCP, UDP, ICMP 트래픽을 분석하여 IPv6 환경에서의 유해 트래픽 검출하는 기법을 제안하였다.

Abstract

The IPv6 environment combined the home network and the Internet with has arrived, the damages cased by the attacks from the worm attacks and the various virus has been increased. In this paper we analyze the traffics of TCP, UDP and ICMP, and propose for a method to detect harmful traffics in the IPv6 environment

I. 서 론

인터넷 웜과 DDoS 공격으로부터 시스템을 보호하기 위해서는 공격 트래픽에 대한 정확한 분석과 탐지가 우선되어야 한다. 그러나 IPv6 환경으로 전환될 때 발생하는 유해 트래픽에 대한 연구가 미약한 상태이다. 그러므로 IPv6 환경에서 NET-SNMP(Simple Network Management Protocol)를 이용하여 IPv6 환경에서 공격을 수행하고 공격 트래픽을 모니터링한 후 공격을 탐지하는 분석 알고리즘을 도출하여 IPv6 환경으로 전환되었을 경우 발생하는 공격을 신속하고 정확하게 검출한다. 네트워크상에 관리되는 IPv6 환경에서 사용되는 MIB(Management Information Base)객체 중 ipv6IfStats InReceives를 통해 지수평활법을 적용하여 예측치로 정상트래픽한계(임계치)를 초과하는 공격을 판별하고 정상트래픽한계를 각각의 MIB(Management Information Base)인 ipv6TcpConn State (synSent(3)), ipv6 UdpLocalPort, ipv6IfIcmpOu t Echo Replies을 30초 간격으로 트래픽을 수집하여 TCP Flooding, UDP Flooding, ICMP Flooding 공격을 검출한다. 또한 이에 보다 정확한 검출을 위해 공격에 사용되는 포트번호를 ipv6TcpConnLocalPort, ipv6 UdpLocalPort을 이용하여 검출하고 수신되는 멀티캐스트주소의 정상임계치를 이용하여 대량의 멀티캐스트 메시지 공격을 검출하는 알고리즘에 적용하였다.

II. IPv6 환경 공격 탐지

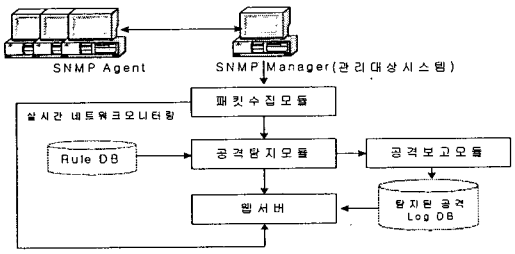
NET-SNMP를 이용하여 패킷을 수집하여 네트워크를 관리하는 것이 아닌 SNMP의 MIB 객체를 30초단위로 분석하여 트래픽 폭주 공격 시 나타나는 특

징을 검출하고 분석하여 신속한 탐지가 이루어지도록 하였으며, 지수평활법을 이용하여 현재트래픽으로 정상트래픽한계(임계치)를 바로 적용시켜 효율을 높였따. 공격에 주로 사용되는 포트번호를 필터링하였으며 단위시간 평균 멀티캐스트 수를 측정하여 폭주 공격에 대한 공격 검출을 향상 시켰다.

2.1 트래픽 분석 모델

IPv6 환경에서 NET-SNMP를 이용한 트래픽 분석 모델은 관리대상시스템의 공격에이전트들로부터 트래픽의 유입을 패킷수집모듈로 수집하여 입력 패킷이 공격인지 침입탐지모듈 판정하여 공격일 경우 관리자에게 침입보고 모듈을 통해 보고하고 현재 트래픽은 MRTG를 통해 웹에 개시하여 트래픽을 모니터링하도록 하였다.

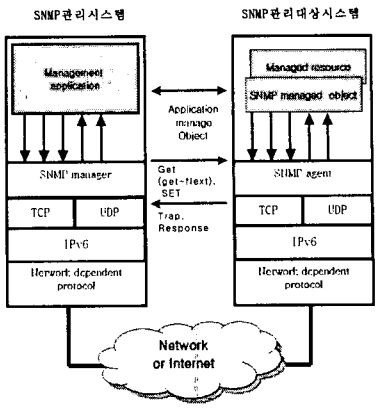
그림 트래픽 분석모델을 관리대상시스템(피해 시스템)의 트래픽을 분석하는 모델로 수행 기능 개념도이다.



▶▶ 그림 2.1 트래픽 분석 모델

2.2. 패킷 수집 모듈

패킷 수집 모듈에서는 관리 시스템과 관리 대상 시스템간에 SNMP를 활성화시킨 후 관리하고자 하는 MIB를 선정하여 정보를 얻게 된다. [그림 2.2]는 SNMP를 이용하여 트래픽을 수집하는 구성도이다. 관리 시스템은 각 선정된 MIB 객체에 대해 snmpd 데몬을 통해 NMS(Network Management System)이 구축되어 snmpget으로 30초 단위로 정보를 획득하게 된다.



▶▶ 2.2 그림 패킷 수집 모듈

[표 2.1] 공격 검출에 사용되는 MIB

MIB 객체	설명
ipv6IfStatsInReceives	수신한 데이터그램의 총수
ipv6TcpConnState (synSent(3))	TCP connection의 스테이트 synSent(3) 세그먼트의 TCP 연결요청
ipv6TcpConnLocalPort	TCP로 connection 수신된 로컬 Port 번호
ipv6UdpLocalPort	UDP로 수신된 로컬 Port 번호 : 목적지 포트에 응용 프로그램이 없는 경우(Null)
ipv6IfIcmpOutEchoReplies	송신된 ICMP 요청 메시지의 총 개수 : EchoReply 송신 메세지수
ipv6IfIcmpInNeighborSolicits	NeighborSolicit 수신 메세지수
ipv6IfIcmpInNeighborAdvertisements	Neighbor Advertisement 수신 메세지수
ipv6IfIcmpInRouterSolicits	RouterSolicit 수신 메세지수
ipv6IfIcmpInRouterAdvertisements	RouterAdvertisement 수신 메세지수

2.3. 공격 탐지 모듈(트래픽 임계치 적용 절차)

TCP, UDP, ICMP, IP데이타그램에 대한 공격 트래픽의 임계치는 지수평활법을 이용하여 계산하여 이전에 수집된 트래픽을 저장하여 임계치를 계산하는 방식에서 탈피하였다.

지수평활법은 일정 시간 간격에 따라 관찰된 과거 데이터의 가중 평균을 다음 시점의 예측치로 사용하는 방법으로, 가중 평균을 계산할 때 최근의 데이터에 더 많은 가중치를 부과하는 발전된 형태의 이동평

균법으로 이 방법은 계산이 쉽고 필요한 자료가 적다는 장점을 가지고 있어 트래픽에 대한 분석기법으로 적합하다.

2.4. 공격 검출에 사용된 변형된 지수평활법

1) 초기화 : 네트워크에서 트래픽 발생하는 매 시점마다 공격을 판단하는 것은 어려운 일이다. 따라서 본 논문에서는 각 프로토콜별 트래픽의 양을 일정한 주기(30초마다) 초기의 MAD 또는 표준편차를 결정한다.

2) 실제치 입력 : 트래픽 측정 장치로부터 t시점에서 실제로 측정된 트래픽 X_t를 입력 받는다.

3) 예측치 존재 판단 : 예측을 처음 시작하였거나 이상상태가 끝난 후, 지수평활법이 재실행되었을 경우에는 그 시점에 대한 예측치(Y_t)가 존재하지 않는다. 예측치가 존재하지 않을 경우에는 예측치가 실제치와 같다고 설정한다($Y_t = X_t$). 이 때 예측오차(E_t)는 0이 된다. 예측치가 존재하는 일반적인 경우에는 예측오차는 실제치와 예측치의 차이가 된다.($E_t = X_t - Y_t$).

4) 정상 범위 계산 :

$UCL = Y_{t+1} + z_\alpha \sigma_t \approx Y_{t+1} + 1.25 \cdot z_\alpha MAD_t$

을 바탕으로 예측치(Yt)와 MAD 또는 표준편차를 이용하여 관리한계의 상한을 결정한다.

5) 이상 상태 파악 실제치(X_t)가 정상트래픽한계를 벗어날 경우 $(X_t > Y_t + z_\alpha \sigma_t)$에서는 네트워크에 이상이 발생하였다고 판단하여 지수평활법을 정지하고, 공격상태처리모듈을 수행한다. 실제치가 정상 범위에 있을 경우 $(X_t \le Y_t + z_\alpha \sigma_t)$에는 다음 단계로 진행하여 지수평활법을 계속 수행한다.

6) 다음 시점 예측, 표준편차, MAD 업데이트 : 관리한계 내의 실제치(X_t)를 사용하여

$Y_{t+1} = \alpha X_t + (1-\alpha),\ Y_t = 0 < \alpha \le 1$에 따라, 다음 시점의 예측치($Y_t + 1$)를 계산한다. 또한 현재의 예측 오차를 바탕으로 식

$\sigma_t^2 = \gamma \cdot E_t^2 + (1-\gamma) \cdot \sigma_{t-1}^2, \quad 0 < \gamma \le 1.$

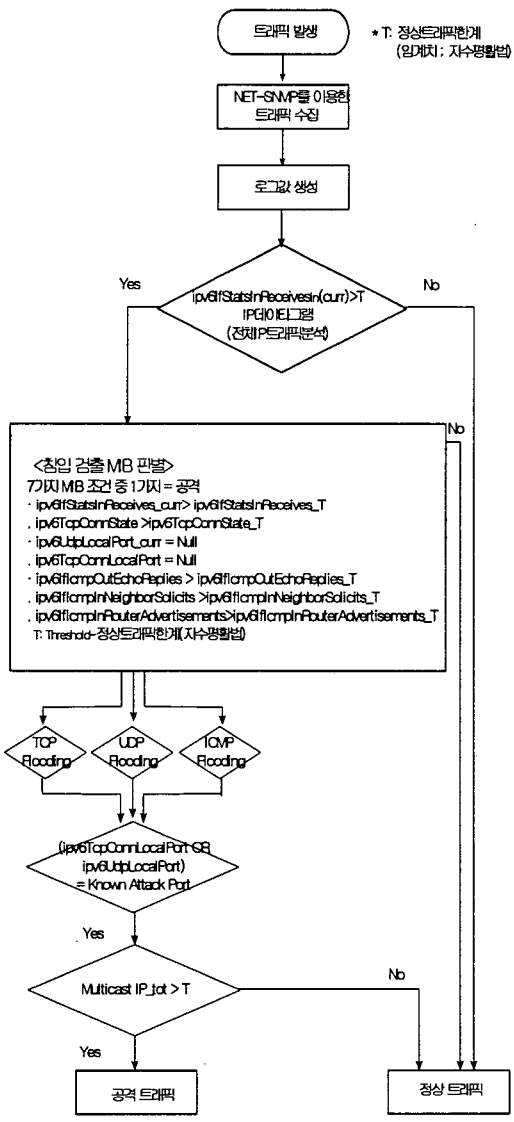
$MAD_t = \gamma |E_t| + (1-\gamma) MAD_{t-1}$를 사용하여, 다음 시점의 정상 범위계산에 필요한 표준편차 또는 MAD를 업데이트한다. 그 후, 다음 시점의 실제치가 입력될 때까지 대기한다.

7) 이상 상태 처리 모듈 : 이상 상태파악단계에서 트래픽의 공격상태가 발견되면 지수평활에 의한 예측을 중지하고, 트래픽이 다시 정상 상태가 되기를 기다린다. 현재의 공격트래픽은 무시하고, 다음 시점의 트래픽을 입력 받는다. 현 시점의 트래픽이 정상적이라고 판단되면, 지수평활법을 다시 시작한다. 다시 시작되는 지수평활법에서, 표준편차 또는 MAD는 이상 발생 이전의 값이 그대로 사용되고, 그 시점에 대한 예측치가 없기 때문에 예측치의 초기값은 실제치와 같다고 설정된다. 입력된 트래픽이 여전히 공격상태로 판단되면 정상상태의 트래픽이 도착할 때까지 대기한다.

2.5. NET-SNMP를 이용한 트래픽 분석 알고리즘

NET-SNMP를 이용한 트래픽 분석 알고리즘은 snmpget으로 수집한 트래픽을 [그림 2.3]과 같이 먼저 ipv6IfStatsIn Receives인 MIB으로 지수평활법을 이용하여 정상트래픽한계(임계치)를 계산하여 수집된 현재 IP데이타그램의 총량이 T(임계치)를 벗어나는 경우 공격으로 판정한다. ipv6TcpConnState (synSent(3))으로는 T를 계산하여 범위를 벗어나면 TCP Flooding 공격으로 판정하고 ipv6UdpLocalPort으로 T를 계산하여 범위를 벗어나면 UDP Flooding 공격으로 판정하고 ipv6IfIcmpInNeighborSolicits, ipv6IfIcmpInRouterSolicits, ipv6IfIcmpOutEchoReplies으로 ICMP

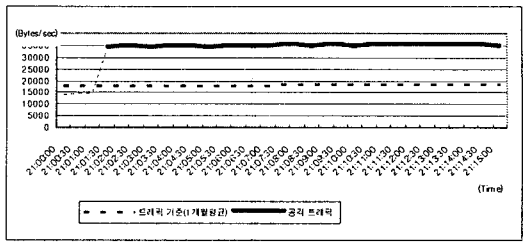
Flooing 공격을 판정하고 ipv6UdpLocalPort와 ipv6TcpConn Local Port을 가지고 기존포트 공격을 검출한 후 멀티캐스트 입력되는 주소를 T(임계치)를 계산하여 공격으로 판정한다. 트래픽이 공격으로 판정되면 관리자에게 alarm을 보낸다.



▶▶ 그림 2.3 NET-SNMP를 이용한 트래픽 분석

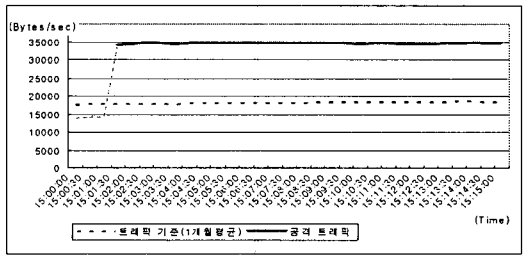
III. 실험결과

NET-SNMP를 이용하여 지수평활법의 T를 적용하여 트래픽의 공격을 검출한 결과 다음과 같은 그래프 구간에서 공격이 검출 되었다.



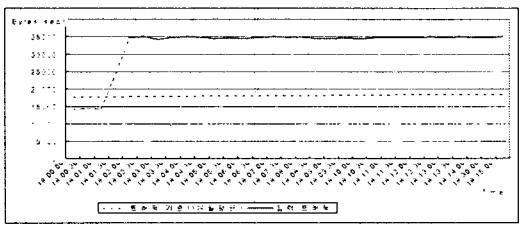
▶▶ 그림 3.1 TCP Flooding 트래픽 검출

[그림 3.1]은 TCP Flooding 공격이 30초 21:01:00~21:01:30에서 TCP트래픽이 폭주하여 21:01:30에서 정상트래픽한계를 벗어나 공격 검출된 공격트래픽구간을 나타내고 있다.



▶▶ 그림 4.2 UDP Flooding 트래픽 검출

[그림 3.2]는 UDT Flooding 공격이 30초 15:01:00~15:01:30에서 TCP트래픽이 폭주하여 15:01:30에서 정상트래픽한계를 벗어나 공격 검출된 공격트래픽구간을 나타내고 있다.



▶▶ 그림 3.3 ICMP Flooding 트래픽 검출

[그림 3.3]은 ICMP Flooding 공격이 30초 18:01:00~18:01:30에서 ICMP 트래픽이 폭주하여 18:01:30에서 정상트래픽한계를 벗어나 공격 검출된 공격트래픽구간을 나타내고 있으며 표 3-1과 같이 기존 공격보다 신속한 탐지가 이루어진다.

[표 3.1] 기존공격탐지와 제안한 공격탐지의 비교

도구 / 비교대상	Ethereal	libpcap (IPv6analizer)	NET-SNMP
분석대상	IPv6 패킷	IPv6 패킷	IPv6 패킷
공격탐지	수동 ,부정확	2단계 가능	가능
공격차단	수동 차단	자동 차단	자동 차단
공격탐지 시간	공격 탐지 수동	공격 탐지 시간 최대 1분	공격 탐지 시간 최대 30 초

V. 결 론

실험결과 현재 1분 단위로 공격이 검출되어지는 트래픽 모니터링에 비해 신속한 30초 단위의 검출이 이루어지고 있으며 수집시간 단위의 평균트래픽 측정치만으로 공격을 검출하는 방식에 지수평활법을 이용한 정상트래픽한계(임계치) 계산은 현재 트래픽만으로 공격을 검출하는 장점이 있어 현재까지 누적치를 보관하는 저장용량이 필요하지 않으며 이전까지 트래픽을 저장하고 불러와서 비교하는 루틴이 줄어들어 처리 효율이 높아졌으며, 기존의 공격 포트를 저장하여 수집트래픽의 포트가 공격인지 판별하였다. 일주일동안 공격트래픽의 IP주소를 통계치를 조사하여 단위 시간내에 동일 멀티캐스트 비율을 조사하여 정상트래픽한계로 공격임을 측정하여 공격트래픽 검출 효율을 높였다.

▌참 고 문 헌▐

[1] 유대성, 구향옥, 오창석, "SNMP를 이용한 유해 트래픽 분석", 한국콘텐츠학회 2004 추계 종합학술대회, pp.215-219, 2004.
[2] 오창석, 생동하는 TCP/IP 인터넷, 내하출판사, 2004.
[3] IPv6 동향 2004, 한국전산원.
[6] H. Wang, D. Zhang, K. G. Shin, "Detecting SYN Flooding Attacks," Univ. of Michigan, 2002.
[7] T. Nordmark, E. Simpson, "neighbor Discovery for IP Version 6," RFC 2461, 1998.
[8] B. Carpenter, K. Moore, "Connection of IPv6 domains via clouds," RFC 3056, 2001.
[9] J. Case, M. Fedor, M. Schoffstall, J. Davin, "A Simple Network Management Protocol(SNMP)," RFC1157, 1990.
[10] http://www.vsix.net/