웜이나 DDoS 공격에 대한 패킷 검사 부하를 줄이는 간편 필터링 기법*

류진형○ 이재국 김상민 김형식
충남대학교 컴퓨터공학과
{jinhyong○, empire, smkim, hskim}@csal.cnu.ac.kr

An On-the-fly Filtering Technique for Reducing Packet Inspection Overhead Against Worms and DDoS Attack

Jin-Hyong Ryu○, Jea-Kook Lee, Sang-Min Kim, Hyong-Shik Kim
Department of Computer Engineering, Chungnam National University

요 약

대부분의 보안 장비들은 웜이나 DDoS 공격들을 탐지하거나 차단하기 위하여 시그너처(signature) 검사방법을 이용한다. 웜이나 DDoS 공격은 네트워크에 부하를 주기 때문에 정상 서비스의 이용을 제한하고 심지어 보안장비를 동작하지 못하게 함으로써 네트워크를 마비시킬 수 있다. 본 논문에서는 패킷 유입량이 보안장비가 처리할 수 있는 범위를 벗어나면, 간편 필터를 이용하여 패킷 검사 오버헤드를 줄여 보안장비들의 가용성을 높이는 기법을 제안한다. 그리고 기존의 대표적인 웜들과 DDoS 공격 성향을 조사하여 타당성을 보인다.

1. 서론

처음 Morris 웜[1]이 등장하였을 때는 그 속도나 파급력이 크지 않았으나, 2001년 CodeRed 웜[2]이나 2003년의 Slammer 웜[3]은 대다수의 보안 장비들을 무력화시키고, 급속도로 네트워크를 통하여 퍼져 나가서 많은 사회적 피해를 주었다. 특히 Slammer 웜은 10분 동안, 전 세계에 있는 75000개 이상의 호스트를 감염시켰다[4]. 이렇게 빠른 속도로 호스트를 감염시킬 수 있었던 이유는 감염 패킷의 길이가 404바이트로 짧아서 패킷을 빨리 생성할 수 있었고 비연결 지향적인 UDP 프로토콜을 사용하였기 때문이다.

현재 대부분의 보안장비들과 소프트웨어 침입탐지프로그램인 Snort는 네트워크 웜 패킷을 찾아내기 위하여 유입패킷을 검사한다. 만약 웜이 많은 패킷을 발생시킬 경우 패킷 검사의 오버헤드로 인하여 정상패킷의 처리속도를 떨어트리고 최악의 경우에는 보안장비의 동작이 멈출 수 있는 문제를 가지고 있다.

웜이나 DDoS 공격들에 의하여 네트워크 시스템의 병목현상을 일으키는 가장 큰 이유는 보안장비들의 비정상 패킷을 탐지하기 위한 패킷 시그너처 검사 오버헤드 때문이다. 네트워크 보안장비들의 검사 능력은 한정되어 있기 때문에 공격이 발생하면 패킷의 유입량이 패킷 처리량보다 많아진다. 따라서 유입 패킷의 양이 보안장비가 처리할 수 있는 능력을 초과하는 경우에도 정상적인 서비스를 제공하기 위하여 패킷처리 오버헤드를 줄일 필요가 있다. 본 논문에서는 패킷으로부터 빠르게 얻을 수 있는 정보만을 이용하여 정상이거나 비정상일 가능성일 가능성을 판단하여 패킷 검사를 생략하거나 패킷을 차단한다. 이 방법은 패킷 검사의 정확도를 희생하는 대신 서비스 가용성을 높인다. 즉, 보안장비들의 패킷 처리 한계 보다 많은 패킷이 유입되었을 때에도 정상적인 서비스를 최대한 제공하고 보안 시스템의 서비스 불능상태를 최소화하기 위한 것이다.

본 논문의 구성은 다음과 같다. 2절에서는 웜 및 DDoS의 특징으로부터 패킷 검사 문제를 해결할 수 있는 방법을 찾는다. 3절에서는 가용성을 향상시키기 위한 간

* 본 연구는 지식경제부 및 정보통신연구진흥원의 대학IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-C1090-0801-0016)

편 필터링 기법을 설명하고 4절에서는 간편 필터링 기법을 적용했을 때의 효과를 알아보기 위하여 네트워크의 통계를 분석하고 대표적인 웜들과 DDoS 공격 성향을 조사하여 타당성을 보인다. 마지막으로 5절에서 결론을 기술한다.

2. 웜이나 DDoS 공격의 특징과 패킷 검사 문제 해결

일반적으로 웜이 이용하는 감염패킷의 길이가 짧을수록 웜의 전파속도는 더 빠르다[5]. 패킷생성의 오버헤드가 작고 전파가 간단하기 때문이다. DDoS 공격일 경우에도 마찬가지로 공격자는 패킷을 빠르게 생성하여 공격하는 경향이 있다. 따라서 생성속도가 빠르고 효과적인, 길이가 짧은 패킷으로 공격할 확률이 높다. 웜과 DDoS 공격을 종합하면 길이가 긴 패킷으로 공격을 할 경우 짧은 패킷으로 공격할 때에 비하여 공격 효과가 떨어지며 공격의 목표가 느끼는 오버헤드는 작다. 따라서 DDoS 공격자나 웜은 가능한 짧은 패킷으로 공격할 가능성이 크다.

그렇지만 현재까지 모든 웜들이 짧은 패킷으로 공격하는 것은 아니며 길이가 긴 감염 패킷을 이용하는 웜이 더 많이 존재하므로 길이가 긴 패킷에 대한 검사도 여전히 필요하다. 웜이 긴 패킷으로 공격하는 이유는 적은 데이터를 이용해서 웜을 제작하기 어렵기 때문이다.

감염 패킷의 길이가 길어 여러 패킷으로 나누어 전송하는 웜은 스캔 행동 단계와 전파 단계를 통하여 감염된다. 스캔 행동 단계에서 웜은 자신이 감염시킬 수 있는 네트워크에 연결된 호스트를 찾는다[6]. 따라서 스캔 행동을 탐지한다면 감염을 미리 예방할 수 있다.

패킷 검사 부하를 줄이는 간편 필터를 위하여 본 논문에서 취한 방법은 기존의 패킷필터 전에서 간단하게 필터링하는 것이다. 패킷에서 빠르게 얻을 수 있는 정보를 이용하여 악의적으로 네트워크에 부하를 일으킬 가능성이 높은 패킷은 차단하고 가능성이 낮은 패킷은 검사를 생략하고 통과시키는 방법이다. 두 조건에 모두 맞지 않으면 기존 필터로 다시 검사한다.

3. 간편 패킷필터링 기법

네트워크의 가용성이 떨어질 경우 스캔 행동을 보이는 호스트를 차단하고 긴 길이의 패킷은 통과시킨다면 기존 패킷 필터의 부하는 많이 줄어들 것으로 보인다. 따라서 본 논문에서는 패킷길이와 스캔 행동 탐지를 이용하여 간편 필터링 기법을 고안하였다. 간편 필터링을 포함한 패킷 검사 부하를 줄이는 구조를 그림으로 타나내면 그림 1과 같다.

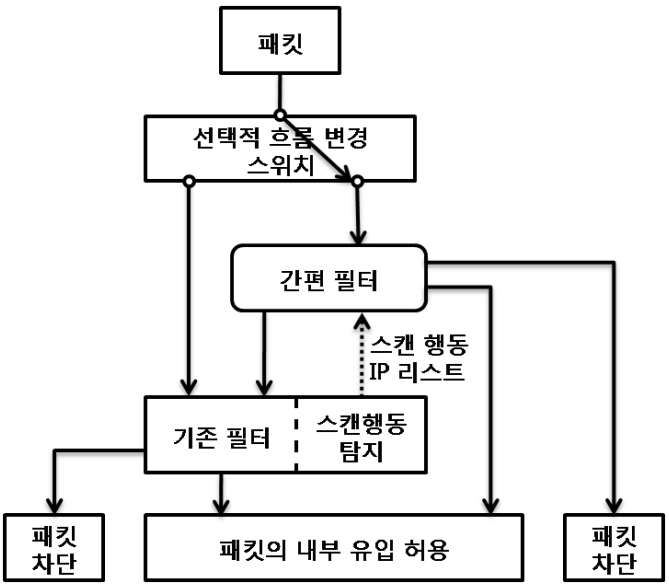

그림 2 패킷 처리 부하를 줄이는 처리 구조

기본적으로는 기존 패킷 필터링을 수행하고, 패킷 처리 부하가 증가되면 패킷 흐름을 변경한다. 변경된 패킷 흐름은 간편 필터를 통과하여 일부 패킷을 차단 또는 허용하는 구조이다. 간편 필터에서는 패킷 길이정보를 비교하고 스캔 행동 IP 리스트와 매치하는지 검사한다. 이 때 스스로 스캔 행동을 탐지하지는 않는다. 단순히 스캔 행동 IP 리스트를 제공받아 필터링만 수행하므로 빠르고 쉽게 필터링을 처리할 수 있다. 스캔 행동 IP 리스트는 TRW(Threshold Random Walk) 방법[7]을 이용해서 생성하였다. TRW는 트래픽 패턴을 분석하여 웜을 찾아내는 방법을 사용한다. 이 TRW 방식은 TCP 프로토콜을 사용한 웜에 대한 것으로, TCP 프로토콜의 처음 연결을 위한

SYN 패킷을 스캔 행동으로 보고 이 정보를 바탕으로 Sequential Hypothesis Testing 방식을 이용해서 비정상 트래픽 패턴을 찾아내게 된다. TRW 방식은 수식은 복잡하지만, 실제 구현 복잡도는 높지 않으며, 빠르게 TCP 웜을 잡아낼 수 있다[8].

스캔 행동이 탐지되면 스캔 행동을 유발하는 IP의 리스트를 간편 필터로 보낸다. 이 리스트가 스캔행동 IP 리스트이다. 패킷 유입량이 많아지면 패킷이 간편 필터를 지날 수 있도록 흐름을 변경한다. 반대로, 일정 시간이 지난 후 패킷 유입량이 줄면 패킷 흐름을 기존 필터로 바꿔주어 필터링을 수행할 수 있도록 한다. 패킷의 흐름을 변경하기 위하여 동적 자기 재설정 시스템[9]을 이용한다. 동적 자기 재설정 시스템은 스스로 자신의 상태를 판단하여 서비스의 효율을 증가시키는 역할을 한다.

간편 필터의 기능은 그림 2와 같다.

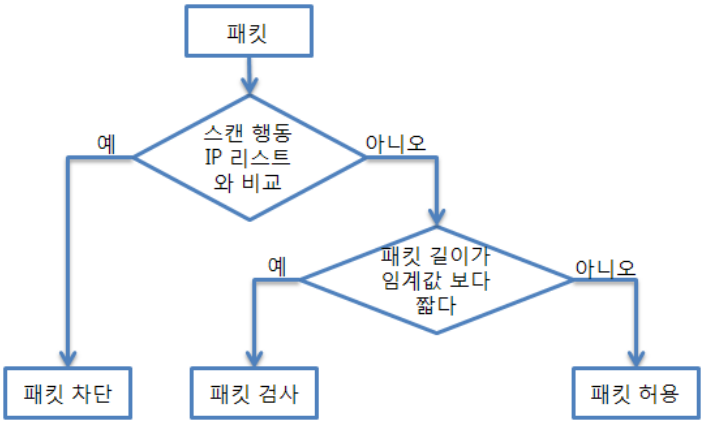

그림 3 간편 필터의 기능

먼저, 패킷의 출발지 IP주소를 스캔 행동 IP 리스트와 비교하여 패킷을 필터링 한다. 리스트에 속해 있지 않은 패킷들은 다시 패킷길이 정보와 미리 정해진 임계값과 비교하여 짧으면 기존의 패킷 검사를 다시 실시한다. 반대로, 비교하여 길 경우 기존 패킷 검사를 하지 않고 패킷 유입을 허용한다. 이 때 임계값은 실제 네트워크와 웜을 조사하여 결정한다.

일시적으로 네트워크가 혼잡할 때는 새로운 서비스 요청보다 기존에 처리되고 있는 서비스에 좀 더 높은 우선순위를 부여하는 것이 좋다. 간편 필터를 사용하면 새로운 연결을 위한 짧은 TCP SYN, ACK 패킷은 처리가 늦어지고 이미 연결 설정을 마치고 데이터를 전송중인 긴 패킷은 빨리 처리된다. 결과적으로 새로운 서비스 요청보다 기존에 처리되고 있는 서비스에 좀 더 높은 우선순위를 부여한 것과 같은 효과를 낼 수 있다.

4. 네트워크 통계분석

간편 필터링 기법을 이용한 필터링 구조가 효율적으로 동작하기 위해서는 실제 네트워크에서 임계값을 넘는 패킷의 비율이 높아야 한다. 만약 임계값을 넘는 패킷의 비율이 낮다면 제시한 방법의 실효성은 떨어질 것이다. 따라서 B 클래스 크기의 캠퍼스 네트워크를 평일 하루 동안 모니터링하여 패킷 길이의 분포를 분석하여 그림 3에 나타냈다.

100바이트 미만의 패킷이 42%정도로 가장 많은 부분을 차지한다. 다음으로 1500바이트 이상의 패킷으로 35% 정도로 두 번째로 많다. 세 번째는 1400바이트 이상 1500바이트 미만의 패킷으로 8% 정도를 차지한다. 만약 임계값을 1400바이트로 설정한다면 전체의 43% 정도의 패킷의 검사를 회피할 수 있다.

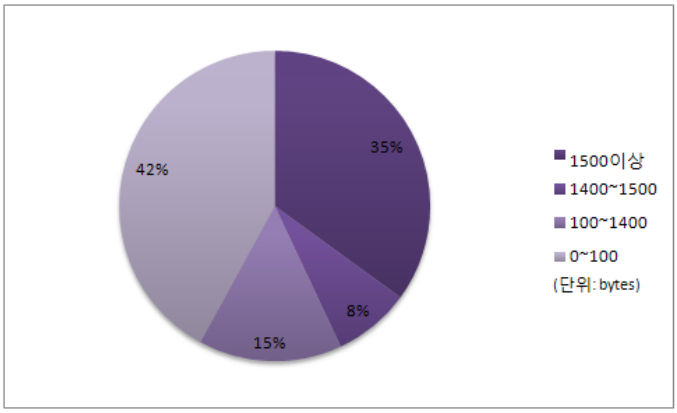

그림 4 캠퍼스 네트워크의 패킷 길이 분류

그림 3의 데이터는 단순히 패킷의 개수를 나타내고 있다. 하지만 패킷 검사 오버헤드는 패킷의 길이에 비례한다. 따라서 전체 패킷 검사 오버헤드에서 길이가 1400바이트 이상의 패킷이 차지하는 비중은 43% 이상이 된다.

실제로 네트워크가 비정상적일 경우에도 그림 3에서 보는 바와 같은 비율로 패킷이 유입된다고 보장할 수는 없지만 기본적으로 네트워크상에서 길이가 긴 패킷의 비율은 높다는 것을 유추할 수 있다. 따라서 패킷의 길이정보를 이용하여 패킷처리 부하를 줄이는 간편 패킷 필터는 효율적인 방법이 될 수 있다.

이전에 발생한 대표적인 웜들의 공격목표 검색방법과 감염 패킷의 길이를 조사하면 표 1과 같다.

표 1 기존 웜들의 감염패킷 사이즈와 타겟 검색방법

이름	타겟검색방법	페이로드 사이즈 (바이트)
Code Red	Scan/Fixed IP Address	1500이상
Nimda	Scan	1500이상
Code Red II	Scan/Fixed IP Address	1500이상
SQL slammer	Scan	404
Blaster	Scan	1500이상
Welchia	Scan	1500이상
Witty	Scan	796~ 1307
Sasser	Scan	1500이상
Zotob	Scan	1500이상
Nyxem	Scan	1500이상

표 1의 결과에 의하면 패킷 길이의 임계값을 1400바이트로 보았을 때 2개의 웜이 짧은 패킷을 이용한다는 것을 알 수 있다. 임계값보다 긴 감염패킷을 이용하는 웜들은 다시 2가지로 분류할 수 있다. SMTP프로토콜을 통해서 전파되는 웜과 스스로 전파되는 웜으로 분류된다. SMTP를 이용하는 웜들은 네트워크에 큰 부하를 주지 않기 때문에 논의에서 제외하고 스스로 전파되는 웜들은 모두 감염 전 스캔 행동을 통해서 감염대상을 찾는다. 따라서 이러한 웜들은 스캔 행동 탐지를 통해서 미리 차단할 수 있다.

이미 출현한 웜들에 대해서 조사한 결과, 네트워크 웜이나 DDoS 공격시 간편 필터링 기법을 이용하여 길이가 긴 패킷을 검사하지 않고 통과 시키더라도 혼잡의 원인이 되는 공격을 탐지하거나 차단하는 것에 큰 문제가 없는 것을 볼 수 있다.

DDoS의 경우에도 통계로 확인되지 않지만 공격 효과를 향상시킬 목적으로 작은 패킷을 이용할 것으로 추정된다.

5. 결론 및 향후 연구계획

본 논문에서는 보안 장비가 처리할 수 있는 능력을 초과하는 패킷이 유입되었을 때 정상 서비스가 방해받거나 보안 장비의 이상동작을 하는 것을 막기 위하여 기존의 패킷 필터링 장비의 패킷 검사 오버헤드를 줄이기 위한 방법으로 간편 필터링 기법을 제안하였다. 비교적 간단한 패킷의 길이정보와 스캔 행동 IP 리스트를 이용한 간편 필터링 기법은 보안장비의 패킷 처리 오버헤드를 줄임으로써 정상 서비스의 가용성을 향상시키고 보안장비의 가용성을 향상시켰다.

또한 이전에 발생한 대표적인 웜들의 예를 조사하고 감염패킷을 스캔 행동을 보이는 웜의 패킷을 필터링 한 후에 길이별로 분류한 결과로 패킷을 검사하지 않고 통과시켰을 때 문제가 없는 것을 보였다.

본 논문에서 제안된 방법에는 몇 가지 한계가 있다. 간편 필터링 기법을 흔하게 사용한다면 DDoS 공격의 패턴이 달라질 수 있다. 공격의 효율성이 떨어지더라도 긴 패킷으로 공격을 할 수 있다. 긴 길이의 패킷을 이용한 공격은 현재 조건의 간편 필터링 기법은 아무런 검사 없이 통과하게 된다. 물론 보안 장비 자체의 오버헤드는 줄지만 보안장비의 본래의 목적은 달성하지 못하게 된다. 또한 향후 발생할 가능성이 있다고 연구되고 있는 Hilist 웜[10]은 스캔 행동 없이 호스트를 감염시키기 때문에 간편 필터링 기법을 적용했을 경우 탐지하기 힘들다.

앞으로 간편 필터링에 맞는 조건들을 더 찾아서 사용자가 여러 조건 중에 네트워크 환경에 맞는 조건을 선택할 수 있는 방법을 연구할 계획이다. 또한 실험을 통하여 간편 필터의 효과를 측정할 계획이다.

참고문헌

[1] http://en.wikipedia.org/wiki/Morris_worm

[2] http://en.wikipedia.org/wiki/Code_Red_worm

[3] http://en.wikipedia.org/wiki/SQL_slammer_%28computer_worm%29

[4] 신승원, 오진태, 김기영, 장종수, "Worm 탐지기법에 대한 연구", 한국정보보호학회, 정보보호학회지 제15권, 제2호, 2005. 4

[5] 김재현, 강신헌, 한국정보보호학회,"네트워크 트래픽 특성을 이용한 스캐닝 웜 탐지기법", 정보보호학회논문지 제17권 제1호, 2007. 2

[6] 전용희, "인터넷 웜의 탐지 및 대응기술", 한국통신학회지 (정보와통신) 제22권 8호, pp. 98-133, 2005.8,

[7] J.Y. Jung, S. Schechter, and Arthur W. Berger, "Fast Detection of Scanning Worm Infections," RAID 2004, Sophia Antipolis French, Sep. 2004

[8] 신승원, 오진태, 김기영, 장종수, "인터넷 웜 공격 탐지 방법 동향", 전자통신동향분석, 제20권 제1호, pp.9-16, 2005년 2월

[9] 류진형, 김혜진, 이재국, 김형식, "CLICK Modular Router를 위한 자기 재설정 기법", 한국정보과학회 2006 가을 학술발표논문집 제33권 제2호(D), 2006, 10

[10] S. Antonatos, P, Akritidis, E.P. Markatos, K.G. Anagnostakis, " Defending against hitlist worms using network address space randomization", Computer Networks: The International Journal of Computer and Telecommunications Networking archive Volume 51 , Issue 12 , August 2007