한국지능시스템학회 논문지 2008, Vol. 18, No. 5, pp. 679-684

퍼지 로직을 이용한 느린 포트스캔 공격 탐지 및 대응 기법

A Slow Portscan Attack Detection and Countermove Mechanism based on Fuzzy Logic

김재광 · 윤광호 · 이승훈 · 정제희 · 이지형

Jaekwang Kim, KwangHo Yoon, Seunghoon Lee, Je-hee Jung and Jee-Hyong Lee

성균관대학교 정보통신공학부

요 약

느린 포트스캔 공격 탐지는 네트워크 보안에서 중요한 분야 중 하나이다. 본 논문에서는 퍼지 룰을 이용한 비정상 트래픽 컨트롤 프레임워크를 이용하여 느린 포트스캔 공격을 탐지하고 대응하는 방법을 제안한다. 비정상 트래픽 컨트롤 프레임워크는 침입차단 시스템으로 동작하면서 의심 단계의 네트워크 트래픽을 대응하는 기능을 가진다. 본 논문에서 제안하는 방법은 공격 혹은 공격 의심 트래픽에 대해 단계적 대응을 한다. 먼저 의심 단계에 있는 트래픽에 대해 대역폭을 줄여 서비스를 하다가 최종적으로 공격으로 판명되면 트래픽을 차단한다. 본 논문에서는 제안한 방법을 프레임워크에 구축하고 실험을 통해 느린 포트스캔 공격에 효과적임을 보인다.

키워드 : 퍼지 로직, 느린 포트스캔, 공격 탐지, 단계적 대응 프레임워크

Abstract

The slow port scan attack detection is the one of the important topics in the network security. We suggest an abnormal traffic control framework to detect slow port scan attacks using fuzzy rules. The abnormal traffic control framework acts as an intrusion prevention system to suspicious network traffic. It manages traffic with a stepwise policy: first decreasing network bandwidth and then discarding traffic. In this paper, we show that our abnormal traffic control framework effectively detects slow port scan attacks traffic using fuzzy rules and a stepwise policy.

Key Words : Fuzzy Logic, Slow Port Scan, Intrusion Detection, Abnormal Traffic Control Framework.

1. 서 론

포트스캔 공격은 Remote-to-Local (R2L) 공격을 위한 가장 초기 단계로서 공격 대상이 되는 시스템의 특정 포트가 열려 있는지 아닌지를 알아내기 위해 살펴보는 행위이다. 포트스캔 공격을 통해 공격자들은 열려있는 포트를 알아내고 알아낸 포트를 통해 공격 대상 시스템의 잠재적인 약점이나 취약성을 알아내어 불법 행위를 시도한다. 오늘날 포트스캔 공격은 매우 빈번하게 발생되고, 그 공격 방법도 점차적으로 고도화되고 있다. 이런 환경에서 네트워크에 연결된 중요 시스템들을 보호하기 위해서는 포트스캔 공격을 탐지하고 대응하는 연구가 매우 중요하다.

기존의 방화벽이나 침입 탐지/차단 시스템에 구현된 포트스캔 공격 탐지 방법은 패킷의 출발지 주소와 목적지 주소, 그리고 포트 정보를 이용하여 공격 패킷의 패턴을 탐지하는 방법이 주를 이루었다. 기존의 방화벽을 비롯한 네트워크 침입 탐지/차단 시스템은 공격 행위가 명확한 open 포트스캔 공격 방법이나 변형이 비교적 단순한 half-open 포트스캔 공격 방법의 대부분을 탐지할 수 있으며, 탐지된 공격 트래픽을 차단하는 방법으로 공격에 대응하였다.

그러나 느린 포트스캔 공격과 같이 공격 여부를 판단하기 어려운 스텔스 포트스캔 공격들은 공격을 탐지해 내는 것과 탐지 후, 대응 방법에 어려움이 있다. 특히 느린 포트스캔 공격은 기존의 탐지 방법만으로는 정상 행위와 구분하기 어렵다. 때문에 엄격한 탐지 및 대응 규칙을 적용하지만 그럴 경우 오탐지율(false positive rate)이 높아져, 오히려 정상 행위를 방해하는 경우가 발생한다 [1].

본 논문에서는 퍼지 로직을 사용하여 느린 포트스캔 공격을 탐지하고 단계적 대응 정책을 사용하여 탐지된 느린 포트스캔 공격에 효과적으로 대응하는 방법을 제안한다. 또, 프레임워크의 구현과 실험을 통해 제안 방법을 검증한다. 실험 결과 제안된 방법을 통해 느린 포트스캔 공격 탐지 및 대응에 효과가 있음을 확인하였다.

본 논문의 구성은 다음과 같다. 2장에서 포트스캔 공격 방법에 대해 설명하고, 3장에는 느린 포트스캔 공격 탐지 방법에 대해 자세히 설명하며, 4장에서는 제안 방법을 이용한 느린 포트스캔 공격의 탐지와 대응 결과를 보인다. 마지막으로 5장에서는 결론을 말한다.

접수일자 : 2008년 5월 23일
완료일자 : 2008년 9월 30일
본 연구는 21세기 프론티어 연구개발사업의 일환으로 추진되고 있는 지식경제부의 유비쿼터스컴퓨팅및네트워크원천기반기술개발사업의 08B3-B1-10M 과제로 지원을 받았습니다.

2. 포트스캔 공격

포트스캔 공격은 크게 open 포트스캔 공격, half-open

포트스캔 공격, 스텔스 포트스캔 공격의 세 가지 방법으로 나눌 수 있다. 각 포트스캔 공격 방법의 공통된 목적은 공격 대상 시스템의 열려 있는 포트와 닫혀 있는 포트를 알아내는 것이다 [2]. Open 포트스캔 공격과 half-open 포트스캔 공격은 침입 탐지/차단 시스템에 의해 접속 로그가 남기 때문에 비교적 쉽게 탐지된다. 스텔스 포트스캔 공격 같은 경우 침입 탐지/차단 시스템이나 방화벽을 우회하도록 다양한 방법을 사용하기 때문에 정확한 탐지가 어렵다.

2.1 Open 포트스캔 공격

2.1.1 Open 포트스캔 공격

Open 포트스캔 공격은 전통적인 3-way TCP/IP 핸드 쉐이킹을 사용하여 연결을 하기 때문에 연결 로그를 통해 탐지하기가 매우 쉽다. 연결 순서는 다음과 같다.

client -> SYN
server -> SYN/ACK
client -> ACK

Client는 연결을 시도하는 노드로서 공격자의 컴퓨터에 해당하고, server는 포트스캔 공격 대상 노드에 해당한다. Client에서 SYN 패킷을 보내고 server에서 SYN/ACK 패킷을 보낸 후, 다시 client에서 ACK 패킷을 보내면 3-way TCP/IP 핸드 쉐이킹에 의해 연결이 완료된 것이다. 즉, 대상 포트가 열려 있는 것을 의미한다. Client는 같은 방법으로 공격 대상 시스템의 포트를 처음부터 마지막 포트까지 연결을 시도하여 열린 포트를 알아낸다. 반대로 닫힌 포트라면 아래와 같은 순서의 연결을 맺게 된다.

client -> SYN
server -> RST/ACK
client -> RST

Open 포트스캔 공격은 완전한 연결을 이루기 때문에 공격 대상 시스템의 특정 포트가 열린 것을 정확하게 알아낼 수 있으며, 빠르고, 쉽게 탐지할 수 있는 장점이 있지만 방화벽이나 침입 탐지 시스템에 의해 쉽게 탐지되는 공격 방법이다.

2.1.1 Reverse ident. 포트스캔 공격

Reverse ident. 포트스캔 공격은 open 포트스캔 공격의 한 종류로서 113번 포트를 통해 ident/auth 데몬으로 질의를 하여 사용자 정보, 엔티티, 프로세스 등의 정보를 얻어내는 공격이다. ident/auth 데몬은 관리자 권한으로 동작하기 때문에 공격자는 이 데몬의 취약점을 이용하여 공격한다. 현재 시중에 있는 대부분의 침입 탐지/차단 시스템은 reverse ident. 포트스캔 공격을 open 포트스캔 공격의 하나로 탐지해 낸다 [3].

2.2 Half-open 포트스캔 공격

Half-open 포트스캔 공격은 이름 그대로 공격자가 3-way 핸드 쉐이킹이 완료되기 전에 연결을 끊는 공격 방법이다. 이렇게 함으로써 공격자는 포트스캔 공격을 시도한 연결 흔적을 남기지 않을 수 있다.

2.2.1 SYN 포트스캔 공격

SYN 포트스캔 공격은 포트의 연결을 시도하는 3-way 핸드 쉐이킹 과정에서 client가 ACK 패킷을 보내는 대신 RST 패킷을 보내므로 정보만 얻어낸 후, 비정상적으로 연결을 종료하는 방법이다. SYN 포트스캔 공격의 연결 순서는 다음과 같다.

client -> SYN
server -> SYN/ACK
client -> RST

공격자는 SYN 패킷을 보내고 공격 대상 시스템으로부터 어떤 패킷이 응답으로 오는가 확인한다. 만일 SYN/ACK 패킷이 오면 공격 대상 시스템의 목표 포트는 열려 있다는 것이며, 반대로 RST/ACK 패킷이 오면 목표 포트가 닫혀 있다는 것이다. 공격 대상 시스템의 목표 포트가 열려 있다는 것을 확인 한 경우, 공격자는 ACK 패킷을 보내 정상적인 연결을 맺는 대신 RST 패킷을 보내 비정상적으로 연결을 끊는다. 공격 대상 시스템의 네트워크 로그에는 client로부터의 연결이 완료되지 않았기 때문에 open 포트스캔 공격으로 판단되지는 않는다. 이 방법을 이용하면 기본적인 침입 탐지 시스템 들을 피할 수 있다. 하지만 이 방법을 실행하기 위해서는 공격자 시스템의 루트 권한이 필요하고, 최신의 침입 탐지 시스템들의 룰셋에 의해서는 탐지되는 한계가 있다.

2.2.2 IP ID header aka "dumb" 포트스캔 공격

ID header 포트스캔 공격은 TCP/IP 연결을 이용한 스캔보다 좀 더 지능화된 방법이다. SYN 스캔 공격 방법을 기본으로 하되, SYN 패킷의 소스 주소를 공격자 시스템의 주소 대신 다른 시스템의 주소로 바꾸어 보낸다. 이로인해 SYN 포트스캔 공격을 탐지할 수 있는 침입 탐지/차단 시스템이라도 진짜 공격자 대신 다른 시스템을 공격자로 오판하게 된다. 진짜 공격자는 침입 탐지/차단 시스템으로 부터 오해를 받고 있는 다른 시스템의 패킷을 스니핑 하여 공격 대상 시스템의 포트가 열렸는지 유무를 알 수 있다. 이 공격은 SYN 포트스캔 공격 외에 다른 포트스캔 공격에도 응용이 가능하다 [4].

2.3 스텔스 포트스캔 공격

"스텔스" 포트스캔 공격이란 말은 Chris Klaus가 쓴 "Stealth Scanning: Bypassing Firewalls/SATAN Detectors" 이란 문서에서 처음 언급되었다. 이 용어는 본래 half-open 포트스캔 공격을 탐지할 수 있는 침입 탐지 시스템을 우회하는 기술을 소개하는데 사용되었다. 오늘날 스텔스 포트스캔 공격은 다양한 방법으로 발전되고 있다. 스텔스 포트스캔 공격은 패킷에서 NULL 플래그를 세팅하는 것, All 플래그를 세팅하는 기술을 포함하여 필터나 방화벽, 라우터들을 우회하는 것, 정상의 네트워크 트래픽으로 위장하는 것, 갖가지 패킷들을 섞어 공격 패턴을 알 수 없도록 하는 등 다양한 방법이 있다. 느린 포트스캔 공격은 스텔스 포트스캔 공격의 한 종류이다 [5].

3. 느린 포트스캔 공격 탐지 방법

본 절에서는 느린 포트스캔 공격을 탐지하고 대응하기 위해 구현한 비정상 트래픽 컨트롤 프레임워크 (ATCF -

Abnormal Traffic Control Framework)와 이 프레임워크에 구현한 느린 포트스캔 공격 탐지 방법을 보인다 [6].

3.1 시스템 구조도

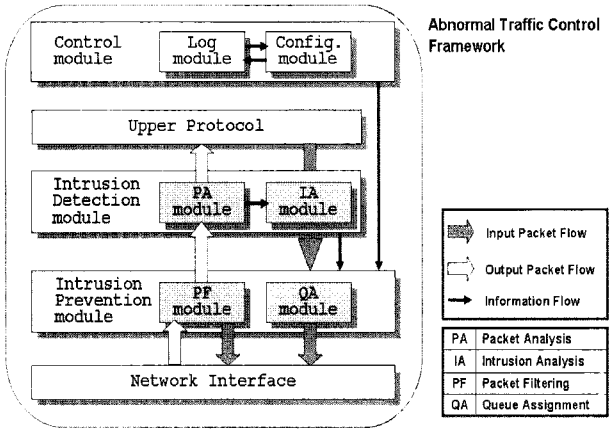

그림 1. 느린 포트스캔 공격 대응 프레임워크
Fig. 1. Abnormal Traffic Control Framework for Slow Portscan Attack

느린 포트스캔 공격을 탐지하고 대응하는 프레임워크의 시스템 구조도는 그림 1이 보이는 바와 같다. 시스템은 공격을 탐지해내는 Intrusion Detection 모듈과 탐지한 공격에 대해 대응하는 Intrusion Prevention 모듈, 그리고 Control 모듈로 구성된다.

Intrusion Detection 모듈은 네트워크층에서 Packet Filtering (PF) 모듈을 통과하여 도착한 패킷을 Packet Analysis (PA) 모듈을 통해 분석하고, Intrusion Analysis (IA) 모듈에서 그 분석결과를 이용하여 공격을 판단한다. IA 모듈에는 퍼지 로직 기반의 느린 포트스캔 공격 탐지 기법이 적용되어 느린 포트스캔을 효과적으로 탐지한다.

Intrusion Prevention 모듈은 탐지한 공격에 대해 대응하는 모듈로 PF 모듈과 Queue Assignment (QA) 모듈로 구성되어 있다. PF 모듈은 공격으로 확실하게 판명된 패킷을 차단하는 모듈이며 QA 모듈은 공격 정도에 따라 대역폭을 줄여 대응하는 모듈이다.

3.2 탐지 방법

느린 포트스캔 공격을 탐지하는데 어려운 점은 공격인지 아닌지 명확한 판단 기준이 없다는 것이다. 퍼지 로직은 명확한 판단이 어려운 명제에 대하여 판단 근거를 제공한다. 그러므로 공격 정도를 퍼지화하여 값을 책정한 후, 공격 대응 근거로 사용할 수 있다. 산출한 값을 사용하여 비정상 트래픽을 조절한다 [7][8][9].

3.2.1 퍼지 멤버십 함수

느린 포트스캔 공격에 대한 퍼지 모델을 만들기 위해 최근 1초, 최근 1분, 최근 1시간 동안 느린 포트스캔 공격으로 여겨지는 패킷의 수를 세어 저장한다. 각 값은 Short (*S*), Middle (*M*), Long (*L*), 세 종류의 타임윈도우에 저장한다. 그림 2는 세 종류의 타임 윈도우 예를 보인다.

또한 각 타임 윈도우마다 세 가지 퍼지 상태를 만들어 Normal (N), Suspicious (S), 그리고 Attack (A)으로 정의한다. 그림 3은 세 가지 퍼지 상태에 따른 퍼지 멤버십 함수를 보인다.

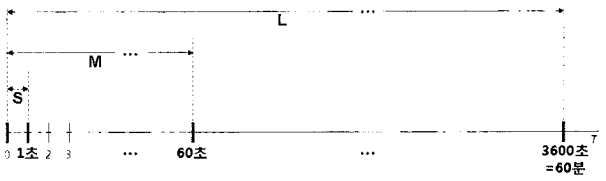

그림 2. 세 종류의 타임 윈도우 예
Fig. 2. The Example of the Three Time Windows

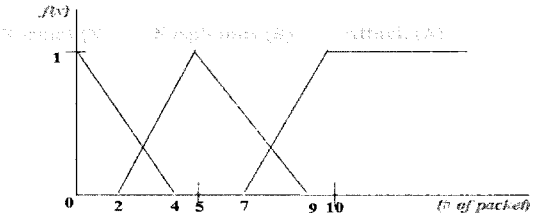

그림 3. 세 가지 퍼지 상태에 따른 퍼지 멤버십 함수
Fig. 3. The Fuzzy Membership Function of Three Fuzzy Terms

그림 3에 사용된 세 가지 상태는 다음과 같은 전문가 의견을 반영하여 정하였다. 먼저 특정 source address에서 특정 destination address의 여러 port로 향하는 패킷을 공격으로 의심되는 패킷으로 정의한다. 다음으로 nmap 포트스캔 도구를 통해 각 단위 시간 별로 느린 포트스캔 공격 트래픽을 분석을 통해 공격으로 의심되는 패킷의 수가 단위 시간당 10회인 때를 Attack (A) 상태로 정한다. 단위 시간당 공격으로 의심되는 패킷의 수가 0인 경우는 Normal (N)로 정의하고 0과 10의 중간인 5인 상태를 Suspicious (S)로 정한다. 이때 퍼지 멤버십 함수는 삼각형 모양의 함수를 따르며 삼각형의 왼쪽 변의 기울기는 1/3, 오른쪽 변의 기울기는 -1/4로 정하였다.

그림 3이 보이는 바와 같이 세 가지 상태는 중복되는 구간을 포함하는데 단위 시간당 패킷의 수가 3개일 때, 8개일 때가 중복되는 구간이다. 이 구간은 정확한 판단이 어려운 구간으로서 정상으로 판단하거나 공격으로 판단할 경우 각각의 에러를 감수할 수밖에 없다. 그러므로 모두 Suspicious (S) 상태로 정하여 정상 상태도 공격 상태도 아닌 구간으로 정하였다.

3.2.2 퍼지 룰

세 종류의 타임 윈도우와 세 가지의 퍼지 상태를 조합하여 퍼지 룰을 작성한다. 표 1은 27 가지의 퍼지 룰 중 일부를 보인다.

표 1이 보이는 바와 같이 입력 열은 27 가지의 조합을 말한다. 출력은 현재 트래픽이 공격인지를 알려주는 공격 정도를 보인다. 예를 들면 룰 27번은 최근 1초 동안 느린 포트스캔 공격으로 의심되는 패킷이 0개 였고(Short = Normal), 최근 1분 동안 의심 패킷이 0개 (Middle = Normal), 최근 1시간 동안 의심 패킷이 0개(Long = Normal)로서 현재 트래픽은 공격 정도 0.9의 값을 얻게 된다.

표 1. 27 가지의 퍼지 룰 중 일부
Table 1. Some Examples of Fuzzy Rule

Rule #	Short	Middle	Long	Attack degree
1	A	A	A	2.7
2	A	A	S	2.6
3	A	A	N	2.5
...	...	...	...	...
12	S	S	A	1.9
13	A	N	N	1.9
14	S	S	S	1.8
...	...	...	...	...
25	N	N	A	1.1
26	N	N	S	1.0
27	N	N	N	0.9

룰 25번의 경우는, Short = Normal 이고 Middle = Normal 이고 Long = Attack 으로서 공격 정도는 1.1이다. 즉, 느린 포트스캔 공격으로 의심되는 패킷이 최근 1초 동안과 최근 1분 동안은 발견되지 않았지만 최근 1시간 동안을 보면 다수가 발견된 경우이다. 이 경우에는 공격 정도를 1.1로 정하였다.

룰 13번의 경우는, Short = Attack 이고 Middle = Normal 이고 Long = Normal 로서 공격 정도는 1.9이다. 즉, 느린 포트스캔 공격으로 의심되는 패킷이 최근 1시간과 최근 1분 동안은 발견되지 않았지만 최근 1초 동안 많이 발견된 경우이다. 이 경우는 위험한 상태로서 공격 정도를 1.9로 정하였다.

표 1이 보이는 바와 같이 공격으로 의심되는 패킷이 최근 1초, 1분으로 단 기간 내에 발견될수록 공격 정도는 더 높게 정하였다.

느린 포트스캔 탐지를 위해 사용한 퍼지 모델은 TSK 모델이며 비퍼지화는 mean of maxima 방법을 사용하였다.

3.2.3 대응 방법

대응 방법은 단계적 전략을 사용한다. 자세한 내용은 다음과 같다.

만일 퍼지 룰을 통해 트래픽이 정상으로 판단되면 100% 대역폭을 제공한다. 반대로 트래픽이 공격으로 판단되면 0% 대역폭, 즉 트래픽 차단을 한다. 하지만 트래픽이 정상인지 공격인지 판단하기 모호한 경우 100% 대역폭을 제공할 수도 없고, 트래픽을 차단할 수도 없다. 만일 판단하기 모호한 트래픽을 모두 차단할 경우, 오탐지율이 증가하게 되며, 반대로 모호한 트래픽을 모두 허용하면 미탐지율이 증거하게 된다.

이러한 상황에 대응하기 위하여 전문가적 의견을 사용하였다. 즉, 판단하기 모호한 트래픽에 대하여 차단하지 않고 대역폭을 0.01%로 낮추어 제공한다. 의심 트래픽에 대해 최소한의 대역폭만을 제공한 채, 관찰을 계속한다. 만약 퍼지 룰에 의해 공격 정도가 증가하여 1.9 이상이 되면 의심 트래픽을 차단한다. 반대로 공격 정도가 감소하여 1.0 미만으로 되면 의심 트래픽에 대해 100% 대역폭을 제공한다. 혹은 지속적으로 공격 정도가 1.0 이상 1.9 미만을 유지할 때에는 트래픽이 모호한 상태로 대역폭을 0.01%로 낮추어 관찰을 지속한다. 표 2는 전문가적 의견을 기반으로 한 단계적 대응 전략을 보인다.

표 2. 전문가적 의견을 기반한 단계적 대응 전략
Table 2. Stepwise Strategy based on Expert Opinion

Attack degree (Ad)	Managing
$Ad \geq 1.9$	Q = 0%
$1.0 \leq Ad < 1.9$	Q = 0.01%
$Ad < 1.0$	Q = 100%

4. 실 험

본 절에서는 느린 포트스캔 공격을 탐지하고 대응하는 제안 방법의 효과를 실험을 통해 보인다.

4.1 실험 시나리오

테스트 베드를 통해 총 16개의 실험 시나리오를 실험하였다. 각 실험 시나리오는 두 가지 요소의 조합으로 정하였다. 첫째 요소는 대응 방법이고, 둘째 요소는 느린 포트스캔 공격의 공격 시간이다. 두 번째 요소인 느린 포트스캔의 공격 시간을 반영할 때, 1초 이상의 공격 시간은 고려하지 않았다. 1초 이상의 느린 포트스캔 공격은 모든 포트를 스캔하는데 너무 많은 시간이 소요되기 때문이다. 표 3은 16개의 실험 시나리오 번호를 보인다.

표 3. 16 가지 실험 시나리오
Table 3. 16 Test Scenarios

Delay Policy	No delay	Delay with 1 ms	Delay with 10 ms	Delay with 1 sec.
No managing	Test 1-1	Test 1-2	Test 1-3	Test 1-4
Drop	Test 2-1	Test 2-2	Test 2-3	Test 2-4
Drop/ control	Test 3-1	Test 3-2	Test 3-3	Test 3-4
Our framework	Test 4-1	Test 4-2	Test 4-3	Test 4-4

4.2 실험 환경

공격자와 공격 대상 시스템은 그림 4가 보이는 바와 같이 간접적으로 연결 되어 있다. 비정상 트래픽 컨트롤 프레임워크는 192.168.1.x와 192.168.2.x 두 개의 다른 네트워크를 연결하고 있다. 각 시스템의 사양은 표 4가 보이는 바와 같다.

표 4. 실험 환경의 시스템 사양
Table 4. Each system in Testbed.

	CPU (hz)	Memory (Bytes)	OS	Network Card
Attacker	M-Pentium III800 M	384 M	Linux (2.6.22)	100Mbps (x1)
ATCF	AMD Athlon 1G (x2)	512 M	Linux (2.4.34)	100Mbps (x3)
Target system	Pentium4 2.8G	1 G	Linux (2.6.22)	1Gbps (x1)

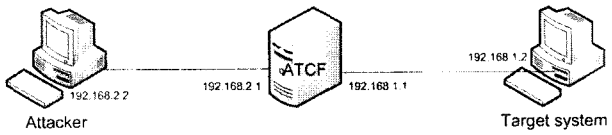

그림 4. 실험 환경
Fig. 4. Testbed

4.3 실험 결과

본 절은 트래픽 그래프를 통해 실험 결과를 보인다. 표 3이 보이는 바와 같이 16개의 실험 시나리오를 수행한 후, 각 트래픽 그래프를 얻었다. Test 1-1, Test 1-2, Test 1-3, 그리고 Test 1-4는 아무런 대응을 하지 않았을 때의 트래픽 그래프이다. 즉, 이 그래프는 실제 포트스캔 공격의 트래픽이다. No delay는 일반 포트스캔 공격이며, Delay with 1ms는 1ms 마다 공격 패킷을 보내는 느린 포트스캔 공격의 트래픽이다. Delay with 10ms는 10ms 마다 공격 패킷을 보내는 느린 포트스캔 공격의 트래픽이며 Delay with 1sec.는 1초마다 공격 패킷을 보내는 느린 포트스캔 공격의 트래픽이다. 그림 5는 아무 대응을 하지 않은 포트스캔 공격 트래픽의 그래프를 보인다. 그림 5(a)-(d)는 test 1-1, 1-2, 1-3, 그리고 1-4에 각각 대응한다. 그림 5(a)는 일반 포트스캔 공격 트래픽을 보인다. 5번의 공격이 연속으로 발생한 것이며 일반 포트스캔 공격은 매우 짧은 순간에 트래픽이 집중되어 있음을 알 수 있다. Y축의 최대값은 200,000이다. 그림 5(b)는 delay 1ms의 느린 포트스캔 공격 트래픽의 그래프를 보인다. 공격 패킷은 12초에서 22초 사이에 나타난다. 그림 5(c)는 delay 10ms의 느린 포트스캔 공격 트래픽의 그래프를 보인다. 그림 5(d)는 delay 1sec.의 느린 포트스캔 공격 트래픽의 그래프를 보인다.

표 3의 실험 시나리오에서 ATCF with fuzzy logic의 경우를 제외하고는 대부분의 실험이 의미 없는 결과를 보였다. 왜냐하면 No managing 방법이나 Drop 방법이나 Drop control 방법을 사용하는 프레임워크에서는 느린 포트스캔을 탐지할 수가 없기 때문이다. 그러므로 test 2-2, 3-2의 그래프는 test 1-2와 같다. 매우 느린 포트스캔 공격인 test 1-4는 원격 로그인이나 이메일 체크, 혹은 웹 서핑 등과 같은 정상 행위와 매우 유사하여 공격 행위와 구분하는 것이 불가능하였다. 비록 실제 공격이라고 하여도 공격이 완료되기까지는 14시간이 소요되어서 매우 비효율적인 공격이다. 그러므로 실험 시나리오 중test 4-2, 4-3의 결과에 집중하여 분석한다. 그림 6은 비정상 트래픽 컨트롤 프레임워크에 의해 탐지 및 대응 되는 느린 포트스캔 공격 트래픽을 보인다. 그림 6(a)는 1ms 속도로 공격을 시도하는 느린 포트스캔 공격의 트래픽이 2초 지점에서 프레임워크에 의해 탐지되어 5초부터 24초까지는 의심 트래픽으로 분류되어 대역폭이 매우 낮아졌고, 느린 포트스캔 공격 패킷이 지속되자 퍼지 룰에 의해 25초 지점에서 공격으로 판단되어 트래픽이 차단되는 것을 보인다. 그림 6(b)은 속도 10ms의 느린 포트스캔 공격에서 트래픽의 변화가 그림 6(a)와 동일한 과정으로 진행됨을 보인다. 트래픽은 16초까지 증가하다가 22초 지점에서 제안 프레임워크에 의해 의심 트래픽으로 판명되어 낮아짐을 보인다. 또, 47초 지점에서는 공격으로 판명되어 차단됨을 보인다. 이러한 결과를 통해 제안 방법과 이를 구현한 프레임워크가 느린 포트스캔 공격을 탐지하고 대응하는데 효과적임을 보인다.

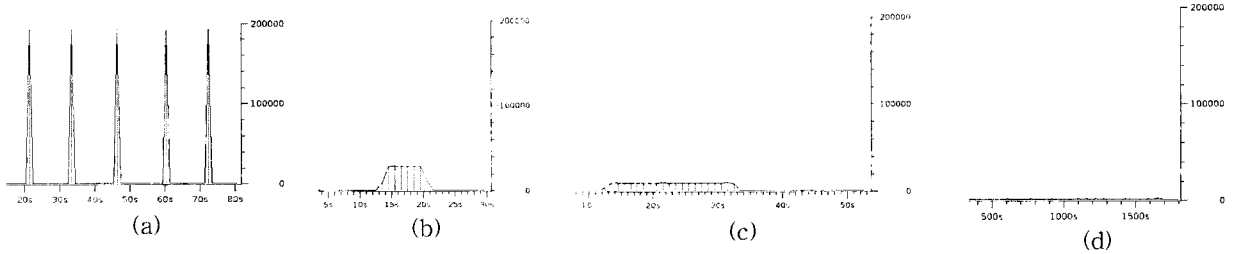

그림 5. 다양한 축에 따른 각 트래픽
Fig. 5. Each Traffic Shape with Different Axis.

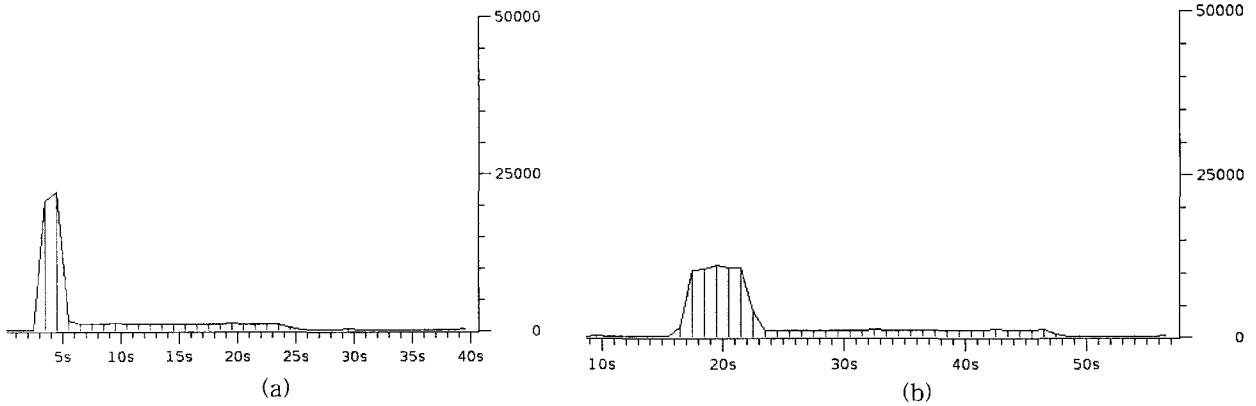

그림 6. 각 속도에 따른 느린 포트스캔 공격 대응 트래픽
Fig. 6. The Traffic Shape of Managing Slow Portscan Attack of Each Delay

5. 결 론

느린 포트스캔 공격의 탐지와 대응은 네트워크 보안 분야에서 매우 중요한 연구이다. 하지만 느린 포트스캔의 공격은 정상 행위와 구분하기가 매우 어렵다. 기존의 탐지 방법으로는 느린 포트스캔 공격을 탐지하기 위해 패턴의 적용을 엄격하게 하여 정상 행위를 차단하는 경우가 많았다.

본 논문에서는 퍼지 로직을 사용하여 느린 포트스캔 공격을 탐지하고 단계적 대응 전략을 사용하여 대응하는 새로운 방법을 제안하였다. 또, 제안된 방법을 프레임워크로 구현하고 실험을 통해 느린 포트스캔 공격을 효과적으로 차단함을 보였다.

참 고 문 헌

[1] K. Ko, E. Cho, T. Lee, Y. Kang, Y. I. Eom, "The Abnormal Traffic Control Framework based on QoS Mechanisms," *LNCS* Vol. 3280, pp. 167-175, 2004.

[2] Fyodor, Art of portscaning, http://www.phrack.com.

[3] O. Afkin, Networking Scanning, http://www.sys-security.com.

[4] Hobbit, FTP bounce attack, http://www.insecure.org/nmap/hobbit.ftpbounce.txt.

[5] Dethy, Examining port scan methods, http://www.totse.com/en/hack/hacking_lans_wans_networks_outdials/162024.html.

[6] H. Wei, Y. Lin, "A Survey and Measurement-Based Comparison of Bandwidth Management Techniques," *IEEE Comm. Soc. Surveys and Tutorials*, Vol. 5, No. 2, pp. 10-21, 2003.

[7] G. Singarju, L. Teo, Y. Zheng, "A Testbed for Quantitative Assignment of Intrusion Detection System using Fuzzy Logic," *Proc. of IWIA'04*, pp. 79-93, 2004.

[8] Z. Jian, D. Yong, and G. Jian, Intrusion "Detection System based on Fuzzy Default Logic," *The IEEE International Conference on Fuzzy Systems*, Vol. 2, pp. 1350-1356, 2003.

[9] A. Ofrila, J. Carbo, A. Ribagorda, "Fuzzy Logic on Decision Model for IDS," *The IEEE International Conference on Fuzzy Systems*, Vol. 2, pp. 1237-1242, 2003.

저 자 소 개

김재광(Jaekwang Kim)
2004년 : 성균관대 정보통신공학부 학사
2006년 : 성균관대 컴퓨터공학과 석사
2007년 : 성균관대 정보통신기술연구소 연구원
2008년 ~ 현재 : 성균관대 전자전기컴퓨터 공학과 박사과정
관심분야 : 네트워크 보안, 기계학습, 지능시스템
Phone : +81-31-290-7987
Fax : +81-31-299-4637
E-mail : linux@ece.skku.ac.kr

윤광호(KwangHo Yoon)
2007년 : 성결대 컴퓨터공학부 학사
2008년 ~ 현재 : 성균관대 전자전기컴퓨터 공학과 석사과정
관심분야 : 게임 인공지능, 지능형 웹, 기계학습
Phone : +81-31-290-7987
Fax : +81-31-299-4637
E-mail : yoonkh2000@gmail.com

이승훈(Seunghoon Lee)
2007년 : 성균관대 컴퓨터 공학부 학사
2008년 ~ 현재 : 성균관대 전자전기컴퓨터 공학과 석사과정
관심분야 : 유비쿼터스 컴퓨팅, 서비스컴포지션, 사례기반추론
Phone : +81-31-290-7987
Fax : +81-31-299-4637
E-mail : reinblame@naver.com

정제희(Je-hee Jung)
2007년 : 목포해양대 소프트웨어과 학사
2007년 ~ 현재 : 성균관대 전자전기컴퓨터 공학과 석사과정
관심분야 : 인공지능, 자막 추출, 영상 처리
Phone : +81-31-290-7987
Fax : +81-31-299-4637
E-mail : gulingi@skku.edu

이지형(Jee-Hyoung Lee)
1993년 : 한국과학기술원 전산학과 학사
1995년 : 한국과학기술원 전산학과 석사
1999년 : 한국과학기술원 전산학과 박사
2002년 ~ 현재 : 성균관대 정보통신공학부 부교수
관심분야 : 지능시스템, 기계학습, 온톨로지
Phone : +81-31-290-7154
Fax : +81-31-299-4637
E-mail : jhlee@ece.skku.ac.kr