ISSN 1598-0170 (Print)
ISSN 2287-1136 (Online)
http://www.jksii.or.kr

# 공격 탐지 임계값을 고려한 비상태기반 방화벽 정책 추론 방법

# An Inference Method of Stateless Firewall Policy Considering Attack Detection Threshold

김 현 우[1] 권 동 우[1] 주 홍 택[1*]
Hyeonwoo Kim Dongwoo Kwon Hongtaek Ju

**요 약**

방화벽 정책 추론은 사전지식 없이 특정 네트워크로의 능동적 탐지기법을 이용한 응답 패킷 분석으로 방화벽 정책을 발견한다. 하지만, 외부에서 특정 네트워크로 추론 패킷을 어떻게 전송하는가에 따라 방화벽에 설정된 공격 탐지 임계값에 의해 네트워크 공격으로 탐지되기 때문에 무분별하게 패킷을 전송하는 방법은 유효하지 않다. 본 논문에서는 방화벽의 공격 탐지 임계값을 고려하여 네트워크 공격으로 탐지되지 않는 범위 내에서 추론 변수를 활용한 패킷 전송 알고리즘을 제안한다. 그리고 제안하는 알고리즘에 의해 전송되는 패킷이 네트워크 공격으로 탐지되는가를 검증한다. 마지막으로 우리는 실제 방화벽 정책과 추론된 정책을 비교하여 제안된 알고리즘의 정확성을 검증한 결과를 제시한다.

☞ 주제어 : 비상태기반 방화벽; 정책 추론; 공격 탐지 임계값; 능동 탐지; 추론 변수; 스윕 라인 알고리즘

**ABSTRACT**

Inferring firewall policy is to discover firewall policy by analyzing response packets as results of active probing without any prior information. However, a brute-force approach for generating probing packets is unavailable because the probing packets may be regarded as attack traffic and blocked by attack detection threshold of a firewall. In this paper, we propose a firewall policy inference method using an efficient probing algorithm which considers the number of source IP addresses, maximum probing packets per second and interval size of adjacent sweep lines as inference parameters to avoid detection. We then verify whether the generated probing packets are classified as network attack patterns by a firewall, and present the result of evaluation of the correctness by comparing original firewall policy with inferred firewall policy.

☞ keyword : Stateless Firewall; Policy Inference; Attack Detection Threshold; Active Probing; Inference Parameters; Sweep-line Algorithm

## 1. 서 론

인터넷 상에서 사이버 공격은 특정 기관의 네트워크 취약점을 수집하고 네트워크 장비의 부하를 감당할 수 없을 정도로 증가시켜 서비스가 정상적으로 제공되지 못하게 하는 목적으로 이루어진다. 가장 대표적인 사이버 공격의 예로는 특정 서버의 서비스를 제공할 수 없도록 다수의 패킷을 해당 서버로 전송하는 서비스거부공격(Denial of Service)이 있다. 각 단체나 기관에서는 내부 네트워크를 보호하기 위해 방화벽과 같은 보안 장비를 설치하여 외부의 공격에 대비하고 있으나, 사이버 공격에 대한 네트워크 취약점이 노출되어 있다.

방화벽은 인터넷과 연결된 네트워크 경로 상에서 가장 앞 단에 배치되며, 기본적으로 외부 또는 내부 네트워크로 향하는 모든 패킷을 검사하고 차단하는 보안 시스템이다. 방화벽을 경유하는 모든 패킷들은 방화벽 정책에 의해 허용되거나 차단된다[1]. 방화벽 정책은 다수 규칙들의 집합으로 구성되며, 각 규칙들은 조건과 허용여부로 구성된다. 각 규칙의 조건은 들어오거나 나가는 패킷들을 분류하기 위한 요소들을 정의하고 있으며, 일반적으로 5-tuple(프로토콜, 출발지 IP 주소, 목적지 IP 주소, 출발지 포트번호, 목적지 포트번호)이 여기에 해당된다.

악의적인 인터넷 사용자들은 특정 네트워크를 공격하기에 앞서 어떤 보안 취약점이 있는지 알아내기 위해서

[1] Computer Engineering, Keimyung University, Daegu, 704-701, Korea.
* Corresponding author (juht@kmu.ac.kr)
[Received 00 January 2013, Reviewed 00 February 2013, Accepted 00 May 2013]
☆ 이 논문은 2012년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2012R1A1A2006331)

(표 1) 방화벽 필터링 규칙의 예제
(Table 1) An example of the firewall filtering rules

| Rule Priority | Protocol | Source IP Address | Source Port Number | Destination IP Address | Destination Port Number | Action |
|---|---|---|---|---|---|---|
| R1 | TCP | Any | Any | 192.168.0.0/16 | 20:80 | Permit |
| R2 | TCP | Any | Any | 192.168.0.0/16 | 20000:30000 | Permit |
| R3 | TCP | Any | Any | 192.168.132.0/24 | Any | Permit |
| R4 | TCP | Any | Any | 192.168.10.0/20 | 1024:10000 | Permit |
| Default | Any | Any | Any | Any | Any | Deny |

먼저 내부 네트워크 토폴로지 구성 및 방화벽 정책 등을 사전에 수집하고자 한다. 이러한 보안 정보들은 외부에 공개적으로 제공되지 않기 때문에 공격자들은 스캐닝 기법을 활용하여 사전 보안 정보들을 알아낸다[2-3]. 대표적인 스캐닝 도구는 Nmap[4], Hping[5] 등이 있으며, 사용자가 원하는 패킷을 생성하고 전송하는 것이 가능하다. 이와 같이 공격자가 공격을 수행하기에 앞서 방화벽의 보안 정보를 알아낼 수 있다면, 효율적으로 다양한 공격이 가능하게 된다. 예를 들면, 방화벽에 정의된 규칙 중에서 가장 우선순위가 낮은 규칙에 해당되는 트래픽을 전송함으로써, 방화벽의 기본 차단 규칙 매칭에 의한 부하를 최대로 유발하여 방화벽 기능을 효율적으로 무력화할 수 있다[2, 6]. 또 다른 예는 방화벽을 통과하는 트래픽을 이용하여 네트워크 내의 특정 서버를 집중 공격할 수 있다.

하지만 외부에서 스캐닝 기법을 이용하여 특정 기관의 방화벽 정책을 알아내는 것은 용이하지 않다. 그 이유는 특정 네트워크로 전송한 다수의 트래픽이 방화벽에서 네트워크 공격 패턴으로 탐지되어 차단될 수 있기 때문이다[7]. 따라서 방화벽 정책 추론이 목적인 프로빙 패킷들은 방화벽의 공격 탐지 임계값에 의해 네트워크 공격으로 오인되지 않기 위해 최소한의 패킷 수와 전송 전략 등을 고려하여 지능적으로 패킷이 전송되어져야 한다. 기존의 방화벽 정책 추론 연구[8-9]들은 정책 추론을 위한 프로빙 패킷을 전송할 때 방화벽의 임계값 기반 공격 탐지 규칙을 고려하지 않았기 때문에 전송된 프로빙 패킷이 공격으로 오인되어 차단될 수 있다. 다음 연구로 H. Kim 등[10]은 방화벽의 공격 탐지 규칙에 영향을 주는 추론 변수를 정의하였으며, 각 추론 변수들의 값에 의한 추론 정확도의 상관계수 분석 결과를 제시하였다.

본 논문에서는 방화벽의 공격 탐지 임계값을 고려하여 네트워크 공격으로 탐지되지 않는 범위 내에서 방화벽 정책을 추론하기 위한 목적으로 제안된 추론 변수를 활용한 패킷 전송 알고리즘을 제안한다. 또한, 우리가 제안하는 추론 방법에 의해 전송되는 패킷이 네트워크 공격으로 탐지되는가를 검증하고자 한다. 마지막으로 T. Samak 등[8]이 제안한 FireCracker의 알고리즘과 정확성 측면에서의 추론 결과를 비교 분석한다. 본 논문의 실험 결과를 활용한다면, 우리가 제안한 방화벽 정책 추론 방법이 방화벽에서 네트워크 공격으로 탐지되지 않고 방화벽의 보안 기능을 회피할 수 있는 향상된 추론 방법을 마련할 수 있다.

우리는 2장에서 방화벽 정책 및 공격 탐지 임계값에 대한 간략한 설명과 방화벽 정책 추론 관련 기존의 연구들을 소개하며, 3장에서 공간상에 표현된 방화벽 정책 구조와 스윕 라인 알고리즘을 통해 방화벽 정책을 알아내는 과정을 설명한다. 4장에서는 방화벽의 공격 탐지 임계값에 영향을 주는 패킷 전송 알고리즘의 입력 매개변수를 추론 변수로 정의하고, 3장에서 언급된 스윕 라인 알고리즘을 기반으로 추론 변수를 활용하여 패킷을 전송하는 추론 방법을 제안한다. 5장에서는 각 추론 변수 설정에 따른 평균 추론 정확도의 실험 결과를 제시하고, 기존 연구인 FireCracker에서 제안한 알고리즘과 정확성 측면에서 비교 검증한 결과를 제시한다.

## 2. 관련 연구

### 2.1 방화벽과 방화벽 정책

표 1은 간단한 방화벽 정책 구성 예를 보여준다. 표 1에서 각 규칙의 번호는 상위에서부터 우선적으로 적용되는 규칙의 우선순위를 의미하며, 방화벽을 통과하고자 하는 패킷은 각각의 규칙에 해당하지 않을 경우 최종적으로 기본 규칙에 적용되어 허용되거나 차단된다. 규칙의 우선순위는 방화벽을 통과하고자하는 패킷이 필터링 규칙과 매칭이 될 순서를 의미하며, 규칙의 우선순위가

높은 순서대로 먼저 적용되어 패킷을 처리한다. 규칙 R1과 R2는 모든 외부 네트워크에서 내부 네트워크의 20~80의 포트 범위와 20000~30000인 포트 범위에 일치하는 패킷을 허용하고, 규칙 R3은 외부 네트워크로부터 목적지 IP 주소 범위 192.168.132.0/24에 해당하는 모든 패킷을 허용하며, 규칙 R4는 목적지 IP 주소 범위가 192.168.10.0/20이면서 1024~10000 포트 범위에 대한 패킷을 허용함을 의미한다. 마지막으로 기본 규칙은 상위의 규칙과 매칭이 되지 않은 모든 패킷들을 차단하는 규칙이다.

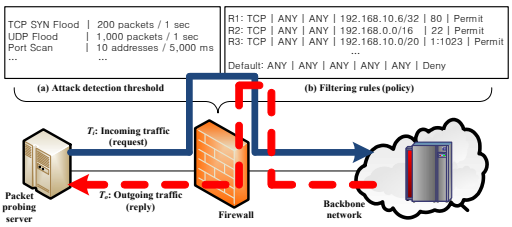
## 2.2 네트워크 공격 유형과 방화벽의 공격 탐지 임계값

방화벽은 표 1과 같이 5-tuple로 구성된 필터링 규칙이 기본적으로 구성되지만, 방화벽을 통과하고자 하는 패킷이 필터링 규칙에 의해 검사되기 이전에 내부적으로 네트워크 공격 유형과 같은 트래픽을 사전 차단하기 위한 목적으로 공격 탐지 임계값 또한 존재한다. 방화벽에서 방어하고자 하는 대표적인 네트워크 공격 유형에는 플러딩(flooding), 스캐닝(scanning), 스니핑(sniffing), 스푸핑(spoofing) 등이 있으며, 전상훈 등[11]은 이 중 스캐닝 공격이 전체에서 46.8%(TCP 서비스 스캔 34.3%, Nmap 스캔 12.5%)를 차지한다고 말한다. 이러한 공격들은 필수적인 서비스를 대상으로 이루어지기 때문에 공격 발생 가능성이 높다.

대부분의 방화벽은 기본적으로 공격 탐지 임계값을 적용하고 있으며, 플러딩, 스캐닝, 스니핑, 스푸핑, 비정상적으로 조작된 패킷 등을 검사할 수 있는 기능이 포함되어 있다. 이 외에도 세밀한 공격 탐지 및 차단을 위해 침입 방지 시스템 등과 같은 보안 시스템이 추가적으로 배치하기도 한다. 그림 1은 방화벽을 통과하는 패킷이 처리되는 과정을 간략하게 표현한 것이다. 그림 1을 보면, 백본 네트워크로 향하는 $T_i$ 트래픽은 먼저 공격 탐지 임계값에 의해 검사된 다음 필터링 규칙과 매칭이 되어 처리되는 것을 나타낸다. 만약 해당 트래픽 $T_i$가 공격 탐지 임계값을 초과하였다면, 필터링 규칙과는 무관하게 폐기된다. 방화벽의 공격 탐지 임계값은 5장에 설명된 방화벽 테스트베드 환경에서 자세히 다루고자 한다.

## 2.3 방화벽 정책 추론 및 분석 연구

T. Samak 등[8]은 패킷 프로빙을 이용하여 방화벽 정책을 추론하는 FireCracker 프레임워크를 제안하였다. 이




(그림 1) 방화벽의 공격 탐지 임계값과 필터링 규칙을 통한 트래픽 처리 과정

(Figure 1) Traffic process sequence through attack detection threshold and filtering rules of a firewall

연구에서는 공간 탐색 알고리즘인 Region Growing, Split-and-Merge, Genetic Algorithm을 이용하여 공간상에서 방화벽 정책 구조를 알아내는 방법을 소개하였다. 그리고 방화벽 정책 추론 실험을 통해서 각 알고리즘의 정확성에 대한 평가 결과를 제시하였다. 그러나 이 연구에서 제안된 알고리즘은 공격 패턴으로의 탐지 및 차단의 위험성을 고려하여 제한된 패킷 수를 이용하고 있지만, 방화벽의 공격 탐지 임계값을 고려한 패킷 전송 방법이 아니다. 만약 방화벽 정책 추론을 위해 전송되는 트래픽이 방화벽에 의해 네트워크 공격 유형으로 분류되어 폐기될 경우 정확한 추론 결과를 도출하기 어려우므로 공격 탐지 임계값을 고려한 패킷 전송 전략이 필요하다.

H. Kim 등[9]은 FireCracker에서 제기한 방화벽 정책 추론 문제를 바탕으로 실제 인터넷 환경에서 대상 네트워크의 방화벽 정책을 추론하는 방법을 제안하였다. 이 연구에서는 공간 탐색 알고리즘 중 하나인 스윕 라인 알고리즘을 이용하였으며, 방화벽 정책 추론 실험을 실제 인터넷 환경에 적용하여 제안된 추론 방법의 정확성을 검증하였다. 이 논문도 FireCracker와 마찬가지로 방화벽의 공격 탐지 임계값을 고려하지 않았지만, 이 문제점을 보완하고자 H. Kim 등[10]은 정책 추론 결과의 정확도 향상을 목적으로 필요한 추론 변수를 정의하였다. 그리고 각각의 추론 변수들이 방화벽 정책 추론의 정확도에 미치는 영향을 조사하기 위해 상관계수 분석을 수행하였다. 본 논문에서는 기존의 추론 변수를 기반으로 한 패킷 전송 알고리즘을 제안하고, FireCracker에서 제안하는 알고리즘과 정확성 측면에서 비교 검증 결과를 제시한다.

방화벽 분석 도구는 설치된 방화벽이나 설치 예정인 방화벽의 정책을 분석하여 방화벽 정책을 검증하는 도구이다. 이 도구들은 방화벽 정책 최적화를 목적으로 사용이 되며 네트워크 운영자가 방화벽을 쉽게 이해하고 보

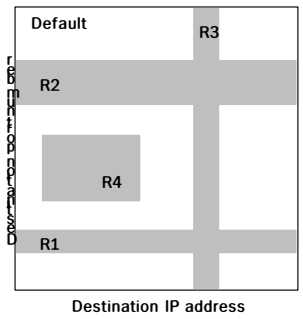
다 완벽한 정책을 수립할 수 있도록 도움을 준다. A. Mayer 등[12]은 방화벽 분석 도구로 FANG을 제안하였다. 이 도구는 네트워크 토폴로지 및 방화벽 구성 파일을 입력 받아서 방화벽 정책을 재구성하고 운영자의 질의에 따라 방화벽 정책 적용 결과를 보여준다. 이 도구를 사용하면 잘못 설정된 방화벽 정책을 쉽게 찾아낼 수 있다. 그리고 A. Wool [13]은 FANG을 확장하여 질의를 자동적으로 생성하도록 개선하였다. J. Hwang 등[14]은 내부적으로 테스트 패킷을 이용하여 방화벽 정책을 검사하기 위한 방법을 제안하였다. 이 방법은 테스트 패킷의 결과를 분석하여 오탐지되는 정책을 운영자에게 알려준다. 그 외의 다양한 연구들[15-19]은 방화벽에 적용된 정책 내에서 규칙 간 중첩되거나 충돌하는 규칙들을 발견하고 수정하는 방법을 제안하였다. 제안된 다양한 방화벽 분석 도구들은 내부에서 운영자에 의해 내부 네트워크 구조 또는 방화벽 규칙을 입력 받아 잘못 수립된 규칙을 검증하는 것이 목표지만, 본 연구에서는 외부에서 어떠한 사전 정보 없이 정책을 추론하고자 하는 연구로서 목적이 다르다. 하지만 본 연구에서 추론 패킷의 전송 과정을 통해 추론 결과를 도출하는 과정에서 방화벽 정책을 이해하고 재구성하는 방법이 활용될 수 있다.

기존의 방화벽 정책 추론 및 분석 연구들은 스캐닝 기법에 의한 네트워크 공격 탐지의 위험성을 언급하고 있지만, 공격 유형을 회피하기 위한 방안은 고려되지 않았다. 본 논문에서는 방화벽 정책을 추론하기 위한 트래픽이 방화벽의 공격 탐지 임계값에 의해 차단되지 않고, 정확히 응답 패킷을 수신하기 위한 방안을 제안하고자 한다. 우리는 실제 방화벽 제품을 테스트베드로 구축하여 수행한 실험 결과를 제시한다.

## 3. 연구 배경 및 추론 방법

### 3.1 공간적 표현의 방화벽 정책 구조

방화벽 정책을 유클리드 공간에서 표현할 경우 각 규칙에 구성된 $n$개의 필드는 $n$차원 공간으로 대응된다[8]. 예를 들어 표 1의 정책에서 목적지 IP 주소와 목적지 포트번호로 구성된 규칙은 2차원 공간에서 그림 2와 같이 표현된다. 그림 2에서 2차원 공간으로만 표현한 이유는 표 1의 정책에서 출발지 IP 주소와 출발지 포트번호가 모든 범위를 나타내고, 동일한 프로토콜을 가지므로 $n$차원 공간에서 전체 영역으로 표현되기 때문에 고려하지 않았다. 하지만, 각 규칙에서 프로토콜이나 출발지 정보에 대




(그림 2) 2차원 공간에서 표현된 방화벽 정책 구조
(Figure 2) The firewall policy structure in two dimensional space

한 필드 값이 설정될 경우 $n$차원으로 확장하여 표현이 가능하다.

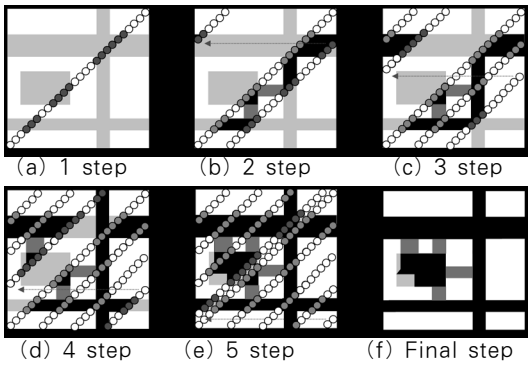
그림 2에서 흰 배경은 기본 정책 공간을 의미하며, 표 1의 정책에서 기본 거부 규칙으로 설정되어 있으므로 이에 대응된다. R1~R4에 해당하는 규칙들은 각각 음영색 도형으로 대응되며, 목적지 IP 주소의 필드 범위와 목적지 포트번호의 필드 범위에 따라 다양한 형태로 표현된다. 그림 2에서 음영색으로 표현된 도형들은 각 규칙들의 허용 규칙을 의미한다. 따라서 표 1과 같은 정책 구조는 그림 2와 같이 다차원 공간에서 표현될 수 있음을 확인할 수 있다.

### 3.2 스윕 라인 알고리즘을 이용한 정책 구조 탐색

본 논문에서는 방화벽 정책 추론 과정을 다차원 공간에서 도형을 찾는 문제로 해석하여 스윕 라인 알고리즘을 적용하고자 한다. 스윕 라인 알고리즘은 유클리드 공간에서 수직선을 이동하면서 특정 지점에서 필요한 계산 수행을 반복하고, 공간 내의 모든 지점에서 계산이 완료될 경우 공간 탐색을 종료한다[20]. 하지만, 수직선의 스윕 라인 알고리즘은 방화벽의 정책 공간을 탐색하기에 여러 문제점을 가지고 있다. 먼저 수직선으로 구성된 스윕 라인에 따라 정책 추론을 위한 패킷을 전송하게 되면, 전송된 패킷들은 포트스캔 공격과 유사한 패턴을 보이므로 방화벽으로부터 스캐닝 공격으로 오인 받을 수 있다[3]. 예를 들면 수직선 형태로 생성된 패킷은 하나의 목적지 IP 주소로 고정되고 포트번호만 증가되는 패턴이므로 일반적인 포트스캔 방식과 동일한 특징을 가진다. 또한 수직선의 스윕 라인을 이용한 공간 탐색 방법은 정책 공간에서 도형으로 표현된 규칙의 경계를 식별하기가 어렵

다. 그 이유는 정확한 경계를 찾기 위해 더 많은 수의 패킷이 전송되어야 하므로 해당 패킷들은 방화벽으로부터 악성 트래픽으로 분류되어 차단될 가능성이 높아진다. 따라서 본 연구에서는 위에서 언급되었던 특정 패턴에 의한 악성 트래픽으로 분류 및 차단되는 문제점을 보완하기 위해 사선 형태의 스윕 라인 알고리즘을 적용하였다. 사선 형태의 스윕 라인은 IP 주소와 포트번호를 임의적 순서로 전송하기 때문에 방화벽에서 특정 패턴으로 분류되는 것을 최소화한다.

본 논문에서 방화벽 정책 추론을 위해 제안하는 스윕 라인 알고리즘의 동작 과정은 그림 3과 같다[10]. 그림 3에서 *x*축은 목적지 IP 주소를 의미하고, *y*축은 목적지 포트번호를 의미한다. 먼저 정책 공간 내에서 사선 형태의 스윕 라인을 생성한다. 그림 3(a)에서 각 원들은 정책 추론을 위해 전송될 각각의 패킷들을 의미하며, 각 원의 좌표는 해당하는 목적지 IP 주소와 목적지 포트번호가 정책 추론을 위한 패킷의 필드 정보임을 의미한다. 그림 3(a)에서 음영으로 표시된 원은 추론 대상인 목적지로 전송하였을 때 응답 패킷을 수신하였음을 나타내고, 음영으로 표시되지 않은 원은 해당 응답 패킷이 수신되지 않았음을 의미한다. 그림 3(a)에서 생성된 스윕 라인에 해당하는 모든 패킷이 전송되었다면, 다음 단계로 진행한다. 그림 3(b)에서 차후 생성되는 스윕 라인은 초기 알고리즘에서 사전에 정의된 일정 간격만큼 이동하여 사선 형태로 생성되며, 이를 기반으로 패킷을 전송한다. 전송이 완료되면, 그림 3(b)에서 이전의 스윕 라인과 현재의 스윕 라인을 *x*축과 *y*축으로 서로 비교하여 동일한 정책 결과를 가지는 경우 두 스윕 라인 사이의 공간 또한 동일한 규칙을 의미한다. 이 과정은 그림 3(c)부터 그림 3(e)까지 반복되며, 최종적으로 스윕 라인을 생성하지 못하게 되면, 그림 3(f)에서 현재까지의 비교결과를 기반으로 전체 정책 구조가 추론된다.




(그림 3) 방화벽 정책 추론을 위한 스윕 라인 알고리즘의 예[10]

(Figure 3) An example of sweep-line algorithm for inferring a firewall policy[10]

### 3.3 추론 패킷 설정 및 응답 패킷 분류

우리는 외부에서 특정 네트워크로 패킷을 전송하여 네트워크 경계에 위치한 방화벽의 정책을 추론하고자 한다. 정책 추론을 위해 필요한 패킷의 헤더 정보는 프로토콜, 출발지 IP 주소, 출발지 포트번호, 목적지 IP 주소, 목적지 포트번호, 플래그, TTL 값이며, 추론 패킷 구성의 예는 표 2와 같다. 만약 정책 추론 대상이 되는 목적지 네트워크가 192.168.0.0/16 대역이라고 가정하였을 때, 해당 네트워크가 보유한 전체 IP 주소가 추론 대상이며 포트번호 또한 전체 범위가 추론 대상이다. 목적지 네트워크의 정보는 앞서 2장에서 언급된 그림 2와 같은 2차원 공간으로 표현된다. 표 2에서 추론 패킷의 출발지 IP 주소는 외부에서 접근 가능한 IP 주소인 것으로 가정한다. 그 이유는 만약 사전에 특정 네트워크의 보안 정보를 취득하고 싶은 외부의 공격자 입장에서 출발지 IP 주소를 스푸핑하여 패킷을 전송할 경우 응답 패킷을 정상적으로 수신할 수 없기 때문에 보안 정책 분석이 불가하다. 이것은 외부에서 사전 보안 정보를 유추하고자 하는 본 연구의 목적상 모든 출발지 IP 주소 범위를 고려하는 것은 무의미하다. 본 논문에서는 정책 추론을 위한 패킷 전송 알

(표 2) 추론 패킷의 설정 정보

(Table 2) The header configuration of inference packets

| Protocol | Source IP Address | Source Port Number | Destination IP Address | Destination Port Number | Flag/Type | TTL |
|---|---|---|---|---|---|---|
| ICMP | 172.16.10.0/24 | - | 192.168.0.0/16 | - | echo | Router/Firewall hop+1 |
| TCP | 172.16.10.0/24 | random | 192.168.0.0/16 | 1:65535 | SYN | Router/Firewall hop+1 |
| UDP | 172.16.10.0/24 | random | 192.168.0.0/16 | 1:65535 | - | Router/Firewall hop+1 |

(표 3) 응답 패킷의 허용 여부 결정
(Table 3) Permit/deny decision based on type of response packets

| Protocol | Flag/Type in Header Information of Response Packet | Decision Action |
|---|---|---|
| ICMP | echo reply (type=0) | Permit |
| | None | Deny |
| TCP | ICMP Time Exceeded Message (type=11) | Permit |
| | ICMP Destination Unreachable Error Message (type=3) | Deny |
| | None | Deny |
| UDP | None | Permit (based TCP rule) |
| | ICMP Destination Unreachable Error Message (type=3) | Deny |

고리즘의 검증 실험을 하고자 출발지 IP 주소의 수를 C 클래스의 네트워크 대역으로 가정하였다. 출발지 IP 주소와 목적지 IP 주소는 각각의 네트워크 크기에 따라 확장하여 실험이 가능하다. 그 외 패킷의 플래그는 표 2와 같이 프로토콜에 따라 특정 플래그로 고정되며, TTL 값은 기존 연구인 Firewalking 기법[21]을 적용하여 라우터/방화벽의 홉 수보다 1만큼 크게 설정한다. 추론 패킷의 목적지 IP 주소와 포트번호, 프로토콜에 대한 설정은 스윕 라인 알고리즘 기반으로 결정된다.

표 2에 따라 설정된 추론 패킷을 목적지로 전송하면, 대상 네트워크의 경로 상에서 방화벽 다음에 위치한 네트워크 장비로부터 표 3과 같은 응답 패킷을 수신하게 된다. 표 3은 전송된 추론 패킷에 의해 수신할 수 있는 응답 패킷의 정보를 나타낸 것이며, 응답 패킷의 종류에 따라 각 규칙의 허용 여부를 결정한다. 예를 들어 목적지로부터 ICMP Time Exceeded Message (type=11)의 응답 패킷을 수신하였다면, 방화벽 다음의 홉에 위치한 네트워크 장비로부터 해당 패킷의 TTL 값이 만료되었기 때문에 전송된 패킷임을 의미한다. 이것은 표 2와 같이 TTL 값으로 설정된 추론 패킷이 방화벽 정책에 의해 방화벽을 통과하였음을 알 수 있다. 하지만, UDP 프로토콜로 구성된 추론 패킷은 UDP 특성상 응답 패킷을 수신하는 것이 보장되지 않으므로 허용 여부를 판단하기 어려운 문제점이 존재한다. 이것은 TCP 프로토콜에 대한 추론 규칙 결과를 참고하여 UDP 규칙을 결정한다.

## 4. 추론 변수와 패킷 전송 전략

이전까지는 방화벽 정책 추론을 위한 패킷 전송 방법을 설명하였다면, 이 장에서는 방화벽의 공격 탐지 임계값을 고려하여 목적지로 전송되어질 트래픽이 네트워크 공격 유형으로 오인되지 않기 위한 추론 패킷의 전송 전략을 설명하고자 한다. 기존의 방화벽 정책 추론 연구[8-9]들은 방화벽의 공격 탐지 임계값을 고려하지 않았기 때문에 추론 패킷의 전송 방법에 따라 전송된 패킷들이 방화벽으로부터 네트워크 공격 패턴으로 탐지될 가능성이 매우 높다. 따라서 우리는 기존의 추론 방법에서 방화벽의 공격 탐지 임계값을 고려하여 패킷을 전송한다면, 공격 패턴을 회피할 수 있는 효율적이고 지능적인 스캐닝 기법으로 개선할 수 있다. 본 논문에서는 방화벽에서 네트워크 공격 패턴에 따른 공격 탐지 임계값을 고려하여 정책 추론의 정확도에 영향을 미치는 추론 변수들을 정의하였고, 정의된 추론 변수를 활용하여 개선된 추론 알고리즘을 제시한다.

### 4.1 추론 변수

본 논문에서 정의하는 추론 변수들은 출발지 IP 주소의 수와 초당 패킷 전송 수, 스윕 라인의 간격, 허용 규칙의 면적이며, 초기의 추론 알고리즘이 동작할 때 각 추론 변수들이 어떠한 값으로 설정되는가에 따라 네트워크 공격의 패턴과 유사하게 보인다[10]. 예를 들어 방화벽의 공격 탐지 임계값에서 내부 호스트로 전송되는 패킷이 초당 100개 이상으로 발생할 경우 해당 패킷들은 차단한다고 가정하자. 이때 공격자가 외부에서 특정 호스트로 초당 200개의 패킷을 전송할 경우 방화벽은 공격 탐지 임계값을 초과하였으므로 해당 패킷들을 통과시키지 않고 버리게 된다. 공격자는 방화벽에 의해 버려진 패킷에 대한 응답 패킷을 수신할 수 없으므로 추론 정확도가 감소한다. 따라서 적절한 추론 변수의 값을 설정하는 것이 추론 정확도를 높이는데 매우 중요하다.

#### 4.1.1 출발지 IP 주소의 수

대상 네트워크의 방화벽 정책을 추론하기 위해서 다

수의 추론 패킷을 대상 네트워크로 전송하여야한다. 그러나 동일한 출발지 주소에서 목적지 네트워크로 많은 수의 패킷을 전송하게 되면, 해당 패킷은 방화벽의 공격 탐지 임계값에 의해 제한을 받게 되고, 최악의 경우 서비스거부공격으로 오인 받을 수도 있다. 이러한 인바운드 트래픽은 플러딩, 스캐닝 공격으로 차단될 수도 있다[22].

위에서 언급한 바와 같이 이러한 문제점들을 해결하기 위해서 본 논문에서는 목적지로 패킷을 전송할 때 다수의 출발지 IP 주소를 고려하여 실험하였다. 패킷 전송이 이루어지는 출발지 주소가 많을수록 방화벽으로부터 스캐닝이나 서비스거부공격과 같은 악성 트래픽으로 분류되지 않을 확률이 높다. 다시 말해서 추론을 위한 패킷이 방화벽에서 공격으로 탐지되지 않다면, 응답 패킷을 수신할 수 있기 때문에 추론의 정확도를 높여주는 것을 의미한다. 또한 빠른 시간 내에 패킷을 효율적으로 전송할 수 있기 때문에 이 변수는 방화벽 정책 추론을 위한 패킷 전송 과정에서 직접적으로 영향을 주는 매우 중요한 변수이다.

#### 4.1.2 초당 패킷 전송 수

이 추론 변수는 출발지 주소에서 방화벽 정책 추론을 위해 초당 발생시키는 패킷의 수를 의미한다. 이 변수는 설정된 값이 커질수록 플러딩 공격과 유사한 성질을 가지므로 네트워크 공격 탐지를 피하는데 매우 중요한 변수이다. 방화벽은 자신을 통과하고자 하는 패킷을 검사할 때 출발지 정보와 목적지 정보에 기반을 두어 초당 전송되는 패킷의 수를 계산한다. 만약 동일한 출발지 정보 또는 목적지 정보로부터 초당 전송된 패킷의 수가 방화벽에 설정된 공격 탐지 임계값을 초과하게 되면, 공격으로 판단하여 이후에 전송되는 해당 패킷들은 정책과 무관하게 버려진다. 이처럼 출발지 IP 주소의 수와 마찬가지로 초당 패킷 전송 수 또한 방화벽 정책 추론을 위한 패킷 전송 과정에서 악성 트래픽으로 분류되는데 직접적인 영향을 주므로 매우 중요한 변수이다.

#### 4.1.3 스윕 라인의 간격

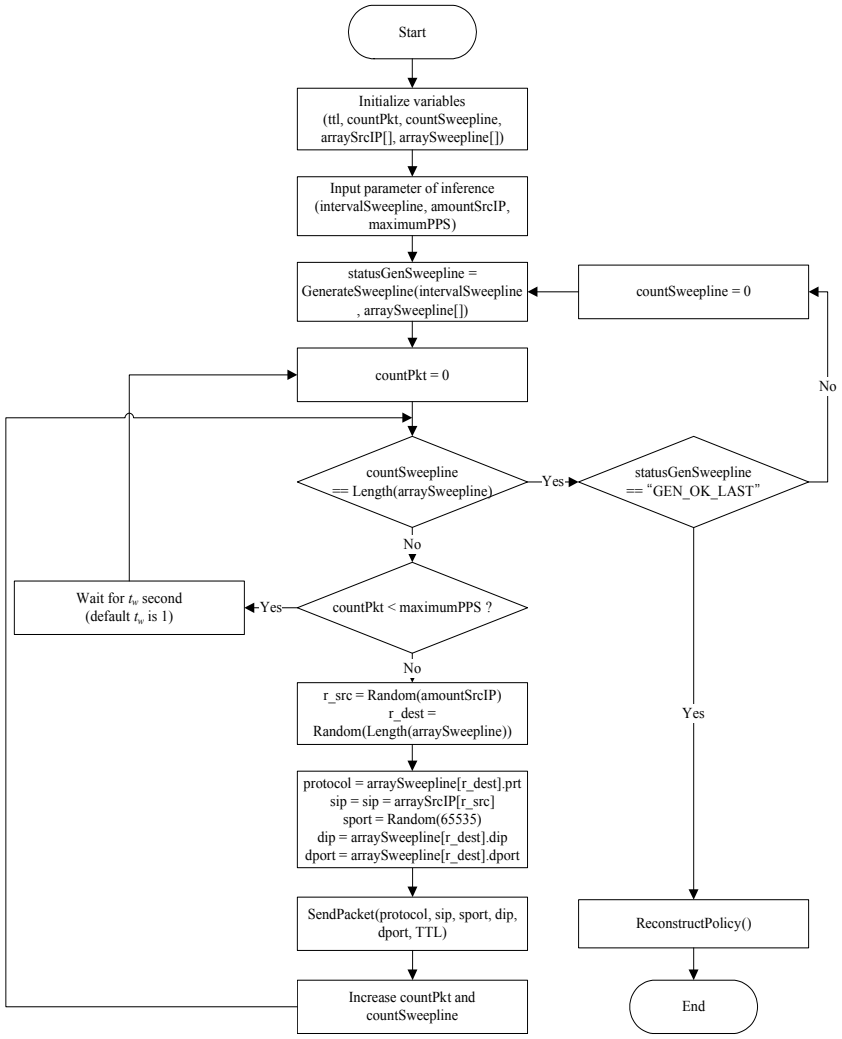
그림 3과 같이 스윕 라인 알고리즘이 동작 중일 때 그림 3(b)를 현재 시점으로 가정한다면, 그림 3(b) 단계에서 생성된 스윕 라인을 현재의 스윕 라인이라 하고, 그림 3(a) 단계에서 생성된 스윕 라인을 이전의 스윕 라인이라 한다. 이 변수는 2차원 정책 구조에서 $x$축 또는 $y$축으로 두 스윕 라인 사이의 거리 간격을 의미한다. 스윕 라인의 간격에 대한 값은 작을수록 각 스윕 라인 사이의 공간 탐색 범위가 좁아지므로 정책 공간에서 세밀한 탐색이 가능하다는 장점이 있지만, 그에 반비례하여 스윕 라인이 생성되는 횟수가 많아지면서 전송되어지는 패킷의 수가 늘어나는 단점이 존재한다. 반대로 스윕 라인 간격의 값이 커진다면 두 스윕 라인 사이의 공간 탐색 범위가 넓어져 추론 정확도가 감소하게 된다. 따라서 이 변수는 설정 값에 따라 장단점이 존재하기 때문에 적절한 설정 값을 찾는 것이 중요하다.

#### 4.1.4 허용 규칙의 면적

기존의 정책 추론 연구[8-10]들은 그림 2처럼 정책 공간상에서 기본 차단 규칙을 기반으로 허용 규칙을 찾는 방법을 제안하였다. 허용 규칙은 그림 2와 같이 2차원 도형으로 대응되며, 2차원의 전체 공간에서 허용 규칙이 차지하는 면적 분포가 클수록 허용 규칙의 형태를 식별하기가 쉬워진다. 반대로 허용 규칙의 면적 분포는 작아질수록 정책을 추론하기 어려워진다. 예를 들어 정책 공간상에서 특정한 허용 규칙의 영역이 작다고 가정하였을 때, 스윕 라인의 간격을 의미하는 변수 값이 크게 설정된 스윕 라인 알고리즘은 허용 규칙의 영역을 식별하지 못할 수도 있기 때문에 추론 정확도에 대한 알고리즘의 성능은 감소한다. 따라서 허용 규칙의 면적 분포는 위에서 언급된 추론 변수 중 하나인 스윕 라인의 간격이 어떻게 설정되는가에 따라 추론 정확도에 간접적으로 영향을 주는 것과 마찬가지로 유사한 특징을 가진다. 우리는 허용 규칙의 면적 분포가 스윕 라인 알고리즘의 초기 단계에서 입력되어야 할 변수는 아니지만, 방화벽의 정책에서 허용 규칙의 면적이 차지하는 분포에 따라 스윕 라인 알고리즘의 추론 정확도 성능에 간접적으로 영향을 주기 때문에 추론 변수로 고려하였다.

### 4.2 추론 변수를 활용한 추론 알고리즘

우리는 방화벽의 공격 탐지 임계값을 고려한 추론 패킷의 전송 전략 방안으로 위에서 정의된 추론 변수를 활용하고자 한다. 방화벽의 공격 탐지 임계값은 2.2절에서 언급된 바와 같이 다양한 네트워크 공격 유형의 패턴에 따라 탐지 및 차단하기 위한 임계값 기반의 규칙으로 구성되어 있다. 이는 우리가 제안하는 추론 패킷의 전송 전략과 관계가 있으며, 패킷 전송 과정에서 적절한 추론 변




(그림 4) 스윕 라인 알고리즘을 이용한 정책 추론 방법의 흐름도
(Figure 4) A flow-chart of policy inference method using sweep-line algorithm

수의 값을 설정하느냐에 따라 네트워크 공격 유형으로 오인되지 않고 안전하게 추론 패킷을 송수신할 수 있다. 방화벽 정책 추론의 정확성은 전송된 패킷에 대한 가능한 모든 응답 패킷을 수신할수록 높아진다. 하지만 추론 패킷이 방화벽에서 악성 트래픽 패턴으로 탐지될 경우 정확한 응답 패킷을 수신할 수 없으며, 추론 정확성 또한 감소하게 된다. 우리는 추론 패킷이 악성 트래픽 패턴으로 분류되지 않기 위해 4.1절에서 정의된 추론 변수를 고려한 패킷 전송 알고리즘을 제시한다.

그림 4는 3장에서 언급된 스윕 라인 알고리즘을 기반으로 패킷 전송 과정 및 추론 방법을 흐름도로 표현한 것이다. 그림 4에서 먼저 추론 변수들의 초기화를 수행한다. 다음으로 추론 변수인 스윕 라인 간격의 설정 값에 따라 그림 3과 같은 사선 형태의 스윕 라인으로 생성되며, 생성된 스윕 라인의 각 좌표들은 목적지 IP 주소와 목적지 포트번호들로 구성된다. 그리고 추론 변수인 초당 패킷 전송 수의 설정 값 이하가 되도록 패킷을 전송한다. 출발지 IP 주소는 추론 변수인 출발지 IP 주소의 수 범위 내에서 무작위로 IP 주소가 추출되고, IP 주소에 대응되는 호스트는 우리의 알고리즘에 의해 생성된 추론

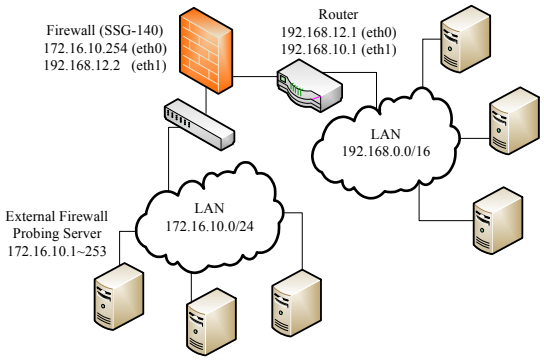
패킷을 목적지로 전송한다. 만약 초당 패킷 전송 수만큼 전송되었다면, $t_w$초만큼 대기한 후부터 다음 추론 패킷을 전송한다. 대기시간 $t_w$는 공격 탐지 임계값이 초기화되는 것을 기다리기 위한 시간을 의미하며, 초 단위로 전송되기 때문에 임계값 이하로 전송한 후 최소 1초 이상 대기하도록 설정하는 것을 권장한다. 이 과정은 모든 스윕 라인에 해당하는 추론 패킷이 전송 완료될 때까지 반복한다. 마지막으로 전송된 추론 패킷의 응답을 분석하여 정책 구조를 파악한다.

## 5. 실험 결과

### 5.1 실험 환경

방화벽에서 네트워크 공격에 대한 정책 추론 방법을 검증하기 위해서 Juniper Networks사의 방화벽(SSG-140)을 네트워크상에 배치한 테스트베드를 구축하였으며, 그림 5와 같이 실험 환경을 구성하였다. 그림 5에서 방화벽 정책을 추론 할 대상 네트워크의 대역은 192.168.10.0/24로 설정되어 있고, 외부에서 정책 추론을 위해 패킷 전송을 담당하는 프로빙 서버들은 172.16.10.0/24 네트워크 대역에서 IP 주소를 각각 할당받고 있다.

본 논문의 목적은 제안된 추론 방법이 방화벽의 공격 탐지 임계값을 고려하여 알고리즘의 추론 정확도 성능을 검증하기 위한 것이므로 그림 5의 테스트베드에 설치된 방화벽의 공격 탐지 임계값이 모두 적용되도록 설정한 상태로 실험하였다. 그리고 각 공격 탐지 임계값은 방화벽을 사용하는 대상 기관의 내부정책 특성에 따라 다르게 설정되기 때문에 방화벽에서 제공되는 기본 값을 기반으로 설정하였다. 방화벽의 공격 탐지 임계값은 표 4와 같다. 먼저 TCP SYN Flood 공격에 대한 규칙은 동일한




(그림 5) 방화벽 정책 추론을 위한 테스트베드 환경 구성도
(Figure 5) The testbed environment configuration for inferring a firewall policy

출발지 IP 주소 또는 동일한 목적지 IP 주소를 갖는 패킷이 초당 200개를 초과하였을 때 탐지 및 차단됨을 의미하며, ICMP/UDP Flood 공격 또한 초당 1,000개 패킷을 초과하였을 때 탐지 및 차단되는 것을 나타낸다. 다음으로 포트스캔에 대한 규칙은 0.005초 동안 10개의 동일한 출발지 IP 주소에서 목적지 네트워크 대역의 포트를 스캔하였을 때 발생되며, IP Address Sweep 또한 포트스캔과 유사하다. 그리고 동일한 출발지 IP 주소에서 목적지 네트워크 대역으로 1초 동안 50개의 주소를 초과하여 스캐닝하면, TCP/UDP Sweep 공격에 해당한다. 마지막으로 출발지 IP 주소와 목적지 IP 주소에 기반을 둔 세션 제한 규칙은 서비스거부공격을 방어하기 위한 것으로 동일한 IP 주소에 대해서 세션이 생성되는 시간동안 최대 128개의 세션 수로 제한됨을 의미한다. 해당 공격 패턴에 대한 패킷이 임계값을 초과하게 되면, 정책과 무관하게 폐기된다.

(표 4) 방화벽에 설정된 공격 탐지 임계값의 예
(Table 4) An example of attack detection threshold of a firewall

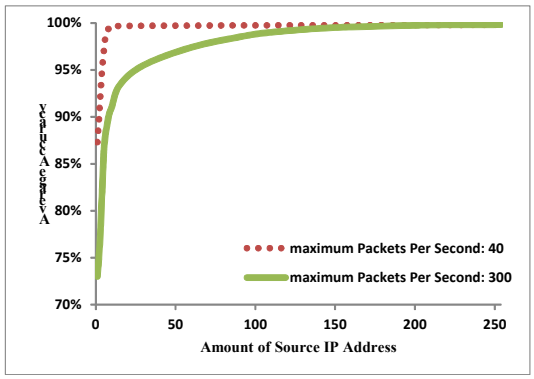
| Network Attacks | Pattern of Packet Header | Threshold of Security Rules |
|---|---|---|
| TCP SYN Flood | same source IP or destination IP | 200 packets / 1 second |
| UDP Flood | same source IP or destination IP | 1,000 packets / 1 second |
| ICMP Flood | same source IP or destination IP | 1,000 packets / 1 second |
| Port Scan | same source IP and destination port | 10 addresses / 5,000 microseconds |
| IP Address Sweep | same source IP and destination network range | 10 addresses / 5,000 microseconds |
| TCP Sweep | same source IP and destination network range | 50 packets / 1 second |
| UDP Sweep | same source IP and destination network range | 50 packets / 1 second |
| Source IP Based Session Limit | same source IP | 128 sessions |
| Destination IP Based Session Limit | same destination IP | 128 sessions |

### 5.2 각 추론 변수에 따른 평균 정확도

우리는 4장에서 정의된 추론 변수를 활용한 추론 알고리즘을 검증하기 이전에 각 추론 변수들의 적절한 초기 값을 결정하여야 한다. 적절한 값으로 설정된 각각의 추론 변수들은 추론 알고리즘에 의해 전송되는 패킷이 네트워크 공격으로 차단되는 비율을 낮추는데 기여한다. 그래서 추론 변수들의 적절한 초기 값을 선택하는 것은 매우 중요하다.

우리는 이전 연구[10]에서 각 추론 변수들의 값을 다양한 범위 내에서 설정하여 정책 추론 실험을 수행하였으며, 실험 결과로 각 추론 변수에 대한 평균 추론 정확도를 도출하였다. 각 추론 변수에 대한 추론 정확도를 평균으로 계산한 이유는 추론 변수들의 값이 설정되는 범위가 다양하기 때문에 각 추론 변수들의 설정 값에 따라 추론 정확도가 다르게 나타나기 때문에 평균값이 높으면 정확성 측면에서 의미가 있다고 판단하였다.

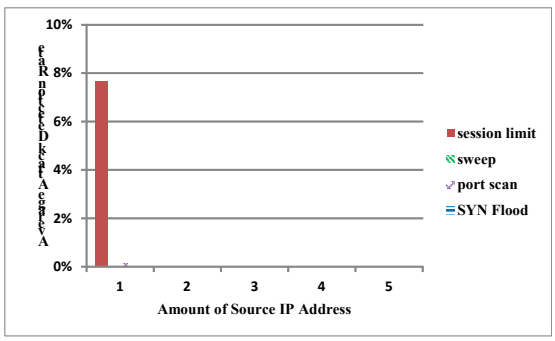
그림 6은 출발지 IP 주소의 수와 초당 패킷 전송 수에 따른 평균 추론 정확도를 보여준다. 표 4에서 Sweep 공격의 임계값은 초당 패킷 전송 수 50으로 설정되어 있고, TCP SYN Flood의 임계값은 초당 패킷 전송 수 200으로 설정되어 있다. 따라서 우리는 네트워크 공격으로 탐지되지 않는 초당 패킷 전송 수인 40과 네트워크 공격으로 탐지가 가능한 초당 패킷 전송 수 300에 대한 실험 결과를 분석하였다. 먼저 초당 패킷 전송 수를 40으로 설정하였을 때의 실험 결과는 7개 이상의 출발지 IP 주소의 수가 할당이 되면 약 2%의 오차 범위 내에서 추론 정확도가 수렴하였다. 그리고 초당 300개의 패킷을 전송한 결과는 150개 이상의 출발지 IP 주소가 할당이 되었을 때 추론 정확도가 수렴하는 것으로 나타났다.



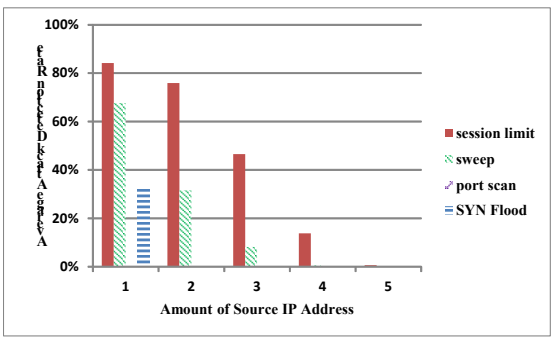

(그림 6) 출발지 IP 주소의 수와 초당 패킷 전송 수의 설정 값에 따른 평균 추론 정확도[10]

(Figure 6) Average accuracy according to the amount of source IP address and maximum packets per second[10]

출발지 IP 주소의 수와 초당 패킷 전송 수는 4장에서 언급된 바와 같이 패킷 전송 전략에 따라 방화벽의 공격 탐지 임계값을 초과할 수 있기 때문에 방화벽에 의해 공격으로 탐지되면 정책 추론의 정확도 성능에 직접적으로 영향을 준다. 그림 7은 두 추론 변수의 설정 값에 따라 각각의 네트워크 공격 유형으로 탐지됨을 보여준다. 그림 7(a)는 초당 40개 패킷을 전송하였을 때 방화벽에서 공격으로 탐지된 결과이며, 하나의 출발지 IP 주소를 가진 서버에서 전송된 트래픽만 방화벽의 공격 탐지 임계값에 의해 플러딩, 스캐닝 공격으로 탐지되었다. 그림 7(b)는 초당 300개 패킷을 전송한 결과로서, 적은 수의 출



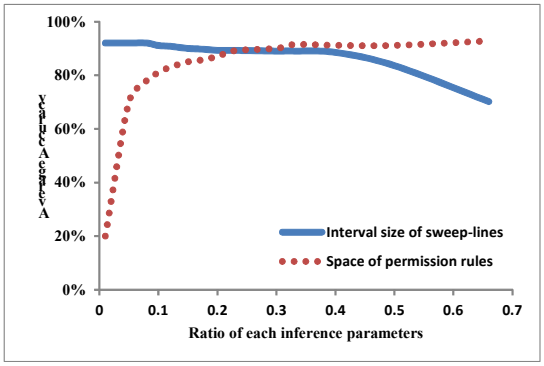

(a) Detection rate about maximum PPS of 40




(b) Detection rate about maximum PPS of 300

(그림 7) 출발지 IP 주소의 수와 초당 패킷 전송 수에 의한 네트워크 공격 유형 별 탐지율

(Figure 7) Attack detection rate through the amount of source IP address and maximum packets per second




(그림 8) 스윕 라인의 간격과 허용 규칙 면적에 따른 평균 추론 정확도[10]

(Figure 8) Average accuracy according to each inference parameters[10]

발지 IP 주소에서 전송된 패킷은 최악의 경우 약 80%가 탐지됨을 알 수 있다. 그러나 그림 7(b)의 결과로 초당 전송되는 패킷의 수가 임계값을 초과하더라도 많은 수의 출발지 IP 주소를 이용하여 패킷을 전송한다면 공격으로 탐지되는 비율을 줄일 수 있었다. 이 결과의 의미는 방화벽의 공격 탐지 임계값이 동일한 IP 주소를 기준으로 검사되기 때문으로 분석된다.

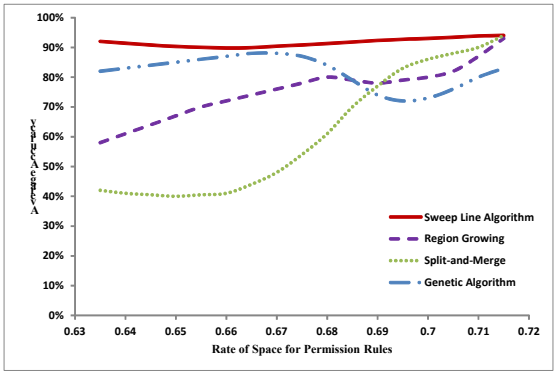
그림 8은 스윕 라인 간격의 비율과 허용 규칙의 면적 비율에 따른 평균 추론 정확도를 보여준다. 스윕 라인 간격의 비율은 추론 대상인 전체 IP 주소 대역에서 스윕 라인의 간격 값이 차지하는 비의 값을 의미한다. 그리고 허용 규칙의 면적 비율은 전체 공간에서 허용 규칙이 차지하는 면적을 전체 공간의 면적으로 나눔으로써 계산된다. 추론 대상이 되는 목적지의 전체 정책 공간은 각 기관 별로 할당된 네트워크 주소에 따라 다르기 때문에 추론하고자 하는 정책 영역의 크기가 유동적이다. 따라서 추론 변수의 고정적인 값은 정책 영역의 크기에 따라서 의미하는 바가 클 수도 있고 작을 수도 있으므로 두 추론 변수에 대해서는 전체의 영역에서 각각의 추론 변수의 값이 차지하는 비율로 표현하는 것이 적합하다. 그림 8에서 보면, 스윕 라인 간격의 비율이 0.4보다 작을 때는 큰 차이가 없으나, 0.4 이상일 때 평균 추론 정확도가 급격히 감소하는 것을 볼 수 있다. 이 결과는 제안된 알고리즘의 특성상 스윕 라인의 간격이 커질수록 넓은 범위의 정책 구조 공간이 동일한 규칙으로 추론되기 때문에 정확도가 감소할 확률이 높음을 알 수 있다. 그리고 그림 8에서 허용 규칙의 면적은 비율이 0.1보다 큰 경우 정확도 측면에서 큰 차이가 없는 것으로 나타나지만, 비율이 0.1보다 낮을 때 평균 추론 정확도가 급격히 감소하는 것을 볼 수 있다. 이 결과는 전체 정책 구조상에서 허용 규칙의 면적이 극단적으로 작게 분포되어 있거나 흩어져 있는 최악의 경우에 해당된다. 그리고 스윕 라인의 간격과 반비례하는 성질 때문에 스윕 라인 간격의 값이 큰 경우에 최악의 성능으로 나타난다. 우리는 이 실험 결과를 통해 스윕 라인의 간격과 허용 규칙의 면적은 최악의 상태를 제외하고 약 90% 이상의 평균 추론 정확도를 보여주는 것을 알 수 있다.

그림 6, 7, 8의 결과를 바탕으로 각각의 추론 변수들은 방화벽에 의해 공격으로 탐지될 경우 추론 정확도에 영향을 주는 것을 확인하였다. 그러나 그림 6처럼 출발지 IP 주소의 수와 초당 패킷 전송 수의 추론 변수 설정 값에 따라 추론 정확도에 더 큰 영향을 준다. 이것은 두 추론 변수가 어떻게 설정되느냐에 따라 네트워크 공격 유형으로 탐지될 수 있다. 우리는 실험 결과를 토대로 정책 추론을 위한 패킷 전송 전략에서 두 추론 변수를 잘 활용한다면, 방화벽으로부터 해당 트래픽이 공격으로 탐지되지 않으면서 정책을 추론할 수 있음을 확인하였다.

## 5.3 각 추론 방법의 평균 정확도 검증

우리는 4장에서 정의된 추론 변수를 활용한 추론 알고리즘을 정확성 측면에서 기존 연구인 FireCracker[8]와 비교 검증하고자 한다. 비교 검증을 위한 각 알고리즘들은 FireCracker에서 제안된 Region Growing, Split-and-Merge, Genetic Algorithm과 본 논문에서 제안하는 스윕 라인 알고리즘으로 구성된다. 각 알고리즘 별로 정확성 검증은 허용 규칙의 면적 비율을 기준으로 비교하였다. 허용 규칙을 기준으로 비교한 이유는 먼저 추론 대상인 방화벽의 기본 정책이 차단 규칙임을 가정하였으며, 추론되는 차단 규칙의 면적 분포는 기본 차단 규칙과 공간상에서 겹치는 것으로 표현되므로 허용 규칙의 면적 분포를 기준으로 정확도를 검증하는 것이 적합하기 때문이다. 또한 4.1절의 추론 변수에서 언급한 바와 같이 허용 규칙의 면적에 대한 파라미터 값은 추론 정확도에 영향을 주기 때문에 허용 규칙의 면적 분포에 따라 정확도 측면에서 각 추론 알고리즘의 성능을 검증하였다.

그림 9는 허용 규칙의 면적 비율에 따른 각 알고리즘의 평균 추론 정확도를 비교한다. 전반적으로 FireCracker에서 제안된 3가지 알고리즘들은 전체 영역 중에서 허용 규칙의 면적 비율이 0.7 이상인 경우 추론 정확도가 증가




(그림 9) 허용 규칙의 면적에 따른 각 알고리즘의 평균 추론 정확도

(Figure 9) Average accuracy of inference algorithm depending on total space of permission rules

하는 것으로 나타났으며, 0.7 이하의 정책 구조에서는 허용 규칙의 면적 비율에 따라 편차가 큰 것으로 나타났다. 그 이유는 각 알고리즘의 특성에 따른 것이며, Region Growing은 *x, y*축 방향으로 지수 탐색(exponential search)과 이진 탐색(binary search)을 반복적으로 수행하기 때문에 허용 규칙의 면적이 전체 공간에서 다양한 영역으로 분포되어 있을 경우 정확히 추론하기 어렵다. 그래서 허용 규칙의 면적 비율이 낮을수록 평균 추론 정확도는 감소한다. Split-and-Merge는 전체 공간에서 4등분으로 분할 및 병합되는 과정 중 연속적인 프로빙 패킷(IP 주소 또는 포트번호) 분포로 인해 공격으로 탐지될 우려가 존재하여 허용 규칙의 면적 비율에 가장 민감한 방법임을 알 수 있다. 그러나 허용 규칙의 면적 비율이 0.7 이상인 정책 구조에서는 Region Growing과 Genetic Algorithm보다 더 높은 평균 추론 정확도를 보여준다. Genetic Algorithm은 이전에 추론된 허용 규칙의 영역에 더 우선적으로 선택하는 연산 과정을 수행하기 때문에 허용 규칙의 영역이 크게 분포된 정책 구조에서는 다른 알고리즘에 비해 평균 추론 정확도가 떨어진다. 또한 Region Growing과 Split-and-Merge는 초기 패킷의 설정에 따라 허용 규칙의 영역에 제한되는 단점이 존재하는 것으로 나타났다. 마지막으로 본 논문에서 제안하는 추론 변수를 활용한 스윕 라인 알고리즘은 각 추론 변수들의 범위 값에 따른 평균 추론 정확도를 보여준다. 스윕 라인 알고리즘은 다른 알고리즘에 비해서 허용 규칙의 면적 비율에 영향을 받지 않음을 알 수 있다. 그 이유는 그림 8과 같이 각 추론 변수들이 설정되는 범위의 값에 따라 허용 규칙의 면적 비율이 0.4 이상일 때 90%이상의 평균 추론 정확도를 보여주기 때문이다.

그림 9의 결과로 허용 규칙의 면적에 따라서 각 알고리즘의 정확도 차이를 보였으며, 전반적으로 허용 규칙의 면적 크기가 클수록(> 0.70) 보다 더 정확히 정책을 추론하였다. 하지만 허용 규칙의 면적이 작은 정책 구조를 추론하는 알고리즘으로는 스윕 라인 알고리즘이 다른 알고리즘에 비해 정책 구조에 민감하지 않으므로 효과적임을 보여준다.

## 6. 결론 및 향후 연구

외부에서 방화벽 정책을 추론하기 위해 전송되는 패킷들은 방화벽에서 악성 트래픽 패턴으로 분류되어 차단되면, 공격자는 정확한 정책 추론을 수행할 수 없다. 방화벽의 공격 탐지 임계값은 악성 트래픽 패턴으로 보이는 패킷들을 사전 차단하기 위한 목적으로 방화벽 내부에서 동작된다. 본 논문에서는 공격 탐지 임계값을 고려하여 패킷 전송 전략에 필요한 추론 변수를 정의하였고, 추론 변수를 활용한 스윕 라인 알고리즘을 제안하였다. 제안된 알고리즘은 정확한 정책 추론을 위해 전송되는 패킷들이 방화벽에서 악성 트래픽 패턴으로 분류되지 않고 정상적인 응답 패킷을 수신하기 위한 패킷 전송 방법이다. 우리는 제안된 정책 추론 방법을 정확하게 검증하기 위해서 실제 방화벽 장비를 배치하여 실험 환경을 구성하였다. 실험 결과로는 실제 방화벽에 구성된 정책과 추론된 방화벽 정책을 비교하여 추론 정확성을 검증하였고, 기존 연구인 FireCracker에서 제안된 알고리즘과 정확도 측면에서 비교 검증하였다.

향후에는 정확도와 효율성 측면에서 제안된 추론 알고리즘을 개선하기 위한 각 추론 변수들의 최적 값을 제시할 것이다. 또한 방화벽의 공격 탐지 임계값 변화에 따른 추론 알고리즘의 정확도를 검증하고자 한다. 마지막으로 방화벽 장비에서 설정된 네트워크 보안의 임계치도 사전에 파악할 수 있는 알고리즘을 고안할 것이다.

## 참고문헌(Reference)

[1] K. Scarfone, and P. Hoffman, Guidelines on Firewalls and Firewall Policy, NIST(National Institute of Standards and Technology) Special Publication 800-41 Revision 1, pp. 1-48, Sept. 2009.

[2] K. Salah, K. Sattar, M. Sqalli, and E. Al-Shaer, "A Probing Technique for Discovering Last-Matching Rules of a Network Firewall," in Proc. International Conference on Innovations in Information Technology (IIT), pp. 578-582, Dec. 2008. http://dx.doi.org/10.1109/INNOVATIONS.2008.4781670

[3] R. J. Barnett, and B. Irwin, "Towards a Taxonomy of Network Scanning Techniques," in Proc. annual research conference of the south african institute of computer scientists and information technologists on IT research in developing countries: riding the wave of technology (SAICSIT), pp. 1-7, 2008. http://dx.doi.org/10.1145/1456659.1456660

[4] Nmap, Retrieved Mar. 18, 2015, from http://nmap.org

[5] Hping, Retrieved Mar. 18, 2015, from http://www.hping.org

[6] H. Hamed, A. El-Atawy, and E. Al-Shaer, "Adaptive Statistical Optimization Techniques for Firewall Packet Filtering," in Proc. the 25th IEEE International Conference on Computer Communications (INFOCOM), pp. 1-12, Apr. 2006. http://dx.doi.org/10.1109/INFOCOM.2006.129

[7] J. Mirkovic, and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communications Review, vol. 34, issue 2, pp. 39-53, Apr. 2004. http://dx.doi.org/10.1145/997150.997156

[8] T. Samak, A. El-Atawy, and E. Al-Shaer, "FireCracker: A Framework for Inferring Firewall Policies using Smart Probing," in Proc. IEEE International Conference on Network Protocols (ICNP), pp. 294-303, Oct. 2007. http://dx.doi.org/10.1109/ICNP.2007.4375860

[9] H. Kim, and H. Ju, "Efficient Method for Inferring a Firewall Policy," in Proc. Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1-8, Sept. 2011. http://dx.doi.org/10.1109/APNOMS.2011.6077015

[10] H. Kim, W. Pak, and H. Ju, "Correlation analysis between inference accuracy and inference parameters for stateless firewall policy," in Proc. Asia-Pacific Network Operations and Management Symposium (APNOMS), pp. 1-6, Sept. 2013.

[11] S. Jeon, and J. Jeon, "A Secure Clustering Methodology and an Arrangement of Functional Firewall for the Enhancement of Performance in the Inbound Network," Journal of Korea Information and Communications Society (J-KICS), vol. 35, no. 7, pp. 1050-1057, July 2010.

[12] A. Mayer, A. Wool, and E. Ziskind, "Fang: a firewall analysis engine," in Proc. IEEE Symposium on Security and Privacy (S&P), pp. 177-187, May, 2000. http://dx.doi.org/10.1109/SECPRI.2000.848455

[13] A. Wool, "Architecting the Lumeta Firewall Analyzer," in Proc. the 10th conference on USENIX Security Symposium, vol. 10, no. 7, pp. 1-13, Aug. 2001.

[14] J. Hwang, T. Xie, F. Chen, and A. X. Liu, "Systematic Structural Testing of Firewall Policies," IEEE Transactions on Network and Service Management, vol. 9, issue 1, pp. 1-11, Mar. 2012. http://dx.doi.org/10.1109/TNSM.2012.012012.100092

[15] T. Abbes, A. Bouhoula, and M. Rusinowitch, "An Inference System for Detecting Firewall Filtering Rules Anomalies," in Proc. ACM Symposium on Applied Computing (SAC), pp. 2122-2128, Mar. 2008. http://dx.doi.org/10.1145/1363686.1364197

[16] A. El-Atawy, T. Samak, Z. Wali, and E. Al-Shaer, "An Automated Framework for Validating Firewall Policy Enforcement," in Proc. 8th IEEE International Workshop on Policies for Distributed Systems and Networks, pp. 151-160, June 2007. http://dx.doi.org/10.1109/POLICY.2007.5

[17] H. Hamed, and E. Al-Shaer, "On autonomic optimization of firewall policy organization," Journal of High Speed Networks - Managing security policies: Modeling, verification and configuration, vol. 15, no. 3, pp. 209-227, July 2006.

[18] E. Al-Shaer, and H. Hamed, "Discovery of policy anomalies in distributed firewalls," in Proc. 23th AnnualJoint Conference of the IEEE Computer and Communications Societies (INFOCOM), vol. 4, pp. 2605-2616, Mar. 2004. http://dx.doi.org/10.1109/INFCOM.2004.1354680

[19] E. Al-Shaer, and H. Hamed, "Firewall Policy Advisor for anomaly discovery and rule editing," in Proc.

IFIP/IEEE 8th International Symposium on Integrated Network Management (IM), pp. 17-30, Mar. 2003. http://dx.doi.org/10.1109/INM.2003.1194157

[20] S. Fortune, “A Sweepline Algorithm for Voronoi Diagrams,” Algorithmica, vol. 2, issue 1-4, pp. 153-174, Nov. 1987. http://dx.doi.org/10.1007/BF01840357

[21] D. Goldsmith, and M. Schiffman, Firewalking: A traceroute-like analysis of ip packet responses to determine gateway access control lists, White paper, Cambridge Technology Partners, Oct. 1998.

[22] W. Eddy, TCP SYN Flooding Attacks and Common Mitigations, RFC 4987, IETF, Aug. 2007.

## ◐ 저 자 소 개 ◑

**김 현 우 (Hyeonwoo Kim)**
2010년 계명대학교 컴퓨터공학과(컴퓨터공학사)
2012년 계명대학교 컴퓨터공학과(공학석사)
2012～현재 계명대학교 컴퓨터공학과 박사과정
관심분야 : 방화벽 정책 추론 및 관리, 네트워크 관리 및 보안
E-mail : hwkim84@kmu.ac.kr

**권 동 우 (Dongwoo Kwon)**
2010년 계명대학교 컴퓨터공학과(공학사)
2012년 계명대학교 컴퓨터공학과(공학석사)
2013～현재 계명대학교 컴퓨터공학과 박사과정
관심분야 : 미디어 스트리밍, 인터넷 침입 예측, 네트워크 관리 및 보안
E-mail : dwkwon@kmu.ac.kr

**주 홍 택 (Hongtaek Ju)**
1989년 한국과학기술원 전자계산학과 학사
1991년 포항공과대학교 컴퓨터공학과 석사
2002년 포항공과대학교 컴퓨터공학과 박사
2002～현재 계명대학교 컴퓨터공학과 교수
관심분야 : 네트워크 및 시스템 관리, IoT 관리, SDN 네트워크 관리, 인터넷 침입 예측, 네트워크 보안
E-mail : juht@kmu.ac.kr