Proceedings of KFIS Autumn Conference 2007 Vol. 17, No. 2.

비정상 트래픽 제어 프레임워크를 위한 퍼지 로직 기반의 포트스캔 공격 탐지 기법

A Portscan Attack Detection Mechanism based on Fuzzy Logic for Abnormal Traffic Control Framework

김재광, 이지형

성균관대학교 정보통신공학부 컴퓨터공학과
E-mail: {linux, jhlee}@ece.skku.ac.kr

요 약

비정상 트래픽 제어 프레임워크에 적용된 비정상 트래픽 제어 기술은 침입, 분산서비스거부 공격, 포트스캔 공격과 같은 비정상 행위의 트래픽을 제어하는 공격 대응 방법이다. 이 대응 방법은 비정상 행위에 대한 true-false 방식의 공격 대응 방법이 가지는 높은 오탐율(false-positive rate)을 낮출 수 있다는 장점이 있지만, 공격 지속시간에만 의존하여 비정상 트래픽을 판단하기 때문에, 공격에 대한 신속한 대응을 하지 못한다는 한계를 가지고 있다. 이에 본 논문에서는 비정상 트래픽 제어 프레임워크에 퍼지 로직을 적용하여 신속한 공격 대응이 가능한 포트스캔 공격 탐지 기법을 제안한다.

Key Words: Fuzzy Logic, Portscan attack, Detection, Abnormal traffic control

1. 서 론

최근 서비스거부 공격 및 분산서비스거부 공격과 같은 네트워크 기반의 공격이 빈번하게 발생하고 있다. 이에 대한 새로운 대응방안으로 주목받고 있는 것은 비정상 트래픽 제어(Abnormal Traffic Control) 기술이다. 이러한 기술을 구현하는데 가장 필요한 것은 공격을 정확히 탐지하는 것이다. 공격을 오판하였을 때엔 정상적인 서비스를 방해하거나, 반대로 공격을 허용하는 일이 발생하기 때문이다.

비정상 트래픽 제어는 공격을 탐지한 후, 단순히 패킷을 차단할 수밖에 없는 기존의 공격 대응방법과는 달리 공격 탐지 오판에 의한 정상적인 서비스를 방해나 공격의 허용율을 줄일 수 있다는 장점이 있다. 하지만 기존의 탐지 방법은 비정상 행위를 탐지 할 때에 규칙 기반의 탐지를 하기 때문에, 규칙에 해당된 공격이 지속되는 정도에 따라 트래픽 제어를 할 수밖에 없다. 이 때문에 공격에 대한 빠른 대응이 불가능하다[1].

본 논문에서는 공격의 정도를 퍼지 로직을 이용한 함수식으로 구하는 방법을 제안한다. 구체적으로 퍼지 로직을 이용한 포트스캔 공격 탐지 기법을 구현하여 이 정보를 비정상 트래픽 제어 프레임워크에 적용한다.

본 논문은 2장에서 배경지식을 소개하고, 3장에서 제안 기법을 소개한다. 4장에서는 기존의 포트스캔 탐지 기법을 적용한 비정상 트래픽 제어 프레임워크와 제안 기법을 적용한 비정상 트래픽 제어 프레임워크의 기능 비교를 소개하고 마지막으로 5장에서 결론을 말한다.

2. 배경 지식

본 절에서는 비정상 트래픽 제어 프레임워크에 대한 간략한 소개와 비정상 트래픽 제어 프레임워크에 사용된 기존의 포트스캔 공격 탐지 및 대응 기법에 대한 소개, 그리고 느린 포트스캔 공격 탐지법에 대해 소개한다.

2.1 비정상 트래픽 제어 프레임워크

비정상 트래픽 제어 프레임워크란 비정상 트래픽을 판별하고, 판별된 비정상 트래픽에 대응하기 위한 프레임워크를 말한다. 비정상 트래픽이란 정상적이지 않은 네트워크 패킷의 흐름을 말하는데 정상적이 않다는 것은 사용자가 기대하지 않은 패킷의 흐름을 의미한다. 특히 비정상 트래픽에는 서비스거부를 유발하는 패킷의 흐름이나, 포트스캔 공격과 같이 특정 시스템의 취약점을 알아내기 위한 공격 등 네트

워크기반의 공격들이 포함된다. 이러한 트래픽에 대응하기 위해 비정상 트래픽 제어 프레임워크는 패킷을 차단하는 방법 외에 서비스품질 보증 메커니즘을 이용하여 트래픽을 제어한다 [1].

비정상 트래픽 프레임워크를 설계하는 것은 두 가지 측면에서 어렵다. 그 이유는 첫째로 비정상 트래픽을 정확히 판별하는 것이 어렵기 때문이고, 둘째는 정확하게 판별되지 않은 비정상 트래픽에 대해 대응 하는 것이 어렵기 때문이다.

그림 1은 리눅스에 구현된 비정상 트래픽 제어 프레임워크의 구조도이다. IA(Intrusion Analysis) 모듈과 IP(Intrusion Prevention) 모듈은 비정상 트래픽을 판별하고, 제어하는 모듈이다.

동작 과정을 간략히 살펴보면, 유입된 패킷은 제일 처음 PF(Packet Filtering) 모듈에 도달한다. PF 모듈은 처음에는 필터링 규칙이 없이 모든 패킷들을 통과시킨다. 다음으로 PA(Packet Analysis) 모듈은 패킷들로부터 유용한 정보들을 얻어낸다. 여기서 유용한 정보란, IA 모듈이 비정상 트래픽을 판단하는데 사용할 정보들을 말한다. IA 모듈은 PA로부터 전달 받은 정보를 통해 유입된 트래픽이 비정상 트래픽인지 여부를 판별한다. IA 모듈의 판단 정보에 의해 IP 모듈은 비정상 트래픽을 대응하는데, PF 모듈에 필터링 규칙을 설정하거나, QA 모듈에 트래픽 제어 규칙을 설정한다 [1].

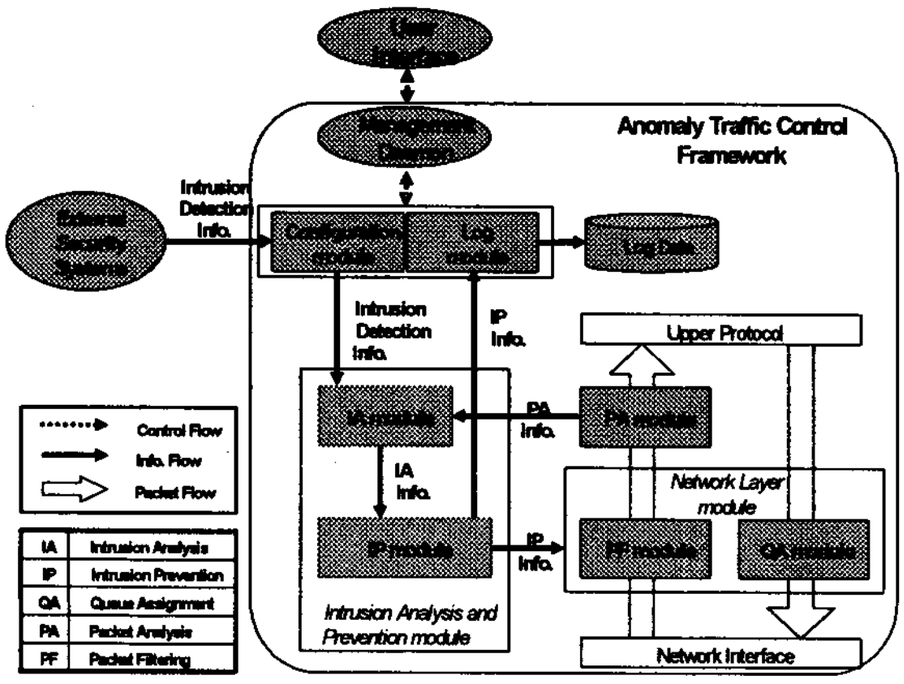

그림 1. ATCF의 구조도

2.2 기존의 포트스캔 공격 탐지 및 대응 기법

그림 1이 보이는 비정상 트래픽 제어 프레임워크를 이용하여 포트스캔 공격을 판별하고 대응할 수 있다. 이때 포트스캔 공격을 탐지하는 방법은 포트스캔 공격의 특징을 이용한다. 포트스캔 공격 탐지법은 패킷의 출발지와 도착지 주소를 확인하고, 동일한 출발지와 도착지 주소이면서 다른 포트 번호에 보내지는 패킷을 카운트 하여 단위 시간에 카운트 된 패킷의 수가 정해진 값 이상이 되면 공격으로 판단한다.

하지만 이러한 포트스캔 공격 탐지법을 사용할 때에는 정상적인 패킷을 공격으로 잘못 탐지하여 차단하는 경우가 발생할 수 있기 때문에, 비정상 트래픽 제어 프레임워크에서는 포트스캔 공격에 대한 새로운 대응법을 사용한다 [1]. 즉, 공격으로 판별된 트래픽이 지속되는 시간을 모니터링 하였다가 공격 시간이 지속되는 정도에 따라 트래픽 제어를 하는 것이다.

그림 2와 그림 3은 포트스캔 공격 탐지기법을 이용하여 공격이 탐지되었을 때, 단순히 차단하는 방법과, 공격이 탐지되었을 때, 공격 지속시간에 따라 트래픽 제어하는 것을 보인다. 그림 2에서는 포트스캔 공격이 잘못 탐지되었을 때, 정상 트래픽이 차단될 수 있지만, 그림 3에서는 공격으로 의심되는 패킷의 대역폭을 제어하고, 공격으로 의심되는 트래픽이 일정 시간 지속되어 공격임이 명백히 졌을 경우에 차단한다.

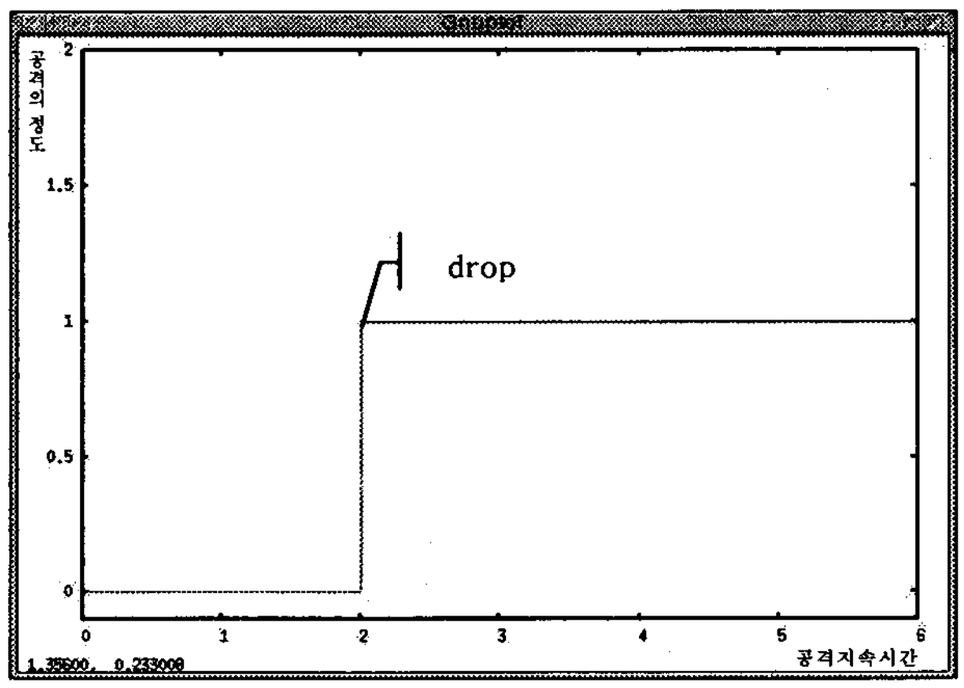

그림 2. 공격지속시간에 따른 공격의 정도(Non-fuzzy)

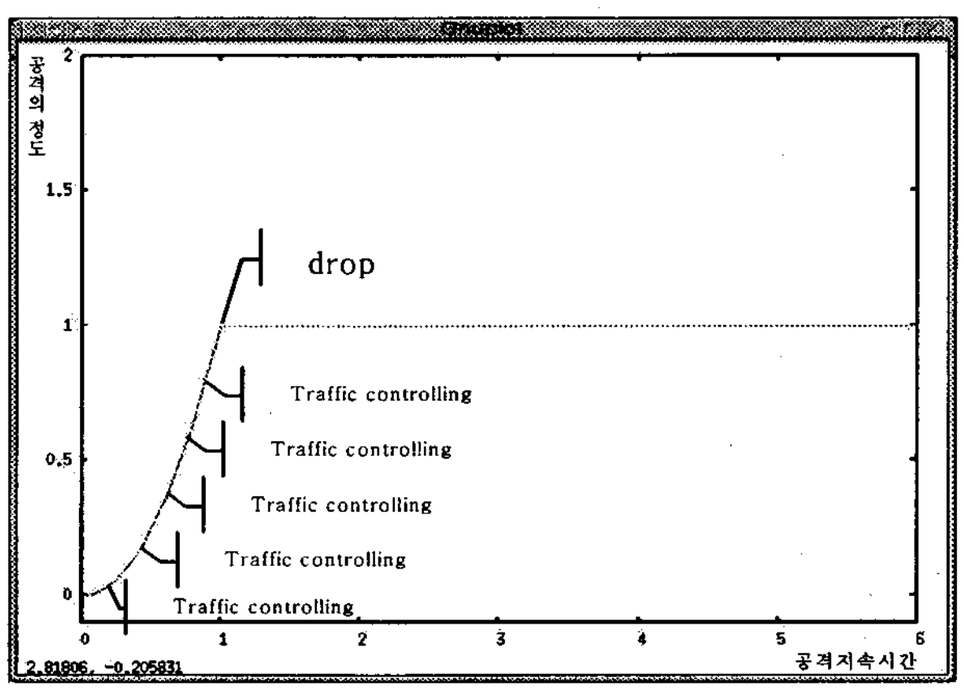

그림 3. 공격지속시간에 따른 공격의 정도(Fuzzy)

2.3 느린 포트스캔 공격 탐지법

포트스캔 공격을 탐지하는 기존의 방법은 정해진 시간 내에 출발지 주소와 목적지 주소가 같고 목적지의 포트번호가 다른 패킷을 포트스캔 공격으로 판단하는 것이다. 하지만 이러한 탐지 기법은 공격자가 공격으로 판단될 수 있는 정해진 시간을 알고 있는 경우, 정해진 시간을 지나 천천히 패킷을 보내 탐지 규칙을 피해 공격하는 느린 공격(slow attack)을 할 수 있다는 문제가 있다. 예를 들어 어떤 방어 프레임워크의 포트스캔 공격 탐지 규칙이 2초 동안 출발지 주소와 목적지 주소가 같고 목적지의 포트번호가 다른 패킷이 5개 이상 올 경우라고 하자. 이 방어 프레임워크의 공격 판단 규칙을 알고 있는 공격자는 2초마다 5개미만의 패킷을 보내므로 이 방어 프레임워크의 포트스캔 공격 탐지를 피하여 포트스캔 공격을 할 수 있다.

포트스캔 공격 중, 느린 공격이 알려지면서 현대의 탐지 기법들은 패킷 탐지 시간을 2, 4, 8, 16, 32, 64, 128배로 증가시켜 복수의 시간을 검사하는 방법으로 느린 포트스캔 공격을 탐지하고 있다. 그림 4는 느린 포트스캔 공격을 포함한 포트스캔 공격 탐지 기법의 함수 그래프를 보인다. 그림 4의 세로축은 공격의 정도를 나타내며 공격일 때 1, 공격이 아닐 때 0의 값을 가진다. 그림 4의 가로축은 시간축으로 단위시간 T의 배수를 나타낸다. 가로축의 값 2는 단위시간 T의 값이 1초 일 경우 2초를 나타낸다.

3. 제안기법

본 절에서는 기존의 포트스캔 공격 탐지법의 문제점을 설명하고, 퍼지 로직을 적용한 탐지법으로 기존의 포트스캔 공격 탐지법의 문제점 해결을 제안한다.

3.1 비정상 트래픽 제어 프레임워크에서 기존의 포트스캔 공격 탐지법을 사용할 때의 문제점

비정상 트래픽 제어 프레임워크에서 그림 4와 같은 포트스캔 공격 탐지 함수를 사용하였을 경우, 이 정보를 이용하여 비정상 트래픽을 제어하기에 적합하지 않다. 그 이유는 그림 4가 보이는 기법은 공격인지 여부를 1과 0의 값으로만 나타내기 때문에, 공격으로 판단되는 패킷을 차단하거나, 트래픽 제어를 하더라도 공격 지속시간을 이용할 수밖에 없기 때문이다.

비정상 트래픽에 대하여 패킷을 차단만 하였을 경우, 공격으로 판단 된 패킷 중 공격 패킷이 아니지만, 포트스캔 공격이나 느린 포트스캔 공격으로 오판되는 경우가 발생한다. 또한 공격 지속시간을 근거로 트래픽 제어를 할 경우에는 느린 포트스캔 공격이 아닌 경우에 트래픽을 차단하기까지 시간이 오래 걸려, 공격을 모두 허용하는 경우가 발생할 수 있다.

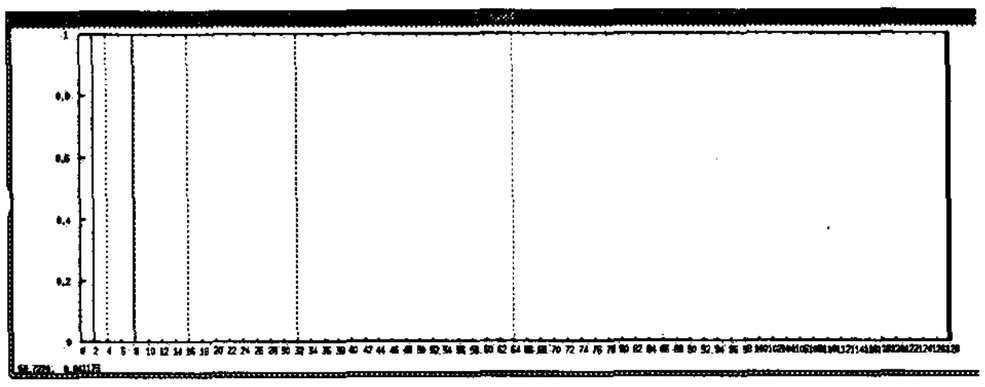

그림 4. 느린 포트스캔 공격을 탐지할 수 있는 포트스캔 공격 탐지 함수의 그래프

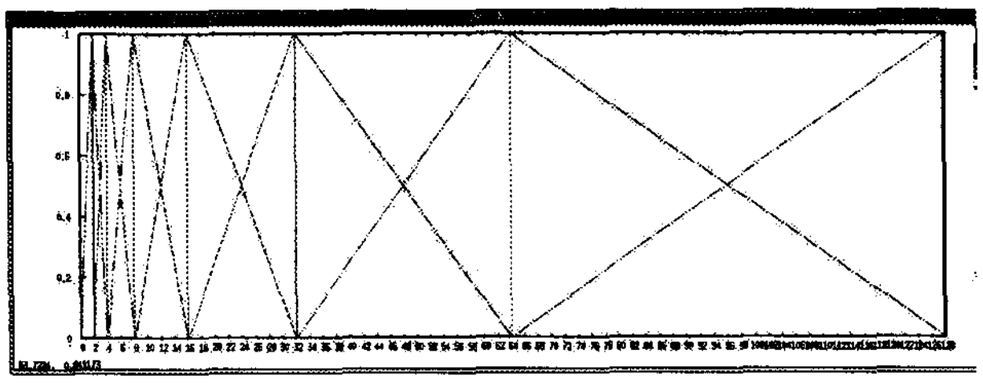

그림 5. 기존 포트스캔 공격 탐지 함수의 그래프에 퍼지 로직을 추가하여 만든 그래프

3.2 퍼지 로직을 이용한 포트스캔 공격 탐지법

본 절에서는 3.1절에서 설명한 문제점을 해결하기 위한 방법으로 비정상 트래픽 제어 프레임워크에 적합한 퍼지로직 기반의 포트스캔 공격 탐지 기법을 제안한다.

퍼지 로직은 판단이 불분명한 명제를 다루는데 적합하다[1]. 그러므로 퍼지 로직을 적용하여 공격의 여부를 판단하는 것은 비정상 트래픽 제어 프레임워크의 공격 탐지 기법으로 유용하다.

그림 5는 퍼지 로직을 이용한 포트스캔 공격 탐지 기법의 함수 그래프를 보인다. 그림 5의 세로축은 공격의 정도를 나타내는 값으로 1과 0 사이의 값을 가진다. 그림 5의 가로축은 그림 4의 가로축과 같이 시간을 나타낸다.

비정상 트래픽 제어 프레임워크에서 필요한 정보는 단위 시간에 어느 정도의 비정상 트래픽이 유입되었을 때, 이것을 어느 정도의 공격으로 판단할 것인가 하는 판단근거이다. 그림 5는 이와 같은 정보를 제공한다.

그림 5는 그림 4의 그래프에 13개의 선분을 추가한 그래프이다. 추가된 각 선분은 1차 함수식으로 나타낼 수 있다. 그림 5가 보이는 그

래프에서 각 시간의 최대값을 연결하여 함수 그래프를 나타낸 것이 그림 6이다.

제안기법은 비정상 트래픽 제어 프레임워크에서 트래픽 제어를 위한 공격의 정도를 판단할 때, 공격 지속시간을 근거로 하지 않고, 그림 6이 보이는 퍼지 로직이 적용된 함수를 이용한다. 그림 6이 보이는 함수 그래프를 이용하면 패킷을 모니터링 하는 모든 시점에서 공격정도를 판단할 수 있기 때문이다[2][3].

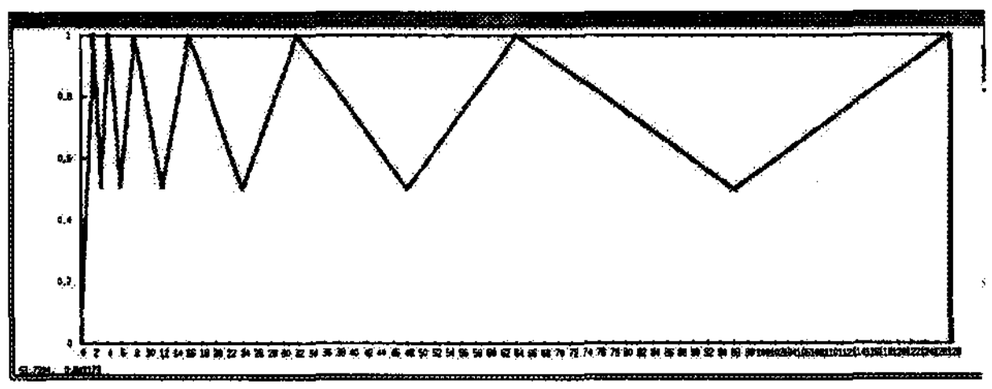

그림 6. 퍼지 로직을 이용한 포트스캔 공격 탐지 함수 그래프

3.4 탐지를 위한 퍼지 함수식 계산

식 1은 그림 6에서 보인 포트스캔 공격 탐지 함수 그래프의 함수식이다. 각 구간마다 1차 함수 그래프가 존재하며 가로축인 시간에 따라 0~1사이의 공격정도 값과 매칭된다. 세로축의 값이 1보다 작은 값이 나오는 시간에는 트래픽 제어하고, 세로축의 값이 1일 때에는 트래픽을 차단한다[4].

$$
\begin{aligned}
a &= (\frac{1}{2T})x && (0 \le x \le 2T)\\
b &= -(\frac{1}{2T})x + 2 && (2T \le x \le 3T)\\
c &= (\frac{1}{2T})x - 1 && (3T \le x \le 4T)\\
d &= -(\frac{1}{4T})x + 2 && (4T \le x \le 6T)\\
e &= (\frac{1}{4T})x - 1 && (6T \le x \le 8T)\\
f &= -(\frac{1}{8T})x + 2 && (8T \le x \le 12T)\\
g &= (\frac{1}{8T})x - 1 && (12T \le x \le 16T)\\
h &= -(\frac{1}{16T})x + 2 && (16T \le x \le 24T)\\
i &= (\frac{1}{16T})x - 1 && (24T \le x \le 32T)\\
j &= -(\frac{1}{32T})x + 2 && (32T \le x \le 48T)\\
k &= (\frac{1}{32T})x - 1 && (48T \le x \le 64T)\\
l &= -(\frac{1}{64T})x + 2 && (64T \le x \le 96T)\\
m &= (\frac{1}{64T})x - 1 && (96T \le x \le 128T)
\end{aligned}
\qquad \text{..(식 1)}
$$

4. 기능 비교

본 절에서는 퍼지 로직을 적용한 비정상 트래픽 제어 프레임워크와 퍼지 로직을 적용하지 않은 비정상 트래픽 제어 프레임워크의 기능 비교 결과를 보인다.

4.1 퍼지 로직을 적용한 결과

퍼지 로직 기반의 포트스캔 공격 탐지 기법을 사용한 비정상 트래픽 제어 프레임워크는 기존의 포트스캔 공격 탐지 기법을 사용한 비정상 트래픽 제어 프레임워크와는 달리 포트스캔 공격의 정도에 따라 신속한 트래픽 제어와 트래픽 차단, 두 가지의 대응이 가능하였다.

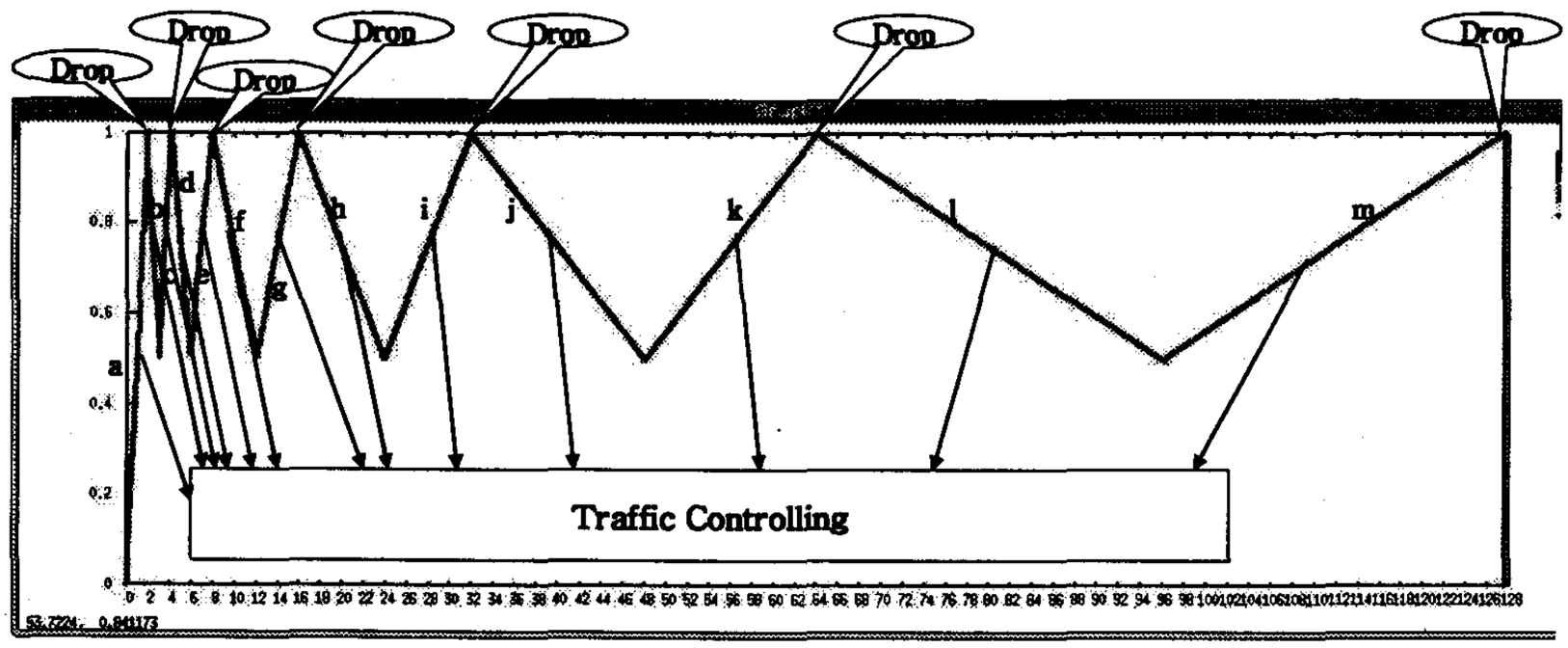

그림 7. 퍼지 로직을 이용한 포트스캔 공격 탐지 그래프에 따른 트래픽 제어와 차단

표 1은 퍼지 로직 기반의 포트스캔 공격 탐지기법을 사용하였을 때, 기존의 탐지 기법을 사용한 비정상 트래픽 제어 프레임워크에 비하여 느린 포트스캔 공격을 탐지하고, 대응하는데 적합함을 보인다.

기능 비교를 위해 그림 4가 보이는 바와 같이 2초, 4초, 8초, 16초, 32초, 64초, 128초 동안 출발지와 도착지가 동일하며 포트 번호가 다른 패킷이 지나는 수를 정하여 기존의 포트스캔 공격 탐지 기법과 퍼지 로직 기반의 포트스캔 공격 탐지 기법에서 동작 결과를 예측한 후, 각각 포트스캔 공격을 탐지할 수 있는지 비교한다.

표 1은 포트스캔 공격으로 의심되는 패킷이 처음 2초 동안 4개 이상 지나면, 공격으로 정하는 규칙 하에서 2초일 때, 지나는 패킷의 수에 따라 기존의 포트스캔 공격 탐지 기법과 퍼지 로직 기반의 포트스캔 공격 탐지 기법의 공격 탐지 결과를 보인다.

표 1. 기존의 포트스캔 공 격 탐지 기법과 퍼지 로직 기반의 포트스캔 공격 탐지 기법의 기능 비교

패킷 수 (2초 동안)	트래픽 분석 결과	
	기존 탐지 기법	퍼지 로직 기반의 탐지 기법
1	공격 정도 = 0	공격 정도 = 1/4
2	공격 정도 = 0	공격 정도 = 2/4
3	공격 정도 = 0	공격 정도 = 3/4
4	공격 정도 = 1	공격 정도 = 1

표 1이 보이는 바와 같이 기존 탐지 기법은 패킷의 수가 기준 값 이하일 때에, 공격 정도가 0이라고 판단하지만, 퍼지 로직 기반의 포트스캔 공격 탐지 기법은 매 시간 패킷의 수에 대한 공격 정도의 값을 퍼지 로직 기반의 함수식을 통하여 얻기 때문에 이 값을 기준으로 트래픽 제어를 한다.

결과를 볼 때, 퍼지 로직 기반의 공격 탐지를 사용할 때, 포트스캔 공격에 대해 신속한 대응이 가능하다는 것을 알 수 있다.

5. 결론

본 논문에서는 퍼지 로직을 이용하여 공격의 정도를 함수식으로 구하는 방법을 제안한다. 또한 퍼지 로직을 이용한 포트스캔 공격 탐지 기법을 제안하고, 기존의 공격 탐지 기법과 제안한 기법을 비정상 트래픽 제어 프레임워크에 사용하였을 경우 포트스캔 공격 탐지 결과를 계산하여 비교하였다. 결론적으로 퍼지 로직을 적용한 포트스캔 탐지 기법이 기존의 포트스캔 탐지 기법에 비하여 포트스캔 공격에 신속히 대응하며, 단계적 트래픽 제어와 차단을 사용하는 비정상 트래픽 제어 프레임워크에 적합하다는 사실을 확인하였다.

본 결과는 이 후로 퍼지 로직 기반의 다양한 네트워크 기반 공격에 대한 탐지 및 대응 방법에 대한 연구에 공헌할 것으로 기대된다.

참 고 문 헌

[1] Kwangsun Ko, Eun-kyung Cho, Taekeun Lee, Yong-hyeog Kang, and Young Ik Eom, "The Abnormal Traffic Control Framework based on QoS Mechanisms," LNCS #3280: ISCIS 2004, Springer-Verlag 2004, pp. 167-175

[2] G. Singarju, L. Teo, Y. Zheng, "A Testbed for Quantitative Assignment of Intrusion Detection System using Fuzzy Logic," Second IEEE IWIA'04, 2004

[3] Z. Jian, D. Yong, and G. Jian, "Intrusion Detection System based on Fuzzy Default Logic," The IEEE International Conference on Fuzzy Systems, 2003

[4] A. Ofrila, J. Carbo, A. Ribagorda, "Fuzzy Logic on Decision Model for IDS," The IEEE International Conference on Fuzzy Systems, 2003