비정상 트래픽 제어 프레임워크를 위한 퍼지로직 기반의 포트스캔 공격 탐지기법

김재광*, 김가을*, 고광선*, 강용혁**, 엄영익*
*성균관대학교 정보통신공학부
**극동대학교 경영학부
e-mail:{linux, zfall, rilla91, yieom}@ece.skku.ac.kr
yhkang@kdu.ac.kr

A Detection Mechanism of Portscan Attacks based on Fuzzy Logic for an Abnormal Traffic Control Framework

Jaekwang Kim*, Kaeul Kim*, Kwangsun Ko*, Yong-hyeog Kang**, and Young Ik Eom*
*School of Info. and Comm. Eng., Sungkyunkwan University
**Dep. of Business Administration, Far East University

요 약

비정상 행위에 대한 true/false 방식의 공격 탐지 및 대응방법은 높은 오탐지율(false-positive)을 나타내기 때문에 이를 대체할 새로운 공격 탐지방법과 공격 대응방법이 연구되고 있다. 대표적인 연구로는 트래픽 제어 기술을 이용한 단계적 대응방법으로, 이 기술은 비정상 트래픽에 대해 단계적으로 대응함으로써 공격의 오탐지로 인하여 정상 서비스를 이용하는 트래픽이 차단되지 않도록 하는 기술이다. 비정상 트래픽 중 포트스캔 공격은 네트워크 기반 공격을 위해 공격대상 호스트의 서비스 포트를 찾아내는 공격으로 이 공격을 탐지하기 위해서는 일정 시간동안 특정 호스트의 특정 포트에 보내지는 패킷 수를 모니터링 하여 임계치와 비교하는 방식의 true/false 방식의 공격 탐지방법이 주로 사용되었다. 비정상 트래픽 제어 프레임워크(Abnormal Traffic Control Framework)는 true/false 방식의 공격 탐지방법을 이용하여 공격이 탐지되었을 때, 처음에는 트래픽 제어로 대응하고 같은 공격이 재차 탐지되었을 때, 차단하여 기존의 true-false 방식의 공격 탐지 및 대응방법이 가지는 높은 오탐지율을 낮춘다. 하지만 포트스캔 공격의 특성상, 공격이 탐지된 후 바로 차단하지 못하였을 경우, 이미 공격자가 원하는 모든 정보를 유출하게 되는 문제가 있다. 본 논문에서는 기존의 True/False 방식의 포트스캔 공격 탐지방법에 퍼지 로직 개념을 추가하여 공격 탐지의 정확성을 높이고 기존의 탐지방법을 이용하였을 때보다 신속한 트래픽 제어 및 차단을 할 수 있는 방법을 제안한다.

1. 서론

최근 발생하는 네트워크 기반 공격의 시작은 공격 대상 공격 대상 호스트의 서비스 포트를 알아내는 포트스캔 공격이다. 포트스캔 공격에 대한 대응책으로 기존에는 공격 패킷으로 의심되는 패킷을 모니터링 하여 일정시간 동안 의심 패킷의 수가 정해진 임계치를 초과하는 경우 공격으로 판단하여 패킷을 차단하는 true/false 방식을 사용하였다. 이 방법은 신속한 대응을 할 수 있다는 장점이 있는 반면, 탐지를 실패하였을 경우, 정상 서비스를 차단하는 오탐지율이 높다는 단점이 있다. 이같은 높은 오탐지율을 낮추기 위한 네트워크 공격에 대한 대응 기술에는 비정상 트래픽 제어(Abnormal Traffic Control) 기술이 있다. 비정상 트래픽 제어 기술을 이용하여 비정상 트래픽 제어 프레임워크(Abnormal Traffic Control Framework)를 구축하는 경우 true/false 방식으로 공격을 탐지한 후, 처음에는 비정상 트래픽의 대역폭을 줄이는 방법으로 대응하다가 같은 공격이 두 번째 탐지된 경우, 그 트래픽을 차단한다. 이러한 대응은 오탐지율을 줄이는 장점이 있지만 포트스캔 공격과 같이 짧은 시간에 이뤄지는 공격을 허용할 수 있다[1].

본 논문에서는 ATCF에 알맞은 포트스캔 공격 탐지기법을 제안한다. 이 기법은 공격여부 정할 때, 공격의 정도를 값으로 수치화하고, 퍼지로직을 이용한 함수식을 이용하여 공격정도 값을 구하여 공격을 판단한다.

본 논문은 2장에서 배경지식을 말하고, 3장에서 제안 기법을 소개한다. 4장은 true/false 방식의 포트스캔 탐지 기법을 적용한 ATCF와 제안 기법을 적용한 ATCF와의 기능 비교를 보이고, 마지막으로 5장에서 결론 및 향후 연구계획을 제시한다.

2. 배경지식

본 절에서는 기존의 true/false 방식의 포트스캔 공격 탐지 방법에 대한 소개와 true/false 방식의 포트스캔 공격 탐지 정보를 ATCF에 적용하여 단계적으로 대응하는 기술을 소개 한다.

2.1 True/false 방식의 포트스캔 공격 탐지기법

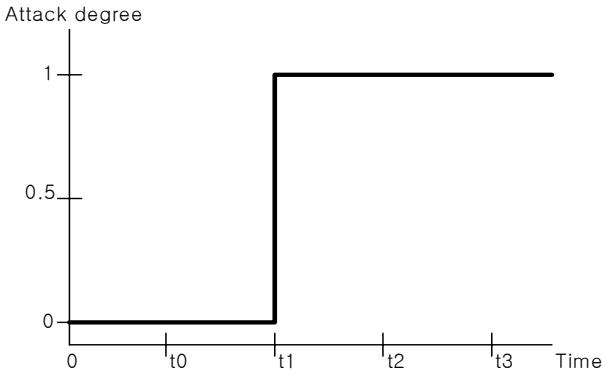
True/false 방식의 포트스캔 공격 탐지기법은 포트스캔 공격이 공격인지 아닌지를 규칙이나 정해진 임계치에 기준하여 명확하게 판단하는 방법이다. 예를 들어, 출발지와 도착지 주소가 동일한 패킷이 포트번호를 달리하여 연속적으로 지날 경우 포트스캔 공격을 의심해 볼 수 있다. true/false 방식의 포트스캔 공격 탐지기법에서는 이렇게 포트스캔 공격으로 의심되는 패킷이 초당 정해진 개수 이상 지나는 것을 공격으로 판단한다. true/false 방식의 포트스캔 공격 탐지기법에서는 그림 1이 보이는 바와 같이 t1 시간에서 공격이 탐지된 경우 그 즉시 공격의 정도는 1이 된다. 이것은 한 번의 공격 탐지로 공격으로 판단되는 true/false 방식의 특징을 잘 나타내준다.

2.2 ATCF를 위한 True/False 방식의 포트스캔 공격 탐지 정보

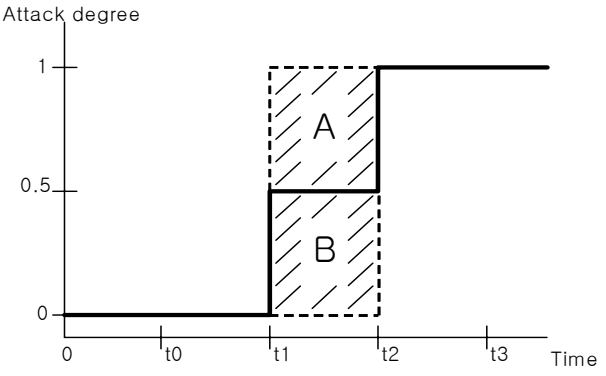
ATCF에서도 기존의 true/false 방식과 동일하게 공격을 탐지한다. 단 ATCF에서는 공격이 처음 탐지되었을 경우 공격의 정도를 0.5로 판단하고, 그 상태에서는 트래픽 제어를 하기 위한 정보로 이용할 수 있다. 공격의 정도가 0.5인 상태에서 같은 공격이 재탐지 되면, 공격의 정도가 1이 되고, 이 정보는 패킷을 차단하는 정보로 이용할 수 있다. 그림 2는 true/false 방식의 포트스캔 공격 탐지기법을 이용하여 공격이 첫 번째 탐지된 시점(t1)과 두 번째 탐지된 시점(t2)을 전후한 공격정도를 보인다.

2.3 느린 포트스캔 공격 탐지기법

포트스캔 공격을 탐지하는 기존의 방법은 일정 시간 내에 출발지 주소와 목적지 주소가 같고 목적지의 포트번호를 바꾸어가며 전송되는 패킷을 포트스캔 공격으로 판단하는 것이다. 하지만 이러한 탐지기법은 공격자가 공격을 탐지하는 루틴을 알고, 공격으로 판단될 수 있는 탐지 시간 간격보다 느린 간격으로 패킷을 보내면 공격의 탐지를 피할 수 있다. 이러한 공격을 느린 포트스캔 공격(slow portscan attack)이라고 한다.[1]. 예를 들어 어떤 방어 프레임워크의 포트스캔 공격 탐지 규칙이 2초 동안 출발지 주소와 목적지 주소가 같고 목적지의 포트번호가 다른 패킷이 5개 이상 올 경우라고 하였을 때, 공격자는 2초마다 5개미만의 패킷을 보내므로 포트스캔 공격 탐지를 피하여 포트스캔 공격을 할 수 있다.



(그림 1) True/False 방식의 포트스캔 공격 탐지기법에서 공격을 탐지한 시점(t1)전후의 공격정도



(그림 2) True/False 방식의 포트스캔 공격 탐지기법을 이용하여 공격이 첫 번째 탐지된 시점(t1)과 두 번째 탐지된 시점(t2)전후의 공격정도

느린 공격이 알려지면서 현대의 탐지기법들은 패킷 탐지 시간을 2, 4, 8, 16, 32, 64, 128배로 증가시켜 복수의 시간을 검사하는 방법으로 느린 포트스캔 공격을 탐지하고 있다. 그림 3는 느린 포트스캔 공격을 포함한 포트스캔 공격 탐지기법의 함수 그래프를 보인다. 그림 3의 세로축은 공격정도를 나타내며 공격일 때는 1, 공격이 아닐 때는 0의 값을 가진다. 그림 3의 가로축은 시간 축으로 단위시간 T의 배수를 나타낸다. 가로축의 값 2는 단위시간 T의 값이 1초 일 경우 2초를 나타낸다.

3. 제안기법

본 절에서는 ATCF에서 사용하던 true/false 방식의 포트스캔 공격 탐지법의 문제점을 지적하고, 그 해결책으로 퍼지로직을 적용한 포트스캔 공격 탐지기법을 제안한다.

3.1 ATCF에서 기존의 포트스캔 공격 탐지기법 사용의 문제점

ATCF에서 그림 3과 같은 포트스캔 공격 탐지 함수를 사용하였을 경우, 이 탐지결과로 얻은 정보로는 비정상 트래픽을 제어하기에는 적합하지 않다. 왜냐하면 그림 3이 보이는 기법은 공격인지 여부를 1과 0의 값으로만 나타내

기고, 이 정보는 공격의 정도에 맞추어 트래픽 제어를 하기에 부적합하기 때문이다. 기존의 ATCF에서는 느린 포트스캔 공격을 포함한 포트스캔 공격 탐지기법으로 2.2절에서 설명한 바와 같이 공격이 첫 번째 탐지되었을 경우, 공격의 정도를 0.5로 정하여 이때의 정보를 트래픽 제어하기 위한 정보로 사용하고, 같은 공격이 두 번째 탐지되었을 경우 공격의 정도를 1로 정하여 이 정보를 트래픽 차단의 결과로 사용하였다. 이렇게 할 경우 그림 2가 보이는 바와 같이 빗금 친 부분 A의 넓이만큼 오탐률을 줄일 수 있지만, 반대로 빗금 친 부분 B의 넓이만큼 포트스캔 공격을 허용하게 된다.

3.2 퍼지로직을 이용한 포트스캔 공격 탐지기법

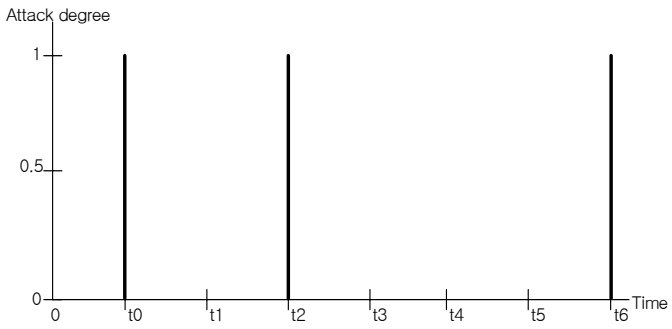
본 절에서는 3.1절에서 설명한 문제점을 해결하기 위한 방법으로 ATCF에 적합한 퍼지로직 기반의 포트스캔 공격 탐지기법에 대하여 설명한다.

퍼지로직은 판단하기 어려운 명제를 다루는 데 적합하다[2]. 이러한 퍼지로직의 특성을 이용하여 공격의 여부를 판단한 정보는 ATCF의 공격 탐지기법으로 유용하다. 그림 4는 퍼지로직을 이용한 포트스캔 공격 탐지기법의 함수 그래프를 보인다. 그림 4의 세로축은 공격의 정도를 나타내는 값으로 1과 0 사이의 값을 가진다. 그림 4의 가로축은 그림 3의 가로축과 같이 시간을 나타낸다. ATCF에서 필요한 정보는 단위 시간에 어느 정도의 비정상 트래픽이 유입되었을 때, 이것을 어느 정도의 공격으로 판단할 것인가 하는 공격 탐지 정보이다. 그림 4는 이와 같은 정보를 제공한다.

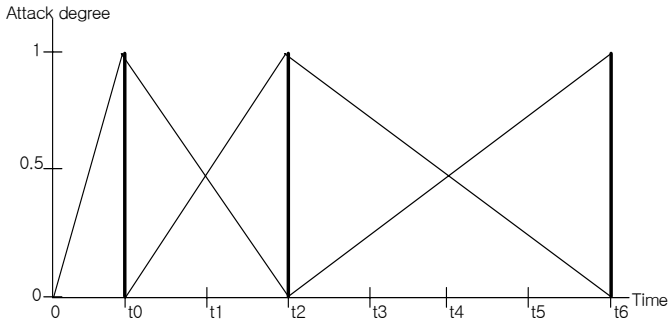
그림 4는 그림 3의 그래프에 13개의 선분을 추가한 그래프이다. 이 선분들은 인접한 값들을 선형으로 연결하여 중간 값을 만들어 내는 퍼지 로직 개념이 추가된 함수 그래프이다. 이 선분들은 모두 1차 함수식이며 이 선분 중에서 각 시간에서의 최대값을 연결하여 함수 그래프로 나타낸 것이 그림 5이다.

본 논문에서의 제안기법은 ATCF에서 트래픽 제어를 위한 공격의 정도를 판단할 때, 공격 지속시간을 근거로 하지 않고, 그림 5가 보이는 퍼지로직이 적용된 함수를 이용한다. 그림 5가 보이는 함수 그래프를 이용하면 패킷을 모니터링 하는 모든 시점에서 공격정도를 알아낼 수 있다[2][3].

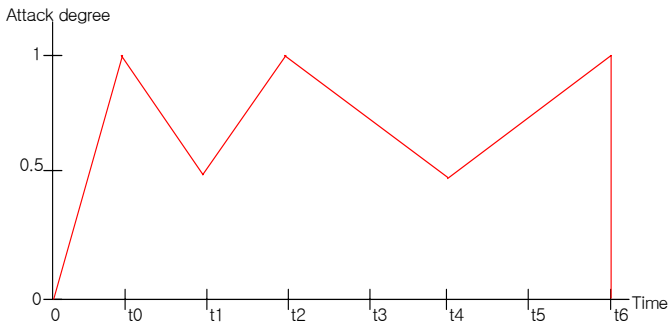
$$
\begin{aligned}
a &= \left(\frac{1}{2T}\right)x && (0 \le x \le 2T)\\
b &= -\left(\frac{1}{2T}\right)x + 2 && (2T \le x \le 4T)\\
c &= \left(\frac{1}{4T}\right)x - \frac{1}{2} && (4T \le x \le 6T)\\
d &= -\left(\frac{1}{8T}\right)x + \frac{7}{4} && (6T \le x \le 10T)\\
e &= \left(\frac{1}{8T}\right)x - \frac{3}{4} && (10T \le x \le 14T)
\end{aligned}
\qquad \text{..(식 1)}
$$



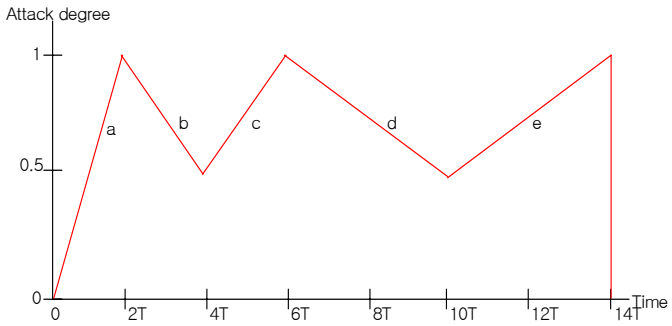
(그림 3) 느린 포트스캔 공격을 탐지할 수 있는 기존의 포트스캔 공격 탐지 함수의 그래프



(그림 4) 기존 포트스캔 공격 탐지 함수의 그래프에 퍼지로직을 추가하여 만든 그래프



(그림 5) 퍼지로직을 이용한 포트스캔 공격 탐지 함수 그래프



(그림 6) 식 1의 함수식과 매칭되는 퍼지로직을 이용한 포트스캔 공격 탐지 그래프

3.3 탐지를 위한 퍼지 함수식 계산

식 1은 그림 5에서 보인 포트스캔 공격 탐지 함수 그래프의 함수식이다. 그림 6이 보이는 바와 같이 그래프는 각 구간마다 1차 함수형태로 존재하며 이 함수 그래프는 시간에 따른 공격정도 값을 0~1사이의 값으로 결정해 준다. 이 결과를 ATCF에 적용하면 공격정도의 값이 1보다 작은 값일 때에는 트래픽 제어로 공격에 대응하고, 공격정도의 값이 1이 되면, 패킷을 차단할 수 있다[4].

4. 기능비교

본 절에서는 퍼지로직을 적용한 ATCF와 퍼지로직을 적용하지 않은 ATCF의 기능비교 결과를 보인다.

4.1 퍼지로직을 적용한 결과

퍼지로직 기반의 포트스캔 공격 탐지기법을 사용한 ATCF는 기존의 포트스캔 공격 탐지기법을 사용한 ATCF와는 달리 포트스캔 공격의 정도에 따라 신속한 트래픽 제어와 트래픽 차단, 두 가지의 대응이 가능하였다. 표 1은 퍼지로직 기반의 포트스캔 공격 탐지기법을 사용하였을 때, 기존의 탐지기법을 사용한 ATCF에 비하여 느린 포트스캔 공격을 탐지하고, 대응하는데 적합함을 보인다.

기능 비교를 위해 포트스캔 공격이 지속된다는 가정하에 기존의 포트스캔 공격 탐지기법과 퍼지로직 기반의 포트스캔 공격 탐지기법이 포트스캔 공격 상태에서 어떻게 동작할지 결과를 예측한 후, 각 탐지 기법의 기능을 비교한다.

표 1은 포트스캔 공격으로 의심되는 패킷이 처음 2초 동안 4개 이상 지나면, 공격으로 정하는 규칙이라 할 때, 2초 동안 지나는 패킷의 수에 따라 기존의 포트스캔 공격 탐지기법과 퍼지로직 기반의 포트스캔 공격 탐지기법의 공격 탐지 결과를 보인다. 표 1이 보이는 바와 같이 기존 탐지기법은 패킷의 수가 기준 값 이하일 때에, 공격정도를 0이라고 판단할 수밖에 없다. 결국 포트스캔 공격 패킷을 이미 4개 허용하였을 경우에 트래픽 제어를 시작하고 다시 공격임을 판단하기 위해 8개의 포트스캔 공격 패킷을 허용한 후에 패킷을 차단하게 되어 이미 많은 정보를 유출하게 된다.

반면 퍼지로직 기반의 포트스캔 공격 탐지기법은 퍼지로직 함수에 의해 매 시간 패킷의 수에 대한 공격정도의 값을 얻고 이 값을 기준으로 신속한 트래픽 제어 및 패킷 차단을 할 수 있다. 뿐만 아니라 퍼지로직 기반의 포트스캔 공격 탐지기법을 이용하면 공격정도에 따라 트래픽 제어의 단계를 더 두어 대응의 정도를 세밀히 조절할 수 있다.

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

[표 1] 기존의 포트스캔 공격 탐지기법과 퍼지로직 기반의 포트스캔 공격 탐지기법의 기능비교

패킷 수 (2초 동안)	기존 탐지기법		퍼지로직 기반의 탐지기법	
	공격정도	대응방법	공격정도	대응방법
1	0	-	1/4	트래픽 제어 1
2	0	-	2/4	트래픽 제어 2
3	0	-	3/4	트래픽 제어 3
4	1	트래픽 제어	1	패킷 차단

5. 결론 및 향후연구

본 논문에서는 퍼지로직을 이용하여 공격의 정도를 함수식으로 구하는 방법을 제안한다. 또한 퍼지로직을 이용한 포트스캔 공격 탐지기법을 제안하고, 기존의 공격 탐지기법과 제안한 기법을 ATCF에 사용하였을 경우 포트스캔 공격 탐지 결과를 계산하여 비교하였다. 결론적으로 퍼지로직을 적용한 포트스캔 탐지기법이 기존의 포트스캔 탐지기법에 비하여 포트스캔 공격에 신속히 대응하며, 단계적 트래픽 제어와 차단을 사용하는 비정상 트래픽 제어 프레임워크에 적합하다는 사실을 확인하였다.

이후 본 결과를 실제 구현하여 다양한 네트워크 기반 공격에 대한 탐지 및 대응방법에 대한 연구로 발전시키고자 한다.

참고문헌

[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, and A. Ribagorda, "Fuzzy Logic on Decision Model for IDS," The IEEE International Conference on Fuzzy Systems, 2003.