2002 년 한국정보처리학회 춘계학술발표논문집 제 9 권 제 1 호

# 기억 탐지자의 제거를 통한 동적클론선택 알고리즘의 개선

김정원*, 최종욱**, 김상진**
*런던 대학 킹스 컬리지 전산학과, **상명대학교 정보과학과
e-mail : jungwon@dcs.kcl.ac.uk juchoi@markany.com netio@sangmyung.ac.kr

# Improving Dynamic Clonal Selection Algorithm by Killing Memory Detectors

Jungwon Kim*, Jong-Uk Choi**, Sang-Jin Kim**
*Dept. of Computer Science, King's College London
**Dept. of Information Science, Sangmyung University

요 약

인공면역시스템을 이용한 침입탐지시스템 개발을 위해 적용한 동적클론선택(Dynamic Clonal Selection) 알고리즘과 그의 문제점을 소개하고 개선된 동적클론선택 알고리즘을 제안한다. 개선된 동적클론선택 알고리즘은 정상행위를 비정상행위로 판단하는 기억탐지자들을 제거함으로써 기존에 동적클론선택 알고리즘이 안고 있던 오류를 감소시키는 방안을 제시한다.

## 1. 서론

네트워크 정보 보안 시스템 기술의 개발 노력중 하나로 개발되고 있는 침입탐지시스템은 시스템의 불법적인 오용이나 남용을 탐지하는 시스템을 칭한다. 현재 사용되고 있는 침입탐지시스템은 대부분 이미 알려진 침입정보를 이용하는 것으로, 새로운 시스템의 헛점을 이용한 알려지지 않은 침입에는 많은 헛점을 드러내고 있다. 이러한 문제점을 극복하기 위한 국내외의 연구노력중 하나로, 외부에서 침입한 병원균을 효과적으로 탐지/파괴하는 인간의 면역 시스템을 응용하여 외부침입 탐지 시스템을 개발하는 연구들이 보고되고 있다 [1].

본 논문에서는 이러한 노력의 일환으로 소개된 동적클론선택 (Dynamic Clonal Selection) 알고리즘의 문제점으로 지적된 false-positive 오류를 감소시키기 위해 개선된 동적클론선택 알고리즘을 소개한다. Kim 과 Bentley[3]는 Hofmeyr[4]의 인공면역시스템을 모델로 한 동적클론선택 알고리즘의 연구보고에서, 이 알고리즘이 지금껏 관찰되었던 정상행위가 합법적인 요인들로 인하여 갑작스러운 변화를 보일경우, 이전에 생성되었던 기억 탐지자의 탐지결과는 심각한 false-positive (FP)오류를 보임을 지적하였다.

본 논문에서는 동적클론선택 알고리즘의 이러한 문제점을 개선하기 위하여, 이전에 생성되었던 기억 탐지자들을 탐지 결과에 따라 선택적으로 제거하는 새로운 방법을 소개한다. 소개된 방법은 기계학습 (Machine Learning) 연구에서 쓰이는 벤치마킹 데이터를 모의적으로 선택하여 동적클론선택 알고리즘에 제공하는 방식으로 그 성능이 평가되었다. 평가결과, 개선된 알고리즘은 기존의 동적클론선택 알고리즘의 문제였던 FP 오류를 0.1% 이하로 감소기키는 결과를 보였다.

## 2. 동적클론선택(Dynamic Clonal Selection) 알고리즘

동적클론선택 (Dynamic Clonal Selection) 알고리즘은 Hofmeyr[4] 인공면역시스템을 모델로한 새로운 인공면역알고리즘으로, 세개의 다른 탐지자 개체군의 상호작용으로 인공면역반응을 생성한다. 이 알고리즘은 [3]에 자세히 기술되어 있으며, 본 논문에서는 그의 주요 운영 메커니즘만을 소개한다.

동적클론선택 알고리즘은 관찰대상의 비정상적인 개별행위를 탐지할수 있는 탐지자 개체군을 지속적으로 생성, 갱신하는 것을 주 골자로 운영된다. 처음 무작위로 생성되는 미성숙 탐지자들은 음성선택(Negative Selection)을 통과하는것으로 성숙탐지자가 된다. 음성선택이란 현재 알고리즘이 관찰하고자하는 어떤 행위에 대한 데이타를 항원으로 간주하여, 일정 자기내성 기간 (Tolerisation Period) 동안 관찰된 모든 정상

본 논문은 한국과학재단 특정기초연구사업(1999-2-511-001-3)의 지원으로 수행되었음

항원 데이터에 대해 탐지 신호를 발산하지 않는 탐지 자들만이 성숙탐지자로 변환되는것을 허락하는 선택 과정을 칭한다. 첫번째 탐지자 생성 경로인 음성선택 (Negative Selection)으로 인하여 탐지자들은 후에 정상행위에 대해 탐지신호를 보내지 않는 자기내성(Self Tolerance)을 갖게된다.

성숙탐지자들은 곧바로 관찰되는 항원데이타들에 대해 탐지과정을 시작한다. 이때 성숙탐지자들이 새로 관찰되는 항원데이터를 비정상행위로 간주하여 탐지 신호를 발산할 경우, 성숙탐지자의 변수인 탐지총합 (Match Count)을 하나씩 증가시킨다. 따라서, 새로운 항원데이타들이 각 성숙탐지자들에 의해 비정상행위로 간주될 때마다, 각 해당 성숙탐지자들의 탐지총합은 증가하게된다. 증가된 탐지총합이 사용자가 미리 정의한 면역 반응 임계값 (Activation Threshold)이 되었을 경우, 성숙탐지자들은 최종 비정상행위 탐지 신호를 사용자에게 보내게 된다. 이는 성숙탐지자들이 음성선택을 통해 자기내성을 갖게되었지만, 자기내성 기간동안 관찰된 정상행위가 관찰시스템이 보일수 있는 모든 정상행위를 포함할수 없기때문에 초래되는 FP 오류를 줄이기 위한 방안이다.

사용자는 성숙탐지자가 보내온 탐지결과를 분석하여 그 결과가 정확하게 비정상행위를 탐지하였을 경우, 성숙탐지자를 기억탐지자로 변환시키어 새로운 항원 데이터 관찰을 위하여 다시 탐지시스템에 보내게 된다. 기억탐지자들은 새로 관찰되는 항원데이타를 비정상 행위로 간주할때, 탐지총합의 증가없이 곧바로 비정상 행위 탐지신호를 사용자에게 보낸다. 이는 기억탐지자가 성숙탐지자와는 달리 이미 비정상행위를 탐지하여 그 유용성을 검증 받았음으로 성숙탐지자들에 비해 FP 오류가 낮을것으로 기대되기 때문이다.

또하나 주목하여야 할점은 성숙탐지자들은 사용자가 미리 정의한 수명(Life Span)이 주어져 있어서, 만일 주어진 수명 기간이내에 그들의 탐지총합이 임계값을 만족시키지 못할 경우 바로 시스템에서 제거된다. 기억탐지자들은 이와는 달리 무한 수명을 가지고, 한번 생성된 경우 지속적으로 관찰되는 항원들에 대해 탐지활동을 벌인다.

따라서, 무작위로 생성된 하나의 탐지자는 일정 자기내성 기간동안 미성숙탐지자로 음성선택과정을 거친후, 탐지총합이 면역 반응 임계값에 미치기까지 성숙탐지자로의 성숙기간을 마친다. 성숙기간을 마친 성숙탐지자는 사용자의 확인을 받고서는 기억탐지자로 변환되어 탐지과정을 시작하게 된다. 이러한 세단계 과정은 항원데이터가 제공되는한 지속적으로 진행된다. 항원데이터가 제공되는 순간 동적클론선택 알고리즘은 우선 기억탐지자에 의해 비정상행위의 탐지를 시작하고, 아직 생성된 기억탐지자가 없을경우엔 항원데이터는 성숙탐지자에게 제공된다. 이때의 항원데이터에 포함되어 있을 비정상행위에 의해 성숙탐지자의 성숙과정을 진행시킨다. 그러나, 생성된 성숙탐지자도 역시 없을경우 항원데이타는 미성숙탐지자에게로 제공되어 음성선택에 쓰이게 된다. 따라서, 최초의 자기내성 기간동안은 시스템의 자기내성을 갖을수 있는 최초의 성숙탐지자 생성을 위한 훈련과정으로서, 비정상 행위가 포함되어 있지 않은 항원데이타만을 제공하는 것을 가정한다.

따라서, 동적클론선택알고리즘 진화와 학습의 한 세대는, 만족할만한 수의 최초의 성숙탐지자가 생성된 이후로는 이상에 서술된 순서, 즉 기억탐지자의 탐지, 성숙탐지자의 성숙, 미성숙탐지자의 내성으로 이루어진다.

## 3. 개선된 동적클론선택 알고리즘

Kim 과 Bentley[3]의 동적클론선택 알고리즘의 연구보고에서는 비성숙탐지자들이 음성선택 평가를 받게되는 성숙과정중 제공되는 항원데이타가 각 세대마다 다른 항원데이타를 포함하여, 전체 항원데이타의 오직 일부분만이 제공될 경우, 적절한 자기내성 기간, 성숙탐지자의 반응 임계값과 수명을 부여하는 것으로 높은 탐지율과 낮은 FP 오류를 보였다.

그러나, 지금까지 관찰되었던 정상행위가 합법적인 요인들로 인하여 갑작스러운 변화를 보일경우, 기억탐지자들의 탐지결과는 심각한 FP 오류를 보이는 문제점 역시 발견되었다. 이는 동적클론선택 알고리즘이 음성선택을 이용하여 낮은 FP 오류의 보장을 의미하는 자기내성을 갖게되었던 까닭으로 설명된다. 비성숙탐지자들의 성숙과정중 보였던 정상행위가 이후 탐지과정중에 어떤 합법적인 요인들로 인해 갑작스러운 변화를 보일경우, 기존에 생성되었던 탐지자들은 새로운 정상행위에 대해 내성을 갖게되지 못하며, 이로 인하여 높은 FP 오류를 보이는 것이다.

이러한 문제점을 개선하기 위하여 본 논문에서는 기억탐지자들을 선택적으로 제거하는 방법을 제안한다. 기존의 동적클론선택 알고리즘에서는 기억탐지자들에게 무한 수명을 부여했었다. 그러나, 실제 인간 면역 시스템의 기억면역세포들은 고정된 수의 기억면역세포군을 유지하기는 하지만, 그를 구성하는 기억면역세포들은 지속적으로 생성되고 제거되는 것으로 알려져있다 [5]. 따라서, 개선된 동적클론선택 알고리즘에서는 기억탐지자들의 탐지결과 또한 사용자가 분석하여 오직 그 결과가 비정상행위를 탐지할 경우에만 기억탐지자들을 지속적으로 기억탐지자들로 남겨둔다. 이와는 반대로, 기억탐지자들이 정상행위를 탐지하는 오류를 범했을 경우에는 기억탐지자들은 바로 시스템에서 제거된다.

## 4. 데이터와 변수값 설정

실험은 UCI 기계학습 벤키마킹 데이터 모음 사이트에서 제공하는 위스콘신 유방암 데이터를 사용하였다 (ftp://ftp.ics.uci.edu/pub/machine-learning-databases). 이 데이터는 악성종양 (Malignant)과 양성종양 (Benign) 두 그룹으로 나뉘어지는데, 악성종양에 해당되는 데이타를 비정상행위로, 양성종양에 해당되는 데이타를 정상행위로 다루어 동적클론선택 알고리즘에 제공하였다. 악성종양의 경우 240 개의 표본을 갖고 있으며, 양성종양의 경우 460 개의 표본을 갖는다.

동적으로 변화하는 분포를 가지는 항원데이터를 자

기내성기간과 성숙기간, 탐지기간중에 제공하기 위해, 정상행위와 비정상행위에 해당하는 데이터를 클러스터링으로 잘 알려진 Expectation Maximization (EM) 알고리즘[4]을 이용하여 각각 3 개의 부군(sub-groups)으로 나누었다. 동적클론선택이 진행되는 매 N 세대동안 오직 세개의 부군중 하나의 부군에 해당하는 항원데이타들의 80%에 해당하는 비정상, 정상의 항원데이터만이 무작위로 선정되어 알고리즘에 제공되었다. N이 커질수록, 생성되는 탐지자들은 가장 최근에 선택된 항원부군에 해당하는 정상행위와 비정상행위만의 분포를 인식하게 된다. 따라서, 비교적 큰값을 갖는 N 세대이후 항원부군을 갑자기 대체하는 것으로 항원데이터의 분포를 바꾸고, 동적클론선택 알고리즘이 새롭게 생성하는 탐지자들이 얼마나 빠르게 새 항원부군의 정상행위와 비정상행위 데이터를 판별할 수 있는지를 관찰, 분석하는것을 실험의 목표로 한다.

동적클론선택 알고리즘은 다양한 변수를 갖고있는데, 그 변수값에 따른 알고리즘의 성능은 [3]에 보고된바 있다. 본 논문의 실험에 쓰인 변수들의 값은 [3]에 보고된 실험결과에 따라 가장 적절한 값으로 선택되었으며, 그 값들은 표 1 에 요약되어 있다.

| 변수 | 값 |
|---|---|
| 자기내성기간 (T) | 30 |
| 성숙탐지자의 수명 (L) | 10 |
| 성숙탐지자의 면역 반응 임계값 (A) | {10, 20, 40} |
| 항원데이터가 동일 항원부군에서 지속적으로 선택되는 세대수 (N) | 30 |

표 1. 동적클론선택 알고리즘에 쓰인 변수들의 값

## 5. 실험결과

개선 이전의 동적클론선택 알고리즘과 개선이후의 알고리즘을 각각 같은 변수값을 부여하여 수행하고 난후 그 결과들을 분석하였다. 각 변수선택 조합에 따른 하나의 실험은 총 2000 세대동안 수행되었고, 각 실험을 5 회 반복수행한 평균 결과값이 그림 1 과 그림 2 에 나타나있다. 그림 1 은 개선 이전의 동적클론선택 알고리즘의 결과이고, 그림 2 는 개선 이후의 동적클론선택 알고리즘의 결과이다. 각 그림에 있는 그래프들의 X 축은 면역과정 진행 세대수를 나타내고, Y 축은 탐지율을 나타낸다. 특히 X 축의 보조선은 매 100 세대 마다 그려져있다.

그림 1 에서 볼수 있듯이 개선전 알고리즘의 결과는 [3]에서 보고된 대로, A 값이 클 경우 FP 오류율의 하락을 가져오기는 하였으나, 가장 낮은 FP 오류율이 0.5%에 도달하여 탐지시스템으로서의 만족할 만한 값을 보여주지 못하고 있다. 그러나, 그림 2 에서 보여지는 개선후 알고리즘의 결과는 A 값에 관계없이 모두 고르게 0.1% 안밖의 낮은 오류율을 보이고 있다. 이러한 그림 2 의 결과는 그림 1 에서 보여진 A 값에 따라 FP 오류율의 변화가 크게 달라진 점과 가장 낮은 FP 오류율 조차도 아주 높았던 점과는 아주 대조적이다.

뿐만아니라 두 그림에 나타난 True Positive(TP) 탐지율에서도 차이점이 발견된다. 두 경우 모두 A 값이 커짐에 따라 TP 탐지율이 하락하는데, 그림 2 에서 보여지는 하락율이 그림 1 에서 보여지는 하락율보다는 눈에띄게 큰것이 발견된다.

이렇게 개선후 알고리즘이 보인 변화된 결과는, 시스템에서 비정상행위 탐지를 수행하는 기억탐지자수중 정상행위자를 실수로 탐지하지 않는 기억탐지자가 얼마나 존재하는 가를 살펴보는 것으로 설명될 수 있다. 예를 들어, 개선전 알고리즘의 경우 항원데이타 부군이 바뀔경우 기억탐지자중 실수로 정상행위를 비정상행위로 탐지하는 경우가 발생하고, 이로 인하여 높은 FP 오류율을 보였다. 이 경우 A 값을 증가시킴으로써 그 오류율을 어느정도는 하락시킬수 있었으나, 만족할만한 수준까지 하락시키기에는 변수 A 만의 증가로는 역부족이었다.

이와는 대조적으로 개선후 알고리즘의 경우, 현재 시스템에 남아 있는 기억탐지자들은 새로운 항원데이타 부군에 속하는 새 항원데이터들의 정상행위를 비정상행위로 판단하는 오류를 범하지 않는 기억탐지자들이다. 따라서, A 값에 상관없이 일관되게 낮은 FP 오류율을 보일수 있었고, A 값이 커질경우 유용한 탐지데이터의 생성을 억제함으로써 TP 탐지율의 하락이 개선전에 비해 크게 나타난 것이다.

| Extended DynamiCS | | | | |
|---|---|---|---|---|
| | 생성 | 제거 | 잔존 | 최종탐지결과 |
| A= 10 | 124.25 (50.7) | 91.5 (33.77) | 32.75 (18.25) | 29.36 (6.28) |
| A= 20 | 78.75 (5.62) | 54.5 (3.83) | 24.25 (14.25) | 20.39 (8.35) |
| A= 40 | 55.25 (4.09) | 40.75 (5.02) | 14.5 (1.67) | 16.43 (11.76) |

표 2. 각 세대마다 생성, 제거 그리고 잔존된 기억탐지자의 수와 사용자에게 보고된 최종탐지 결과 횟수

따라서, 개선된 알고리즘의 경우 작은값의 A 를 선택하는 것이 더 효과적인 것으로 판단된다. 하지만, 이러한 성급한 결론을 내리기에는 우려되는 부수적인 결과도 관찰되었다. 표 2 는 개선된 알고리즘의 수행중 각 세대마다 생성된 기억탐지자의 수, 제거된 기억탐지자의 수와 제거되지 않고 살아남은 기억탐지자의 수를 보이고 있다. 이 결과 역시 5 회 반복수행의 평균 결과값이며 괄호안의 값은 분산값을 나타낸다.

이표의 마지막열은 탐지자가 최종탐지결과를 사용자에게 보내는 횟수를 나타낸다. 즉, 최종탐지결과가 사용자에게 보내질때 마다 사용자는 그 결과를 분석해야한다. 따라서, 이 횟수가 클수록 사용자의 도움이 더 자주 요구되므로, 이 횟수를 작게 유지하면서 만족할만한 TP 탐지율과 FP 오류율을 보일때, 인공면역시스템이 이상적인 효과를 보인다 하겠다. 표 2 의 최종탐지결과 보고 횟수는 막 생성된 기억탐지자의 수와 이전에 생성된 기억탐지자들중 제거되지 않고 살아남은 기억탐지자들을 합한수로 계산되었다. 앞서 TP 탐지율의 하락없이 낮은 FP 오류율을 보인것을 근거로 A 값이 작은 경우가 선호되었으나, 표 2 의 결과를 보면 이 경우 최종탐지결과 보고 횟수는 훨씬 크게 나타나는 것을 알 수 있다. 오히려, 최종탐지결과 보고 횟수를 줄일수 있는 큰 값의 A 를 선택하는 것이 침입탐지시스템에 쓰이기에는 더 이상적이라 하겠다. 이는 정상/비정상행위 판별을 근간으로 하는 침입탐지시스템의 가장 심각한 문제는 높은 FP 오류율로 인한 사용자의 시스템에 대한 신뢰 상실인 것으로 분석된바 있기 때문이다 [1]. 따라서, 본 논문에서 제안된 개선된 동적클

론선택 알고리즘은 높은 TP 탐지율과 낮은 FP 오류율을 유지하면서 동시에 최종탐지결과 보고횟수를 줄일 수 있는 방안이 부가적으로 개발되어야만이, 비로소 침입탐지시스템에 쓰이기에 적합한 알고리즘으로 판단될 수 있다 하겠다.

## 6. 결론 및 향후연구

본 논문에서는 인공면역시스템을 이용한 침입탐지시스템 개발을 위해, 동적클론선택 알고리즘과 그의 문제점을 소개하고, 개선된 알고리즘을 제안하였다. 동적클론선택 알고리즘과 개선된 알고리즘은 침입탐지시스템이 흔히 접하게 되는 상황, 즉 과거 안정적으로 관찰되었던 정상행위가 합법적인 요인들로 인하여 갑작스러운 변화를 보일경우를 모의 실험하여 그 탐지율과 오류율을 분석하였다. 실험은 기계 학습 벤치마킹에 쓰이는 유방암의 데이타의 악성종양의 경우를 비정상행위로 양성종양의 경우를 정상행위로 간주하여 실시되었다.

기존의 동적클론선택 알고리즘의 기억탐지자들의 탐지결과는 심각한 FP 오류를 보였고, 이는 탐지자들의 성숙과정중 보였던 정상행위가, 이후 탐지과정중에 갑작스러운 변화를 보일경우 현존하는 기억탐지자들은 새로운 정상행위에 대해 내성을 갖게되지 못한 때문으로 분석되었다. 이에따라, 개선된 알고리즘은 정상행위를 비정상행위로 오류판단하는 기억탐지자들을 제거하는 것으로 FP 오류를 감소시키는 방안을 제안하였고, 그 결과 약 0.1% 미만의 낮은 FP 오류율을 보였다.

그러나, 이러한 만족스러운 결과는 사용자의 참여에 의해서 가능했으므로, 탐지자가 최종탐지결과를 사용자에게 보내는 횟수가 아주 낮은 값일때만이 비로소 효과적일수 있는 방안이라 하겠다. 이러한 문제점을 보완할 향후연구로는, 높은 TP 탐지율과 낮은 FP 오류율을 유지하면서, 동시에 탐지자가 최종탐지결과를 사용자에게 보내는 횟수를 줄일 수 있는 방안의 개발이다. 그러한 방안으로 인간면역시스템의 체세포 돌연변이 (somatic hypermutation)를 이용한 기억탐지자 클론 방법을 동적클론선택 알고리즘에 첨가하였고, 곧 그 실험결과가 보고될 계획이다.

## 참고문헌

[1] Allen, J. et al, (2000), " State of the Practice of Intrusion Detection Technologies" , Technical Report CMU/SEI-99-TR-028, Software Engineering Institute, Carnegie Mellon University.

[2] Hofmeyr, S., (1999) An Immunological Model of Distributed Detection and Its Application to Computer Security, PhD Thesis, Dept of Computer Science, University of New Mexico.

[3] Kim, J. and Bentley, P. (2002), "Towards an Artificial Immune System for Network Intrusion Detection: An Investigation of Dynamic Clonal Selection", the Congress on Evolutionary Computation (CEC-2002), Hawaii, May 12-17. to appear.

[4] Mitchell, T. (1997), Machine Learning, McGraw-Hill. Paul, W. E., (1993), "The Immune System: An Introduction", in Fundamental Immunology 3rd Ed., W. E. Paul (Ed), Raven Press Ltd.

[5] Tizard, I. R., (1995), Immunology: Introduction, 4th Ed, Saunders College Publish

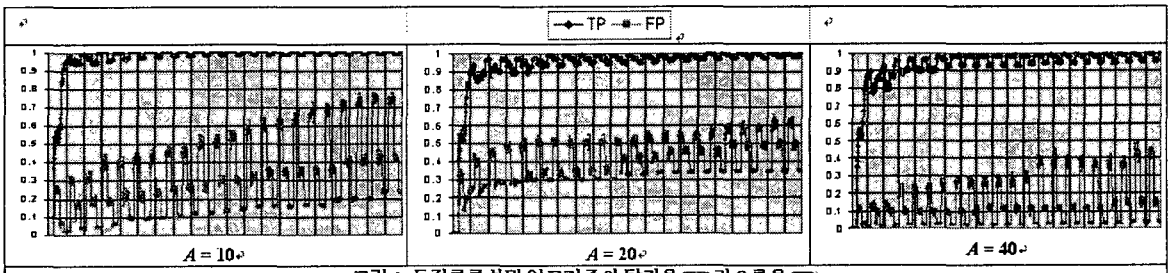


그림 1. 동적클론선택 알고리즘의 탐지율(TP)과오류율(FP)

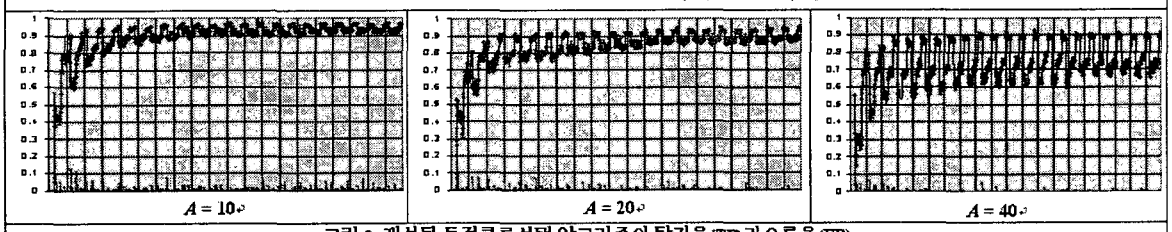


그림 2. 개선된 동적클론선택 알고리즘의 탐지율(TP)과오류율(FP)