Proceedings of KFIS Fall Conference, 2003. 5. 3

인공 면역계기반의 침입탐지 학습 알고리즘

Intrusion Detection Learning Algorithm based on Aritificial Immune System

양재원 · 이동욱 · 심귀보
Jae-Won Yang, Dong-Wook Lee, Kwee-Bo Sim

중앙대학교 전자전기공학부

요 약

나날이 발전하는 인터넷 기반의 네트워크 환경에서 보안의 중요성은 아무리 강조해도 지나치지 않다. 바이러스와 해킹 기술의 발전 속도는 항상 방어자의 능력을 앞지르고 있으며, 공격자들의 능력과 무관한 해킹 툴의 보급은 누구나가 해커가 될 수 있도록 하는데 일조하고 있다. 이제 더 이상 해킹과 바이러스로부터 안전지대는 없다고 해도 과언이 아니다. 이에 본 논문에서는 일정한 환경에서의 침입에 대해 학습을 하여 그 침입을 탐지할 수 있는 디텍터를 생성할 수 있는 알고리즘을 제안한다. 공격 유형의 수에 비해 적은, 그러나 인공 면역계의 T 세포 형성과정인 부정선택을 이용한 학습알고리즘을 기반으로 생성된 디텍터들은 상대적으로 다양한 공격의 침입을 탐지한다. 이의 유효성을 시뮬레이션을 이용하여 확인한다.

Key words : T-cell, negative selection, negative 디텍터, learning algorithm

1. 서 론

인터넷은 정보검색뿐만 아니라 모든 일상생활에 필요한 정보들의 장소, 시간, 공간에 구애받지 않고 연결시켜주는 네트워크이다. 하지만 이러한 생활의 편리함을 제공해주는 네트워크의 장점과는 대비되는 많은 단점들이 존재하는 것도 사실이다. 특히 악의적 목적으로 서비스를 제공해주는 서버 시스템에 침입하여 시스템의 오동작을 유발시키는 행위나 시스템의 자원을 고갈시키고 데이터를 훼손시키는 공격자들이 존재한다는 것이다. 이와 같은 유형의 공격을 탐지하고 사전에 방어하기 위해서 시스템 관리자들은 각종 백신 프로그램과 침입 탐지 시스템을 호스트기반과 네트워크 기반의 방어벽을 설치하고 있다. 하지만, 방어를 위한 기술력보다는 방어벽을 허물고 성공적으로 시스템에 침입하기 위한 기술 및 도구들이 최근 몇 년간 지속적으로 개발되고 있는 실정이다[1-4]. 이와 같은 흐름은 각종 방어 유틸리티나 탐지 프로그램의 향상을 도모시키는 순기능도 있지만 현재의 기술력으로 해킹 방식을 따라잡기에는 다소 버거운 감이 있다. 특히 수개월 전에 발생하여서 국내의 네트워크를 다운시켜서 악명을 떨쳤던 SQL_Overflow웜은 이를 반증하고 있다. 그래서 바이러스와 해킹 관련 연구는 국내외의 여러 관련분야 기술자뿐만 아니라 전 세계적으로 많은 학자들의 연구대상이기도 하다. 특히 생체면역계의 특성인 항원, 항체 면역반응의 모델을 응용한 연구가 현재 미국의 포레스트와 다스굽타 등의 학자들에 의해서 이루어지고 있다. 이들은 생체 면역계의 면역세포 생성원리를 모델링하여 구성한 negative 디텍터를 이용하여 변이된 네트워크 공격의 침입을 탐지하는 알고리즘을 제안하고 있다[4]. 포레스트 등의 연구는 주로 자기 시스템에 의해서 부정선택되는 negative 디텍터를 기반으로 외부로부터 유입되는 침입을 탐지하는 알고리즘으로써 주로 네트워크 관련 침입에 대응하는 연구를 하고 있다. 이에 반해 다스굽타는 생체 면역계의 면역세포들이 상호간에 유기적으로 연결되어 있는 원리를 응용하여 로봇 제어에 관한 연구를 하고 있다. 각각의 면역세포들은 자율적으로 분산되어 있는 독립된 대행체로서 뇌의 통제를 받지 않는다. 또한 각 면역세포는 독립적인 기능을 가지고 있으며 특정 자극에 의해 자신의 임무를 완수한다. 이렇듯, 생체 면역계의 기능은 아직 밝혀지지 않은 부분도 있지만 현재까지 확인된 기능만으로도 관련 연구가 활발히 이루어지고 있다. 특히 T 세포의 항원 수용체(TcR)는 T 세포 표면에 위치하여 자기 세포와 비자기 세포를 구분하는 안테나 역할을 하는 분자이다. 또한 T 세포는 네 종류의 리셉터 단백질 분자(α, β, γ, δ사슬)가 존재하는데, 각각이 유전자들의 조합으로 매우 다양하다. 이에 본 논문에서는 생체 면역계의 T 세포의 생성원리인 유전자의 조합방식과 두 가지 선택 방식 중 negative selection을

본 연구는 산업자원부의 2000년 Spin-off 과제에 의해서 수행되었습니다. 연구비 지원에 감사드립니다.

모델링 하여 학습시키는 알고리즘을 제안한다. 2장에서는 생체 면역계에서 항원 리셉터의 단백질 분자들의 유전자 재조합 방식과 그에 관련된 생체 면역계의 면역세포 생성원리에 대해서 설명하며, 3장에서는 이를 모델링한 침입탐지 학습알고리즘에 관해 다룰 것이다. 마지막으로 시뮬레이션을 이용한 침입탐지 학습알고리즘의 유효성을 확인한다.

2. 생체 면역계

2.1 NIS(Natural Immune System)

생명체의 방어체계인 면역계는 박테리아, 기생균, 병원균, 독소, 바이러스 등과 같이 항원이라고 통칭하는 매우 다양한 외부유기체나 단백질에 대하여 생명체의 세포와 장기를 방어할 수 있는 매우 정교하고 복잡한 시스템이며 개체를 건전한 상태로 유지시키기 위해 반드시 필요한 기능이다. 또한 면역계는 virus 감염과 종양발생에 의해 변이한 자기세포를 배제하는 작용도 가지고 있다. 이러한 생명체의 면역계는 중앙 처리 장치인 뇌의 명령에 따르는 것이 아닌 각 요소의 자율적인 행동이 유기적으로 결합되어 형성된 자율분산시스템으로 항원을 인식하는 기능, 정보처리 기능, 학습 및 기억능력, 자기와 비자기의 구별능력, 분산시스템으로서 전체의 조화를 유지하는 능력 등을 가지고 있다.

2.2 면역세포 형성 원리

NIS에서 가장 중요한 역할을 하는 면역 세포가 외부에서 침입한 항원을 제거하는 면역 반응을 정상적으로 수행하기 위해서 각각의 면역 세포들은 2가지의 요소에 의존하게 된다. 하나는 각각의 세포 사이의 협력과 공조이다. 또 다른 하나는 항원의 인지 능력과 구별 능력이다. 면역 세포의 항원을 인지하는 능력은 자기 세포와 구별되는 항원을 구별하고 이의 항원결정소의 특성을 가지고 있는 면역 세포를 통해 항원을 제거하는 면역 반응을 일으키는 가장 중요한 능력인 것이다. MHC 단백질은 세포의 개인적인 특징을 나타내며 이것을 인식하는 부분이 T세포의 항원 수용체에 의해 부정 선택되어야 한다. 항원 수용체는 T 세포가 생성될 때 유전자 분자들인 다양한 종류의 리셉터 단백질 분자(α, β, γ, δ사슬)들이 돌연변이 및 교차를 통해 다양성을 확보한다. 자기를 판별해주는 MHC 단백질을 인식하는 부분과 항원의 종류를 판별하는 항원 수용체의 특성을 지니는 대표적인 면역 세포는 세포독성 T세포이다. 세포독성 T세포는 항원에 감염된 자기 세포를 제거하는 역할로 먼저 자기 세포인지를 판별하고 자기 세포에 항원이 존재하는가를 검사하므로 이 두 가지의 인식부를 모두 가지고 있다. 이러한 T세포의 인식부를 T세포 수용체(T-cell receptor, TcR)라고 한다[5]. T세포 수용체가 면역계에서 정상적으로 동작되지 않으면 자기 세포를 항원으로 인식하게 되어 공격하게 된다. 따라서 면역계는 면역 세포 초기 생성시 MHC 인식부와 항원 수용체의 정상적인 동작여부를 확인하면서 면역 세포를 생성하여 면역계를 구성한다. 수용체의 정상적인 동작여부를 가리는 방법으로 사용되는 것이 흉선에서 이루어지는 선택 방법들인 긍정 선택과 부정 선택법이다[5].

부정선택법은 항원의 인식에 있어서 자기 세포를 항원으로 인식하는 것을 배제하기 위한 방법이다. 항원수용체가 MHC 단백질을 항원으로 인식하면 모든 자기 세포를 항원으로 인식하게 된다. 때문에 항원으로 MHC 단백질을 인식하지 못하게 하기 위해 면역세포에 MHC 단백질을 결합시켰을 때 항원수용체가 부정적인 선택을 하는 세포만으로 구성된다. 이때 긍정적인 선택을 하는 면역세포는 MHC 단백질을 항원으로 인식하는 세포들이므로 죽이거나 다시 항원 수용체를 형성하는 단계를 거치게 된다. 이에 반해 긍정 선택법은 각 면역세포의 MHC 단백질의 인식기능을 확인하는 선택 방법이다.

이 두 가지 선택을 거친 면역세포는 MHC 단백질을 자신으로 인식하면서 이를 항원으로 인식하지 못하게 구성되어 생명체에서 정상적인 면역반응을 형성한다.

3. 부정선택을 기반한 학습알고리즘

3.1 부정 선택 알고리즘

흉선에서 T세포를 생성하는 것과 유사하게, 디텍터 스트링들은 랜덤하게 생성될 수 있다. 보호되어야 할 자기 스트링들과 매칭 되는 것들은 제거 된다. 어떤 자기 스트링들과 매칭 되는데 실패한 것들로만 디텍터 집합, R을 구성한다. 이때 사용되는 선택 방법이 부정 선택이다. 이 과정은 요구되는 방어 수준에 이를 때까지 계속된다.

그 과정은 우선 랜덤하게 생성된 스트링, R_0 를 이미 설정해 두었던 자기 스트링, S와 매칭을 시킨다. 이때 자기 스트링과 패턴이 같다고 판단되었을 경우에는 reject시키고 그렇지 않고 새로운 패턴일 경우에만 accept를 시킨 후, 기존의 디텍터, R을 갱신하는 데 사용된다. 그림 2에서, 부정 선택을 이용하여 S와 다른 스트링을 디텍터 집합으로 설정하게 되는 것이다. 이는 특정 징후에 의해 선택하는 긍정 선택과는 다르게 변이된 스트링에 대해서 탐지를 하기 위한 방식이다. 부정 선택을 이용하는 알고리즘은 그 생성과정이 긍정 선택의 방식 중 선택방법이 반전된 알고리즘이다. 즉, 자기 data와

매칭 되지 않은 데이터 집합으로 negative detector(ND)를 구성하여 침입의 시도를 탐지하는 것이다.

3.2 학습 알고리즘

T 세포의 항원 수용체 부분의 유전자 단백질 분자인 α, β, γ, δ사슬들은 각각의 유전자 재조합으로 구성된다. 이들의 역할은 다양한 외부의 병원균으로부터 자신을 보호하기 위해 항체를 생성하는 것이다. 그러나, 초기에는 그 수가 적지만 항원과 반응하기위해서 리셉터 유전자 분자인 네 가지 사슬들의 조합으로 다양하면서도 강력한 항체분자들을 생성할 수 있는 것이다. 이러한 기능을 모델링하여 외부의 침입을 탐지할 수 있는 디텍터들을 생성하여 학습시키는 알고리즘이다. 초기화된 디텍터들은 위에 언급한 부정 선택 알고리즘에 의해 선택되어진다. 그 후 일정한 매칭 평가를 거친 후 선택되어진 디텍터에 한해서 일정한 변이율에 의해서 변이(mutation)가 이루어진다. 우수한 디텍터의 보존을 위해서 선택 방식은 엘리트 선택과 순위 선택법을 이용하였다. 상위 절반에 해당되는 디텍터들은 변이가 이루어지고 이를 재 선택하여 평가하는 방식으로 학습알고리즘은 이루어진다. 다음은 부정선택에 기반 한 학습알고리즘이다.

Initialize (detector);
{
  pattern matching detector with compare_string
  for(i=0; i<detector_number; i++)
   if (NO)
    the detector survived
    (YES)
    the detector is eliminated
}
Evaluation (detector);
{
  Initialized detectors is matched with attack_string
  for(i=0; i<detector_number; i++)
  first step:
  Hamming Distance is evaluated between detectors and attack_string. The first value of evaluation is H.D.
  second step:
  Specific bits of attack_string is matched with that of detector. Also the count of matched specific bits is second value of evaluation.
  third step:
  Finally, the two value is summed. The value is to be a fitness value.
}
Selection (detector); elite observation method, ranking selection method are used.
Mutation (detector); mutation rate = 0.05

4. Experiment

위의 알고리즘을 토대로 다음과 같은 조건으로 시뮬레이션을 하였다. 초기 디텍터의 수는 100개이고, 이에 침입 탐지대상인 공격유형의 개수는 1,000개이다. 이를 0.05의 변이율을 적용하여 200세대까지 진화시킨 결과 다음과 같은 적합도의 추이를 보여주었다.

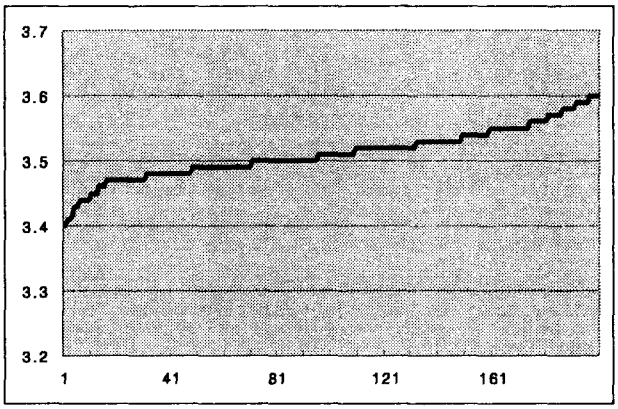

그림 1. 평균적합도

Fig. 1 Average Fitness

위의 결과를 토대로,. 침입의 유형을 정해진 환경이라고 한다면, 이를 탐지하는 디텍터의 환경에 대한 학습이 이루어졌음을 알 수 있었다. 다만, 한 개체의 최대 적합도가 8임을 감안한다면 다소 수렴정도가 적음을 보였다. 이는 향후 학습율을 높이기 위한 연구가 필요하다 하겠다.

5. 결 론

생체 면역계는 구조적으로 자율 분산 시스템이며, 각각의 독립된 면역 세포들 간의 유기적인 협조를 통해서 외부의 공격으로부터 자신을 방어한다. 특히 2차 방어를 하기 위해서 학습과 기억이라는 메커니즘이 동원된다. 학습이라는 메커니즘은 기존의 공격에 대해 유전자의 조합을 통해 이루어지며 학습된 데이터는 기억세포를 이용하여 따로 저장하게 되는 것이다. 이에 본 논문에서는 생체 면역계의 면역 세포를 모델링 함으로써 컴퓨터 환경에서 발생된 침입시도에 대해서 대처하는 학습 알고리즘을 제안하였다. T세포의 생성과정인 부정 선택을 기반 하여 선택된 디텍터들은 이후 학습알고리즘을 거치게 되어 정상적인 접근에 대한 인식과정은 물론 비정상적인 침입에 대해서도 인식과정을 거치기 때문에 침입 탐지의 신뢰도를 향상시킨다.

참고문헌

[1] Computer Emergency Response Team, "TCP SYN Flooding and IP Spoofing Attacks", *CERT Advisory: CA*, pp. 96-21, 1996.
[2] S.Y. Lee and Y.S. Kim, "A RTSD Mechanism for

Detection of DoS Attack on TCP Network," Proceedings of KFIS 2002 Spring Conference, pp. 252-255, 2002.

[3] P.D' haeseleer, S, Forrest, and P. Helman. "An immunological approach to change detection: Algorithms, analysis and implication," *Proceeding of the 1996 IEEE Symposium on Research in Security and Privacy*, Los Alami. 1996.

[4] A. Somayaji, S. Hofmeyr, and S. Forrest, "Principles of a Computer Immune System," *New Security Paradigms Workshop*, pp. 75-82, 1998.

[5] 황상익, *면역의 의미론*, 한울과학문고, 1998.

[6] J. B. Gu, D. W. Lee, K. B. Sim, and S. H. Park, "An Immunity-based Security Layer against Internet Antigens," *Transactions on IEICE*, vol. E83-B, no.11, pp. 2570-2575, 2000.

[7] D. Dasgupta, and S. Forrest, " An Anomaly Detection Algorithm Inspired by the Immune Systems and Their Applications," *Springer*, pp. 262-276, 1999.