중앙 집중형 망에서 인공면역체계 기반의 적응적 망 이상 상태 탐지 모델 설계

정회원 유 경 민*, 양 원 혁*, 이 상 열*, 정 혜 련*, 종신회원 소 원 호**, 김 영 천*°

An Adaptive Anomaly Detection Model Design based on Artificial Immune System in Central Network

Kyoung-Min Yoo*, Won-Hyuk Yang*, Sang-Yeol Lee*, Hye-Ryun Jeong* ***Regular Members***,
Won-ho So**, Young-Chon Kim*° ***Lifelong Members***

요 약

기존의 망 이상 상태 탐지 시스템들은 주로 정상 상태의 시스템 사용률 등과 같은 통계 값으로 결정된 임계값을 기반으로 탐지하기 때문에 이상 상태임에도 불구하고 정상 상태와 비슷한 시스템 통계 값을 가지면 탐지하지 못하는 문제점이 있다. 이러한 단점들을 해결하기 위하여 본 논문에서는 인간면역체계의 학습, 적응, 기억 능력 등의 특성을 이용하는 인공면역체계 기반의 적응적 망 이상 상태 탐지 모델을 제안한다. 이를 위하여 인간면역 시스템의 수지상 세포 (Dendritic Cell)와 T 세포 사이의 상호 작용을 이용한 탐지 모델을 설계하고 각 구성 요소 및 기능을 정의한다. 중앙 집중 제어 노드는 각 라우터 노드로부터 전달받은 정보를 분석하여 대응 방법을 해당 라우터들에게 전달한다. 또한 라우터 노드는 학습을 통해 얻어진 데이터를 기반으로 이상 상태를 탐지할 뿐만 아니라 중앙 집중 제어 노드로부터 전달받은 정보를 이용하여 이상 상태를 처리한다. 최종적으로 제안된 이상 상태 탐지 모델의 타당성을 검증하기 위하여 구성 모듈을 설계하고 flooding 공격에 대한 시뮬레이션을 수행한다.

Key Words : central network; anomaly detection; artificial immune system.

ABSTRACT

The traditional network anomaly detection systems execute the threshold-based detection without considering d ynamic network environments, which causes false positive and limits an effective resource utilization. To overco me the drawbacks, we present the adaptive network anomaly detection model based on artificial immune system (AIS) in centralized network. AIS is inspired from human immune system that has learning, adaptation and mem ory. In our proposed model, the interaction between dendritic cell and T-cell of human immune system is adopte d. We design the main components, such as central node and router node, and define functions of them. The ce ntral node analyzes the anomaly information received from the related router nodes, decides response policy and sends the policy to corresponding nodes. The router node consists of detector module and responder module. The detector module perceives the anomaly depending on learning data and the responder module settles the anomaly according to the policy received from central node. Finally we evaluate the possibility of the proposed detection model through simulation.

* 전북대학교 컴퓨터공학과 차세대통신망 연구실(mini0729@chonbuk.ac.kr), ° : 교신저자(yckim@chonbuk.ac.kr), 전북대학교 영상정보신기술연구소
** 순천대학교 컴퓨터교육과
논문번호 : KICS2008-08-377, 접수일자 : 2008년 8월 31일, 최종논문접수일자 : 2009년 3월 5일

Ⅰ. 서 론

최근 서비스 거부 공격과 같은 네트워크 공격과 바이러스 프로그램 등의 확산으로 인하여 경제적 손실까지 발생하고 있다. 그러나 기존의 Firewall이나 침입 탐지 시스템들은 알려진 공격의 증거에 대해서만 탐지 가능하고 정해진 대응 방법만을 이용하기 때문에 새로운 형태의 네트워크 공격 발생 시에는 탐지하지 못하는 문제점이 있다.

또한 기존의 망 이상 상태 탐지 기법들은 주로 미리 정해진 매개 변수들의 통계 값을 기반으로 임계값을 정하여 망의 이상 상태 여부를 판단하기 때문에 알려지지 않은 이상 상태도 탐지할 수 있다. 그러나 감시되는 시스템 변수에 따라 정상 상태임에도 불구하고 이상 상태로 오인되는 false positive 발생이 높은 단점이 있다. 이는 실제 네트워크 상태의 동적 변화로 인하여 정상 상태와 이상 상태의 구분이 모호한 상태가 종종 발생한다는 점을 고려하지 않았기 때문이다.

따라서 알려지지 않은 이상 상태를 탐지할 수 있을 뿐만 아니라 오탐지율을 줄이기 위하여 최근 학습, 적응, 기억 능력 등의 특징을 가지는 인공면역체계 기반의 이상 상태 탐지 기법들이 연구되고 있다[2],[3]. 처음으로 인공면역체계 기반의 협응적 이상 상태 탐지 알고리즘이 [3]에서 제안되었으나 네트워크 공격과 같은 이상 상태 발생 시에 확산 정도를 파악하기 어렵고 대응이 느린 단점이 있다. 특히 서비스 거부 공격과 같은 망 공격이나 망 혼잡, 과다 CPU 사용률 등 망 이상 상태 발생 시에는 확산을 막는 것이 중요한데 이를 위해서는 여러 노드들의 정보를 종합하여 판단을 내리는 중앙 집중형 제어 구조가 적합하다. 이처럼 최근 제시되고 있는 차세대 통신망(NGN, BCN)들은 안정성, 안전성 그리고 QoS 을 효과적으로 제공하기 위해서 중앙 집중형 제어 기술을 채택하고 있는 실정이다[1]. 한편 [4]에서 인공면역체계를 이용한 중앙 집중형 이상 상태 탐지 구조가 제시되었으나 임계값 기반으로 이상 상태를 결정하기 때문에 false positive가 많이 발생하는 문제점을 갖는다.

본 논문에서는 중앙 집중형 망에서 망의 트래픽 변화에 적응적으로 이상 상태를 탐지할 뿐만 아니라 이상 상태의 확산을 초기에 차단하여 망 자원의 효율성을 높일 수 있도록 인공면역체계 기반의 망 이상 상태 탐지 모델을 제시하고 성능 평가를 통해 타당성을 검증하고자 한다. 제안하는 모델은 인간면역 시스템의 수지상 세포 (Dendritic Cell)와 T 세포 사이의 상호 작용을 이용하여 이상 상태를 탐지하고 망 이상 상태에 따른 대응 방법을 결정하도록 한다. 이에 따라 중앙 집중 제어 노드는 각 라우터 노드로부터 전달받은 정보를 종합하여 대응 방법을 해당 라우터들에게 전달한다. 또한 모든 라우터 노드는 학습을 통해 얻어진 데이터를 기반으로 이상 상태를 탐지하고 중앙 집중 제어 노드로부터 전달받은 정보를 이용하여 새로운 형태의 이상 상태에도 대응할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 본 논문에서 적용하고자 하는 인간면역시스템의 항원 인식 및 면역 반응 활성화 과정에 대해 기술한다. 3장에서는 중앙 집중형 망을 위한 인공면역체계 기반의 망 이상 상태 탐지 시스템을 설계하고 각 구성 요소의 기능을 정의한다. 4장에서는 제안된 모델을 이용하여 Flooding 공격에 대한 시뮬레이션 결과를 보인다. 마지막으로 5장에서 본 논문의 결론을 맺고 향후 연구에 대하여 다룬다.

Ⅱ. 관련 연구

인간면역체계는 특정 조직, 기관, 세포나 화학 물질 등의 복잡한 네트워크로 구성되며 외부 병원체를 인식하고 이를 무력화시키거나 제거하는 기능을 가지고 있다.

일반적으로 특별한 면역반응을 일으키는 물질을 항원이라고 하며 효과적인 방어 체계를 구축하기 위해서 면역 시스템은 오직 외부 항원에만 반응해야 한다[2]. 즉, 자기(self) 세포에 해당하지 않는 항원의 구별이 필수적인 특성인데 그림 1은 면역 세포인 T 세포와 B 세포가 항원을 인식하고 면역반응을 일으키는 과정을 보인다. (II)단계는 (I)단계에서 침입한 항원에 대해 수지상 세포 (Dendritic cell)와 같은 항원 제시 세포 (Antigen Presenting Cell: APC)가 항원을 섭취하는 것을 보여준다. 그림에서 보는 바와 같이 항원은 펩타이드 조각들로 이루어져 있고 이러한 펩타이드 조각은 MHC (Major Histo-compatibility Complex) 분자와 반응하여 APC의 표면에 MHC/펩타이드 복합체로 나타난다. (III)단계에서는 이러한 복합체를 인식할 수 있는 수용체를 가진 T 세포가 복합체를 인식하고 (IV) 단계에서는 활성화된 T 세포가 림포카인을 분비함으로써 면역 시스템을 작동시키며 B 세포도 활성화시키는 과정이다[4]. B 세포는 MHC 분자의 도움 없이도 항원을 인식할 수 있는 수용체를 가지고 있기 때문에 (V)단계에서 보는 바와 같이 수용체를 이용하여 특정 항원에 직접 반

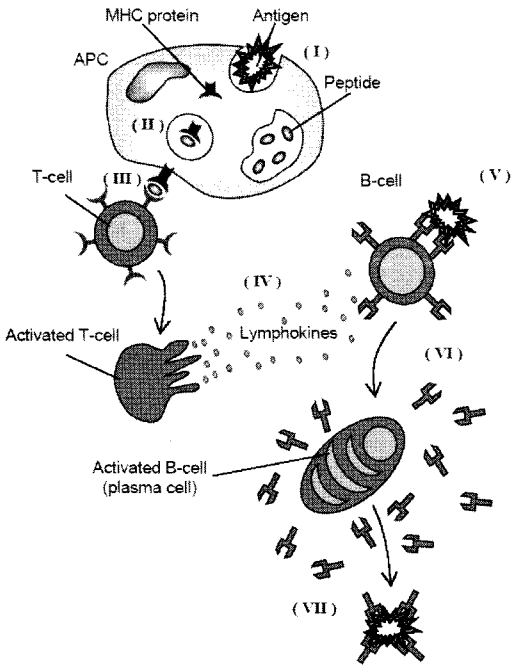


그림 1. 항원 인식 및 면역 세포 활성화 과정

응한다. 항원 결합 반응이 일어나면 B 세포는 활성화되어 급격히 증식하게 되고 증식된 다량의 개체는 항체를 생성한다. 결국 (VI)단계에서 분비된 항체들이 (VII)에서 항원을 파괴하게 된다.

특히 T 세포의 면역 반응 과정은 다음과 같다. (II)단계에서 보는 바와 같이 T 세포의 항원 인식은 T 세포 표면에 있는 항원 수용체를 통하여 이루어지는 데, 이러한 T 세포 표면의 항원 수용체를 T 세포 수용체 (T cell receptor: TCR)이라고 부른다. 말초 혈액의 성숙된 T 세포가 MHC와 항원의 복합체를 인식하게 되면, 그 T 세포는 증식 (proliferation)과 분화 (differentiation)가 시작되어, 특정한 T 세포의 수가 늘어난다. 이와 같이 활성화된 T 세포가 보조 T 세포(Helper T-cell)이면 면역 반응을 촉진시키게 되고, 세포 독성 T 세포(Cytotoxic T-cell; CTL)이면 표적 세포 살해와 같은 세포 면역 반응이 나타난다. 본 논문에서는 앞서 언급한 수지상 세포의 항원 제시 과정과 이에 따른 T 세포의 면역 반응 과정을 망 이상 상태 탐지 시스템 설계에 적용한다.

Ⅲ. 인공면역체계 기반의 이상 상태 탐지 모델 설계

인공면역체계는 인간면역체계의 주요 특성을 복잡한 공학적 문제, 분류 작업, 그리고 최적화 처리

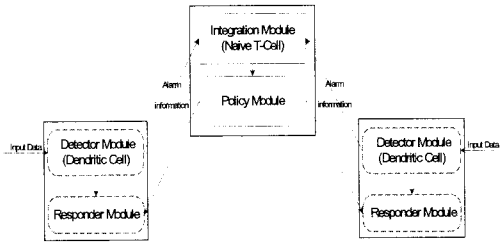


그림 2. 제안한 AIS 기반 망 이상 상태 탐지 시스템

등에 적용하는데 그 목적이 있다. 이에 따라 인간면역체계의 긍정/부정 선택과 복제 선택 등을 이용하여 침입 탐지, 이상 상태 감지 그리고 고장 감내 등 다양한 분야에 적용되고 있다.

본 논문에서 제안하는 인공면역체계 기반 망 이상 상태 탐지 모델은 그림 2와 같이 중앙 집중 제어 노드와 라우터 노드들이 유기적인 관계를 맺으며 망 이상 상태에 대응하도록 설계되었다. 여기서는 소단원에 관한 내용을 간단히 살펴본다. 여기서는 소단원에 관한 내용을 간단히 살펴본다.

3.1 중앙 집중 제어 노드

중앙 집중 제어 노드는 그림 3에서 보는 바와 같이 Integration 모듈과 Policy 모듈로 구성된다.

Integration 모듈은 여러 라우터들로부터 수신한 이상 상태 정보들을 통합하여 이상 상태의 심각성 및 확산 정도를 판단할 수 있도록 Policy 모듈에 전달하는 역할을 수행한다.

Policy 모듈은 CTL, Th1 Cell, Th2 Cell 모듈로 구성된다. Th1 Cell 모듈은 일정 시간동안 여러 라우터들로부터 발생한 경고 신호들을 감시하여 이상 상태의 확산 정도를 판별하기 위한 모듈이다. CTL 모듈은 Th1 Cell 모듈에서의 모니터링 결과 이상 상태가 여러 라우터로 확산되었다고 판별되었을 때 각 라우터의 CTL 모듈에게 이상 상태에 있는 라우터 정보를 전달함으로써 각 라우터들이 해당 라우터에 데이터를 전송하지 않도록 한다. Th2 Cell 모듈은 하나의

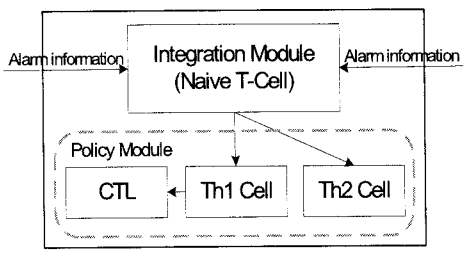


그림 3. 중앙 집중 제어 노드 구성도

라우터에서만 경고 신호가 발생하는 경우로 그 심각성이 높다고 판단되는 경우 다른 라우터들에게도 해당 라우터의 정보를 전송하여 이상 상태가 발생한 라우터에게 데이터 전송률을 줄이도록 요청한다.

3.2 라우터 노드

각 라우터 노드는 그림 4와 같이 Detector 모듈과 Responder 모듈로 구성된다. Detector 모듈은 입력 데이터를 분석하는 Antigen 모듈과 이상 상태를 검출하고 관련 정보를 집중 제어 노드에 전달하는 Alarm Signal 모듈로 구성된다.

먼저 Antigen 모듈에서는 입력 트래픽의 특성을 추출하는 기능을 수행하는데 미리 정해진 트래픽 파라미터 값들을 계산하여 Alarm Signal 모듈에 전송한다. Alarm Signal 모듈은 미리 생성된 검출기 집합(detector set)과 Antigen 모듈로부터 수신한 트래픽 파라미터 값을 비교하여 경고 신호 발생 여부를 결정한다.

네트워크 이상상태를 탐지하기 위한 검출기 집합은 그림 5와 같이 인간면역체계에서 비자기 세포 식별의 기본이 되는 부정 선택 원리를 이용하여 생성한다. 이 때 정상 상태 데이터 집합과 무작위로 발생된 상태 데이터를 비교하여 서로 일치하지 않는 경우에만 검출기 집합에 추가하기 때문에 검출

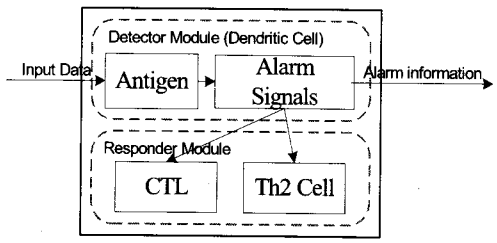


그림 4. 라우터 노드 구성도

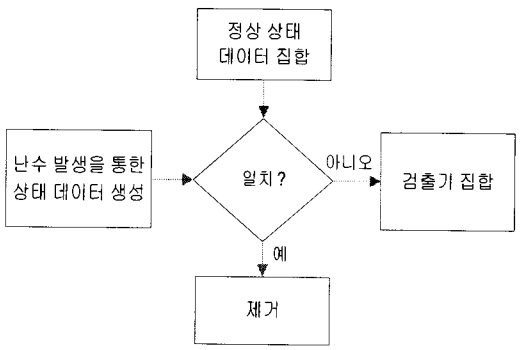


그림 5. 부정 선택 기반의 검출기 집합 생성 과정

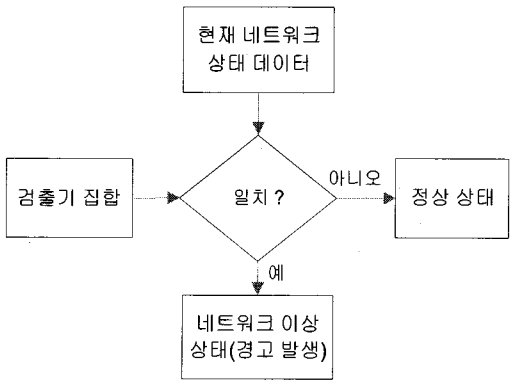


그림 6. 검출기 집합과 비교를 통한 네트워크 경고 발생

기 집합은 이상 상태 데이터들로 이루어진다. 최근 다양한 네트워크 공격 발생과 동적인 네트워크 상태의 변화로 인해 주기적인 정상 상태 데이터의 갱신을 통한 검출기 집합의 갱신이 요구된다.

각 라우터의 Alarm Signal 모듈에서는 이렇게 생성된 검출기 집합과 망의 상태를 비교하여 서로 일치하는 경우 이상 상태를 알리는 경고를 발생시킨다. 이때 검출기 집합은 이상 상태 데이터로 구성되어 있기 때문에 정상 상태를 이상 상태로 잘못 인식하는 false positive 발생이 적은 장점을 가진다. 망의 이상 상태 탐지에 따른 경고 신호 발생 과정은 다음 그림 6과 같다.

각 라우터 노드는 경고 신호가 발생하는 경우 경고 신호와 관련된 라우터 정보를 집중 제어 노드의 Integration 모듈과 자신의 Responder 모듈에 각각 전송한다.

Responder 모듈은 Detector 모듈로부터 전달받은 이상 상태 정보와 중앙 집중 제어 노드의 Policy 모듈로부터 전달받은 네트워크 제어 정보를 기반으로 망의 공격 상태 제거나 패킷 유입량 조절 등을 수행하는 역할을 한다. Responder 모듈은 CTL 모듈과 Th2 Cell 모듈로 구성되는데 자신의 노드에서 발생하는 경고 신호의 심각성을 판별하고 심각성이 높은 경우 CTL 모듈에서 즉각 대응한 후 집중 제어 노드의 제어 정보를 기다린다. 심각성이 낮은 경우에는 Th2 Cell 모듈에서 집중 제어 노드의 제어 정보에 따라 데이터 전송률을 조절한다. CTL 모듈과 Th2 Cell 모듈 모두 집중 제어 노드의 제어 정보를 기다리는 이유는 이상 상태의 발생이 단일 노드에서 발생한 상황인지 여러 노드에서 동시에 발생하는 상황인지를 판별함으로써 분산 공격 등을 판단하여 이상 상태의 확산을 미리 막기 위해서이다.

Ⅳ. 시뮬레이션 및 성능 평가

제안한 탐지 시스템에서 이상 상태를 탐지할 수 있도록 각 라우터 노드의 검출기 모듈(Detector Module)을 다음과 같이 설계하여 시뮬레이션을 수행하였다.

4.1 Antigen 모듈 설계

먼저 Antigen 모듈의 기능인 입력 트래픽 특성 추출을 위해 네트워크 상태를 특징지을 수 있는 파라미터를 정의하기 위한 실험을 수행하였다.

이를 위하여 flooding 공격으로 인한 네트워크 이상 상태를 가정하고 OPNET 시뮬레이터를 이용하여 트래픽 발생 모델을 설계하였다. 설계한 모델을 이용하여 1,000초 동안 트래픽을 발생시켰으며 61~120, 221~460, 561~620, 721~960초 사이에 총 600초 동안 flooding 공격을 수행하였다. 트래픽 발생 결과 버퍼 상태 변화는 그림 7과 같은 결과를 보여 버퍼 상태를 이용하여 네트워크 이상 상태를 확인할 수 있음을 확인하였다.

또한 망의 정상 상태의 특성을 보다 정확히 추출하기 위하여 다양한 버퍼 상태의 통계 정보(평균, 분산, 표준편차 등)를 분석한 결과 버퍼의 평균 상태 및 변화율(표준편차)과 패킷 손실률이 상태를 특징짓기에 적합함을 확인하였다[5].

따라서 본 논문에서는 정상 상태와 이상 상태를 특징지을 수 있는 매개변수로 버퍼의 '패킷 손실률'과 '평균+2*평균의 표준편차' 값을 이용하였으며 그림 8과 9에서와 같이 정상 상태와 이상 상태에 따라 큰 차이가 확인되었다. 참고로 표현을 단순화하기 위하여 버퍼 상태는 제한된 크기의 버퍼 점유율을 기반으로 정규화하여 계산하였다. 즉, 버퍼를 10개의 구역으로 나누어 해당 구역에 해당하는 인덱스 값을 이용하는 것으로, 만일 10 Bits 크기의 버퍼를 이용한다면, 버퍼의 80~90% 상태가 점유되어 있을 때의 버퍼 상태 값은 8로 설정하였다.

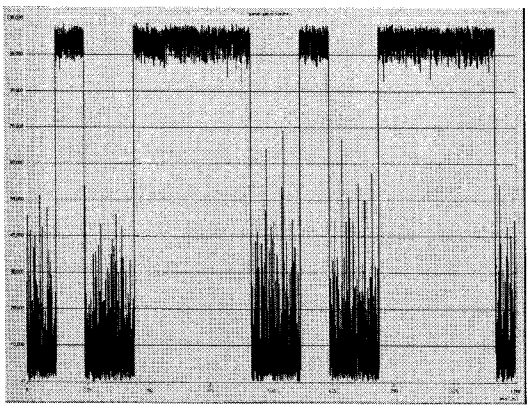


그림 7. Flooding 공격 발생 시 버퍼 상태 변화

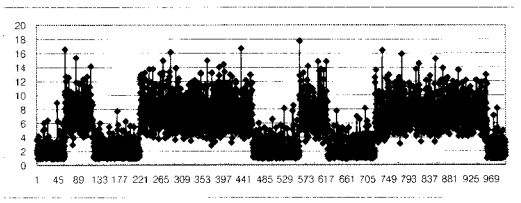


그림 8. 공격 발생 시 "평균+2*평균의 표준편차" 변화

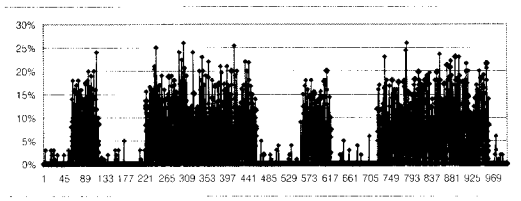


그림 9. 공격 발생 시 패킷 손실률 변화

결과적으로 Antigen 모듈은 주기적으로 버퍼의 '패킷 손실률'과 '평균+2*평균의 표준편차' 값을 계산하여 Alarm Signal 모듈에 전송한다.

4.2 부정 선택 기반의 검출기 집합 생성

Alarm signal 모듈에서 네트워크 이상 상태 탐지를 위해서는 이상 상태 후보 데이터들로 구성된 검출기 집합을 유지해야 한다. 이를 위하여 본 논문에서는 self 데이터나 비정상 상태의 데이터를 표현하는 방법으로 2차원 공간을 이용하는 Real-valued 방법을 선택하고 부정 선택 기반의 검출기 집합을 생성하였으며 그 과정은 다음과 같다.

먼저 정상 상태의 self 데이터를 수집하기 위하여 3,000초 동안 정상 트래픽을 발생시켰다. 주기를 1초로 앞서 파라미터로 결정된 버퍼의 '패킷 손실률'과 '평균+2*평균의 표준편차'를 분석하였으며 이렇게 발생된 self 데이터는 두 가지 유전자의 순서쌍으로 표현되어진다. 따라서 Self 집합, S는 다음 식 (1)과 같이 정의된다.

$$S=\{S_1, S_2, \cdots, S_n\} \quad S_i=(Gene1, Gene2) \qquad (1)$$

여기서 self 데이터 집합은 2차원 공간에 표시되어질 수 있으며 Gene1과 Gene 2는 각각 버퍼의 '패킷 손실률'과 '평균+2*평균의 표준편차'를 의미한다.

다음으로 부정 선택 기반의 검출기 집합을 생성하

기 위해서는 앞서 생성된 self 데이터 집합과 무작위(Random)로 발생된 검출기 후보 데이터 사이의 매칭 검사가 이루어져야 한다.

본 논문에서는 두 데이터 간 Euclidean 거리를 계산하여 매칭 여부를 결정하였으며 검출기 집합, Ag는 다음 식(2)과 같이 정의된다.

$$Ag = \{Ag_1, Ag_2, \cdots, Ag_n\} Ag_i = (Gene1, Gene2) \quad (2)$$

따라서 self 집합과 검출기 집합 원소 사이의 매칭 여부는 식(3)과 같은 Euclidean 거리 계산법으로 결정되는데 D의 값이 2 이상인 경우를 매칭이 되지 않는 것으로 결정하였다.

$$D = \sqrt{\sum_{i=1}^{2} (S_i - Ag_i)^2} \quad (3)$$

마지막으로 수집된 정상 상태 데이터 집합과 선택된 매칭 기법을 이용하여 그림 5에 제시된 알고리즘을 이용하여 부정 선택 기반 검출기 집합을 생성하였다. 검출기 생성 과정은 초기 검출기 집합 생성 과정과 학습 과정을 거친다. 초기 검출기 집합 생성 과정에서는 먼저 self 데이터 집합과 무작위(random)로 발생된 후보 데이터 사이의 매칭 검사를 수행한다. 매칭 검사 결과 self 데이터와 매칭되는 경우 검출기 후보 데이터는 정상 상태의 데이터와 동일한 것으로 간주되어 삭제되고, 매칭되지 않는 경우는 이상 상태 데이터로 간주되어 검출기 집합에 추가된다. 앞의 과정을 반복하여 수행하면 초기 검출기 집합이 생성된다.

한편, 제한된 self 데이터 집합으로 생성된 초기 검출기 집합은 정확성이 낮으므로 새로운 정상 데이터에 적용하는 학습 과정을 거침에 따라 보다 정확한 검출기 집합이 생성되도록 하였다.

4.3 Alarm Signal 모듈 설계

Alarm signal 모듈의 주요 기능은 Antigen 모듈에서 전달된 매개 변수들의 값들과 검출기 집합과의 비교를 통하여 검출기 집합과 일치하는 경우 이상 상태로 판단하고 경고 신호를 발생시키는 것이다.

본 논문에서는 일단 생성된 검출기의 성능 평가를 위하여 그림 7과 같은 형식으로 flooding 공격을 발생시키고 그림 6의 순서도에 따라 네트워크 이상 상태 탐지 여부를 평가하였다.

그림 10은 경고 발생 주기를 1초로 했을 때, 설계한 Alarm signal 모듈을 통하여 1,000초 동안 발생된 경고 신호들을 나타낸 그래프로 61~120, 221~460, 561~620, 721~960초에서 많은 경고 신호가 발생한 것을 확인할 수 있었다. 결과적으로 AIS 기반의 이상 상태 탐지 결과 flooding 공격 구간을 탐지할 수 있었으며 공격 상태가 아닌 시간에 경고를 발생하는 오탐지율이 0.5 %로 낮게 나타났다.

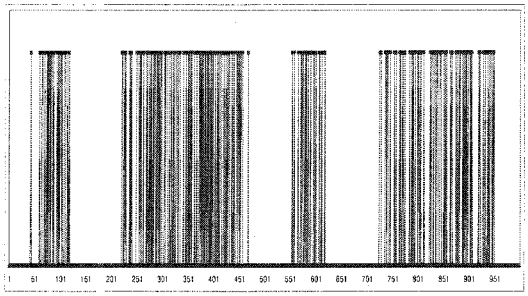


그림 10. 부정 선택 기반의 경고 발생 결과(경고 발생/초)

V. 결 론

최근 DDoS 공격과 같은 네트워크 공격이 증가하고 있고 망의 정상 상태와 이상 상태의 구분이 모호한 경우가 많이 발생하고 있다. 이러한 네트워크 환경을 고려해 볼 때 호스트 기반의 이상 상태 탐지보다는 중앙 집중형 탐지 구조가 false positive를 줄일 수 있을 뿐만 아니라 망의 이상 상태의 확산을 초기에 막을 수 있는 장점을 가진다.

본 논문에서는 중앙 집중형 망에서 인공면역체계 기반의 망 이상 상태 탐지 모델을 제안하고 각 구성 요소들의 기능을 정의하였다. 또한 Detector 모듈의 Antigen 모듈과 Alarm Signal 모듈을 설계하고 시뮬레이션을 수행하였다. 본 논문에서는 오탐지 감소를 위해 부정 선택 기반의 검출기 집합을 생성하였으며 flooding 공격 탐지를 통하여 검출기의 성능 평가를 수행하였다.

성능 평가 결과 flooding 공격 발생 구간을 탐지할 수 있었으며 낮은 오탐지율을 보였다. 한편 동적인 네트워크 상태로 인하여 정상 상태와 이상 상태의 구분이 모호한 경우가 발생하기 때문에 공격 발생 구간 중에 이상 상태를 정상 상태로 오인하는 false negative가 발생함을 알 수 있었다. 향후 이를 보완하기 위하여 Alarm signal 모듈에서 검출기 집합과의 부합 여부를 판단할 뿐만 아니라 퍼지 이론 등을 이용한 이상 상태 심각도 계산을 통하여 false negative를 낮추기 위한 연구가 필요하다.

참 고 문 헌

[1] 김영선, "BcN의 기술적 이슈와 전망," *한국정보통신기술협회*, 2005.

[2] F. Gonzalez, "A Study of Artificial Immune Systems Applied to Anomaly Detection," *Dissertation for Ph. D degree*, 2003.

[3] J. Kim, W. O. Wilson, U. Aickelin, and J. McLeod, "Cooperative Automated Worm Response and Detection ImmuNe Algorithm (CARDINAL) Inspired by T-Cell Immunity and Tolerance," *LNCS 3627*, pp. 168-181, 2005.

[4] K. Luther, R. Bye, T. Alpcan, A. Muller and S. Albayrak, "A Cooperative AIS Framework for Intrusion Detection," *In Proceeding of ICC '07*, pp.1409-1416, June 2007.

[5] 하기룡, 이도헌, "인공면역체계와 기계학습," *정보과학회지*, 제25권 제 3호, pp. 76-82, 2007.

[6] Fabricio Sergio de Paulo and Paulo Licio de Geus, "Attack Evidence Detection, Recovery, and Signature Extraction with ADENOIDS," ICT 2004, *LNCS 3124*, pp. 1083-1092, 2004.

[7] M. S. Abadeh, J. Habibi, M. Daneshi, M. Jalali and M. Khezrzadeh, "Intrusion Detection using a Hybridization of Evolutionary Fuzzy Systems and Artificial Immune Systems," *In the Proceeding of CEC 2007*, pp. 3547-3553, Sept. 2007.

유 경 민 (Kyoung-min Yoo) 정회원

한국통신학회 논문지 제33권 제3호 참조

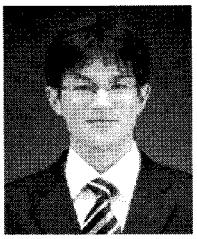
현재 전북대학교 컴퓨터공학과 박사과정

양 원 혁 (Won-Hyuk Yang) 정회원

한국통신학회 논문지 제33권 제8호 참조

현재 전북대학교 컴퓨터공학과 박사과정

이 상 열 (Sang-Yeol Lee) 정회원



2007년 2월 전북대학교 컴퓨터공학과 졸업

2007년 3월~현재 전북대학교 컴퓨터공학과 석사과정

<관심분야> 광통신, 인공면역체계 기반 망 제어

정 혜 련 (Hye-Ryun Jeong) 정회원

1996년 2월 전북대학교 산업기술대학원 졸업 공학석사

1999년 3월~현재 전북대학교 컴퓨터공학과 박사과정

소 원 호 (Won-ho So) 종신회원

한국통신학회 논문지 제29권 제9B호 참조

현재 순천대학교 컴퓨터교육과 조교수

김 영 천 (Young-Chon Kim) 종신회원

한국통신학회 논문지 제19권 제2호 참조

현재 전북대학교 전자정보공학부 교수