●5주차(20170326-20170331)

-Adaboost algorithm이 machine learning 에서 어떤 방향으로 활용될 수 있는지에 대해서 알아보았다.

-WSN에서 사용되는 IDS에 대해서 조사해 본다. IDS에서 보편적으로 Adaboost 알고리즘이 사용된다.

-Wireless Sensor Networks(WSN)는 다양한 Sensor Nodes(SNs)에서의 온도, 소리, 압력, 빛 등의 데이터 수집 및 기지국에서의 분석을 통해 환경이나 특정 영역을 monitoring 하는 데 사용된다. Wireless Sensor Networks(WSN)은 기본적으로 환경을 모니터링 하는 데 사용되는 작은 센서들인 수백 Sensor Nodes(SNs)로 구성되어 있다. 이러한 센서들의 장점은 가혹한 기후 조건이나 수중 감시 등 인간에 의한 감시가 불가능한 장소에 설치할 수 있다는 것이다. Wireless Sensor Networks(WSN)은 의료 및 지역 모니터링에서 환경 및 산업 모니터링 시스템에 이르기까지 다양한 분야에서 사용되고 있다.

효율적인 IDS는 침입 방지를 위한 의료 분야에서 제안되어왔다. 검색 방법론에 따라 IDS는 3가지 모델로 분류된다 : Anomaly based IDS, Signature based IDS and Hybrid based IDS.

이 중 Signature based IDS가 Adaboost Algorithm을 기반으로 사용하게 된다. Signature based IDS 또는 misuse based IDS는 다양한 규칙에서 작동되고, 새로운 정보 패킷과 미리 알려진 신호를 비교하여 침입을 탐지한다. Abraham et. al. 이 3 개의 fuzzy 규칙 기반 접근 방식을 비교했다. 하지만 이러한 방식들은 모두 클래스에 대해서 정확히 하나의 결과를 얻을 수 없었기 때문에 다른 분류자 조합인 새로운 모델을 제안했다. 제안된 heavy weight model은 모든 공격에 대해서 100%의 정확도를 얻을 수 있었고, light weight는 모든 공격에 대해서 최소 94%의 정확도를 얻을 수 있었다. Signature based matching을 기반으로 유명한 알고리즘은 Adaboost Algorithm이며, 이 알고리즘은 네트워크 기반 IDS에 포함되어 있다.

-Anomaly based IDS는 시스템 활동을 모니터링하고 정상 및 비정상 중 하나로 분류하여 네트워크 침입 및 컴퓨터 침입 및 오용 모두를 검출하기 위한 침입 탐지 시스템이다.

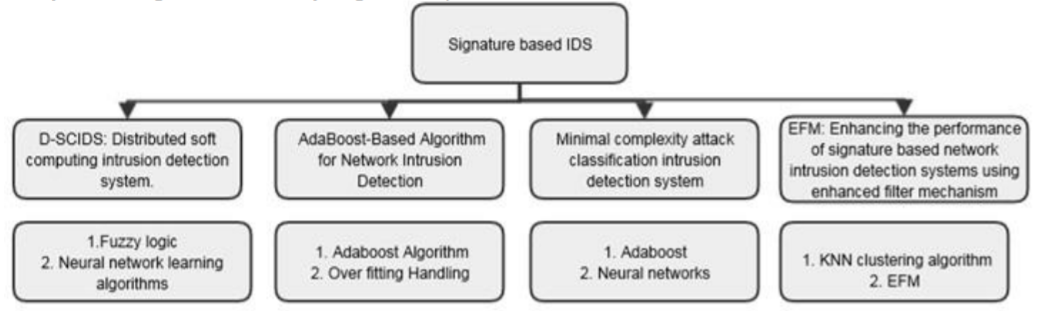
-Signature based IDS는 네트워크 트래픽의 바이트 순서나 악성코드가 사용하는 알려진 악의적인 명령 시퀀스 등 특정 패턴을 검색하여 공격을 탐지하는 것을 말한다. 이 용어는 signature라고 하는 검출된 패턴을 가리키는 anti-virus software에서 파생되었다. Signature based IDS는 알려진 공격을 쉽게 감지할 수 있지만, 어ᄄᅠᆫ 패턴도 사용할 수 없는 새로운 공격을 감지하는 것은 불가능하다.

그림 1. Signature based IDS