탐지 패킷 전송 방법에 따른 방화벽 정책 추론의 정확도 분석

김현우, 주홍택*
계명대학교 컴퓨터공학과
e-mail : {hwkim84, juht}@kmu.ac.kr

Analysis Correctness of Firewall Policy Inference According to Probing Packet Transmission Method

Hyeonwoo Kim, Hong-taek Ju
Dept. of Computer Engineering, Keimyung University

요 약

외부에서 특정 네트워크의 방화벽 정책을 추론하기 위해서는 Active Probing 을 이용한 탐지 패킷의 응답을 분석하여야 한다. 하지만, 외부에서 특정 네트워크로 탐지 패킷을 어떻게 전송하는가에 따라 방화벽에서 네트워크 공격으로 탐지되기 때문에 무분별하게 탐지 패킷을 전송하는 방법은 위험하다. 본 논문에서는 방화벽 장비가 Active Probing 을 이용한 방화벽 정책 추론 방법에 어떠한 영향을 주는지에 대해서 분석한다. 그리고 실제 방화벽 정책과 추론된 방화벽 정책을 비교하여 방화벽 정책 추론 방법의 정확성을 검증한다.

1. 서론

최근의 인터넷에는 스마트폰 또는 태블릿 등 인터넷에 쉽게 접속할 수 있는 장치가 발달하면서 인터넷 사용자가 폭발적으로 증가하고 있다. 이러한 추세로 인터넷 보안에 대한 중요성도 대두되고 있는 실정이다. 인터넷 보안의 취약점을 노리는 악의적인 공격자는 악성 트래픽을 이용하여 네트워크 공격을 유발함으로써 대상 네트워크가 정상적인 서비스를 제공할 수 없도록 만든다. 따라서 각 단체나 기관에서는 내부 호스트를 보호하기 위해 방화벽과 같은 보안 장비를 설치하여 외부의 공격에 대비한다.

방화벽은 일반적으로 네트워크 경계의 가장 앞 단에 배치되어 있다. 그래서 방화벽은 외부 또는 내부 네트워크로 향하는 모든 패킷을 검사하기 때문에 네트워크 보안 시스템 중에서 가장 기본이 되고 중요한 역할을 하는 보안 시스템이다. 방화벽을 통과하고자 하는 모든 패킷들은 방화벽 정책에 의해 통과되거나 차단된다[1]. 방화벽 정책은 다수 규칙들의 집합으로 구성되고, 각 규칙은 조건과 통과여부로 구성된다. 각 규칙의 조건은 들어오거나 나가는 패킷을 분류하기 위한 요소로 정의되며, 프로토콜, 출발지 IP 주소, 목적지 IP 주소, 출발지 포트번호, 목적지 포트번호 등이 해당된다. 규칙의 허용여부로는 조건에 의해 패킷을 허용 또는 차단하도록 결정하는 요소로 구성된다.

방화벽 정책은 외부에 공개적으로 제공하지 않는 보안 정보이기 때문에 네트워크 공격자들은 특정 네트워크를 공격하기에 앞서 사전 정보로 취득하고자 한다. 만약 공격자가 방화벽의 보안 정보를 얻을 수 있다면 네트워크에 대해서 악의적인 행동을 수행할 수 있다. 하지만 외부에서 방화벽 정책을 추론하는 것은 쉽지 않다. 가장 단순한 방법으로 가능한 모든 탐지 패킷을 보내서 응답 여부를 보고 방화벽 정책을 추론할 수 있다[2]. 그러나 이 방법은 보내야 할 탐지 패킷이 너무 많기 때문에 현실적으로 불가능한 방법이다. 또한 많은 탐지 패킷은 대상 네트워크에 대한 인터넷 공격으로도 오인될 수 있다[3]. 탐지 패킷이 인터넷 공격으로 오인 받으면 탐지 패킷을 전송하는 시스템으로부터의 모든 패킷이 차단될 수 있기 때문에 정상적인 응답 패킷을 수신할 수 없게 된다.

우리는 이전 연구에서 스윕 라인 알고리즘을 이용한 방화벽 정책 추론 방법을 제안하였다[4]. 제안된 추론 방법은 한정된 수의 탐지 패킷으로 대상 네트워크의 방화벽 정책을 파악할 수 있었다. 하지만 우리가 제안한 방화벽 정책 추론 방법이 실제 방화벽 장비에서 네트워크 공격으로 오인되지 않고 정책을 정확하게 추론하는지 검증이 필요하다.

본 논문에서는 Active Probing 을 이용한 방화벽 정책 추론 방법이 방화벽에서 네트워크 공격으로 탐지되는가를 검증하고, 방화벽이 끼치는 영향에 대해서 분석한다. 그리고 방화벽 정책을 추론하였을 때 추론 방법에서 발생되는 False Positive 오류와 False Negative 오류에 대해 정확성 측면에서 분석한다.

2. 관련 연구

방화벽 정책을 추론하는 연구로 미국 DePaul 대학교의 Samak T. 등은 방화벽 정책을 추론하기 위한 프레임워크를 제안하였으며, 프레임워크 이름은 FireCracker 라고 지칭하였다[2]. 이 연구에서는 방

화벽 정책 추론을 공간 탐색 문제로 해석하여 공간 탐색 알고리즘인 Region Growing, Split-and-Merge, Genetic Algorithm 을 적용하여 방화벽 정책을 추론하였다. 그리고 방화벽 정책 추론 실험을 통해서 각 알고리즘의 정확성과 효율성에 대한 비교 평가를 제시하였다.

그리고 FireCracker 에서 제기한 방화벽 정책 추론 문제를 바탕으로 실제 인터넷 망에서 대상 네트워크의 방화벽 정책을 추론하는 방법을 제안하였다[4]. 이 연구에서는 새로운 공간 탐색 알고리즘으로 스윕 라인 알고리즘을 제시하였으며, 이론적 배경과 실험 결과를 통해 방화벽 정책을 효율적으로 추론할 수 있음을 제시하였다. 하지만, 실제 인터넷 망에 적용하여 실험하였기 때문에 실제 방화벽 정책과 추론된 정책을 비교 검증하기 어려운 문제점이 있다.

이전 연구에서는 방화벽 정책을 추론하기 위해 다양한 정책 구조를 대상으로 실험하여 적절한 스윕 라인 알고리즘의 이동속도를 도출하였다[5]. 도출된 이동속도는 본 논문에서 적용되어 네트워크 공격에 대한 검증 실험을 하였다.

3. 방화벽 정책 추론의 Confusion Matrix

3.1. Confusion Matrix

방화벽 정책 추론 방법은 공간 탐색 알고리즘을 이용한 정책 추론 과정 중에 두 가지 관점에서 규칙을 잘못 추론하는 오류가 발생한다. 첫 번째 오류는 공간 탐색 알고리즘의 특성상 탐지 패킷이 전송되지 않은 영역에 대해서 발생한다. 두 번째 오류는 정책 추론을 위한 탐지 패킷이 방화벽에서 네트워크 공격으로 탐지되어 올바른 응답 패킷을 수신할 수 없을 때 발생한다. 본 논문에서는 언급된 두 가지 오류에 관해서 실제 방화벽 정책과 추론된 방화벽 정책을 자세히 비교 검증하기 위해 Confusion Matrix 를 적용한다. Confusion Matrix 는 실제 값과 예측 값의 관계를 나타내는 행렬로써, 예측 분석에서 많이 사용된다[6].

실제 방화벽 정책은 2 개의 목적지 IP 주소와 목적지 포트번호를 이용하여 2 차원 공간으로 표현할 수 있다. 2 차원 공간에서 각 점들은 각 규칙에 해당하는 허용 여부 값을 가진다. Confusion Matrix 는 2 차원 공간에서 각각의 정책 규칙에 대응되는 좌표 점의 수로 표현한다.

Confusion Matrix 에는 True Positive, False Negative, False Positive, True Negative 가 존재하며, 표 1 과 같이 나타낸다. True Positive 는 실제 방화벽의 허용 규칙에 해당하면서 추론 결과도 허용하는 것으로 일치하는 값이다. False Negative 는 실제 방화벽의 허용 규칙이 추론 결과 차단하는 것으로 불일치한 값이며, False Positive 는 False Negative 의 반대다. True Negative 는 실제 방화벽의 차단 규칙이 추론 결과와 일치하는 값이다.

<표 1> 방화벽 정책 추론의 Confusion Matrix

		추론 규칙	
		허용	차단
실제 규칙	허용	True Positive	False Negative
	차단	False Positive	True Negative

3.2. False Positive 오류와 False Negative 오류

다음은 3.1 장에서 언급하였던 추론 과정 중에 알고리즘에 의한 오류와 방화벽의 영향에 의한 오류가 발생시키는 False Positive, False Negative 에 대해서 설명한다. 첫 번째로 방화벽과는 무관하게 우리가 제안하는 추론 알고리즘에 의해서 발생되는 오류는 False Positive 오류와 False Negative 오류 모두 관련이 있다. 하지만, 두 번째 관점으로 추론 방법의 문제가 아닌 방화벽의 영향에 의해서 발생되는 오류는 False Negative 오류만 연관이 있으며, False Positive 오류는 발생할 수가 없기 때문에 관련이 없다. 그 이유는 2 차원 공간에서 서로 허용되는 좌표 점을 이어서 허용 규칙을 추론하는 추론 알고리즘의 특성 때문이다. 만약 탐지 패킷이 방화벽의 영향에 의해서 차단되는 경우에는 추론 알고리즘의 특성상 두 점을 이을 수 없게 되므로 False Positive 오류가 발생하지 않는다. 따라서, 본 논문에서 방화벽의 영향에 의해 네트워크 공격으로 탐지되는지를 검증하기 위해서는 네트워크 공격으로 탐지되었을 때의 False Negative Rate 와 네트워크 공격으로 탐지되지 않았을 때의 False Negative Rate 의 변화를 비교한다.

4. 변수 설정에 의한 탐지 방법

4.1. 출발지 IP 주소 설정

프로빙 서버는 대상 네트워크의 방화벽 정책을 추론하기 위해서 다수의 탐지 패킷을 대상 네트워크로 전송하여야 한다. 그러나 프로빙 서버에서 대상 네트워크로 많은 수의 패킷을 빠르게 전송하게 되면, 출발지 IP 주소 기반 세션 수에 제한을 받게 되고, 최악의 경우 서비스거부공격으로 오인 받을 수도 있다. 또한 동일한 출발지 IP 주소에서 발생하는 패킷의 경우 TCP/UDP Sweep 공격으로 차단될 수도 있다.

위에서 언급한 바와 같이 이러한 문제점들을 해결하기 위해서 본 논문에서는 프로빙 서버의 IP 주소를 여러 개로 할당하여 사용한다. 프로빙 서버에 할당되는 출발지 IP 주소의 수를 다양하게 설정하면 출발지 IP 주소의 수가 많을수록 방화벽의 서비스거부공격에 대한 탐지를 피할 수 있으며, 스캔 공격에 대해서도 회피할 수 있는 방안이 되기 때문이다. 그리고 대상 네트워크로 전송되는 출발지 IP 주소의 수에 따라 서비스거부공격에서부터 분산서비스거부공격까지 표현할 수도 있다. 우리는 프로빙 서버의 출발지 IP 주소를 네트워크 C 클래스에 해당하는 1~254 개의 범위로 설정하였다.

4.2. 초당 패킷 전송(PPS) 설정

초당 패킷 전송 값은 공격자 또는 방화벽 정책 추

론 시스템에서 방화벽 정책 추론을 위해 초당 발생시키는 패킷의 수를 의미한다. 이 값은 네트워크 공격 탐지를 피하는데 매우 중요한 매개변수이다. 방화벽은 자신을 통과하고자 하는 패킷을 검사할 때 각각의 네트워크 공격 패턴에 부합하는 패킷의 수를 계산하고, 초당 패킷 전송의 임계치를 초과하게 되면, 공격으로 판단하여 정책과 무관하게 해당 패킷을 버린다.

4.3. 순차적 vs. 임의적 IP 주소 생성

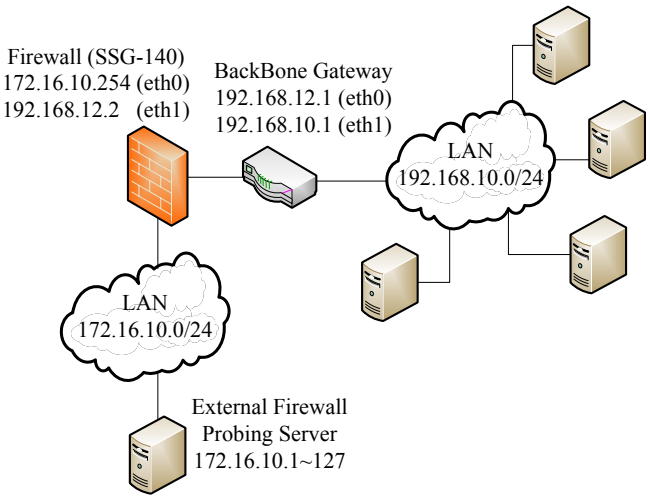
방화벽 정책 추론 방법은 이전 연구에서 제안된 스윕 라인 알고리즘을 이용한 방화벽 정책 추론 방법으로 탐지 패킷을 전송한다. 방화벽 정책 추론 방법에 대한 자세한 내용은 이전 연구에서 제안하였기 때문에 본 논문에서는 생략하였다.

방화벽 정책을 추론하기 위해서는 먼저 추론 방법에 의해 탐지 패킷의 정보가 결정된다. 탐지 패킷의 정보로는 각 헤더 필드에 해당하는 패킷 정보로 구성되어 있고, 스윕 라인 알고리즘의 이동속도와 초당 패킷 전송 수, 출발지 IP 주소의 수가 포함된다. 이러한 탐지 패킷의 정보가 결정되면 출발지 정보와 목적지 정보를 어떤 방식으로 전송할 것이지도 결정이 되어야 한다. 탐지 패킷의 전송 방법은 어떻게 전송되느냐에 따라 네트워크 공격으로 탐지될 수도 있기 때문에 중요하다. 본 논문에서는 탐지 패킷의 전송 방법을 순차적과 임의적으로 전송하여 그 결과를 제시한다.

5. 실험 환경

방화벽에서 네트워크 공격에 대한 정책 추론 방법을 검증하기 위해서 실제 방화벽 장비인 Juniper Networks 사의 방화벽(SSG-140)을 배치하였으며, 그림 1 과 같이 실험 환경을 구성하였다. 그림 1 에서 대상 네트워크는 192.168.10.0/24 대역이 설정되어 있고, 외부에서 정책 추론을 위한 프로빙 서버는 172.16.10.0/24 네트워크 대역에서 254 개의 IP 주소를 할당하였다.

방화벽 장비에는 기본적으로 보안 옵션을 제공하며, Flood 공격과 Scan, Sweep, Spoof, 서비스거부공격 등에 대한 보호 기능으로 구성된다. 본 논문의 목적은 방화벽 정책 추론 방법이 방화벽에 영향을 받는지를 검증하고자 하기 때문에 방화벽 장비에서 네트워크 공격에 대한 보안 옵션은 모두 설정한 상태로 실험을 하였다. 그리고 각 옵션에 대한 임계치는 방화벽을 사용하는 대상 기관의 특성에 따라 다르게 설정되기 때문에 먼저 기본값에 대해서 실험을 하고자 한다. 방화벽의 기본 임계치 설정 값으로는 ICMP/UDP Flood 공격에 대해서 1,000pps, TCP SYN Flood 공격에 대한 기본 임계치는 200pps 와 경고 로그를 발생시키는 임계치 1,024pps 로 설정된다. 스캔 공격에 대한 설정은 TCP/UDP Sweep 패턴에 대한 임계치 50pps, IP 주소 Sweep 과 포트 스캔 공격에 대한 5,000ms 임계치로 설정되었다. 그 외 서비스거부공격을 방어하기 위해 출발지 IP 주소와 목적지 IP 주소에 기반한 세션 제한은 128 개의 세션 수로 임계치



(그림 1) 방화벽 정책 추론 시스템과 실험 네트워크 환경 구성도

가 설정되어 있다. 해당 공격 패턴에 대한 패킷이 임계치를 초과하게 되면, 정책과 무관하게 버려진다.

6. 실험 결과

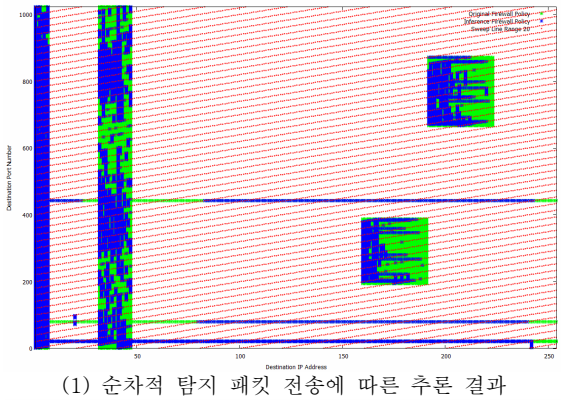
6.1. 탐지 패킷 전송 방법에 대한 실험 결과

이 장에서는 방화벽 정책 추론을 위한 탐지 패킷의 정보를 어떻게 전송하느냐에 따라서 정책 추론 결과가 달라지는지를 확인하고자 한다. 탐지 패킷의 전송 방법은 4.4 장에서 언급한대로 순차적 방식과 임의적 방식으로 탐지 패킷을 전송하였다. 그림 2 는 순차적과 임의적 전송 방식에 따른 방화벽 정책 추론 결과 분포도를 보여준다. 그림 2 에서 녹색으로 나타난 영역은 실제 방화벽 정책의 허용 규칙을 표현한 것이고, 파란색 영역은 추론 알고리즘에 의해 추론된 허용 규칙을 의미한다. 그리고 흰 배경은 방화벽 정책의 기본 차단 규칙을 의미하며, 빨간색 대각선은 스윕 라인을 표현한 것으로 탐지 패킷이 전송된 영역과 같다. 그림 2 에서 보면 순차적으로 탐지 패킷을 전송한 결과와 임의적으로 탐지 패킷을 전송한 결과가 뚜렷한 차이점이 나타난다. 먼저 순차적 전송 방법은 왼쪽에서 오른쪽 방향으로 순차적 증가를 하기 때문에 추론 결과가 왼쪽으로 치우친 것을 확인할 수 있다. 그리고 임의적 전송 방법은 순차적 전송 방법과 달리 정책 영역에 고르게 분포한 것을 확인할 수 있다. 일정한 간격으로 특정 부분에 대해서 오류가 발생한 영역은 방화벽의 보안 기능에 영향을 받은 것이다.

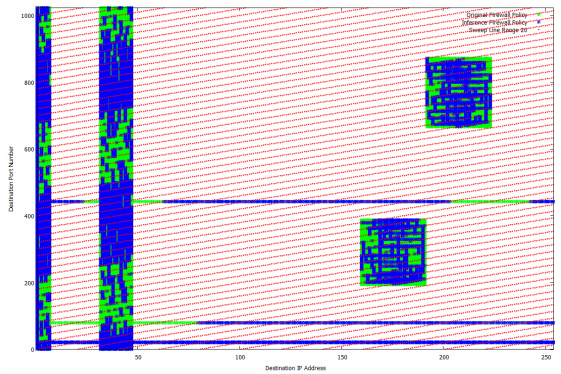
6.2. False Negative 에 대한 방화벽 영향 분석

False Negative 오류는 3.2 장에서 언급한 바와 같이 네트워크 공격으로 탐지되어 방화벽의 영향으로 올바른 응답 패킷을 수신할 수 없을 때 발생된다. 그리고 정책 추론 방법의 특성으로 인한 오류는 False Negative 와 False Positive 오류가 존재하게 된다.

그림 3 은 PPS 외에는 동일한 값으로 실험하였을 때 출발지 IP 주소 수에 따라 False Negative 오류가

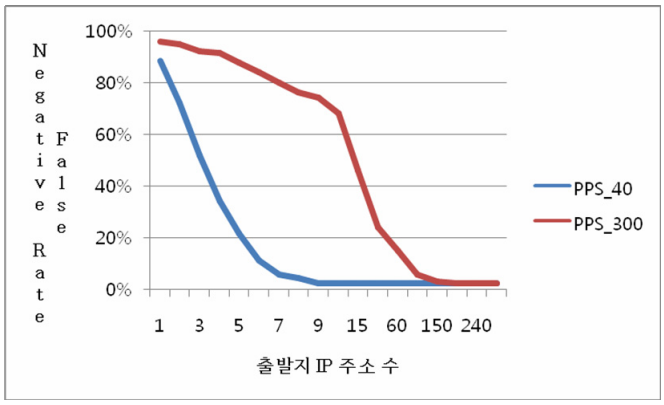


(1) 순차적 탐지 패킷 전송에 따른 추론 결과



(2) 임의적 탐지 패킷 전송에 따른 추론 결과

(그림 2) 탐지 패킷 전송 방식에 따른 방화벽 정책 추론 결과 분포도



(그림 3) 출발지 IP 주소 수에 따른 False Negative Rate 분포

발생하는 비율 분포를 보여준다. 그림 3 에서 40 PPS 의 경우에는 방화벽에서 네트워크 공격으로 탐지가 되지 않았고, 300 PPS 는 방화벽의 TCP SYN Flood 와 TCP Sweep, 출발지 IP 주소 기반의 세션 제한의 임계치를 초과하여 네트워크 공격으로 탐지되었다. 각기 다른 PPS 에 따라 False Negative 의 비율이 다르게 나타난 것으로 보아 임계치를 초과한 경우 방화벽 정책 추론 방법이 방화벽의 보안 기능에 영향을 받는 것을 알 수 있다. 40 PPS 일 때는 출발지 IP 주소의 수가 7 개 이상일 때 2%의 오차 범위에서 정책을 정확하게 추론할 수 있었다. 그리고 300 PPS 일 때는 출발지 IP 주소의 수가 약 150 개 이상일 때 정확하게 정책을 추론할 수 있었다.

본 실험에서는 False Positive 오류가 나타나지 않았다. 그 이유는 우리가 제안하는 공간 탐색 알고리즘의 특성상 이전 연구에서 제시한 이동속도를 이용한다면 False Positive 오류가 발생하지 않거나 발생하더라도 적은 분포로 나타난다.

7. 결론 및 향후 연구

본 논문에서는 active probing 을 이용하는 방화벽 정책 추론 방법이 방화벽에서 네트워크 공격으로 판단되는지를 분석하였다. 네트워크 공격에 대한 방화벽 정책 추론 방법을 정확하게 검증하기 위해서 실제 방화벽 장비를 배치하여 실험 환경을 구성하였다. 실험 결과로는 실제 방화벽에 구성된 정책과 추론된 방화벽 정책을 비교하여 정확성을 검증하였다. 그리고 네트워크 공격으로 탐지되었을 때와 탐지되지 않았을 때의 False Positive 와 False Negative 에 대한 오류를 비교 제시하였다. 실험 결과를 통해 이전 연구에서 제안한 스윕 라인 알고리즘을 이용한 방화벽 정책 추론 방법이 방화벽에서 네트워크 공격으로 탐지되지 않고 방화벽 정책을 추론할 수 있음을 제안하였다.

방화벽 정책 추론 결과에서 False Negative 오류의 비율을 줄이기 위한 해결 방안으로 단계적 접근 방식을 마련하여 정책 추론 방법을 개선하고자 한다. 또한 방화벽 장비에서 설정된 네트워크 보안의 임계치도 사전에 파악할 수 있는 방안을 마련하여 정책 추론 방법을 개선시키고자 한다. 그 외에 방화벽 정책 추론 결과를 네트워크 핑거프린트로 활용하는 방법과 방화벽 정책에서 존재하는 이상 규칙(Anomaly Rule)을 탐지하고 검증하는 방안을 마련할 것이다.

Acknowledgement

이 논문은 2012 년도 정부(교육과학기술부)의 재원으로 한국연구재단의 지원을 받아 수행된 기초연구사업임(2012R1A1A2006331). *교신저자: 주홍택.

참고문헌

[1] Wack, J., Cutler, K., Pole, J., “Guidelines on Firewalls and Firewall Policy,” Special Publication 800-41, NIST(National Institute of Standards and Technology), p. 64, January, 2002.

[2] Samak, T., El-Atawy, A. and Al-Shaer, E., “FireCracker: A Framework for Inferring Firewall Policy using Smart Probing,” in Proc. IEEE Network Protocols(ICNP), pp.294-303, October, 2007.

[3] Shirey, R., “Internet Security Glossary”, RFC 2828, IETF, May, 2000.

[4] Hyeonwoo Kim and Hongtaek Ju, “Efficient Method for Inferring a Firewall Policy,” in Proc. Network Operations and Management Symposium (APNOMS), September, 2011.

[5] 김현우, 주홍택, “탐지 패킷을 이용한 방화벽 정책 추론”, 통신망운용관리학술대회 논문집, May, 2012.

[6] Ian H. Witten, Eibe Frank, “Data Mining: Practical Machine Learing Tools and Techniques,” Second Edition, Morgan Kaufmann.