The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 17, No. 4, pp.11-17, Aug. 31, 2017. pISSN 2289-0238, eISSN 2289-0246

https://doi.org/10.7236/JIIBC.2017.17.4.11
JIIBC 2017-4-2

내부자 정보 유출 탐지 방법에 관한 연구

A Study on Method for Insider Data Leakage Detection

김현수*

Hyun-Soo Kim*

요 약 최근 많은 기업 및 기관에서 내부정보가 유출되는 사고가 지속적으로 발생하고 있으며, 이러한 내부정보 유출 사고는 대부분 권한 있는 내부자에 의해 발행하고 있다. 본 논문에서는 은닉 마르코프 모델(HMM)을 이용하여 내부자의 정상행위에서 생성된 정보를 모델링한 후 내부자들의 비정상행위를 탐지하는 내부정보 유출 탐지 기법에 대해 제안한다. 보안시스템들의 로그를 통해 내부자들의 행위에 대한 특징을 추출하여 입력 시퀀스를 생성하고, HMM 모델에 학습하여 정상행위에 대한 모델을 생성한다. 이상행위에 대한 판정은 사용자 행위에 대한 관측열을 정상행위 모델에 적용하여 확률값을 계산하고, 이 값을 특정 임계값과 비교하여 이상행위를 탐지한다. 실험을 통해 내부자 정보유출 행위를 탐지하기 위한 최적의 HMM 매개변수를 결정하였고, 실험결과 제안한 시스템이 내부자 정보유출 행위에 대해 20%의 오탐율과 80%의 탐지율을 보여주었다.

Abstract Organizations are experiencing an ever-growing concern of how to prevent confidential information leakage from internal employees. Those who have authorized access to organizational data are placed in a position of power that could well be abused and could cause significant damage to an organization. In this paper, we investigate the task of detecting such insider through a method of modeling a user's normal behavior in order to detect anomalies in that behavior which may be indicative of an data leakage. We make use of Hidden Markov Models to learn what constitutes normal behavior, and then use them to detect significant deviations from that behavior. Experiments have been made to determine the optimal HMM parameters and our result shows detection capability of 20% false positive and 80% detection rate.

Key Words : Insider Data Leakage, Abnormal Behavior Detection, Hidden Markov Model

Ⅰ. 서 론

최근 많은 기업에서 내부정보가 유출되는 보안사고가 빈번히 발생하고 있으며, 이러한 내부정보 유출 사고는 기업 이미지 손실을 비롯해 첨단기술의 경쟁사 유출로 인한 금전적 손실을 초래하는 등 사고가 발생한 기업에게 심각한 피해를 초래하고 있다.

내부정보 유출 사고의 원인을 살펴보면 외부자 침입에 의한 정보유출과 내부자에 의한 정보유출로 구분할 수 있다. 과거에는 외부 해킹 공격에 의한 정보 유출 사고의 비중이 높았지만 최근 발생한 대부분의 내부정보 유출 사고들은 특정 권한을 가지고 있는 내부자에 의해 발생하고 있다. 국가정보원 산업기밀보호센터의 조사에 따르면 산업기밀 유출 범죄의 주체의 80%가 전·현직 직원으로 나타났으며, US. Justice Department의 조사에서는 미국 기업내에서 발생하는 정보유출사고의 74%가 내

*정회원, 국방과학연구소 연구원
접수일자: 2017년 7월 11일, 수정완료: 2017년 8월 5일
게재확정일자: 2017년 8월 11일

Received: 11 July, 2017 / Revised: 5 August, 2017 /
Accepted: 11 August, 2017
*Corresponding Author: hyunsookim@add.re.kr
Dept of Computer Science, Agency for Defense Development, Korea

부자에 의해서 이루어지고 있는 것으로 나타났다[1]. 실제로 공기업 K사에서는 공사관리팀장이 이메일 및 USB 형태로 자사의 첨단 기술을 민간 설계 업체로 빼돌리다가 적발된 사례가 있으며, 자동차 부품 제조업체인 A사에서는 해외영업팀장이 B 경쟁사에게 같은 제품을 개발할 수 있는 비밀문서를 전달하여 실형을 선고받은 사례 등 다양한 내부정보 유출 사고가 지속적으로 발생하고 있다. 2013년에는 CIA요원이자 NSA 직원이었던 Edward Snowden이 개인의 모든 정보를 감청하는 PRISM에 대한 국가기밀정보를 언론매체에 공개하면서 미국이 전 세계의 질타를 받기도 하였으며, 2016년에는 NSA 협력업체 직원이었던 헤롤드 마틴이 국가 1급 기밀이 포함된 50TB 규모의 데이터를 유출하는 사건이 발생하는 등 기업의 입장에서는 내부자에 의한 정보유출을 차단할 수 있는 방안이 시급한 실정이다.

현재 많은 기업에서는 내부정보 유출 사고를 방지하기 위한 노력으로 유출경로에 대한 통제가 가능한 DLP 시스템과 내부에서 생성되는 문서를 보호하기 위한 DRM 시스템 등 다양한 보안시스템을 도입하여 운영하고 있다. 하지만 이러한 보안시스템들도 특정 권한이 있는 내부자가 악의적인 목적으로 정보 유출을 시도할 경우 정상적인 절차에 따라 외부로 반출되기 때문에 실질적인 대응이 어렵다. 또한, 내부자들의 경우 조직 내의 존재하는 IT 시스템들의 환경을 충분히 파악하고 있기 때문에 보안시스템을 우회하여 정보를 유출할 수 있으며, 팀 동료들의 계정정보를 탈취하여 정보 유출을 시도할 수도 있다. 기존의 단순 패턴 탐지 방식으로 운용되고 있는 현재의 보안시스템으로는 내부자의 정보유출을 탐지하는데 한계가 있으며, 내부자 공격 특성에 맞는 탐지 방법이 필요하다.

본 논문에서는 내부자에 의한 정보유출 탐지 방법으로 이상행위 탐지 개념을 적용한 머신러닝 기반의 탐지 방법에 대해서 제안하고자 한다. 내부자에 의해 발생하는 모든 정상행위들을 은닉마르코프 모델을 기반으로 모델링하여 외부로 반출되는 모든 문서들에 대한 비정상 절차에 대해서 즉각적으로 탐지할 수 있는 매커니즘을 제안한다. 본 논문에서 제안한 정상행위 모델링에는 HMM(Hidden Markov Model)을 사용하였으며, HMM 입력 시퀀스로 파싱/변환하는 전처리 과정을 수행하여 내부자의 비정상 유출 행위를 탐지하였다.

본 논문의 구성은 총 5장으로 구성되었다. 2장에서는 내부자 정보 유출 탐지 기법에 관한 선행 연구를 살펴보고 3장에서는 논문에서 제안한 탐지방법에 대해 소개한다. 4장에서는 제안한 탐지방법을 사용하여 실험한 결과를 분석한 후 5장에서는 결론 및 향후 연구에 대하여 제시하였다.

II. 관련 연구

내부자 정보 유출에 대한 사회적 관심이 많아지면서 다양한 학문 분야에서 내부자의 정보 유출 탐지 방안에 대한 연구가 수행되었다. 심리학 분야에서는 사회적 이론을 활용하여 악의적인 내부자들에게서 나타나는 특정 행동들을 지표화하여 정보 유출을 탐지하는 연구가[2][3] 수행되었으며, 범죄학 분야에서는 억제 이론(deterrence theory)과 사회유대 이론(social bond theory)을 통해 악의적인 내부자를 탐지하는 연구가[4][5] 수행되었다. 특히, 시스템 개발 측면의 선행 연구들을 살펴보면 정상 행위를 모델링하여 이를 벗어난 outlier를 탐지하는 이상행위 기반의 탐지 기법을 활용한 연구가 많이 이루어지고 있다. Liu et al[6]은 외부 침입을 탐지하는 방식을 적용하여 사용자들의 컴퓨터 OS 레벨에서 이루어지는 파일복사, USB 복사, 악성코드 설치 등의 이벤트 로그를 이용하여 내부자들의 이상 행위를 탐지하는 연구를 수행하였고, Kwon et al[7]은 외부 침해시도를 탐지하기 위하여 빅데이터 기반의 패턴탐지 방법과 이상탐지 방법을 병합하는 연구를 수행하였다. Maloof and Stephens[8]는 “need to know” 원칙에 따라 권한 이상의 접근을 시도하는 내부자들을 탐지할 수 있는 ELICIT이라는 시스템을 제안하였다. ELICIT 시스템은 이상 행위 시나리오를 기반으로 76개의 탐지기를 구현하여 이로부터 탐지된 행위들을 Bayesian Ranking에 따라 점수화하였으며, 실제 기관에 적용하여 효과적으로 내부자의 이상행위가 탐지되는 것을 검증하였다.

이상행위 기반의 탐지 기법은 외부 네트워크 공격에 대응하기 위한 침입탐지시스템(Intrusion Detection System)에서 많이 활용되었던 방식으로 일반적으로 통계 모델을 이용한 탐지 기법과 머신러닝을 이용한 탐지 기법이 있다. 통계적 탐지 기법은 사용자 행위를 시간에 따라 측정하고 평균과 표준편차를 모델링하여 정상과 비정상을 탐지하는 방식이며, 머신러닝 탐지 기법은 사용

자 행위를 추출하고 학습을 통해 정상행위를 모델링하여 비정상을 탐지하는 방식이다. 통계적 기법을 이용한 기존 연구의 경우 악의적인 내부자도 대부분의 행위가 정상 행위로 구성되어 있기 때문에 탐지에 어려움이 있었으며[9], 최근의 연구에서는 대부분 머신러닝을 이용한 탐지 시도가 이루어지고 있다. 머신러닝을 이용한 이상행위 탐지의 경우 정상행위를 어떻게 모델링하는지에 따라 성능이 좌우되며 비교적 쉽게 정의 가능한 외부 침입 공격에 비하여 내부자의 유출 행위는 정상 행위를 정의하기 어렵기 때문에 내부자의 공격 특성에 맞는 탐지 방법이 필요하다.

표 1. 내부자 정보 유출 탐지에 관한 접근 방법 비교
Table 1. Comparison of different approaches for insider data leakage

저자	관찰 행위	데이터	탐지 방법
Parveen et al[14]	Unix 명령어	가상	비지도
Maloof et al[8]	사용자의 모든 행위 기반 탐지	가상	지도
Legg et al[10]	사용자 행위 및 역할 기반 탐지	가상	지도
Gavai et al[11]	조직 내 사회적 관계 및 온라인 행위 기반 탐지	실제	비지도/지도
Eldardiry et al[12]	사용자 PC에서 발생하는 행위 (6개 특징 추출)	실제	지도
Rashid et al[13]	사용자 PC에서 발생하는 행위 (16개 특징 추출)	가상	지도
제안연구	사용자 PC에서 발생하는 행위 (18개 특징 추출)	실제	지도

머신러닝 기반의 최근의 연구들을 살펴보면 Eldardiry et al[12]은 사용자 행위를 기반으로 log on, device, file, http, email sent/revieved 6가지 특징을 추출하여 내부자 위협을 탐지하는 시스템을 제안하였으며, Rashid et al[13]은 CMU CERT에서 공개되어 있는 가상데이터를 활용하여 사용자 행위에 대한 특징을 추출하여 HMM 모델에 적용하여 내부자 위협을 탐지하는 연구를 수행하였다. Parveen et al[14]은 UNIX Shell에서 타이핑되는 커맨드를 특징으로 추출하여 비지도 학습 기반의 스트림 마이닝 기법을 활용한 내부자 위협을 탐지하는 시스템을 제안하였다. 이들 연구는 모두 가상 시나리오를 기반으로 만들어진 인위적인 데이터를 활용하여 연구가 이루어 졌으며, 내부자 행위에 대한 특징 추출이 세분화되어 있지 않아 특정 시나리오에서만 탐지가 가능한 한계가 있다. 또한, 비지도 학습 기반의 탐지는 내부자 정보 유출 행위가 정상행위에 비하여 극히 드물게 분포되어 있고 새롭게 진화하는 이상 행위를 탐지 가능한 장점이 있지만 지도 학습 기반의 탐지에 비하여 탐지 성능이 떨어지는 문제가 있다. 본 연구에서는 다양한 내부자 정보 유출 행위를 탐지 할 수 있도록 사용자 행위에 특징 추출을 좀 더 세분화 하여 HMM 모델을 학습하였으며, 실제 조직에서 발생한 내부자 정보 유출 데이터를 기반으로 검증하는 작업을 수행하였다.

Ⅲ. 3장 내부자 정보 유출 탐지 기법

1. 내부자 정보 유출 탐지 환경 구성

대부분의 국내 조직은 내부 위협에 대응하기 위하여 다양한 보안시스템을 도입하여 운영하고 있다. 이를 통해 USB, 웹메일, CD/DVD, 스마트폰 등 유출 경로에 대한 사전 차단이 이루어지고 있으며, 특정 승인 절차에 따라 외부 반출이 이루어지고 있다. 이러한 국내 조직의 환경을 고려하여 내부자의 정보 유출 행위와 관련된 데이트를 생성하기 위하여 일반적으로 조직에서 운영 중인 DRM, DLP, 보안USB, 이메일시스템 등의 보안시스템과 그룹웨어의 로그를 활용하였다.

내부정보 유출은 대부분 문서파일과 인쇄의 형태로 이루어지고 있기 때문에 문서를 생성, 열람, 편집, 인쇄하는 행위에 대한 정보가 필요하며 이에 대한 데이터는 DRM 로그를 활용하였다. 문서파일을 외부로 반출하기 위한 수단으로 많이 활용되는 이메일, USB, CD/DVD, 메신저, 스마트폰 등에 대한 정보는 DLP 시스템과 메일 시스템의 로그를 활용하였으며, PC를 통해 내부 시스템에 접속하는 정보에 대해서는 NAC 시스템에서 생성되는 로그를 활용하였다.

2. 내부자 정보 유출 탐지 과정

본 연구에서는 시계열 기반의 내부자 행위 특징을 사용하여 HMM을 학습하고 이를 이용함으로써 이상 행위를 탐지한다. 시스템의 전체 처리 과정은 그림 1과 같이 전처리 단계(preprocessing), 학습 단계(learning phase),

탐지 단계(detection phase) 등 크게 3 단계로 구성된다. 먼저 전처리 단계에서는 보안시스템들의 로그를 통해 내부자들의 행위에 대한 특징을 추출한다. 그리고 이렇게 추출된 특징들을 사용자 기반으로 시퀀스 형태의 입력 데이터를 생성한다. 학습단계에서는 시계열 훈련 데이터를 이용하여 HMM 학습을 통해 정상 행위에 대한 모델을 생성한다. 마지막으로 탐지 단계에서는 테스트 데이터를 HMM 모델에 적용하여 확률값이 임계값 T보다 작을 경우 이상행위로 탐지한다.

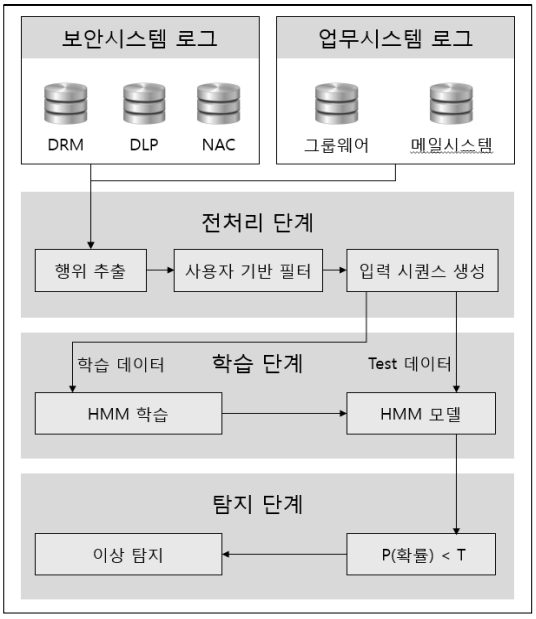

그림 1. 정보 유출 탐지 처리 과정 개요
Fig. 1. Overall Process of Data Leakage Detection

3. 내부자 행위 특징 추출

HMM은 시계열의 데이터를 기계학습의 특징(feature)으로 추출하여 인식할 수 있다. 즉 악의적인 내부자가 정보 유출을 시도하기 위한 특정 행위가 시간에 따라 일정한 패턴의 순서로 존재할 경우 특징을 추출하여 HMM의 시퀀스에 적용할 수 있다. 본 연구에서 제안 하는 탐지 기법은 특징 추출을 위해 사용자 PC에서 발생하는 다양한 행위 정보들이 기록되는 보안시스템의 로그를 활용하였다. DRM 로그의 경우 사용자ID, 문서명, 문서파일 크기, 열람/편집 날짜, 인쇄 날짜, 인쇄 IP 등에 대한 정보들이 포함되어 있어 누가, 언제, 어디서, 무엇을 출력하였는지 인쇄 행위에 대한 확인이 가능하다. 이러한 보안시스템들의 로그를 취합하여 PC 로그온, 문서 사용, 문서 인쇄, 문서 복호화, 이메일, USB, CD/DVD, Fax, 메신저, 스마트폰, 인터넷 접속 총 11개의 행위 특징을 1차적으로 추출하였다. PC 로그온 특징의 경우 내부자 정보 유출 시도가 주로 업무외 시간에 이루어지는 점을 고려하여 업무 시간 로그인(오전 8시 ~ 오후 6시), 업무외 시간 로그인(오후6시 ~ 오전 8시), 주말 로그인(토요일, 일요일)으로 세분화 하였다. 이메일 특징의 경우에는 수신 주소의 도메인을 비교하여 내부직원에게 발송되는 메일인지 외부로 발송되는 메일인지 구분화 하여 특징을 추출하였다. 문서 인쇄의 경우 프린트 IP 대역대를 비교하여 사무실내에 위치한 프린터를 사용하는지 아니면 다른 부서에 위치한 프린터를 사용하는지 구분 하였다. 이러한 세분화 작업을 통해 표 1과 같이 총 18개의 특징을 추출하였다. 추출된 특징들은 정수값으로(1~18)으로 관찰 가능한 기호(Symbol)로 정의한 후 각각의 로그 데이터에 기호를 부여하였다. 이후 모든 로그 데이터를 사용자 ID를 기반으로 하나 데이터로 조인하고 시간순서에 따라 정렬하는

표 2. 특징 추출
Table 2. Feature Extraction

구분	특징	내용
1	업무 시간 로그인	평일 일과시간 (오전8시 ~ 오후6시) 내에 PC 로그온
2	업무외 시간 로그인	평일 일가시간 외에 PC 로그온
3	주말 로그인	주말 시간 PC 로그온
4	지정 로그인	지정된 PC를 통한 로그인
5	비지정 로그인	다른 직원의 PC를 통한 로그인
6	사무실 인쇄	사용자 사무실에 위치한 프린터 인쇄
7	사무실외 인쇄	사용자 사무실이 아닌 다른 사무실에서 인쇄
8	일반문서	일반문서 생성/열람/편집
9	보안문서	보안문서 생성/열람/편집
10	문서 복호화	문서를 외부로 반출하기 위한 DRM 해제
11	내부메일	내부직원에게 메일 발송
12	외부메일	외부인에게 메일 발송
13	USB	USB에 파일 복사
14	CD/DVD	CD/DVD에 파일 굽기
15	Fax	Fax 발송
16	메신저	메신저를 통해 파일 전달
17	인터넷	인터넷 사이트 접속
18	스마트폰	스마트폰을 PC로 연결

과정을 거쳤다. HMM에 적용 가능한 시퀀스(Sequence) 형태의 입력값을 생성하기 위하여 1주 단위로 그룹화하는 작업을 거쳤으며, 이렇게 생성된 데이터는 1주 동안 시간에 따라 이루어진 내부자의 모든 행위 리스트를 나타낸다.

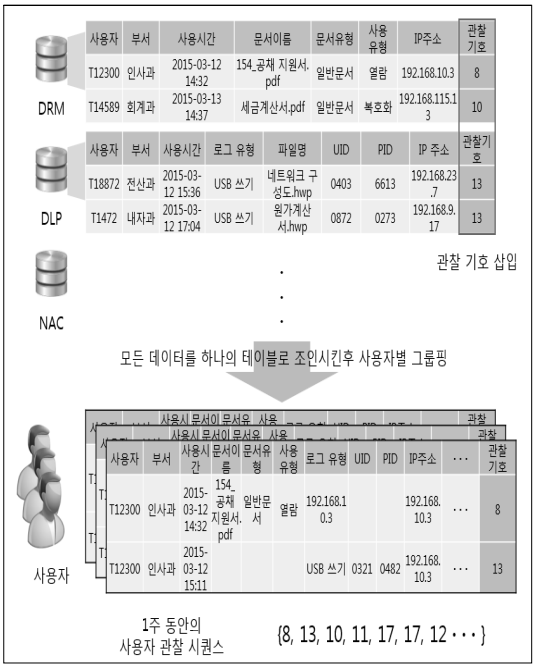

그림 2. 내부자 행위 시퀀스 생성 과정
Fig. 2. Creation Process of Insider Behavior Sequence

4. HMM 기반 내부자 정보 유출 탐지

내부자 정보 유출 탐지를 위해서는 정상 행위에 대한 모델이 필요하며, 정상 행위 모델은 내부자 행위 시퀀스를 기반으로 HMM의 매개변수를 결정하는 과정이다. HMM 매개변수 결정은 관측열 O가 해당 모델 λ로부터 관측될 확률인 $P(O\lambda)$ 값이 최대가 되도록 $\lambda=(\pi,A,B)$을 조정한다. 본 논문에서는 관측열 $O=\{O_0,O_1,\cdots,O_{T-1}\}$이 모델 $\lambda=(\pi,A,B)$ 에서 관측되었을 확률을 최대로 하는 매개변수를 구하기 위하여 Baum-Welch 알고리즘을 사용하였다.

정상행위 모델 모델을 생성한 후에는 1주 단위의 내부자 행위 시퀀스를 입력하여 각 정상 행위에서 현재 행위가 생성되었을 확률을 구한다. 각 모델별로 구해진 확률은 특정 임계값(Threashold)과 비교하여 더 낮은 값을 가질 경우 내부자 정보 유출로 판단한다.

Ⅳ. 실험 및 결과

1. 데이터

실험 데이터는 A기업에 도입되어 운영중인 DRM, DLP, NAC 등 보안시스템들의 로그를 사용하였다. 데이터 정제 작업을 통해 퇴직하거나 신규로 입사한 직원은 제외하였으며, 업무 특성상 외근이 잦은 직원들도 데이터에서 제외하여 총 580명의 내부자들이 선정되었다. 이들로부터 생성된 6개월 동안의 보안시스템 로그를 데이터셋으로 활용하였다. 데이터셋 안에는 15건의 내부정보 유출로 의심되는 행위정보들이 포함되어 있으며, 이외에는 모두 정상행위들로 구성되어 있었다. 데이터셋은 HMM 정상행위 모델 생성하기 위한 학습용 데이터셋과 이상행위에 대한 탐지를 실험하기 위한 테스트 데이터셋으로 분리하였다. 학습용 데이터는 정상행위로만 구성된 데이터로 전처리 과정을 통해 4주 동안의 HMM 입력 시퀀스 변환하여 모델을 학습하였으며, 나머지 20주의 데이터셋은 15건의 내부자 정보유출 행위를 포함하여 이상행위에 대한 탐지를 위한 테스트 데이터셋으로 활용하였다.

각 실험 결과는 ROC(Receiver Operating Characteristic) 곡선을 사용하여 비교하였으며, 본 논문에서는 상태수와 매개변수 조정에 따른 탐지율과 false-positive 오류율의 변화를 ROC 곡선을 사용하여 보여준다. 바람직한 내부정보 유출 탐지시스템은 낮은 false-positive 오류에서 높은 탐지율을 보여주어야 하므로 곡선이 왼쪽 위로 있을수록 좋은 성능을 나타낸다. 정상행위 평가값은 확률값에 자연로그를 취한 실수값으로 [0,1]의 범위를 갖는다.

2. 결과

본 실험에서는 내부정보 유출 탐지시스템이 최적이 성능을 보일 수 있도록 HMM 매개변수를 결정하기 위한 실험을 수행하였다. 상태수를 10, 20, 30, 40으로 변경하여 ROC 곡선을 얻은 결과는 그림 2에서와 같이 상태수가 증가할수록 조금 더 높은 탐지율을 보여주었다. 하지만 상태수가 증가할수록 계산에 소요되는 시간이 급격히 증가하였다. 6개월 동안의 데이터를 한 번에 처리하는 분석과정을 거쳤기 때문에 본 실험에서는 많은 시간이 소요되었지만 실제 시스템을 구축하여 온라인 방식으로 새롭게 생성되는 데이터만을 실시간으로 처리할 경우 분석 시간에 대한 문제는 해결할 수 있다. 상태수 증가에 따른 탐지 성능 향상정도가 5% 내외로 미미하였기 때문에 상

태수는 10으로 고정하여 이후의 실험을 진행하였다.

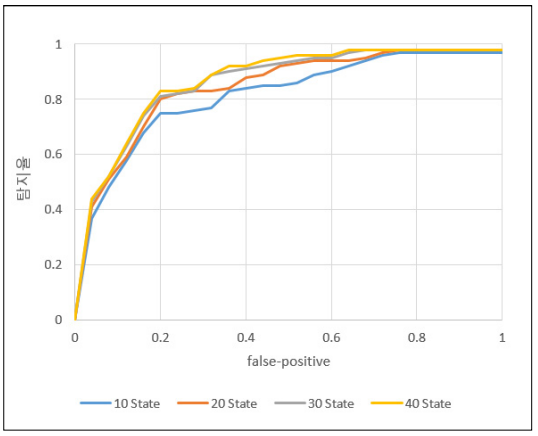

그림 3. 상태수에 따른 ROC 곡선
Fig. 3. ROC Curve with varying number of states

표 3. 상태수에 따른 AUC
Table 3. AUC for each of states

상태수(States)	Area Under Curve(AUC)
10	0.732
20	0.758
30	0.786
40	0.791

상태수에 대한 설정값 이외에 탐지성능에 중요한 영향을 미치는 매개변수 λ에 대해서도 0.1부터 0.9까지 값을 변화하여 실험을 수행하였다. 그림 3과 같이 매개변수 λ가 0.1으로 설정된 경우와 0.9로 설정된 경우를 비교하였을 경우 탐지율에 큰 차이가 발생하는 것을 볼 수 있다. λ = 0.1일 때 AUC = 0.823으로 가장 높은 탐지율을 보였으며, 대부분의 내부정보 유출 행위를 탐지할 수 있는 것으로 나타났다. λ = 0.1은 과거의 행위를 지속적으로 반영하기 위해서는 너무 작은 값으로 생각될 수 있지만 HMM의 확률값은 매개변수 λ가 작은 값일 때 더 넓게 분포되어 있는 것을 의미한다. 그림 3에서와 같이 탐지율 80%에서는 20% false-positive 오탐율을 보여주었으며, false-positive 오탐이 발생한 부분은 학습시 정상행위로 모델링되지 않아 발생한 것으로 성능을 개선하기 위해서는 정상행위와 비정상행위를 명확히 구분할 수 있는 추가적인 특징을 반영할 필요가 있다.

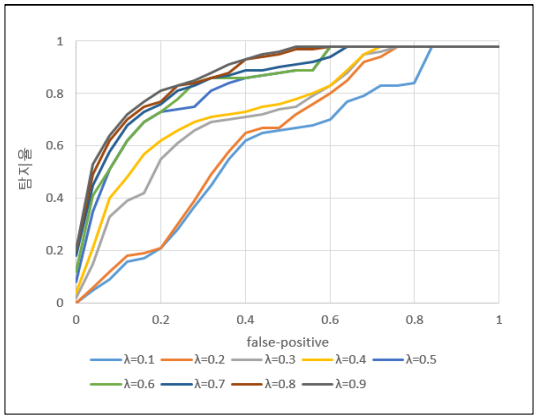

그림 4. 매개변수 λ 변화에 따른 ROC 곡선
Fig. 4. ROC Curve with varying the parameter λ

표 4. 매개변수 λ 따른 AUC
Table 4. AUC for each of parameter λ

λ	Area Under Curve(AUC)
0.9	0.521
0.8	0.584
0.7	0.687
0.6	0.701
0.5	0.764
0.4	0.779
0.3	0.782
0.2	0.808
0.1	0.823

V. 결 론

본 논문에서는 HMM을 사용하여 내부자들의 정상행위를 모델링한 후 시간순서에 따라 생성되는 내부자들의 행위 시퀀스를 분석하여 내부자의 정보 유출 행위를 탐지하는 방법을 제안하였다. 실제 기업에서 생성된 보안 시스템 로그 데이터를 활용하여 검증을 수행하였으며, 실험 결과 내부자 정보 유출 행위를 적절히 탐지함을 확인할 수 있었다.

향후 연구로는 정상 행위 모델을 생성하기 위해 사용되었던 HMM을 LSTM과 같은 딥러닝 알고리즘을 활용하여 탐지 성능을 보다 정교하게 개선할 수 있는 방안이 필요하다. 또한 내부자들의 심리적인 상태와 사회적 관계에서 나타나는 특징들을 반영하여 정상행위를 세부적으로 모델링하는 연구가 필요하다.

References

[1] Fyffe, George. "Addressing the insider threat." Network security 2008.3 (2008): 11-14.

[2] Schultz, E. Eugene. "A framework for understanding and predicting insider attacks." Computers & Security 21.6 (2002): 526-531.
DOI: http://dx.doi.org/10.1016/S0167-4048(02)01009-X

[3] Magklaras, G. B., and S. M. Furnell. "Insider threat prediction tool: Evaluating the probability of IT misuse." Computers & Security 21.1 (2001): 62-73.
DOI: http://dx.doi.org/10.1016/S0167-4048(02)00109-8

[4] Theoharidou, Marianthi, et al. "The insider threat to information systems and the effectiveness of ISO17799." Computers & Security 24.6 (2005): 472-484.
DOI: http://dx.doi.org/10.1016/j.cose.2005.05.002

[5] Kwang-su Im et al. "A Study on Influence of Information Security Stress and Behavioral Intention for Characteristic factors of Information Security Policy Perceived by Employee", The Journal of The Institue of Inernet Broadcasting and Communication(JIIBC), Vol.16, No.6, pp.243-253, 2016
DOI: https://doi.org/10.7236/JIIBC.2016.16.6.243

[6] Liu, Alexander, et al. "A comparison of system call feature representations for insider threat detection." Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC. IEEE, 2005.
DOI: http://dx.doi.org/10.1109/IAW.2005.1495972

[7] Young-baek Kwon, In-seok Kim. "A study on Anomaly Signal Detection and Management Model using Big Data." The Journal of The Institue of Inernet Broadcasting and Communication(JIIBC) Vol.16 No.6, 2016
DOI: https://doi.org/10.7236/JIIBC.2016.16.6.287

[8] Maloof, Marcus, and Gregory Stephens. "Elicit: A system for detecting insiders who violate need-to-know." Recent Advances in Intrusion Detection. Springer Berlin/Heidelberg, 2007.
DOI: http://dx.doi.org/10.1007/978-3-540-74320-0_8

[9] Patcha, Animesh, and Jung-Min Park. "An overview of anomaly detection techniques: Existing solutions and latest technological trends." Computer networks 51.12 (2007): 3448-3470.
DOI: http://dx.doi.org/10.1016/j.comnet.2007.02.001

[10] Legg, Philip A., et al. "Automated insider threat detection system using user and role-based profile assessment." IEEE Systems Journal (2015).
DOI: http://dx.doi.org/10.1109/JSYST.2015.2438442

[11] Gavai, Gaurang, et al. "Supervised and Unsupervised methods to detect Insider Threat from Enterprise Social and Online Activity Data." JoWUA 6.4 (2015): 47-63.

[12] Eldardiry, Hoda, et al. "Multi-source fusion for anomaly detection: using across-domain and across-time peer-group consistency checks." JoWUA 5.2 (2014): 39-58.

[13] Rashid, Tabish, Ioannis Agrafiotis, and Jason RC Nurse. "A New Take on Detecting Insider Threats: Exploring the use of Hidden Markov Models." Proceedings of the 2016 International Workshop on Managing Insider Security Threats. ACM, 2016.
DOI: http://dx.doi.org/10.1145/2995959.2995964

[14] Parveen, Pallabi, et al. "Unsupervised ensemble based learning for insider threat detection." Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing (SocialCom). IEEE, 2012.
DOI: http://dx.doi.org/10.1109/SocialCom-PASSAT.2012.106

저자 소개

김 현 수(정회원)

- 2010년 : 카네기멜론 대학교 전자공학과 졸업(학사)
- 2013년 : 연세대학교 정보대학원 졸업(석사)
- 2016년 ~ 현재 : 국방과학연구소 연구원