디지털산업정보학회 논문지 제13권 제3호-2017년 9월
http://dx.doi.org/10.17662/ksdim.2017.13.3.019

자가적응모듈과 퍼지인식도가 적용된 하이브리드 침입시도탐지모델*

이 세 열**

An Hybrid Probe Detection Model using FCM and Self-Adaptive Module

Lee Seyul

〈Abstract〉

Nowadays, networked computer systems play an increasingly important role in our society and its economy. They have become the targets of a wide array of malicious attacks that invariably turn into actual intrusions. This is the reason computer security has become an essential concern for network administrators. Recently, a number of Detection/Prevention System schemes have been proposed based on various technologies. However, the techniques, which have been applied in many systems, are useful only for the existing patterns of intrusion. Therefore, probe detection has become a major security protection technology to detection potential attacks. Probe detection needs to take into account a variety of factors ant the relationship between the various factors to reduce false negative & positive error. It is necessary to develop new technology of probe detection that can find new pattern of probe. In this paper, we propose an hybrid probe detection using Fuzzy Cognitive Map(FCM) and Self Adaptive Module(SAM) in dynamic environment such as Cloud and IoT. Also, in order to verify the proposed method, experiments about measuring detection rate in dynamic environments and possibility of countermeasure against intrusion were performed. From experimental results, decrease of false detection and the possibilities of countermeasures against intrusions were confirmed.

Key Words : Cloud, FCM, Hybrid Probe, IoT, SAM

Ⅰ. 서론

오늘날 컴퓨터의 발전과 함께 이슈가 된 것은 바이러스, 웜 그리고 랜섬웨어 등과 같은 악성코드 관련이며 인터넷과 네트워크의 확장 및 성장으로 함께 이슈가 된 것은 침입과 관련된 해킹 및 정보보안 관련 측면일 것이다. 이로 인하여 여러 자동화된 정보보안 대안이 개발되고 일선현장에 적용되고 있다. 또한, 인터넷 사용자 환경은 편리성 및 이동성이 강조된 환경으로 점점 변해가고 있는 추세이다. 그러나 이러한 사용자 환경을 지원하기 위하여 각종 서

* 본 논문은 2015학년도 청운대학교 학술연구조성비 지원에 의해 수행되었음.
** 청운대학교 컴퓨터학과 교수

버, 클라우드, 단말기기 등은 기하급수적으로 늘어가고 있으며 반대로 매일 새로운 하드웨어 및 소프트웨어의 취약점과 새로운 공격형태가 나타나는 등 보안취약점 및 보안위협은 늘어가고 있는 추세이다. 특히, 해킹공격으로 인하여 사회기반 시설 및 사회구성원들의 피해는 날이 갈수록 피해정도가 크게 발생하고 있어 이를 위한 대안 등에 많은 투자와 연구가 진행 되고 있다.

이러한 새로운 형태의 해킹공격에 대한 방어대책으로 데이터마이닝, 패턴인식, 네트워크 세션분석, 퍼지 논리, 신경망, 전문가 시스템 등을 적용한 탐지기법이 연구되었고 탐지율과 효율성을 높이기 위한 여러 방법들이 지속적으로 연구되고 있다. 그러나 기존 의 탐지기법 중 네트워크 기반의 탐지기법은 정적인 특징을 가지는 룰(rule)을 기본적으로 사용하기에 사물인터넷 및 클라우드 이슈 이전의 환경에서는 크게 문제가 되지 않았으나 최근 동적인 환경을 가지는 사물인터넷 및 클라우드 같은 새로운 이슈의 등장으로 동적인 환경에 맞는 탐지기법을 고려할 수밖에 없는 실정에 이르렀다. 정적인 특징을 가지는 네트워크기반 탐지기법은 동적인 환경 변화를 고려하기에는 한계가 있으며, 이러한 한계는 탐지성능 저하로 이어 질 것이다.

그러므로 오늘날은 네트워크 기반 탐지에 동적인 환경을 고려 할 수 있는 방법이 필요하게 되었고 이에 본 논문에서는 기존 연구되었던 정적인 특징을 이용한 기존 탐지기법과 성능비교를 위하여 저자가 개발한 적응형 퍼지인식도가 적용된 침입시도탐지기법에 추가로 동적인 환경을 고려할 수 있는 자가적응 모듈(Self Adaptive Module)을 사용하여 동적인 환경 변화를 고려하기 위한 적응형 룰(rule)을 생성하고 이를 퍼지인식도가 적용된 침입시도탐지에 추가하는 하이브리드 침입시도탐지모델을 제안한다.

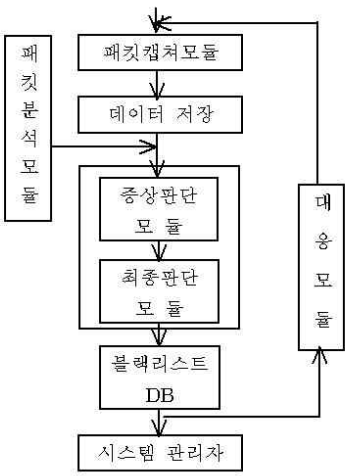
자가 적용 모듈은 Monitor, Analyze, Plan, Execute의 컴포넌트로 구성되며 각 컴포넌트는 환경 적응형 네트워크의 시스템 환경 정보의 수집, 임계값을 적용한 환경 변화 식별, 비정상적인 환경 변환 식별, 발생 가능한 공격 유형 식별, 공격 유형에 맞는 기법 수행 및 적응 값 생성, 환경 적응형 룰이 적용된 탐지기법이다.

본 논문의 구성은 다음과 같다. 2장에서는 관련연구에 대하여 살펴보고, 3장에서는 제안한 동적 적응형 침입시도 탐지 및 실험을 다루며 마지막으로 4장에서는 결론과 향후 과제를 논한다.

Ⅱ. 관련연구

2.1 기존의 네트워크 기반 침입탐지

기존의 네트워크 기반 침입탐지는 조금씩 형태와 구성의 차이는 있으나 대부분 <그림 1>과 같이 여러 모듈 구조로 이루어져 있다[1].



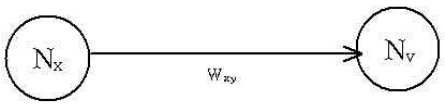
<그림 1> 기존의 네트워크기반 탐지모듈구조

전체적인 구조는 들어오는 패킷을 이용하여 패킷

을 분석하고 제어하는 모듈과 데이터저장, 판단모듈, 대응모듈이 있다. 여기에 패킷캡쳐모듈은 패킷 파싱을 통하여 수집된 파라미터를 패킷 판단모듈로 보내어 정상과 비정상 패킷으로 1차 구분하며 비정상 패킷은 기존 룰을 기반으로 하는 판단모듈을 통하여 블랙리스트 DB에 저장되고 이런 일련의 과정을 통하여 재차 공격시 블랙리스트 DB와 각 패킷의 구성 파라미터의 비교를 통하여 탐지하고 대응모듈을 가동하게 된다.

2.2 퍼지인식도가 적용된 침입시도탐지

탐지모듈 중 판단모듈에 퍼지인식도(Fuzzy Cognitive Maps : FCM)의 Causal Knowledge Reason(CKR)을 이용하여 지능적 판단모듈구조를 설계한다. 퍼지인식도는 주어진 문제영역내의 각 개념들 사이에 존재하는 인과관계를 나타내는 방향성 그래프이다. <그림 2>는 퍼지인식도를 표현한 것으로써 각 노드와 노드 사이의 가중치가 Wxy=0인 경우에는 각 노드사이에는 아무런 관련이 없는 것을 의미하며 Wxy≠0 경우에는 <그림 2>의 설명과 같은 의미를 부여한다. 단순한 퍼지인식도에서는 인과관계 가중치는 {-1, 0, 1}로 취할 수 있다. 따라서 이 경우의 인과관계는 최대/최소의 정도를 발생한 것을 의미한다[2, 3].

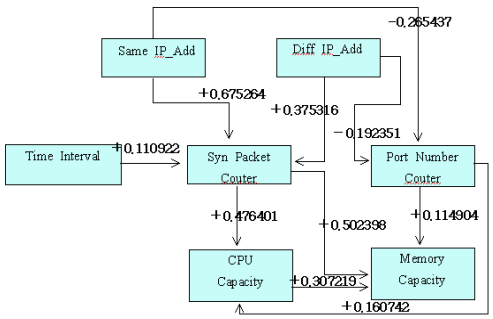


W_{xy}>0 ; N_x 수치 증가로 인한 N_y 수치 증가인 경우

W_{xy}<0 ; N_x 수치 증가로 인한 N_y 수치 감소인 경우

<그림 2> 퍼지인식도의 개념

판단모듈에서는 여러 파라미터 중 어떤 파라미터에 의존성을 부여함으로써 가장 최적의 탐지를 할 수 있는 것이 가장 큰 관건이다. 그뿐만 아니라 탐지한 파라미터를 침입시도로 간주하고 블랙리스트 DB에 저장하여야 하는지도 결정하여야 한다. 퍼지인식도는 이러한 여러 가변 파라미터의 인과관계에 가중치를 적용하여 최적의 판단을 내리게 된다. <그림 3>은 적응적 가변파라미터를 적용된 퍼지인식도 판단모듈을 나타낸 것이다[4-6].

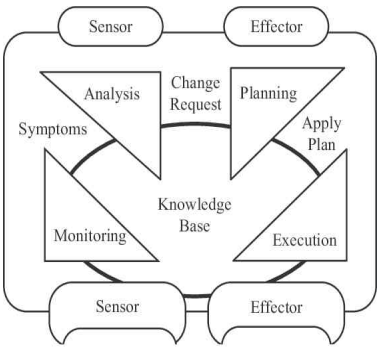


<그림 3> 퍼지인식도가 적용된 가변파라미터

2.3 자가 적응 모듈(SAM)

자가 적응 모듈의 대표적인 것으로는 IBM에서 제안한 MAPE-K를 사용한다[7, 8]. MAPE-K는 크게 4개의 구성요소를 가지고 있으며 Monitor, Analyze, Plan, Execute이다. Monitor는 환경변화를 감시 및 정보를 수집하는 요소로써, MAPE-K에서 대상으로 하는 시스템의 환경을 지속적으로 감시하고, 정보를 수집하는 작업을 수행하게 된다. 이때 수집되는 정보를 Managed Element라고 하며 사용자의 정의에 따라서 결정된다. Analyze는 Monitor로부터 수집된 정보를 분석하여 환경의 변화나 이상 징후들을 식별한다. 환경의 변화나 이상 징후들을 식별하는 방법은 Managed Element에 따라서 정의 할 수 있으며,

임계 값 또는 의사 결정 모델을 사용 할 수 있다. 또한, Analyze는 환경의 변화나 이상 징후가 식별 될 시 이에 대한 대응을 위하여 Plan으로 정보를 전달하는 역할도 수행한다. Plan은 Analyze에서 식별된 환경 변화나 이상 징후에 대응하기 위한 계획을 수립하는 것으로 서비스가 환경 변화나 이상 징후에 적응 할 수 있도록 서비스를 변경/생성하는 작업을 수행한다. Execute는 Plan에서 수립된 계획에 대해 실제로 동작을 수행한다. Plan에서 수립된 계획을 서비스로 생성하고 생성된 서비스를 시스템에 적용 시켜 MAPE-K의 수행 결과를 반영한다. 4개의 구성요소는 서로 연결되어 지속적으로 반복적으로 수행된다. 또한 4가지 주요 요소 이외도 Sensor, Effector, Knowledge등의 요소가 존재한다. Sensor는 Monitor 기능을 수행하기 위하여 실제 Element의 정보를 수집하고 Effector는 Execute의 동작 수행시, 변경된 서비스를 시스템에 적용하는 역할을 한다. Knowledge는 Monitor에서 수집한 정보를 저장하는 역할을 한다. <그림 4>는 MAPE-K의 구조이다.

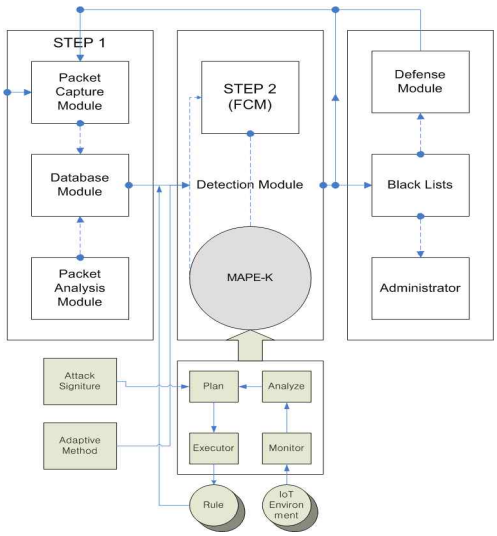


<그림 4> IBM의 MAPE-K 구조

Ⅲ. 자가 적응 모듈을 적용한 FCM

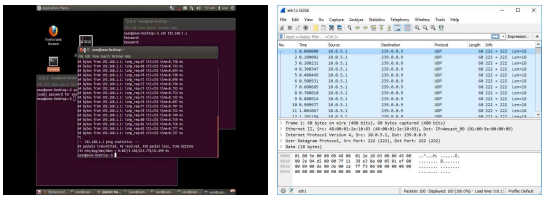
3.1 하이브리드 침입시도탐지

본 논문에서 제안하는 모델은 자가 적응 모듈이 적용된 FCM 기반의 하이브리드 침입시도탐지모델(FCM-Self)로써 <그림 5>이다. 제안한 방법의 검증을 위하여 전통적인 네트워크 기반 탐지시스템인 K-Means, Fuzzy-ART, SVM과 적응형 탐지시스템인 FCM과 자가 적응 모듈을 적용한 탐지율을 측정 및 비교를 통하여 측정한다. 정적인 환경측면 측정을 위하여 KDD CUP 99데이터를 이용한다[9, 10].



<그림 5> 자가 적응 모듈이 적용된 FCM 기반 하이브리드 침입시도탐지 구조

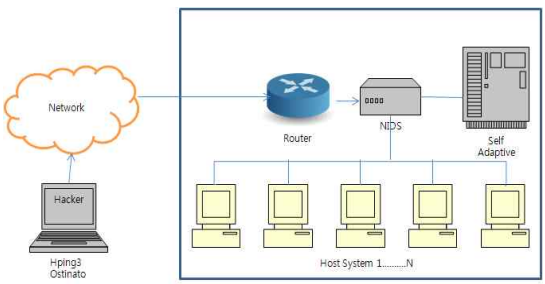
동적인 환경측면 측정을 위하여 모의 침투 테스트 도구로써 <그림 6>과 같은 Hping3과 Ostinato Ver. 0.8를 이용하였다[11, 12].



<그림 6> 모의테스트도구 Hping3과 Ostinato Ver.0.8

실험환경은 <그림 7>과 같이 Windows 8 64bit, Snort2.9.9, Winpcap 4.1.2이며 동적인 환경에서 외부 침입에 대한 탐지율 측정과 침입에 대한 대응 가능성을 확인하기 위한 실험으로 모의 침투 테스팅(Penetration Testing)을 이용하였다.

실험에서 사용한 환경은 Free, Normal, Busy로 정의하고 각 환경의 범위는 Sensor가 수집한 환경정보의 평균값을 이용하여 설정한다. 또한, 모의 침투 테스팅은 다양한 침입 방법을 사용하여 수행이 가능하지만 본 논문에서는 다양한 침입 방법 중 DoS 공격을 이용하여 실험을 진행하며 모의 침투 테스팅을 위하여 다음과 같은 3가지 가정을 설정하고 DoS공격을 테스팅한다. Free한 환경에서는 900EA/sec의 패킷에서 DoS공격을 발생하며, Normal에서는 600EA/sec, Busy에서는 300EA/sec에서 DoS공격을 발생하다고 가정한다.



<그림 7> 테스트베드 실험환경

Ostinato 도구를 이용하여 여러 프로토콜을 가지는 패킷을 생성하여 탐지시스템에 전송하며 전송하는 패킷은 100~1000EA/sec로 설정한다. 이때, 기존 탐지시스템에는 Normal환경에서 DoS공격을 탐지하는 룰을 적용하며 동적 적응형에는 MAPE-K를 적용한 룰을 적용한다. 이후 기존방식과 동적 적응형을 서로 분석하고 Busy상태에서 Free 상태로, Free상태에서 Busy상태로 변화한 환경에서 각각 수행한다.

3.2 실험결과

본 논문에서 제안한 동적인 환경하의 자가적응모듈과 퍼지인식도가 적용된 하이브리드 침입시도탐지모델(FCM-Self)은 <그림 8>에서 보듯이 기존의 여러 가지 탐지기법 중 K-Means, Fuzzy-ART와는 차이가 많이 발생하였다. 또한, 여러 실험 및 평가에서 탐지능력이 인정된 SVM(Support Vector Machine), 그리고 저자의 기존 FCM 탐지기법과도 차이가 발생하였다. False Positive 에러율은 기존의 여러 가지 탐지기법에 비하여 월등히 성능이 우수함을 알 수 있으며 저자의 기존 FCM을 적용한 Probe 탐지방법보다 전반적으로 개선되었음을 확인할 수 있다.

<그림 8> 동적측면에서의 정상탐지율과 오탐지 비교

<그림 9> 정적측면에서의 정상탐지율과 오탐지 비교

또한, 정적측면에서의 탐지 성능의 결과는 <그림 9>에서 보듯이 동적측면에서의 탐지 성능의 결과보다는 탐지 성능의 차이가 기존의 탐지기법 대비 성능차이가 줄었으나 탐지 성능이 개선되었음을 확인할 수 있다.

Ⅳ. 결론

본 논문에서 기존의 네트워크 기반 침입 탐지 시스템이 동적인 환경 변화를 고려하지 못하는 한계를 해결하고 이를 통하여 탐지 성능을 개선하기 위하여 진행되었다. 제안한 방법에서는 동적인 환경 변화에 적용하기 위한 방법으로 자가 적응 모듈을 적용한 IoT환경 적응형 하이브리드 침입시도탐지모델을 제안하였다. 이를 위하여 자가 적용을 위하여 MAPE-K를 통하여 구현하였으며 주요요소인 Monitor, Analyze, Plan, Execute를 이용하여 환경 변화 정보를 수집 및 분석하고 변화된 환경에 적응하기 위한 환경 적응형 룰을 생성했다. 자가 적응 모듈을 통하여 생성된 룰은 환경 변화에 맞는 탐지 정보를 가질 수 있었으며, 이러한 룰을 기존 침입탐지 룰에 적용함으로써 동적 환경을 고려한 동적 적응형 침입시도탐지모델이 기존의 침입탐지시스템 보다 탐지 성능이 개선되었음을 확인 할 수 있었다.

그러나 제안방법에서 사용한 룰을 생성하기 위해서는 모델이 정의되어 있어야 한다는 가정이 필요했다. 이러한 한계를 해결하기 위하여 향후연구에서는 자동으로 룰을 생성하기 위한 방안에 대하여 연구가 요구된다.

참고문헌

[1] B. Mukherjee, “Network intusion detection,” IEEE Network, Vol. 8, No. 3, 1994, pp. 26-41.

[2] M. Stula, “Fuzzy cognitive map for decision support in image post-processing,” 18th International Conference on systems signal and image processing, Vol. 11, 2011, pp. 4-9.

[3] S. Lee, Y. Kim, and B. Lee, “A Probe Detection Model using the Analysis of the Fuzzy Cognitive Maps,” International Conference Cyber and Security, Vol. 3480, 2005, pp. 320-328.

[4] J. Park, and M. Park, “A Whitelist-based Scheme for Detecting and Preventing Unauthorized AP Acess using Mobile Device,” Journal of the Korea Information Communications Society, Vol. 10, No. 3, 2012, pp. 632-640.

[5] W. Xiang, “Application of BP neural network with L-M algorithm in power transformer fault diagnosis,” International Power system protection and control, Vol 10, No. 1, 2011, pp.

100-104.

[6] S. Y. Lee, “An Adaptive Probe Detection Model using Fuzzy Cognitive Maps,” Ph. D. Dissertation, Daejeon University, 2003.

[7] Y. Brum, G. Serugendo, and M. Litoiu, “Engineering Self Adaptive Systems through Feedback Loops,” In Software Engineering for Self Adaptive Systems, Springer-Verlag, 2009, 2013, pp. 48-70.

[8] J. Moon, and Y. Chang, “A Malware Detection Application Framework Based on Normal Behavior,” The Journal of the Convergence on Culure, Vol. 2, No. 1, 2016, pp. 79-85.

[9] 조성래·성행남·안병혁, “의사결정트리와 인공 신경망 기법을 이용한 침입탐지 효율성 비교 연구,” 디지털산업정보학회논문지, 제11권, 제4호, 2015, pp. 33-45.

[10] 양환석, “프로토콜 기반 분산 침입탐지시스템 설계 및 구현,” 디지털산업정보학회논문지, 제8권, 제1호, 2012, pp. 81-87.

[11] Ostinato: http://ostinato.org/

[12] Hping3: http://tools.kali.org/

■ 저자소개 ■

이 세 열
(Lee Seyul)

2004년 3월 ~현재
청운대학교 컴퓨터학과 교수
2000년 1월 ~2001년 2월
인소콱(주)부설연구소 연구소장
2003년 8월 대전대학교 대학원 컴퓨터공학과
(공학박사)

관심분야 : 정보보안, 사물인터넷 보안,
네트워크보안, 시스템보안,
보안관제시스템, Web of Things
E-mail : pirate@chungwoon.ac.kr

논문접수일 : 2017년 08월 25일
수 정 일 : 2017년 09월 06일
게재확정일 : 2017년 09월 07일