The effects of Artificial Intelligent on online Intrusion Detection System

Article · December 2015

Muzhir Al-Ani
University of Human Development, Sulaymaniyah

International Journal of Business and ICT
Edited in association with the American Society of Competitiveness
December 2015, Vol.1, No.3-4
ISSN 2412-9917 www.IJBICT.com

The effects of Artificial Intelligent on online Intrusion Detection System

Khattab M. Ali Alheeti[1]
School of Computer Sciences and Electronic Engineering
University of Essex, Colchester, United Kingdom
University of Anabr – College of Computer - Anbar -Iraq

Muzhir Shaban Al-Ani[2]
College of Computer, CS Department,
Anbar University, Anbar, Iraq

Abd Al-Karim Al-Aloosy[3]
College of Computer, IS Department, Anbar University, Anbar, Iraq

Abstract

The intelligent intrusion detection system is an interesting approach which is designed to protect host/network systems from the potential attacks. The intrusion detection system is the most important techniques that were used to improve system security and reduce the number of attacks. In our paper, we propose an intelligent intrusion detection system (IDS) to improve the detection rate and decline the false alarms that generated from the proposed detection system. The detection process based on KDD - Cup 2000 benchmark data that collected by Defense Advanced Research Projects Agency (DARPA). In other word, the detection system depends on the features that described the normal/ abnormal behavior of the network /host system as well as we used a significant feature which reflected behavior in real–world. The online detection is considered main contribution in our proposal security system. The proposed IDS utilize soft computing techniques such as Self-Organizing Map (SOM) and Backpropagation neural network. The experimental result shows the efficiency and effectiveness of the proposed system in the protection and deterrence.

Keywords: Security, intrusion Detection, artificial intelligence, neural networks.

I. Introduction

The progress and successful the research project heavily depend on achievements of security system. In other words, each online model cannot establish its work without sufficient protection to secure the data and sensitive information from any potential attacks. Basically, we can be divided the security system into two layers are:

- First layer: Prevention layer.
- Second layer: Detection layer.

As we know, the first security layer has the ability to secure the networks/hosts from any external attacks, but they cannot prevent or detect any internal attacks such as encryption/decryption [1]. At this point, we need to detection system to secure and detect each internal attack that try to apply unathentication access to the important data.

In our paper, we design an intelligent intrusion detection system (IDS) to identify and block each internal intruder. The IDS has a vital role in providing a sufficient security for the networks/host systems. It has been used to secure a sensitive information systems along with prevention based mechanisms such as authentication and access control [2]. The contribution mainly addresses the issue of online identifying a significant input feature for intrusion detection system. Our proposed IDS has the ability to online detect and block each malicious connection on online application as well as reducing the number of features from the trace file. The total of extracting features is 41 that describes the normal and the abnormal behaviour on the system. However, we reduce the number of the features to reasonable number to enhance the detection rate and decline the number of false alarms.

In other words, the reduction of number features helps to save size, faster training and possibly more accurate results, it is critical to be able to identify the important features of network traffic data for intrusion detection in order to get a maximal performance of the proposed IDS. In our experiments, we used the benchmark that was originated from MIT's Lincoln Lab [3]. The KDD 2000 was developed for intrusion detection system evaluations by DARPA and is considered a benchmark for intrusion detection evaluations [3]. We utilize the Artificial Intelligent (AI) in designing the IDS because of it plays an important role in a built-in security system such as neural network and fuzzy logic. We apply experiments to measure the rank the importance of input features for each of the five classes (Normal, Probe, DOS, U2R, and R2L) of patterns in the DARPA benchmark. The high weight features directly reflect on classification, reduces the training time and testing time of the intelligent classifier.

We would like to mention some direct and indirect relate works. All related works target to improve the security system of the host/networks.

Ali and et al. present security system to secure sensitive data from the potential attacks. The security system based on Fuzzy Petri Net (FPN) to identify and malicious connection that try to get illegal access to the control or private data [4].

Ali and et al. have been proposed offline security system to protect smart card from attacks. This system based on the same data that extracted from the KDD 2000. It can provide sufficient security to users of the smart card from any fraud or illegal online access from abroad [5].

II. Introduction to Intrusion Detection System

Intrusion detection systems (IDSs) were designed for integrated prevention-based security measures. An intrusion is defined as a violation of the protection policy of the system [6]. The IDS refers to the approach are developed to identify and block any malicious behaviour in external or internal communication of the systems. The IDS to integrated to the existing security system such as a firewall by achieving crucial information to administrators about type of intruders that may be undetected by traditional security technologies. These systems have the ability to provide an important information that will allow administers to trace back the origins of attacks and aid in the prosecution of the attackers.

In general, the IDS divide into two types based on data detection: *Anomaly-based* detection and *misuse based*- or signature-based detection. Signature detection systems match incoming network traffic to a database of known attack signatures to detect intrusions. While an anomaly detection system enjoys a high rate of success at detecting known attacks, they are ineffective in detecting new or unknown attacks. However, pre-know detection system establish a normal profile for each the node in the network and it consider any behaviour deviations from the normal profile as probable intrusions. The anomaly systems predict anomalous behavior and can detect new and novel attacks [7].

IDS's need to reach to the good step in secure online system because they have problem to provide the sufficient security to block and detect any illegal access to the sensitive data and information. The motivation of this research to provide intelligent IDS that has ability to detect a novel attack.

Moreover, we use the best 12 features that were selected from the whole data set, 41 attributes that describe the different features of the corresponding connection (19 of them describe the properties of connections to the same host in the last two seconds and 22 of these features describe the connection itself).

III. The Data Set

The benchmark used in evaluating performance of the proposed IDS is collected from the DARPA KDD cup 2000 [3]. It was set up to acquire raw TCP/IP dump data for a network by simulating a typical U.S. Air Force LAN. The LAN was operated like a true environment, but being blasted with multiple attacks. They contain from 494021 records and each record composed from the 41 features that describe the time, type communication between nodes. More than 20% of data describe the normal connection [8]:

The malicious pattern divided into four main categories:
1. DoS: Denial of Service.
2. R2L: unauthorized access from a remote machine.
3. U2R: unauthorized access to local super user (root) privileges.
4. Probing: surveillance and other probing.

IV. Ranking of Inputs Features

The number and type of the features are an important issue in the proposed IDS. We have 41 features that describe the normal and malicious behaviour of the host/networks system.

Which are truly useful, which are less significant? The question is relevant because the elimination of useless audit trail reduction enhances the accuracy detection while speeding up the computation, thus improving the overall performance of an IDS. We can reduce the number of features and improve the performance of the proposed IDS without affecting the accuracy of detection in statistically significant ways.

A. Data filtering

The data filtering is very important to reduce the amount of data that used to design the IDS. This date has some features may be not useful to the IDS and thus we should eliminate before design security system. Reducing the number of the features has many benefits such as:

- Decreasing storage space.
- Reducing processing time.
- Improving the detection rate.

B. Feature selection

Some features may be hindered or have a direct negative impact on detection process. At the same point, extra features can increase computation time as well as negative impact on detection accuracy [3]. We based on trial-and-error to select the best and highest weight of features from the DARPA. The selection of features depends on the type of the IDS, such as a Network intrusion detection system (NIDS) try to analyse information related to packet, type of protocol and duration of connection etc.

V. The Proposed Model IDS using Neural Networks

In our research, we selected 12 high rank of features in design IDS using Artificial Neural Networks (ANNs). These features have more influence in the accuracy detection to protect the networks/host system from the external and internal attacks.

The proposed security system has the ability to divide the output into five classes: Normal, Prob, DoS, U2R and R2L that is shown in the figure 1.

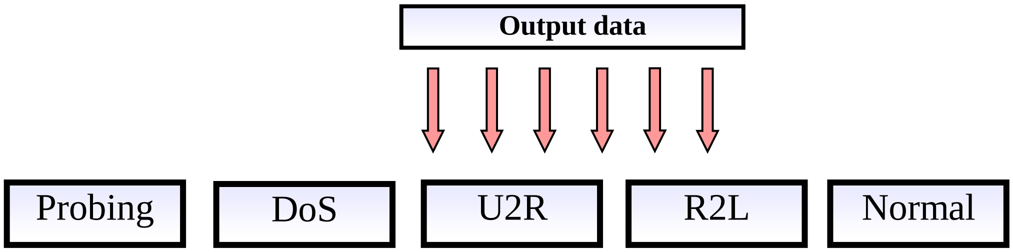

Figure 1 Shows the output

The steps below explain methodology for proposed security system:

- Collect Benchmark KDD 2000 from DRAPA.
- Data Set transformation.
- Uniform Selection.
- Normalization.
- Training and test data with ANNs.
- Then identify the significant features.

The life cycle of proposed IDS is shown in figure 2:

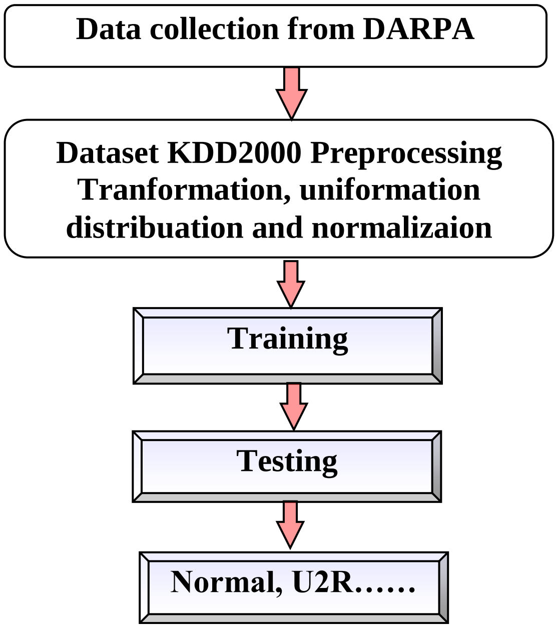
Data collection from DARPA
Dataset KDD2000 Preprocessing Tranformation, uniformation distribuation and normalizaion
Training
Testing
Normal, U2R……

Figure 2 shows Architecture of IDS

VI. Experiments and Results

In this subsection, we evaluate the performance of the proposed IDS. The result of train the proposed security system as shown in table 1.

Table 1 Performance Materics for all features

Attack Class	41 – Features data set		
	Train(s)	**Test (s)**	Accuracy (%)
Normal	1.20	0.18	**99.75%**
Prob	1.35	0.04	**96.20%**
DOS	3.22	0.10	**99.21%**
U2R	1.12	0.03	**46.00%**
R2L	**1.21**	**0.01**	**91.52%**

The main problem with 41 detection system with U2R attack, it does not have the ability to detect this type of attacks. Now, we are testing the IDS with significant features that have been extracted from KDD2000. Table 2 shows the performance metrics or IDS with 12 features:

Table 2 Performance of classification for 12 features

Attack Class	12 – Fatures data set		
	Train(s)	**Test (s)**	Accuracy (%)
Normal	1.10	0.18	**99.81%**
Prob	1.30	0.04	**99.20%**
DOS	4.10	0.07	**99.01%**
U2R	1.05	0.03	**99.12%**
R2L	**1.44**	**0.02**	**97.4838**

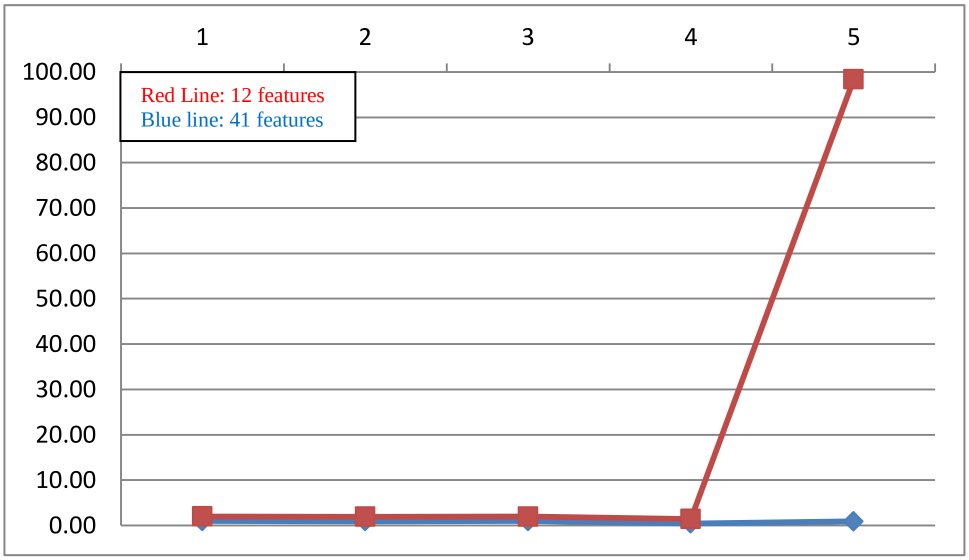

Figure 3. Comparison between 41 and 12 features

According to figure 3, we can easily notice the role of proposed IDS on detection U2R from 46% to 99% as well as the online detection is considered a big challenge to each security system. The alarm system is considered another indicator to measure the performance metrics for each proposed security system, as shown in table 3. Table (4) and table (5) show miss records and unknown records.

Table 3 alarm rate

Attack Class	The percent of Alarm Rate
True Positive	99.8434
True negative	100
False negative	0.1566
False Positive	0

Table 4 type of miss records

Attack Class	Miss Records
Normal	6
Prob	26
DOS	33
U2R	0
R2L	35
Unknown	**0**

Table 5 unknown records

Attack Class	Unknown
Normal	**6**
Prob	**0**
DOS	**31**
U2R	**0**
R2L	**18**

VII. Conclusions

We proposed an online intelligent detection system to protect sensitive information that connected with the external environment of the internet as well as was evaluated its performance on the DARPA benchmark intrusion detection. The security has the ability to predicate the future attacks on systems. The IDS with 12 features more efficient from the IDS with all features 41 as well as it needs less time to precess and less memory to store data. The modern technology encourages researchers to design efficient and effective detection system to secure this data because of so many systems directly connect to the internet. This property made them facing to different attacks such as DoS and different types of Sink hole attacks. The future work is design security system based on a fuzzy-neural network that has ability anomaly detection for any a novel attack.

References

[1]. K. M. Ali Alheeti, A. Gruebler, K. D. McDonald-Maier, (2016) "Prediction of DoS Attacks in External Communication for Self-driving Vehicles Using A Fuzzy Petri Net Model", accepted to ICCE 2016 - IEEE, Las Vegas, Nevada- USA.

[2]. K. Ali Alheeti, W. Venus, M. Suleiman, (2009) "Affect Fuzzication on Neural Networks Behavior as Intrusion Detector", the 4th IEEE Conference on Industrial Electronics and Applications (ICIEA 2009), ISBN: 978-1-4244-2799-4, to be held on May 25-27, Xi'an Chine.

[3]. Http://kdd.ics.uci.edu/databases/kddcup99/task.html.

[4]. K. M. Ali Alheeti, (2015) " The Affect of Fuzzy Petri Net on Feed Forward Neural Networks Intrusion Detection System ", Published in International Journal of Business and ICT Edited in association with the American Society for Competitiveness (IJBICT), Vol. 1, No.1, America.

[5]. K. M. Ali Alheeti, (2015) " A Novel Security System For Protection DataBase By Using Backprogration Algorithm", Published in International Journal of Business and ICT Edited in association with the American Society for Competitiveness (IJBICT), Vol. 1, No.1, America.

[6]. S. Chebrolu, A. Abraham, J. Thomas, (2005)" Feature detection and ensemble design of intrusion detection systems," Compute Secur; 24: 2005, pp. 295–307.

[7]. A. Patcha, J. Min Park, (2007) " Network anomaly detection with incomplete audit data," Bradley Department of Electrical and Computer Engineering, Elsevier.

[8]. MIT Lincoln Laboratory, http://www.ll.mit.edu.

Authors

[1]**Khattab M. Ali** was born in Anbar-Iraq in 1978. He received his B.Sc. from Al_M'ammon college university in 2000, Baghdad, Iraq. The MSc. degree from CS Department in Al al-Bayt University, Jordan 2008. Currently, he is a second year PhD student at the university of Essex, Colchester, UK. The research file is security external communication of self-driving and semi self-driving cars.

[2]**Muzhir Shaban Al-Ani** has received Ph. D. in Computer & Communication Engineering Technology, ETSII, Valladolid University, Spain, 1994. Assistant of Dean at Al-Anbar Technical Institute (1985). Head of Electrical Department at Al-Anbar Technical Institute, Iraq (1985-1988), Head of Computer and Software Engineering Department at AlMustansyria University, Iraq (1997-2001), Dean of Computer Science (CS) & Information System (IS) faculty at University of Technology, Iraq (2001-2003). He joined in 15 September 2003 Electrical and Computer Engineering Department, College of Engineering, Applied Science University, Amman, Jordan, as Associated Professor. He joined in 15 September 2005 Management Information System Department, Amman Arab University, Amman, Jordan, as Associated Professor, then he joined computer science department in 15 September 2008 at the same university. He joined in August 2009 Computer Science Department, Anbar University, Anbar, Iraq, as Professor.

[3]**Abdul Kareem A. Najem Al-Aloosy**, has received Ph.D., Polytechnic of Wroctaw, Wroctaw, Poland, 1992. He received training course in UTBM & Polytech Engineering School at Marseille - France 2006. He worked 1992 – 1994 lecturer at the Computer Engineering Department, College of Engineering, Sabha University – Libya. He worked 1995 – 1998 in private sector in engineering field. He worked 1999 -2003 Lecturer at the Computer Eng. Dept. College of engineering / Al Nahrain University – Baghdad. He worked 2004 – 2006 assistant head of Computer Eng. Department, College of Eng. / Al Nahrain University–Baghdad. He worked 2006 – 2009 head of Computer Eng. Department in Computer Man College in Sudan. He worked 2009 – 2011 associate professor in informatics college in Arab International University in SYRIA. 2011—till now he joining as head of information system department in Computer College/ Anbar University.