International Engineering Journal For Research & Development

Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

A NOVEL APPROACH TO ARTIFICIAL INTELLIGENCE FOR EFFECTIVE KIND OF CYBER SECURITY

Gaurav K. Wadnere
Department of Information Technology
P.R.M.I.T & R, Badnera
Amravati, INDIA
gauravwadnere@gmail.com

Aditya O. Sable
Department of Computer Science & Engineering
P.R.M.I.T & R, Badnera
Amravati, INDIA
adityasable89@gmail.com

Smeet D. Thakur
Department of Information Technology
P.R.M.I.T & R, Badnera
Amravati, INDIA
smeet87@gmail.com

Abstract-

Cyber infrastructures are vastly vulnerable to intrusions and other threats. Physical devices and human interference are not sufficient for monitoring and protection of these infrastructures. Cyber security is the main concern for today's digital world, there are still uncertainties about the impact of AI. Corporates and government sectors are trying to master AI and Machine Learning for the protection of data and creating more opportunities in the respective field. AI permits you to automate the finding of threat and combat even without the involvement of the humans. Controlling your data to stay more secure than ever. Since AI is totally machine language driven, it gives surety you complete error-free cyber-security services. Researchers have also started to put more resources than ever for boosting AI driven technologies. The most important component used to detect cyber attacks or malicious activities is the intrusion detection system (IDS). Artificial intelligence plays a vital role in detecting intrusions and widely considered as the better way in adapting and building IDS. This paper focuses on different current AI techniques that can be used in support of Intrusion Detection Systems to provide better Intrusion Detection & Prevention.

***Keywords*— Artificial Intelligence, Network Intrusion Detection and Prevention, Machine Learning, Cyber security, Network security**

I. INTRODUCTION

The Internet has become a part of daily life and an important tool today. It helps people in many areas, such as business, entertainment and education, etc. In particular, Internet has been used as an main component of business models. For the business process, both business and customers apply the Internet application such as website and e-mail on business activities. Thus, information security of using Internet as the media needs to be carefully concerned. Intrusion detection is one most important research problem for business and personal networks. As there are a lot of risks of network attacks under the Internet environment, there are various systems designed to block the Internet-based attacks. Mainly, intrusion detection systems (IDSs) aid the network to resist external attacks. That is, the goal of IDSs is to provide a wall of protection to confront the attacks of computer systems on Internet. IDSs can be used on detect difference types of malicious network communications and computer systems usage, whereas the conventional firewall cannot perform this task. Intrusion detection is based on the assumption that the behavior of intruders different from an authorized user. In general, IDSs can be divided into two groups: anomaly and misuse (signature) detection based on their detection approaches. Anomaly detection tries to find out whether deviation from the established normal usage patterns can be flagged as intrusions. On the other hand, misuse detection uses patterns of well-known attacks or weak spots of the system to recognize intrusions. Numbers of anomaly detection systems are developed based on several different machine learning techniques. For example, some studies apply single learning methods, such as neural networks, genetic algorithms, support vector machines, etc. On the other hand, a few systems are based on combining different learning techniques, such as hybrid or ensemble techniques. In particular, these methods are developed as classifiers, which are used to classify or recognize whether the incoming Internet access is the normal access or an attack [1].

Security personnel and everyone who has a accountability for providing protection for a network and its users, have serious concerns about intruder attacks. Network administrators try to provide a protected environment for users' accounts, network resources, personal files and passwords. Attackers may behave in two

ways to carry out their attacks on networks; one of these ways is to build a network service unavailable for users or violating personal information. Denial of service (DoS) is one of the most normal cases representing attacks on network resources and making network services unavailable for their users [2]. There are many types of DoS attacks, and every type has it is own behavior on consuming network resources to accomplish the intruder's aim, which is to render the network unavailable for its users [3].

Intrusion Detection System (IDS) becomes an important part for building computer network to capture these kinds of attacks in early stages, because IDS works against all intruder attacks. IDS uses classification methods to make decision about every packet pass through the network whether it is a normal packet or an attack (i.e. DOS, U2R, R2L, PROBE) packet [2].

II. THREAT ATTACKS

ISO 27005 defined threat as, "A potential cause of an accident, which may effect in harm of systems and organization." ENISA defined threat as, "Any circumstance or event with the potential to adversely impact an asset through unauthorized access, destruction, disclosure, modification of information, and/or denial of service." A threat maybe intended or sometimes accidental. Threats are hard and soft types of threats. The threats maybe categorized as-

A. Physical Threats

Physical threats may directly result in devastation of the computer systems hardware and infrastructure. Some of the internal threats include power supply, fire in the rooms, etc. Earthquakes or any natural disaster are types of external threats. As stated previous, most of the human threats are accidental or intentional.

B. Non-physical Threats

The non-physical attacks target the information and other software on our computer system. A few of the non-physical threats include virus, spyware, malware, adware, Trojans, phishing, DOS attacks, DDOS attacks, unauthorized computer access, etc [4].

III. OVERVIEW OF INTRUSION DETECTION SYSTEMS

Intrusion Detection is defined as the procedure of intelligently monitoring the events occurring in a computer system or network and analyzing them for signs of violations of the security policy [1]. The primary aim of Intrusion Detection Systems (IDS) is to defend the availability, confidentiality and integrity of critical networked information systems. Intrusion Detection Systems (IDS) are defined by both the method used to detect attacks and the placement of the IDS on the network. IDS may perform either misuse detection or anomaly detection and may be installed as either a network-based system or a host-based system. This results in four general sets: misuse- host, misuse-network, anomaly-host and anomaly-network. Misuse detection relies on matching known patterns of hostile activity against databases of past attacks. They are extremely effective at identifying known attack and vulnerabilities, but rather poor in identifying new security threats. Anomaly detection will look for something rare or unusual by applying statistical measures or artificial intelligence to compare current activity against historical knowledge. Ordinary problems with anomaly-based systems are that, they often require extensive training data for artificial learning algorithms, and they tend to be more computationally expensive, because several metrics are often maintained, and these need to be updated against every systems activity. Some IDS merge qualities from all these categories (usually implementing both misuse and anomaly detection) and are known as hybrid systems. Artificial Intelligence techniques have been applied both to misuse detection and also for anomaly detection. SRI's intrusion Detection Expert System (IDES) [2] encodes an expert's knowledge of known patterns of attack and system vulnerabilities as if-then rules. Time-based Inductive machine (TIM) for intrusion detection [3] learns sequential patterns. Recently, techniques from data mining area have been used to mine usual patterns from audit data [6,7,8]. Several approaches applying artificial neural networks in the intrusion detection system have been proposed [9,10,11]. NeGPAlM [12] based on trend analysis, fuzzy logic and neural networks to reduce and control intrusion. Existing intrusion detection especially commercial intrusion detection systems that must resist intrusion attacks are based on misuse detection approach, which means these systems will only be able to detect known attack types and in most cases they tend to be useless due to various reasons like non-availability of attack patterns, time consumption for developing new attack patterns, insufficient attack data, etc [5].

IV. IDPS TECHNOLOGIES AND ITS TYPES

Intrusion prevention is a threat prevention technology or network security, which observes network traffic, flows to detect and prevent susceptible traffic misuse. This deals with only the non-physical threats. The IPS often sits directly at the back of firewall and it provides a complementary layer of analysis that negatively selects for dangerous content. The Intrusion Detection System (IDS), different its predecessor—which is was passive system that scans traffic and reports back on threats—the IPS is placed inline (in the direct communication path between source and destination), actively analyzing and taking automated actions on all traffic flows that enter the network.

IDS computerize the intrusion detection process. IPS has the capabilities that IDS has and also helps in preventing those threats. The types of detection methodologies are:

1. Signature-based detection
2. Anomaly based detection
3. Stateful protocol analysis
4. Stateless protocol analysis.

In addition, the categories of IDPS systems are Network-based, Wireless, Network behavior analysis (NBA) and Host-based. The network traffic for exact network segments and devices are analyzed and monitored by Network-based technology.

Wireless does the similar thing except that it does for wireless network traffic. Network behavior analysis (NBA) identifies unusual traffic flows and observes network traffic such as malware. The actions and characteristics of a single host are identified and monitored by Host-based technology [4].

V. GOALS AND PROPOSED ARCHITECTURE

Our goal is to design and develop an Intelligent Intrusion Detection System. (IIDS) and Intrusion Prevention that would be accurate, not easily cheated by small differences in patterns, adaptive and be of real time.

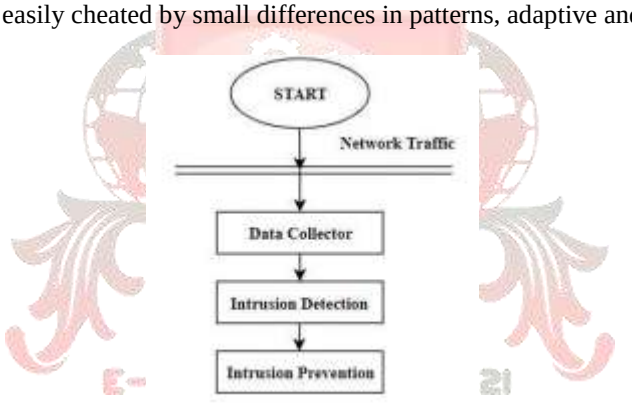

Fig. a) Basic steps for proposed method

Fig.a) shows basic steps for proposed method which consist of Intrusion detection and Intrusion prevention. The system consists of two main phases, as described in Figure 1. At data collector phase, we use SNORT [16], a. leading and well-known open source packet sniffer. The data processor and classifier summarizes and tabulates the data into cautiously selected categories i.e. the attack types are carefully correlated. This is the stage where a kind of data miniing is executes on the collected data [5].

At Intrusion detection phase, we use Neural Networks for intrusion detection. Neural Networks can be used to construct profiles of software behavior and make attempts to distinguish between normal and anomalous/malicious software behavior. The main objective in using Neural Networks is for the Intrusion Detection to be able to simplify from insufficient data and be able to classify between malicious and safe networks. An artificial neural network consists of processing units, or nodes, and connections between them. The connection between any two units has some weight, which is used to determine how much one unit will affect the other. By assigning activation (value) to each input value, and allowing the activations to broadcast through the network, a neural network performs a mapping from one set of values (assigned to the input nodes) to another set of values (retrieved from the output nodes). A classical feed-forward multi-layer perceptron rule can be used to make an intrusion detection system as given above. Also, back-propagation network is used

successfully in network intrusion detection since back-propagation is used for learning and this will help the Intrusion Detection System to construct and learn profiles of anomalous behaviors [13].

Intrusion prevention phase consist of 4 phases.

1) The sniffer phase: The first phase starts with a packet sniffer that utilizes Winpcap tool[11], which capture packets from the network with different levels of detail and display them on the control unit in the next phase in order to examine data from a live network or from a capture file on a disk.

2) The NIPS phase: This phase includes numerous actions; it starts with analysis of the captured packet, then takes the appropriate decision, such as passing or dropping, and logs it into a file (storing the log file in an offline DB) based on a set of rules defined in the Snort tool.

3) Advanced analysis phase: This phase generates new rules which help to improve defined rules that were used in the previous phase. Data mining algorithms is used due to their effectiveness in working with a vast database, would help an analyst to discover new rules from hidden traffic behaviour between the source and the destination, which the Snort tool cannot see as obvious rules. In order to do this; two sub-phases of the Data Mining approach will be relied upon. The first sub-phase is an improved K-mean algorithm to categorize the log file of the Snort tool to clusters in an effective manner. Records will be taken from the resulting clusters as an input to the second sub-phase, which is the FP-growth algorithm that will generate the frequent patterns to these records, which in turn will help to create new rules from these patterns, leading to improvements to the Snort tool. The use of Data Mining techniques to analyse the collected data in an offline database is important in performing NIPS because all connections have already over; therefore, these techniques can process and check all features without dropping packets when flooded with data, resulting in a faster process and increasing the performance and accurateness of NIPS [8, 10].

4) Control Analyst Interface: This final phase is used to decide recent rules that enable anomaly detection. It also takes suitable decisions about the new rules, which lie in the middle of clustering. In addition to updating the proposal, a smart new rule file will be searched for in case normal traffic has still not resumed or there is suspicion about the appropriate actions [14].

VI. CONCLUSION AND FUTURE WORK

AI is considered as a standout amongst the most encouraging development in the information age and cyber security. New techniques, algorithm, tools and enterprises offering AI based services are constantly rising with respect to the worldwide security showcase. This proposed work has the following two contributions. First, this paper provides a intrusion detection by using neural network to improve their capability to detect intrusion. Second it proposes a novel approach to select best feature for intrusion prevention. The proposed system speeds up the detection of attacks and malicious code that are targeted to the security system with high accuracy and real-time. So the proposed system can be used to detect and prevent attacks over networks where security matters. Future works includes, as for detection, some evolutionary algorithms such as genetic algorithm or immune algorithms approaches can be combined with it.

REFERENCES

C. Tsai, Y. Hsu, C. Lin and W. Lin, “Intrusion detection by machine learning: A review,”, , pp. 1–7,2009.

M.Alkasassbeh, and M.Almseidin, “Machine Learning Methods for Network Intrusion Detection,”, , pp. 1–7,2018.

[3] N. Huy and C. Deokjai, "Application of data mining to network intrusion detection: classifier selection model," Challenges for Next Generation Network Operations and Service Management, pp. 399--408, 2008.

[4] S. Das, and M. Nene, “A Survey on Types of Machine Learning Techniques in Intrusion Prevention Systems,”, , pp. 1–4,2017

[5] N Idris, and B. Shanmugam, “Artificial Intelligence Techniques Applied to Intrusion Detection,”, IEEE Indicon 2005 Conference INDIA , pp. 1–4,2005.

[6] Lee, Stolfo S., Mok K., "Mining audit data to build data to build intrusion detection models," Fourth international conference on knowledge

discovery and data mining, New York, AAAI Press 66-72, 1998

[7] Mukkamala, R., Gagnon J., Jaiodia S., "Integrating data mining techniques with intrusion detection methods", Research Advances in Database and Information systems security, 33-46, 2000

[8] Stolfo S., Lee, Chanm,"Data mining-based Intrusion detectors: An overview-of the Columbia IDS", Project SIGMOD Record, Vol 30, No 4,2001

[9] Debar, Becker M., Siboni D., "A neural network component for an intrusion detection system," IEEE Computer Society Symposium on Research in Computer Security and Privacy, 240-250, 1992

[10] Tan K., "The Application ofNeural Networks to UNIX Computer security", IEEE International conference on Neural Networks Vol 1, 476-481, 1995

[11] Wang J., Wang Z., Dai K., "A Network intrusion detection system based on ANN", InfoSecuO4, ACM 2004(ISBNI-581 13-955-1)

[12] Botha M., Solms R., Perry K., Loubser E., Yamoyany G., "The utilization of Artificial Intelligence in a Hybrid lntrusion Detection System",

SAICSIT, 149-155, 2002

[13] K. Napanda, and H. Shah, L. Kurup, "Artificial Intelligence Techniques for Network Intrusion Detection",IJERT, 2278-0181, Vol. 4 Issue

11, 2015

[14] A.Hamami, and G.Saadoon, "Development of a Network-based Intrusion Prevention System using a Data Mining Approach",Science and

Information Conference, London,pp. 1-4,2013