TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 5734 - 5738

Survey of Bio-Inspired Techniques based on System Resource Usage in Intrusion Detection

[1]Inadyuti Dutt, [2]Samarjeet Borah, [3]Indrakanta Maitra
1Department of Computer Applications, Sikkim Manipal Institute of Technology Sikkim Manipal University, Majhitar, East Sikkim-737136, inadyuti@gmail.com
2Department of Computer Applications, Sikkim Manipal Institute of Technology Sikkim Manipal University, Majhitar, East Sikkim-737136, samarjeetborah@gmail.com
3B. P. Poddar Institute of Management & Technology, MaulanaAbulKalam Azad University of Technology, Kolkata, West Bengal-700052, ikm1975@yahoo.com

Article Info
Volume 82
Page Number: 5734 - 5738
Publication Issue:
January-February 2020

Article History
Article Received*: 18 May 2019*
Revised*: 14 July 2019*
Accepted*: 22 December 2019*
Publication*: 28 January 2020*

Abstract:
The presented work is a study of literatures inspired by nature and natural organisms in detecting intrusions. The study takes into consideration the usage of system resources of a computer or a network. The paper focuses on the notion that intrusion and intrusive activities are less frequent in comparison to the normal activities of a system. And in order to capture such intrusive activities, there must be a provision for incorporating an intrusion detection system that can constantly examine the day-to-day activities of the system. Therefore, an intrusion detection system would check the system activities by keeping a log or account of the system behavior. To ascertain whether the activity is normal or not, one has to monitor the system behavior based on the system resources being utilized. Resource usages can be captured to check the currently running programs, their network bandwidth usages, memory usage, processor usages etc. Similarly, user-based behaviors can be obtained from their login frequency or the number of password attempts to a known system. All these behaviors can be taken into consideration for further validating the assumption that whether an intrusion has actually occurred or not. This paper presents some literatures inspired by nature and natural organisms. It emphasizes on the literatures based on some biological principles.

Keywords: *Intrusion Detection System, Resource usage, Immune System, Multi-agents, Honey bee algorithm.*

1. Introduction

For the last two decades, there has been an immense advancement in Internet and its services. Number of users of internet and its facilities across the world has increased tremendously in the last decade. Internet and communication has become synonymous to each other. With the increase in such facilities, the computers have become prone to several threats and exploitation. As more and more number of private networks gets connected to the public network, Internet, these private computers have become susceptible to viruses and other network prone attacks. Therefore, both the internet as well as intranet is exposed to threats that are network-prone. In order to address this issue, firewalls have been introduced to monitor the external access with that of the internal access. These firewalls help the network administrator to introduce a common check point that restricts the illegitimate accesses by the hackers, spies to enter or leave the protected network.

An IDS (Intrusion Detection System) is another tool or software that has been introduced to address the issues of network threat. However, IDS is a different breed than a firewall. Its main concept is based on detection rather than prevention. It focuses on the idea that when and under any circumstances if the preventive measures fail to restrict the outside attacks, IDS is able

January - February 2020
ISSN: 0193 - 4120 Page No. 5734 - 5738

to spot those attempts or intrusions. IDS are software tools that monitor, keep a log of the network activity and apply detection algorithms for detecting intrusions in a network [1]. The IDS analyzes the real-time data of network traffic and tries to detect the unauthorized access not only from the Internet but also from the intranet services. It tries to keep a log of overall network activities that arrive from the Internet and also user behavior in the intranet.

There are primarily two approaches of IDS, Host based i.e. HIDS and Network based i.e. NIDS. In HIDS, the data is collected from a host or a server (for example, host or server traffic analysis log files) while in NIDS the data arrives directly from the network. These two are further classified into signature-based and behavior-based IDSs.

In signature-based IDS, attack signatures are stored in a repository and are constantly checked with the current network activity or event. Such type of IDS examines the real-time traffic against the attack signatures in the database. The major problem that this type of IDS faces is that the signature database has to be constantly updated and if a signature-definition is too specific then the IDS may miss the variation. These systems are unable to detect attacks that are totally new or unknown in appearances [2].

In behavior-based IDS, the main objective is to capture normal behavior of the network. Then the IDS is introduced to find out whether the ongoing traffic deviates from the normal network or not. Any deviation would signify that an anomalous behavior or activity has taken place. This type of IDS is able to identify attacks that get unnoticed in signature-based IDS [2]. Behavior-based model works well for systems where the normal traffic is already known. For this the model needs to first ascertain the normal traffic in order to find out the deviation of the incoming traffic from it. In most of the cases, it becomes difficult to determine the traffics that can be considered as the normal ones.

1.1 Resource Usage: Normal and Abnormal Behaviors

The behavior of a system has to be constantly monitored for inferring whether the behavior is normal or not. It can be inferred that the behavior which is frequently exhibited during a particular span of time can be coined as the normal behavior of the system. Similarly, the behavior which is rarely being exhibited in a particular span of time can be designated as an anomaly or abnormal behavior.

The most and least frequent behaviors of the system can be obtained from the system resources that have been consumed during the particular period of time. To ascertain whether the traffic is normal or not, one has to monitor the system behavior based on the system resources being utilized. These system resources usually exhibits normal usage patterns in most of the situations. However, they may exhibit abnormal usages in some circumstances. In such situations, checking or monitoring of system resources can become crucial in order to detect the abnormalities in the system resource usages [3]. System resource usages can be captured to check the currently running programs, their network bandwidth usages, memory usage, processor usages etc. Similarly, user-based behaviors can be obtained from their login frequency or the number of password attempts to a known system. All these behaviors can be taken into consideration for further ascertaining that an intrusion has occurred or not.

Researchers have adapted different approaches to develop a model based on the behavior of the system. The main issue in developing such a model is its dynamic behavior which increases the complexity of the system. For this reason in order address the problem, researchers have divided the whole system into host, user and the network environment. A model based on the behavior of any of these groups would address a solution for identifying the normal or anomalous behavior respectively.

This paper mainly focuses to survey the past literatures related to resource usages. It has attempted to highlight the different approaches the researchers have chosen. The next section is primarily elaboration of the concepts used by them. Finally, the last section

January - February 2020
ISSN: 0193 - 4120 Page No. 5734 - 5738

concludes the paper by inferring the approaches that can be carried forward in building a model based on resource usage.

2. Literature Review

This section primarily presents some of the influential works from the past literature. Literature reviews based on resource usage techniques have been taken into consideration. Then the approaches are classified with the help of two domains of intrusion detection systems: bio-inspired techniques (approach/method) and resource usage (attack area).

In paper [4], the authors utilized the concept of monitoring agents that traces the abnormal behavioral patterns or resource usages at each levels i.e. user process and network/ packet level. The authors have developed a multi-agent based system inspired by immune system. These agents are dynamic in nature and interact with each other in order to take necessary steps for addressing the anomalies at different levels.

In paper [5], the authors have adapted genetic modeling techniques for detecting intrusions. It simultaneously monitors the system at host level, process level and packet level. This gene based classifier is a large pool of population that has to be matched with the identifier.

Danger Theory of immune system is implemented in [6] which entails that when a cell dies unnaturally it eventually sends some negative signals to the neighboring cells. According to their approach, signals would infer the usage of resources that could be related to memory, disk activity etc. Any high or low usage would signify a danger signal. Network bandwidth, CPU monitoring and other user activities could also put some more light on the accuracy of the anomaly detection.

In [7] the author introduces an intrusion-detection device named honey files. The work is inspired by honey bees and their ability to detect honey from flowers located in geographically dispersed lands using honey bee algorithm. Honey files are not original files as they are used to entice the illegitimate users to access.

The authors in [8] used an agent-based system (called CIDS) using immune system. The CIDS is a multi-layered system that has the important agents like the manager agent that interact with other security agents.

In [9] the authors have taken into consideration the way by which doctors diagnose diseases in real life. Any resource usage based on CPU, memory, network, etc are defined as a "symptom" of the program. These symptoms are programmed to match with a factor called certainty factor (CF) to find out whether the program possesses a virus or not.

In [10], resource usages are captured by creating traffic profiles based on network utilization, CPU usage, and login failure using immunological principles. These resource usage based outlines with respect to both system and user usages can better visualize the abnormalities.

In [11], the authors considered system activities at user, process and network levels in order to determine intrusive activities using the immunological principles.

In paper [12][13], the authors introduced an autonomic cyber defense system that would have subsystems which are flexible, scalable and adaptable. Such systems would identify anomalies or discrepancies that are associated with willful attacks. The system is able take automated responses depending upon the type of intrusive activities. In [13], they have adapted artificial immune system to introduce a system called libtissue. It has clients namely, antigen, signal and response. Antigen clients capture the usages of CPU and memory and forward them to a libtissue server, signal clients monitor system behavior (CPU and Memory usages) and response clients provide the messages accordingly. Other system and user usage profiles could be considered for better alert response.

A novel AIS (the TLR algorithm) have been proposed by authors in their paper [14] that uses both the layers of natural immune system i.e. the innate and adaptive systems. It captures the system call information and uses runtime statistics of process memory and file usage to signify intrusive activities.

In [15], the authors have used the danger theory of the immune system and have considered multiple agents that interact with each other to calculate a value called mature context antigen value (MCAV). This

January - February 2020
ISSN: 0193 - 4120 Page No. 5734 - 5738

value gets updated according to the security responses. The system takes time while communicating with the agents and adapt with the environment.

The authors in [16] have utilised network and system usage parameters and evaluated a function for each of these parameters. The authors have proposed good approach to carry the individual indicators and generate a global one so as to receive anomalies from multiple dimensions.

In [17], the authors have used immunological principles where antibodies are chosen from an adaptive pool. These antibodies exhibit 'intelligent' behavior and depending upon their better matches with the antigens they are allowed to be increased in concentrations in the pool.

The AIS-based IDS in [18] has a centralized engine which is introduced at the checkpoint of each LAN and detection sensors introduced at each client. Each one them have agents which coordinate with one another for identifying any anomaly in the network or system.

Authors in [19] proposed immune-inspired Danger Theory that handles the intrusion by taking into consideration the immune response of each Antigen Presenting Cell. These cells generate signals depending upon the state of the cell. A dead cell or stressed cell would immediately denote some malicious activities underneath.

In [20], the authors have categorized their proposed system into censoring stage and monitoring stage respectively. In censoring stage, the detectors generate the system changes. Any change which is not reflected earlier is accepted and stored in this stage whereas others are rejected. A change would only signify intrusion or any malicious activities. Then using these change detectors, the system activities are monitored in the monitoring stage.

The authors of [21] have considered different agents, and all agents in the system monitor, acquire, respond and control the intrusive activities. Although the system exhibits efficiency in controlling false alarms but it takes time while communicating with the agents and adapt with the environment. In paper [22], the authors have captured the behavior of the system calls for detecting anomaly in the system.

3. Conclusion

The review of literatures related to biologically-inspired resource usage-based IDS depict that immune system has innate coherence with the intrusion detection system. Authors in [4, 5] used immunological principles in designing resource usage based IDS at different levels. Subsequent works from the same researchers [8][11][19], shows utilization of multi-agents for accessing the different levels of abstraction. In paper [6], another author has suggested implementation of Danger Theory of Immune System for Intrusion Detection System. In [12], [13], [19], and [22] the authors have used the system calls based on resource usages. Many of them have adapted immunological principles for matching of antigens or unknown behaviors. In the rest of the papers [7], [9], [10], [14], [15], [16], [17], [18], [20] and [21] some immunological principles and agent-based monitoring system have been implemented in order to detect the anomaly in the behavior of the system. The above literature reviews reveal that the researchers have used information based on resource usage of the system as well as the users' specific activities. This information can become very crucial in detecting an anomaly based on system behavior. And immune-inspired IDS can explore these resource-based usage techniques in order to provide more information in solving the issues of intrusive activities.

References

[1] SA Hofmeyr, S Forrest, "Architecture for an Artificial Immune System", Evolutionary Computation, 2000, vol. 8, issue 4, pp. 443-473.

[2] Dutt, S. Borah and I. Maitra, "A Proposed Machine Learning based Scheme for Intrusion Detection," *2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, Coimbatore, 2018, pp. 479-483. doi: 10.1109/ICECA.2018.8474803.

[3] https://msdn.microsoft.com/en- us/library/

[4] D. Dasgupta, "Immunity-Based Intrusion Detection System: A General Framework", In Proc. of the 22nd *NISSC, 1999, vol. 1, pp. 147-160*.

January - February 2020
ISSN: 0193 - 4120 Page No. 5734 - 5738

[5] D. Dasgupta, F. A Gonzalez, "An Intelligent Decision Support System for Intrusion Detection and Response", In Proc. Int'l Workshop on *Mathematical Methods, Models and Arch. For Computer Networks Security, 2001, pp. 1—14.*

[6] U. Aickelin, "The Danger Theory and Its Application to Artificial Immune Systems", Proceedings of the 1st*International Conference on Artificial Immune Systems (ICARUS-2002), 2002, pp. 141-148*.

[7] Jim Yuill, Mike Zappe, Dorothy Denning, and Fred Feer, "Honeyfiles: Deceptive Files for Intrusion Detection", *Proceedings of the IEEE, 2004, ISBN 555555555*.

[8] D. Dasgupta, F. Gonzalez, K. Yallapu, J. Gomez, R. Yarramsettii, "CIDS: An Agent-based Intrusion Detection System", *Computers & Security 2005, Elsevier, vol. 24, issue 5, pp. 387-398.*

[9] Hsien-Chou Liao, Yi-Hsiang Wang, "A Memory Symptom-based Virus Detection Approach", *International Journal of Network Security, 2006, vol.2, issue 3, pp.219–227*.

[10] D. Yang, A. Usynin, J. W. Hines, "Anomaly-Based Intrusion Detection for SCADA Systems", 5th Intl. Topical Meeting on Nuclear Plant Instrumentation, Control and Human Machine Interface Technologies (NPIC & HMIT 05), 2006, pp. 12-16.

[11] D. Dasgupta, "Immuno-inspired Autonomic System for Cyber Defense", *Information Security, Tech. Rep., 2007, volume 12, issue 4, pp. 235-241*.

[12] Jamie Twycross, UweAickelin, "An Immune-Inspired Approach to Anomaly Detection", Handbook of Research on Information Security and Assurance, *Information Science Reference, Hershey, New York, 2008.*

[13] Jamie Twycross, UweAickelin, Amanda Whitbrook, "Detecting Anomalous Process Behaviour using Second Generation Artificial Immune", *International Journal for Unconventional Comp., 2010, vol. 6, issue 3–4, pp. 301–326.*

[14] Tarek S. Sobha, Wael M. Mostafab, "A Cooperative Immunological Approach for Detecting Network Anomaly", *Applied Soft Computing, 2011, volume 11, pp. 1275–1283.*

[15] Carlos A. Catania, Carlos GarcíaGarino, "Automatic Network Intrusion Detection: Current Techniques and Open Issues", *Elsevier, Computers & Electrical Engineering, 2012, vol. 38, issue 5, pp. 1062–1072.*

[16] Chung-Ming Ou, "Host-based Intrusion Detection Systems Adapted from Agent-based Artificial Immune Systems", *Neurocomputing, 2012, vol. 88, pp. 78–86*.

[17] Manoj Rameshchandra Thakur, Sugata, Sanyal, "A Multi-Dimensional Approach Towards Intrusion Detection System", *International Journal of Computer Applications (0975 – 888), 2012, vol. 48, issue 5*.

[18] FarhoudHosseinpour, SureswaranRamadass, Andrew Meulenberg, PayamVahdaniAmoli, Zahra Moghaddasi, "Distributed Agent Based Model for Intrusion Detection System Based on Artificial Immune System", *International Journal of Digital Content Technology and its Applications , 2013, vol. 7, issue 9*.

[19] U. Aickelin, D. Dasgupta, "Search Methodologies: Introductory Tutorials in Optimization and Decision Support Techniques", *Artificial Immune Systems, 2014, Chapter 13, pp. 1-29*.

[20] Walid Mohamed Alsharafi and MohdNizam Omar, "A Detector Generating Algorithm For Intrusion Detection Inspired By Artificial Immune System", *ARPN Journal of Engineering and Applied Sciences, 2015, ISSN: 1819-6608, vol. 10, issue 2, pp. 608-612.*

[21] JingXu, SenXu, YongzhongLi, "Multi-Agent Intrusion Detection System Based on Immune Principle", *International Journal of Innovative Research in Computer and Communication Engineering,2015, ISSN (Online): 2320-9801, ISSN (Print): 2320-9798 vol. 3, issue 4*.

[22] Esra N. Yolacan, David R. Kaeli, "A Framework for Studying New Approaches to Anomaly Detection", *International Journal of Information Security Science,2016, vol.5, issue 2.*