Journal of Engineering Design and Analysis
Volume 3, Issue 2 - 2020, Pg. No. 101-103
Peer Reviewed Journal

Article

Soft Computing Techniques for Intrusion Detection - A Survey

Bijaya Kumar Panda

Gandhi Institute for Technological Advancement, Bhubaneswar, Odisha, India.

I N F O

E-mail Id:
bijay_cse@gita.edu.in
Orcid Id:
https://orcid.org/0000-0002-6916-3225
How to cite this article:
Panda BK. Soft Computing Techniques for Intrusion Detection - A Survey. *J Engr Desg Anal* 2020; 3(2): 101-103.

Date of Submission: 2020-11-04
Date of Acceptance: 2020-12-15

A B S T R A C T

Due to the extensive use of computers and data communication among computers, in recent years, network security is emerging as an important field in protecting the communication networks from the cyber crime, cyber threats, unauthorized access, etc. Intrusions are the set of actions that violates the integrity, availability or confidentiality of a network resource. It can be thought of as a successful attack on network Intrusion Detection System (IDS) is a system which detects the attacks and informs it. This paper presents the soft computing based techniques that can be used for detection of intrusions.

Keywords: Intrusion, IDS, Soft Computing, Threat, Attacks

Introduction

Last two decades saw a rapid growth of use of internet by the various organizations for information processing and sharing. Information is very vital for organisations in these days. Due to fall in cost of information processing, availability of new technologies and rapid growth in Internet accessibility, organizations are becoming increasingly vulnerable to potential cyber threats such as network intrusions. That is why protecting computer networks from internal and external threats have become a high priority.

The conventional approach for securing computer system and computer network is to design security mechanisms, like firewalls, authentication mechanisms, Virtual Private Networks (VPN), etc. that creates a protective "cover" or shield around these systems. But, such security mechanisms almost always have inevitable vulnerabilities and they are usually not sufficient to ensure complete security of the infrastructure. This has created the need for security technology that can monitor systems and identify computer attacks. This component is called intrusion detection and is a complementary to conventional security mechanisms.

Intrusions can be thought of as actions that attempt to bypass security mechanisms of computer systems or the network. One of the most popular definitions for intrusion[1] is that it represents a malicious, externally induced, operational fault.

Intrusions can be divided into 6 main types:

- Attempted break-ins, which are detected by atypical behaviour profiles or violations of security constraints
- Masquerade attacks, which are detected by atypical behaviour profiles or violations of security constraints
- Penetration of the security control system, which are detected by monitoring for specific patterns of activity
- Leakage, which is detected by atypical use of system resources
- Denial of service, which is detected by a typical use of system resources
- Malicious use, which is detected by atypical behaviour profiles, violations of security constraints, or use of special privileges

Intrusion Detection System (IDS) collects information from a computer or network of computers and attempts to detect intruders or system abuse.

There are many types of IDSs architecture. They are divided into the following two groups based on the type of events that they monitor and the way in which they are deployed:

- Host Based Intrusion Detection System (HIDS)

Copyright (c) 2020: Advanced Research Publications

- Network Based Intrusion Detection System (NIDS).

NIDS responsibility is to protect the whole network in general, where any traffic across the network will be analyzed, but for critical end points, HIDS is used instead.

Host based intrusion detection systems usually use systems and application logs to obtain records of events, analyze them to determine if there is an intrusion. Host Based Intrusion Detection monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Host-based IDSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

Network Based Intrusion Detection which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers.

Mainly the Intrusion Detection is classified into two types: Misuse Detection and Anomaly Detection.[2] Misuse/ Signature Based Detection is mostly followed some fixed patterns. So it is very effective at detecting the known attacks but very poor in detecting unknown threats. Anomaly based systems basically attempt to map events to the point where they "learn" what is normal and then detect an anomaly that might indicate an intrusion. The anomaly detection method always tries to find the normal behaviour pattern with the assumption that an intrusion will generally include some deviation from this normal behaviour.[3]

Anomaly detection systems are computationally expensive because of the overhead of keeping track of, and possibly updating, several system profile metrics.

Soft computing is an emerging approach to computing which parallel the remarkable ability of the human mind to reason and learn in a environment of uncertainty and imprecision. Soft computing consists of several computing paradigms including Artificial Neural Network(ANN), Fuzzy set theory and fuzzy logic, Approximate reasoning, Derivative-free optimization methods such as Genetic Algorithms (GA) and Simulated Annealing (SA).

Soft computing utilizes human expertise in the form of fuzzy if-then rules, as well as in conventional knowledge representations, to solve practical problems. Inspired by biological neural networks, artificial neural networks are employed extensively in soft computing to deal with perception, pattern recognition and nonlinear regression and classification problems. Soft computing applies innovative optimization methods arising from various sources like genetic algorithms, simulated annealing, the random search method and the downhill Simplex method. These optimization methods do not require the gradient vector of an objective function, so they are more flexible in dealing with complex optimization problems. Soft computing relies mainly on numerical computation. Incorporation of symbolic techniques in soft computing is an active research area within this field. The best approach for an Intrusion Detection System may be to combine the advantages of both the anomaly detection and misuse detection components into a single compound scheme that can also accommodate the imprecision inherent in the domain of network security.

Soft Computing Based Techniques for Intrusion Detection

Artificial Neural Network (ANN) is one of the oldest systems that have been used for Intrusion Detection System (IDS). ANN can be used as a pattern recognition technique. Supervised learning based techniques can be used for supervised ANN- based intrusion detection. Supervised ANN applied to IDS mainly includes Multi Layer Feed Forward (MLFF) neural networks and recurrent neural networks Unsupervised learning based techniques can be used for unsupervised ANN-based intrusion detection, combination of above techniques can be used for hybrid ANN-based intrusion detection. The main limitations of ANN-based IDS is lower detection precision, especially for low-frequent attacks example: Remote to Local (R2L).

Self Organizing Map (SOM) is one of the most popular competitive learning based neural network models. It can be used for clustering data without knowing the class memberships of the input data. Self Organizing Maps (SOM) can be used as anomaly intrusion detectors.

Fuzzy systems have demonstrated their ability to solve different kinds of problems in various applications domains. In general, the traditional intrusion detection relies on the extensive knowledge of security experts, in particular, on their familiarity with the computer system to be protected. Fuzzy systems based on fuzzy if-rules have been successfully used in many applications areas. Fuzzy if-then rules were traditionally gained from human experts. It is possible to develop an anomaly based intrusion detection system which detects the intrusion behaviour within a network.

Support vector machine with associated learning algorithms can be used to analyze data and recognize patterns which will be useful for classification and regression analysis. Support Vector Machines (SVM) are the classifiers which were originally designed for binary classification. The classification applications can solve multi class problems. Intrusion detection can be considered as two-class classification problem or multi-class classification problem. So SVM can be used for detecting intrusion.

Related Work

Several intrusion detection methods have been proposed for detecting intrusion. Expert System (IDES)[4], one of earliest intrusion detection system which was developed at the Stanford Research Institute. The IDES always eyed on user behaviour and detected the suspicious events to be occurred.

In[5], it is suggested that an intrusion detection method is used to detect the intrusion efficiently.

In[6], Denning considered that any changes or any differences in the normal behaviour of user are treated as anomalous. For observing and detecting user's events, an expert system of instrution detection was developed by Stanford Research Centre. This centre also developed next generation mechanism which includes audit profilesof user's and can monitor the current status of the user, if any change occurs with user's activity in compared to audit profile of user then it will produce an alarm.

In[7], it is stated that intrusion detection systems have been generally built using expert system technology. But, Intrusion Detection System (IDS) researchers have been focused in building systems which are difficult to handle, inconvenient to use in real life and lack of insightful user interfaces. To find out attacks the proposed adaptive expert system has used fuzzy sets.

In[8], it has shown a method that detects real-time network anomaly attack for discovering suspicious activity against computer network by using Fuzzy Bayesian. By combining fuzzy and Bayesian classifier, the overall performance of the intrusion detection system (IDS) based on Bayes has been improved.

In[9], it is briefly explained about an advanced fuzzy and data mining methods based on hybrid model to find out both misuse and anomaly attacks. Their primary objective was to decrease the quantity of data processing and also to improve the detection rate of the existing IDS using attribute selection process and data mining technique respectively. An improved fuzzy data mining algorithm is used for implementing fuzzy rules which enabled the generation of if-then rules that show common ways of expressing security attacks. They have achieved faster decision making using Mamdani inference mechanism with three variable inputs in the fuzzy inference engine which they have employed.

In[10], back propagation model for intrusion detection is briefly described. This method makes training pair with a combination of input and equivalent target were generated and implemented into the network. Performance success can be measured by false alarm and detection rate. Detection rate was proven to be less than 80% for U2R, R2L, DoS and Probe attacks. However, the major issue of the method was found to be much inefficient to detect hidden attackers present in the system.

Conclusion

From the literature review it can be concluded that various types of soft computing techniques can be used to detect various types of intrusion. Each technique has its own capability and limitations. Various techniques can be combined together to form a hybrid technique that can use the capability of various technology to detect almost all type intrusion successfully.

References

1. Powell D, Stroud R. Conceptual Model and Architecture, Deliverable D2, Project MAFTIA IST-1999-11583, IBM Zurich Research Laboratory Research Report RZ 3377, 2001.
2. Zhong S, Khoshgoftaar T, Seliya N. Clustering based network intrusion detection. *Int Journal of Reliability Quality and Safety* 2007; 14(2): 169-187.
3. Pakkurthi S, Avadhani PS, Korimilli V et al. Approaches and Data Processing Techniques for Intrusion Detection System. 2009; 9(12): 181-186.
4. Lunt TF, Tamaru A, Gilham F et al. Computer Science Laboratory, SRI International, Menlo Park, CA, USA, Final Technical Report, 1992.
5. Shah K, Dave N, Chavan S et al. Adaptive neuro fuzzy intrusion detection system. IEEE International Conference on Information Technology: Coding and Computing. *Society* 2004; 70: 74.
6. Anderson D, Frivold T, Valdes A. Next- generation intrusion detection expert system (NIDES): A summary Technical Report SRI CSL. *Computer Science Laboratory, SRI International* 1995.
7. Stephen FO, Reuven RL. An adaptive expert system approach for intrusion detection. *International Journal of Security and Networks* 2006; 1(3/4): 206-217.
8. Shi Z, Shi Z, Olumide S et al. Network Anomalous Intrusion Detection using Fuzzy Bayes. *IFIP International Federation for Information* 2007 228: 525-530.
9. Bharanidharan S, Idris NB. Improved Intrusion Detection System Using Fuzzy Logic for Detecting Anamoly and Misuse Type of Attacks. International Conference of Soft Computing and Pattern Recognition. 2009; 212-217.
10. Jaiganesh V, Sumathi P, Mangyakarsi S. An analysis of intrusion Detection System using back propagation. *Neural Network* 2013.

ISSN: 2582-5607