RESEARCH REVIEW JOURNALS
Volume-03
Issue-12
December -2018

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Analysis of Network Intrusion Detection System using Laser Algorithm

[1]Shobha Bhatia & [2]Dr. R Vivekanandam

[1]Research scholar, Sri Satya Sai University, Sehore (India)
[2]Professor, Sri Satya Sai University, Sehore (India)

ARTICLE DETAILS

Article History
Published Online: 10 December 2018

Keywords
Intrusion Detection, SVM

ABSTRACT

This Intrusion detection system has become popular security intelligence component to provide security with capability of detecting attacks and patterns. Now day's globally use of IDS raising some lagging points like detecting false alert to be checked. Here new approach of support vector mechanism with swarm intelligence for selecting appropriate parameters to achieve high rate of attack detection and lower the false alarm than regular IDS. Recently, Support Vector Machines (SVM) has been employed to provide potential solutions for IDS. With its many variants for classification SVM is a state-of-the-art machine learning algorithm.

1. Introduction

Intrusion Detection System (IDS) are software or hardware systems that automate the process of monitoring and analyzing the events that occur in a computer network, to detect malicious activity. Since the severity of attacks occurring in the network has increased drastically, Intrusion detection system have become a necessary addition to security infrastructure of most organizations. Intrusion detection allows organization to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. Given the level and nature of modern network security threats the question for security professionals should not be whether to use intrusion detection but instead which intrusion detection features and capabilities can be used. Intrusions are caused by: Attackers accessing the systems, Authorized users of the systems who attempt to gain additional privileges for which they are not authorized, Authorized users who misuse the privileges given to them.

Intrusion detection systems (IDS) take either network or host based approach for recognizing and deflecting attacks. In either case, these products look for attack signatures (specific patterns) that usually indicate malicious or suspicious intent. When an IDS looks for these patterns in network traffic then it is network based (figure 1). When an IDS looks for attack signatures in log files, then it is host based. Various algorithms have been developed to identify different types of network intrusions; however there is no heuristic to confirm the accuracy of their results. The exact effectiveness of a network intrusion detection system's ability to identify malicious sources cannot be reported unless a concise measurement of performance is available.

Security is major concern critical issue as the Internet applications and networking is growing. The current security technologies are going with on encryption, firewall and access control But still these technologies cannot assumable security. The system security can be enhanced by Intrusion detection. The ability of IDS to classify a large variety of intrusions in real time with accurate results is important. The process, patterns of user activities and log records are examined and the intrusions are located. IDSs are classified, based on their functionality, as misuse detectors and anomaly detectors. Misuse detection system uses well defined patterns of attack which are matched against user behaviour to detect intrusions. Nowadays, the use of networks and especially the Internet has become a big part of daily life. Various private as well as government organizations store valuable data over the network. Almost every activity has a corresponding term that begins with an e (ebanking, e-learning). According to rapid development and widespread use of network systems, diverse intrusive approaches have grown extensively in the recent years. Multiple protection techniques have been used in order to manage the security network risks (encrypting sensitive data, access control, firewall policies). These methods do not suffice, as each of them have proven their inefficiency. Therefore, the use of intrusion detection systems as an additional defence mechanism is almost indispensable. An Intrusion Detection System (IDS) dynamically monitors the events taking place in a system, and decides whether these events are symptomatic of an attack (intrusion) or constitute a legitimate use of the system . Based on the adopted data analysis approach, an IDS may belong to one of the two main groups: misuse detection (or signature based detection) or anomaly detection. The first approach is most widely used and it detects only known attacks that have their signature included in the database. The anomaly detection approach creates a normal behaviour profile and detects intrusions based on significant deviations from the normal profile. Many challenges need to be considered when building an intrusion detection model, such as obtaining a high attack Detection Rate without generating many false alarms (low False Alarm Rate). Since the appearance of IDS, multiple techniques have been proposed in order to improve the performances of these systems. Recently, several machine learning techniques have been applied

2. Review of Literature

The common parameters or characteristics of home security system are 24 hours monitoring of the intruder Ease of use Reliability Efficient Fast and precise notification system. Today a number of home security systems are available in market a new method of moving object/body detection by combination of pixel illumination with its Chroma in YUV colour space is made implemented. The algorithm of maintenance

with 3 key values is discussed in this paper. In case of swaying objects, it is very robust and effective way of false alarms discusses the detection and description based on an object oriented, statistical multi feature analysis of video sequences.

The system described in monitors everything by moving cameras. The system can increase the efficiency of monitoring and can eliminate the blind spots of fixed cameras.

In this system, a mobile manipulator is developed which is equipped with cameras at the arm end for purpose of monitoring. The system is based on SMS technology using any GSM modem/mobile is presented in The proposed remote control system works from anywhere in the world. A low cost Short Message System (SMS) based home security system equipped with motion sensor, smoke detector, temperature sensor, humidity sensor and light sensors has been studied in The sensors are controlled by a microprocessor PIC 18F4520 through the SMS having password. As mentioned earlier about security systems, there are more advanced security systems, like image processing security system and communication based security systems.

As mentioned above there are two home-security network systems and according to its operating function we could divide into cabled system and wireless system mainly explored the methods for conducting data transmitting with power lines in home environment. In spite of the less expenditure and easy construction, the transmitting quality was easily disturbed by noise, therefore, the method would be difficult to keep the data complete and accurate and cause problems in safety.

Mainly explored the methods for constructing home-security network with TCP/IP standard communication protocol layout of wires of which was too complicated to meet the demand for modern home

3. The Intrusion Detection Algorithm

Related studies have already raised many intrusion detection models. According to the method of analysis, these models can be divided into two categories: feature-based intrusion detection model and anomaly-based intrusion detection model. Related researches have proposed some feature-based intrusion detection systems, but there are some problems in extracting and analyzing the features. There are also some related researches having proposed anomaly-based intrusion detection systems. Through statistical analysis of the data, anomaly-based intrusion detection systems can identify the anomalistic data which deviate from the mean value seriously. Data mining technology can effectively mine the regular pattern of the data; thus, it can be applied to intrusion detection on the Internet of Things.

We use data mining technology to design and implement the intrusion detection system. The system has three advantages:

1) The value of mining has little effect on the results;
2) The cutoff value used to determine the abnormal node is easy to determine;
3) The algorithm is fast and efficient.

Overview of k-Nearest Neighbor (KNN) Classification Algorithm.k-nearest neighbor (KNN) classification algorithm is a data mining algorithm which is theoretically mature with low complexity. The basic idea is that, in a sample space, if most of its k- nearest neighbor samples belong to a category, then the sample belongs to the same category. The nearest neighbor refers to the single or multidimensional feature vector that is used to describe the sample on the closest, and the closest criteria can be the Euclidean distance of the feature vector.

4. Support Vector Machine (SVM)

This method performs regression and classification tasks by constructing nonlinear decision boundaries. Because of the nature of the feature space in which these boundaries are found, Support Vector Machines can exhibit a large degree of flexibility in handling classification and regression tasks of varied complexities. There are several types of Support Vector models including linear, polynomial, RBF, and sigmoid.

5. Conclusion:

Security applications are effortlessly refined, as the laser techniques can be mounted on a level plane or vertically. Evenly, they make a huge, wide detection zone that can adjust to the coveted area of intrigue. Mounted vertically, they can make a vast undetectable laser divider. This divider could be as high as 50 feet and cover a territory more than 150-feet wide. Run of the mill vertical applications incorporate fence lines, doors and the sides of structures. For a fence line, a laser technique can secure the fence and space above it up to the detector. Yet, not at all like different sorts of detection, a laser can have custom zones for entryways or doors that can be controlled independently of whatever remains of the security region. For instance, an entryway could be a garage with a 16 all inclusive opening, alongside a different 4 all inclusive walker walkway, with whatever is left of the fence to 70 feet in the two headings, all controlled with independent zones. This errand is simple for a laser scanner however relatively unimaginable for different sorts of industrially accessible sensors or cameras. A laser technique can hand-off information about everything in its viewable pathway back to a scientific server. This incorporates not just the area and size of every single moving article, yet in addition the greater part of the information about static items.

References

1. T. Xiao, G. Qu, S. Hariri, and M. Yousif, “An Efficient Network Intrusion Detection Method Based on Information Theory and Genetic Algorithm ”, in Proc. of the 24th IEEE International Performance Computing and Communications Conference (IPCCC 2005), Phoenix, AZ, USA, 2005,pp.11–17.
2. X. R. Yang, J. Y. Shen and R. Wang, “Artificial immune theory based network intrusion detection system and the algorithms design”, in Proc. of 2002 International Conference on Machine Learning and Cybernetics, Beijing, China, 2002, pp.73–77.

3. D. Karaboga and C. Ozturk, “A novel clustering approach: Artificial Bee Colony (ABC) algorithm”, Applied Soft Computing, Elsevier Science Publishers B. V. Amsterdam, The Netherlands, Vol. 11(1), pp. 652–657, Jan. 2011.
4. The-History-of-Home-Security 4th July 2010 [Online]. Available: http://ezinearticles.com.
5. V. Karri and J. S. Daniel Lim, “Method and Device to Communicate via SMS After a Security Intrusion”, 1st International Conference on Sensing Technology, Palmerstone North, New Zealand, (2005) November 21-23.
6. Y. Zhao and Z. Yet, “Low cost GSM/GPRS BASED wireless home security system”, IEEE Trans. Consumer Electron, vol. 56, no. 4, (2007) January, pp. 546-567.
7. Z. Bing, G. Yun hung, L. Bo, Z. Gangway and T. Tina, “Home Video Security Surveillance”, Info-Tech and Info net, 2001, Proceedings, ICII 2001-Beijing. 2001 International Conference, vol. 3, pp. 202-208.
8. M. Meyer, M. Hotter and T. Ohmacht, “A new system for Video-based Detection of moving objects and its integration into digital networks”, Security Technology 1996, 30th Annual 1996 International Carnahan Conference, (1996), pp. 105-110.
9. Mae , Y,; SaaS , N .; Inonu ,K. ; Await.; “Person Detection by Mobile Manipulator for Monitoring”,SICE 2003 Annual Conference, pages-2801-2806.
10. V. Chunduru and N. Subramanian, “Effects of PowerLines on Performance of Home Control SystemPower Electronics, Drives and Energy Systems,”Proc. of International Conference on PowerElectronics, Drives and Energy Systems, Delhi, India,2006, pp. 1-6.
11. I.K. Hwang and J.W. Baek, “Wireless Access Monitoring and Control System based on Digital Door Lock,” IEEE Transactions on ConsumerElectronics, 53(4), 2007 pp. 1724-1730.
12. David Meyer, Friedrich Leisch, and Kurt Hornik.The support vector machine under test.Neurocomputing 55(1–2): 169–186, 2003.
13. (PDF) A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network. Available from: https://www.researchgate.net/publication/275071876_A_New_Intrusion_Detection_System_Based_on_KNN_Classification_Algorithm_in_Wireless_Sensor_Network [accessed Aug 23 2018].

