International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 05 | May-2016 www.irjet.net p-ISSN: 2395-0072

Fuzzy Based Research Techniques for Intrusion Detection and Analysis: A Survey

Mr. Krunal Khurana[1], Dr. Priti S. Sajja[2], Ms. Zankhana Bhatt[3]

[1]*Assistant Professor, Anand Institute of Information Science, Anand, Gujarat, India*
[2]*Professor, Department of Computer Science, Sardar Patel University, Vallabh Vidyanagar, Gujarat, India*
[3]*Assistant Professor, Anand Commerce College, Anand, Gujarat, India*

Abstract

In the recent time, the rate of attacks on networks has extremely increased and hence the interest in network intrusion detection has increased among the researcher scholar. This paper provides a survey on latest trends in intrusion detection along with various technologies implemented by some researchers in this research area. We recommend fuzzy based IDS to achieve desired security to prevent current attacks and next generation network.

Key Words: Network Security, Intrusion Detection, Traffic Analysis, Security Attacks

Introduction:

With the rapid growth in the Internet based technology since last two decades, new application areas for network security have emerged. In addition, new entities like hacking, worms, trojans and viruses bring some additional panic not only into the business networking but also into social networking. In the current situation network defences are considered to be a weak. However, due to the popularity of the computer networks, their connectivity and our dependency, on the other side with the all possible threat can have highly destructive consequences. Securing such an important network resources has become the high priority research area for many researchers.[1]

Types of IDS

Intrusion Detection Systems (IDS) are categorized based on certain criteria such as their monitoring activity and detection technique.

Intrusion detection based on monitoring activity:

There are mainly two types of IDS characterized on the basis of different monitoring and analysis approach called Network based system and Host based system.

a) **The Host Based Intrusion Detection System (HIDS):** The HIDS is kept on host machine and hence analyzed traffic data separately in each host. The HIDS monitors the various file systems, network events and system calls to detect any possible threat to the system.

b) **The Network Based Intrusion Detection System (NIDS):** The Network based intrusion system monitors the packets passing through the entire network and validate the packets. Network Based Intrusion Detection System is particularly useful for monitoring traffic of many systems all at once.

Intrusion detection based on detection technique:

Intrusion Detection System is also classified on the basis of the technique used by the IDS for checking presence of vulnerabilities. They are mainly classified into Signature Based Detection and Anomaly Detection.

a) Signature Based Detection: A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known attacks. Signatures specify a combination of packet header and packet payload (or content) inspection rules to identify the malicious traffic. Packet header rule consists of a filter on packets 5-tuple which includes source and destination IP addresses and ports. Packet content inspection rule consist of a string or known pattern that has to be matched against the packet data. Other side, packet header matching requires classification techniques that can be implemented using TCAM-Ternary Content Addressable Memories, matching pattern requires deep packet inspection that involves scanning every bit of packet data. Traditionally, patterns have been specified as exact match strings. Naturally, due to their wide adoption and usage several high speed and efficient string matching algorithms have been proposed recently. These often include various string matching algorithms such as Aho-Corasick, Commentz-Walter, and Wu-Manber, and use a pre-processed data-structure to perform high-performance matching. Among these, Aho-Corasick has been adopted most widely.

b) Anomaly Based Detection: With the description of signature based NIDS, we now focus on anomaly detection for NIDS. Although not yet commercially available, it has emerged as the future of the NIDS design. The value and effectiveness of anomaly based NIDS is that they can automatically detect attacks which are yet unknown, and hence undetectable by signature based NIDS. An anomaly detection system consists of two different steps: the first step is called training phase where a normal traffic profile is generated; the second phase is called anomaly detection, where the learned profile is used to compare the current traffic to look for any deviations in order to find presence of anomaly. A number of anomaly detection techniques and system has been proposed recently to detect such deviations, which can be categorized into statistical methods, rule-based method, data-mining methods and machine learning based methods. We present a brief description of each of method, and introduce some well known and recent algorithms in among all categories.

Intrusion Detection Techniques

As network attacks are rapidly increasing, there are many intrusion detection techniques implemented to guard computer network. These techniques vary in terms of how it is working, way of implementation, and many more factors. However these techniques just help to detect intrusion in network, prevention will be carried out when we will have reliable intrusion detection system. [1] The fundamentals of various techniques used to detect intrusions are described below.

Genetic Algorithm and Fuzzy Sets Applications

Kim et al. (2004) proposed a new method and technique for intrusion detection which can detect attacks using genetic algorithm. The algorithm is applied to computer security system and shows its effectiveness in intrusion detection [2].

Sekeh and Bin Maarof (2009) proposed a fuzzy intrusion detection system which is host-based and uses data mining method and services of the underlying operating system calls. The result of the proposed system shows that the performance is improved and decreases the size of the database as well as time complexity and the rate of false alarms [3].

Mabu et al. (2011) proposed fuzzy network intrusion detection method based on class-association-rule mining in genetic network programming. The proposed method is dynamic and efficient for both misuse and anomaly detection in networks and it can handle mixed databases which contain both discrete and continuous attributes to mine important class-association rules needed for improved intrusion detection. The result of the proposed method provides as high detection rate in comparison with other machine-learning techniques [4].

Ojugo et al. (2012) proposed a Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS) for managing more system security, data confidentiality, data integrity and resource availability in networked settings. The proposed system uses a set of set of rules obtained from network audit data and the support-confidence framework, used as fitness function to evaluate the quality of each rule [5].

Hassan (2013) developed an IDS based on genetic algorithm and fuzzy logic for efficient detection of various intrusive traffic within a network. The system is more adaptable and cost-effective as it can update rules once new intrusive activities become known. The result of experiments and evaluations showed that the proposed system achieved reasonable intrusion detection rate [6].

Jongsuebsuk et al. (2013) came with a model, network IDS based on a fuzzy rules and genetic algorithm. Fuzzy rules are mainly used to classify network attacks, Moreover, genetic algorithm optimizes finding appropriate fuzzy rule in order to obtain the optimal result. The evaluation results shows that the proposed system can detect network attacks in real-time or within 2-3 seconds depends on the arrival of data to the detection system with the detection rate of over 97.5% [7].

Chaudhary et al. (2014) presented an intrusion detection system to detect the packet dropping attacks in mobile ad hoc networks using fuzzy logic. The simulation results demonstrated that proposed system has the capability to detect the attacks on packet dropping with high positive and low false positive rates under all speed levels of mobile nodes [8].

Benaicha et al. (2014) proves a new network intrusion detection model based on Genetic Algorithm approach with an improved early population and selection operator used to optimize the search of attack scenarios in audit files and provide the list of potential attacks within realistic processing time. They used genetic algorithm approach because it boosts the performance and reduces the false positive rate [9].

Padmadas et al. (2014) proposed a genetic algorithm based intrusion detection system for monitoring and assessing activities in a given network to determine whether they are legitimate or malicious based on the available information resources, system integrity and data confidentiality. The experimental results showed that the proposed system efficiently detect R2L attacks with 90% accuracy [10].

Harinee.k, Veeramuthu(2014) proposed method which can be flexibly applied to both misuse and anomaly detection in network based intrusion detection system. It can extract important rules which provides detection rate for prediction based approach.[11]

Vishnu Balan E, Gokulnath C, Prof.Usha Devi G, Priyan M K(2015), came with a new model for identifying the abnormal behaviour of user and node by intrusion detection system with fuzzy logic technique and also to identify the type of attacks.[12]

Han, M. Kamber(2006), The goal of using ANNs for intrusion detection is to be able to generalize data from incomplete data and to be able to classify data as being normal or intrusive. Types of ANN used in IDS are as: Multi-Layer Feed-Forward (MLFF) neural nets, Multi-Layer Perceptions (MLP) and Back Propagation (BP). [13]

The summary of existing IDS techniques is presented with their strengths and limitations.

IDS technique	Characteristics/advantages	Limitations/challenges
Signature based detection	Identifies intrusion by matching captured patterns with knowledge base data.	Cannot detect new or variant of known attacks.
	High detection accuracy for previously known attacks.	High false alarm rate for unknown attacks.
	Low computational cost.	
Anomaly detection	Uses statistical test on collected behaviour to identify intrusion.	More time is required to identify attacks
	Can lower the false alarm rate for unknown attacks.	Detection accuracy is based on amount of collected behavior or features.
ANN based IDS	Classifies unstructured network packet efficiently.	Requires more time and more samples training phase.
	Multiple hidden layers in ANN increase efficiency of classification.	Has lesser flexibility.
Fuzzy Logic based IDS	Used for quantitative features.	Detection accuracy is lower than ANN.
	Provides better flexibility to some uncertain problems.	
Association rules based IDS	Used to detect known attack signature or relevant attacks in misuse detection.	It cannot detect totally unknown attacks.
		It requires more number of database scans to generate rules.
		Used only for misuse detection.
GA based IDS	It is used to select best features for detection.	It is complex method.
	Has better efficiency.	Used in specific manner rather than general.
Hybrid techniques	It is an efficient approach to classify rules accurately.	Computational cost is high.

Conclusion:

The study of intrusion detection systems is having wide range of areas for researchers and this topic offers a number of opportunities for future research work. During survey is observed that the different Intrusion detection systems are uses the different sources of data and specific techniques to analyze this data. Based on review of various survey literatures, the idea is clear that to secure a network against the unknown attacks; the fuzzy based intrusion detection is the best practice to tackle attacks. Moreover, Due to its complexity there are still problems with respect to its reliability and this issue lead to high false positives in any fuzzy based IDS.

References:

1) Peyman Kabiri and Ali A. Ghorban "Research on Intrusion Detection and Response:A Survey"
2) D. W. Kim, J. W. Yang, K. B. Sim, (2004) "Adaptive Intrusion Detection Algorithm based on Learning Algorithm", The 30th Annual Conference of the IEEE Industrial Electronics Society, Vol. 3,pp. 2229 – 2233.
3) M. A. Sekeh, M. A. Bin Maarof, (2009) "Fuzzy Intrusion Detection System via Data Mining Technique with Sequences of System Calls," Fifth International Conference on Information Assurance and Security (IAS '09.), Vol.1, pp.154-157.
4) S. Mabu, C. Chen, L. Nannan, K. Shimada, K. Hirasawa, (2011) "An Intrusion-Detection Model Based on Fuzzy Class-Association-Rule Mining Using Genetic Network Programming," IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, Vol.41, No.1,pp.130-139.
5) A.A. Ojugo, A.O. Eboka, O.E. Okonta, R.E Yoro(Mrs), F.O. Aghware, (2012) "Genetic Algorithm Rule-Based Intrusion Detection System (GAIDS)," Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 8, pp. 1182 – 1194.
6) M. Md. M. Hassan, (2013) "Network Intrusion Detection System Using Genetic Algorithm and Fuzzy Logic", International Journal of Innovative Research in Computer and Communication Engineering,Vol. 1, No. 7.
7) P. Jongsuebsuk, N. Wattanapongsakorn, C. Charnsripinyo, (2013) "Real-time intrusion detection with fuzzy genetic algorithm," 10th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp.1-6.
8) A. Chaudhary, V. N. Tiwari, A. Kumar, (2014) "Design an anomaly based fuzzy intrusion detection system for packet dropping attack in mobile ad hoc networks," IEEE International Conference on Advance Computing (IACC), pp. 256-261.
9) S. E. Benaicha, L. Saoudi, S. E. Bouhouita Guermeche, O. Lounis, (2014) "Intrusion detection system using genetic algorithm," Science and Information Conference (SAI), pp. 564-568.
10) M. Padmadas, N. Krishnan, J. Kanchana, M. Karthikeyan, (2013) "Layered approach for intrusion detection systems based genetic algorithm," IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp.1-4.
11) Harinee. K. Veeramuthu(2014), J. Han, M. Kamber, Data Mining Concepts And Techniques (2nd Edition)Morgan Kaufmann Publishers (2006)
12) Vishnu Balan E, Gokulnath C, Prof.Usha Devi G, Priyan M K(2015), Fuzzy Based Intrusion Detection Systems in MANET
13) J. Han, M. Kamber Data mining concepts and techniques(2nd edition)Morgan Kaufmann Publishers (2006)