ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

Misuse and Anomaly Based Combined Hybrid Approaches for Intrusion Detection: A Survey

B.Sujata[1], M.Priyanka[2], M. Beulah Rani[3]

Assistant Professor, Department of CSE, MVGR College of Engineering, Vizianagaram, India[1,2,3]

Abstract: Intrusion Detection Systems (IDS) can be defined with various detection techniques. Misuse based and anomaly based detection techniques are some of the techniques used for identifying the known and unknown attacks. This paper shows a survey on both misuse and anomaly based detection techniques for IDS where it is observed that these two techniques when applied at a time gives better results than when applied individually on a particular dataset and it has been depicted in this paper by considering a case study where decision support system and expert rule based approach are applied on KDD 99 dataset for observing both normal and abnormal behaviour of the data.

Keywords: Intrusion Detection Systems, Misuse based systems, Anomaly based systems.

I. INTRODUCTION

Intrusion Detection Systems: An illegal access to a system is detectable with the support of intrusion detection systems [1] which are dynamic in nature when compared to firewalls where firewalls are static in nature. Intrusion detection systems are designed for both networks and computer systems. These systems work as network sniffers for monitoring a network in a uninhibited mode. This system is proficient in detecting all types of malicious network traffic and computer usage which includes exploitation of vulnerable services by network threats, data focused attacks on applications, attacks on host-based systems such as privilege acceleration, illegal logins and access to sensitive files and malware. System alerts notify administrators, upon a rule violation occurring in network packets by pattern matching with the help of the suitable algorithm. Types of Intrusion detection systems are:

Misuse of Signature based detection techniques: Misuse detection techniques are capable in determining the known attacks by matching the signatures or the attack descriptions in inconsistency of the audit data stream. Here the suspicious traffic is divided into 4 types: Probe attacks, Dos attacks, Remote to Local (R2L) and User to Remote (U2R).

Merits : False Positives can be produced by analysing the audit data.
Demerits: Detects only notorious attacks for which a signature has already been defined.

Anomaly based detection techniques: Abnormal or unidentified attacks that diverge from normal behaviour can be perceived using the Anomaly based detection techniques.

Merits: Unknown attacks can be identified.
Demerits: These systems are difficult to train in highly dynamic environments.

Hybrid Intrusion detection systems: It's a combination of both misuse and anomaly detection systems and it proves to be more efficient.

Merits: Hybrid systems prove to be more efficient than implementing individually.

II. REVIEW ON INTRUSION DETECTION TECHNIQUES

A. Misuse or Signature based detection techniques: Kumar and Spafford [2] proposed a mechanism of pattern matching to identify the known attacks misuse detection techniques with the help of Colour Petri Nets and found beneficial in the context of generality, portability and flexibility. However its evaluation and implementation was not performed.

Cannady [3], proposed a misuse detection based on analytical strength of artificial neural networks by providing a potential to identify and classify network activity based on nonlinear, incomplete and limited data sources. However here the system is unable to receive the inputs directly, hence demands the further research in this regard.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

Prakash et al. [4], proposed misuse detection techniques in contrast to the two previous cases where pattern matching with known attack signatures is done with the help of various data mining techniques like Clustering, , Outlier detection, Classification, Association rule mining for addressing the security issues in E-Commerce.

B. Anomaly based detection techniques: Patcha and Park [5] , performed a survey on various anomaly detection techniques and founded that known attacks reliably with a low false positive rate upon the usage of Machine learning; Statistical anomaly detection, Data mining techniques. However Teodaro et al. [6], discovered known attacks in an NIDS by applying mechanisms like Knowledge-based techniques, Machine learning based NIDS schemes, Bayesian networks, Markov models, Genetic algorithms, Clustering and outlier detection, Neural networks, Fuzzy logic techniques on KDD datasets for improving security and protection of networks. However Low detection efficiency, Low throughput and high cost were observed to be the drawbacks.

Wang et al. [7], proposed the mechanism of finding unknown attacks or the abnormal behaviours with the help of Traffic classification, Anomaly detection, Extreme learning machine, Support vector machine, L1- norm minimization and finally proposed that ELM found to be advantageous. However resource requirement was not adequate and performance was comparatively low.

C. Hybrid Intrusion Detection Techniques

Depren et al. [8], proposed the combination of both misuse and anomaly detection combination in the form of hybrid approach for getting better results than applying individually. J.48 decision tree was applied for classifying various attacks in misuse detection component and Self Organizing Map structure is proposed for identifying from the normal behaviour anomaly detection components. However dataset can be further classified and supplied for the two components to obtain better results.

Liao et al. [9], reviewed) Stateful Protocol Analysis (SPA), Signature-based Detection (SD) and Anomaly-based Detection (AD) and proposed several rule-based approaches for detection of unknown attacks. However the approach could hardly identify unknown attacks.

Kim et al. [10], proposed that anomaly detection can be improved when combined with known attacks in the form of hybrid detection with the help of one-class SVM and C 4.5 Decision tree to reduce the false positive and false negatives. However for significant improvement in the performance of hybrid detection the data used can be even more divided into subsets.

Guo et al. [11], exploited the strengths of misuse detection and anomaly detection, an intensive focus on intrusion detection combines the two. A hybrid approach was proposed towards the achievement of a high rate of detection and with a low false positive rate. The authors proposed an anomaly detection component 1 in level one with the help of change of clusters method and the outcomes based on normal and attack based will be supplied to the both anomaly detection component 2 and misuse detection component in level 2 with the help of k-NN algorithm to identify the exact normal behaviour and attacks. This approach can be further developed by the use of additional intelligent algorithms.

Table I shows both pros and cons of IDS systems and the summary of Intrusion detection techniques is shown in Table

Table I Pros And Cons of ID Techniques

Misuse Detection	**Anomaly Detection**	**Hybrid detection**
Pros Analyse audit data and produce low false positives. Cons Detects only known attacks.	Pros Detects unknown attacks and helps in identifying attack information. Cons Difficult to implement in highly dynamic environments.	Pros Combining misuse and anomaly based detections improves the efficiency of IDS.

Table II Summary of Intrusion Detection Techniques

Type of ID	**References**	**Highlighting features**	**Methodology**
Misuse detection	Kumar and Spafford [2]	detection of specific, exactly representable techniques of computer system exploitation.	Pattern matching with Colour Petri Nets
	Prakash et al. [4]	Matching patterns with known attack signatures.	Classification, Clustering, Outlier detection, Association rule mining misuse detections.
	Cannady [3]	Artificial neural networks to identify and classify network activity based on limited,	Provides the potential to identify and classify network activity based on limited, incomplete and nonlinear data

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

		incomplete, and nonlinear data sources.	sources.
Anomaly Detection	Teodaro et al. [6]	NIDS processing on KDD data set can be considered by performing data mining to find that the methods are useful in improving the security and protection of networks and computer infrastructure.	Knowledge-based techniques, Machine learning based NIDS schemes, Bayesian networks, Markov models, Genetic algorithms, Clustering and outlier detection, Neural networks, Fuzzy logic techniques.
	Wang et al. [7]	Extreme Learning Machine (ELM) proves to be efficient in detecting traffic.	Traffic classification, Anomaly detection, Extreme learning machine, Support vector machine, L1- norm minimization.
	Patcha and Park [5]	Known attacks can be detected reliably with a low false positive rate.	Anomaly detection; Machine learning; Statistical anomaly detection.
Hybrid detection	Liao et al. [9]	Detection of unknown attacks.	Signature-based Detection (SD), Anomaly-based Detection (AD) and Stateful Protocol Analysis (SPA).
	Kim et al. [10]	False positive and false negative rates will be reduced.	Hybrid intrusion detection, One-class SVM, Anomaly detection, C 4.5 Decision tree.
	Depren et al. [8]	Anomaly detection module uses a Self-Organizing Map (SOM) structure to model normal behaviour.	A decision support system, SOM and J.48 decision tree.
	Guo et al. [11]	To achieve a high detection rate with a low false positive rate.	Change of clusters method with K-Means and K- Nearest Neighbour algorithm.

III. CASE STUDY

(Comparison of KDD 99 dataset results on implementation of various algorithms)

A. "An Intelligent Intrusion Detection System (IDS) for Anomaly and Misuse detection in Computer Networks", by Depren et al., 2005.

Depren et al. [8], applied decision support system on KDD 99 dataset and found the following results for various IDS techniques. In Table III shows the simulation results of both anomaly and misuse detection modules based on the KDD 99 data set as shown. A detected rate of 98.95% and a missed rate of 1.00% for anomaly module was obtained and also a detected rate of 99.62% and a low false positive rate of 0.21% are obtained for the misuse detection module. From the observed results, misuse module gives very low false positive rates whereas anomaly detection module detects some type of attacks that misuse module misses like the 'ftp write' attack. However, anomaly module also provides comparatively higher false positive rate. The proposed hybrid IDS takes the advantages of both modules and combines the outputs of these two modules based on a simple decision support mechanism. As a result, a detection rate of % 99.91 and a false positive rate of % 1.26 are obtained by the proposed hybrid IDS approach and it is observed that the proposed approach, hybrid IDS gives better performance than individual approaches.

B. "Hybrid Network Intrusion Detection System Using Expert Rule Based Approach", by Aneetha et al., October 2012.

Aneetha et al. [12], proposed a new frame work based on a hybrid intrusion detection system for known and unknown attacks in an efficient way. This mechanism has the ability to detect intrusion in real time scenario from the link layer. This has been accomplished by combining rule base with appropriate clustering techniques for both supervised and unsupervised data. The notorious attack patterns are recognized, with the help of misuse detection system using the rule base approach and with anomaly

Table III Intelligent IDS System Results

Detection Module	Total # of Instances	Total # of attacks	Detected	Missed	False Positives	Detection rate	Missed rate	FP rate
Anomaly	199677	128452	127118	1334	716	98.95%	1.04%	1.00%

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

Misuse	199677	128452	127950	502	127	99.62%	0.39%	0.21%
Hybrid	199677	128452	128236	114	782	99.91%	0.1%	1.26%

detection new attacks are identified by deploying clustering techniques. The new attacks have been rationalised in the rule base with the knowledge from an expert database that improved the efficiency of the system. The detection rate of the hybrid system has been found to increase as the unknown attack percentage increases whereas in misuse, detection rate is found to decrease and in anomaly detection rate remains constant.

The performance of system was evaluated with detection rate. Different combination of known attacks and unknown attacks forms different data sets for evaluation. The dataset description are given in the table 4. The detection rate (DR) of misuse detection based on expert rule for known intrusion and the detect rate of anomaly based on clustering analysis for all intrusions are integrated under hybrid system detection rate. The detection rate of hybrid IDS framework was independent of intrusion proportions. In case of misuse model when known intrusion is greater than unknown intrusion, detection rate will be higher and when known intrusion decrease, detect rate will decrease.

Table IV Data Set Description

Datasets	**Known attacks (%)**	**Unknown attacks (%)**
SET A	90	10
SET B	80	20
SET C	60	40
SET D	50	50
SET E	40	60

C. Comparison of detecting anomaly and normal instances by performing clustering with the help of Fuzzy c-means and k-means clustering algorithms.

Fuzzy c-means and k-means algorithms are both unsupervised techniques and perform clustering of the given data but fuzzy c-means is more beneficial than k-means in terms of identifying the instances belonging to more than one cluster whereas k-means can identify only the outliers which does not belong to any cluster.

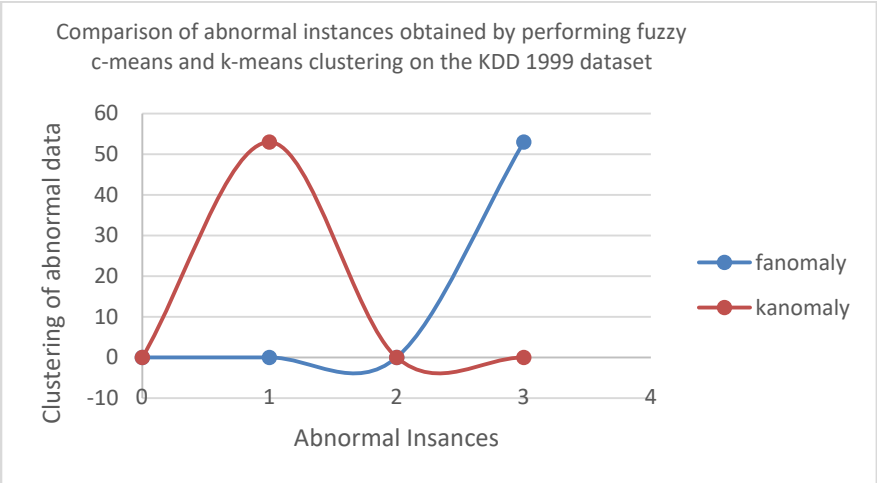

Fig. 1 Graph showing the comparison of abnormal instances obtained by performing Fuzzy C-means and K-means clustering on the KDD 1999 dataset.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 7, Issue 9, September 2018

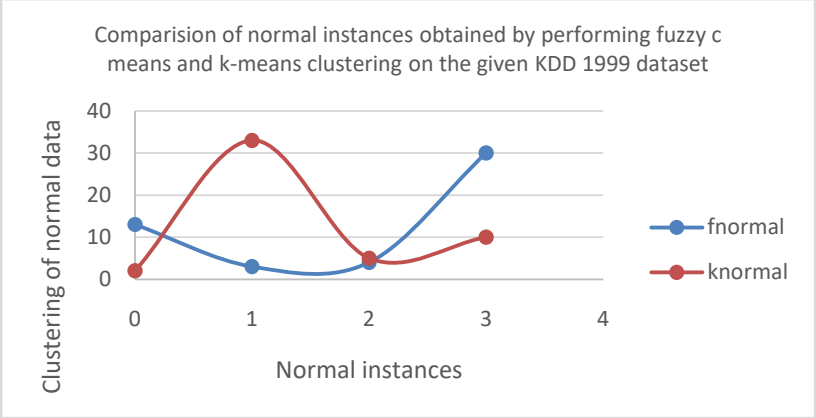

Fig. 2 Graph showing the comparison of normal instances obtained by performing Fuzzy C-means and K-means clustering on the KDD 1999 dataset.

CONCLUSION

The combination of misuse detection and anomaly detection named as hybrid detection systems proved to be more efficient in this paper. When surveyed and shown in the form of case studies the hybrid detection is found more beneficiary than when applied separately. The first one shows that when applied hybrid approach on KDD 99 dataset, it has more detection rate and high FP rate. In the second case the KDD 99 is divided into five various sets with different combinations and it ws observed that they have equal distribution o known and unknown attacks and as high the known attacks will be the higher will be the detection rates and hence when combined with unknown attacks gives the hybrid approach.

REFERENCES

[1]. G. V. Richard A.Kemmerer, "Intrusion Detection a brief history and overview," Seurity and Privacy, 2002.
[2]. E. H. S. Sandeep Kumar, "A Pattern Matching Model for Misuse Intrusion Detection," 11th National Computer Security Conference, pp. 11-21, October 1994.
[3]. J. Cannady, "Artifiicial Neural Networks for Misuse Detection".
[4]. R. K. J. S. Jay Prakash, "Survey om Misuse Detection Systems using Intelligent Agents," International Journal of Emerging Technology and Advanced Engineering, vol. 5, no. 1, April 2015.
[5]. J. P. A. Patcha, "An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends," Elsevier, Computer Networks, vol. 51, pp. 3448-3470, February 2007.
[6]. J. V. F. P.Garcia Teodoro, "Anomaly based Network Intrusion Detection: Techniques, Systems and Challenges," Elsevier, Computer and Security, vol. 28, pp. 18-28, 2009.
[7]. D. Z. Y.B.Wang, " Anomaly detection in traffic usingL1-norm minimization extreme learning machine," Elsevier, Neurocomputing, vol. 149, pp. 415-425, 2015.
[8]. T. M. A. M. Depren.O, "An intelligent intrusion detection system for anomaly and misuse detection in computer networks. Expert Systems with Applications," Elsevier, Expert Systems with Applications, vol. 29, pp. 713-722, 2005.
[9]. C. H.J. Liao, "Intrusion detection system : A comprehensive review," Journal of Network and Computer Applications, vol. 36, pp. 16-24, 2013.
[10]. S. G.Kim, "A novel hybrid intrusion detection method integrating anomaly detection with misuse detection," Elsevier, Expert Systems with Applications, vol. 41, pp. 1690-1700, 2014.
[11]. Y. P. N. L. S.-S. L. Chun Guo, "A Two level hybrid approach for intrusion detection," Elsevier, Neuro Computing, 2016.
[12]. T. I. D. S. A.S.Aneetha, "Hybrid Network Intrusion Detection System Using Expert Rule Based Approach," Acm, 2012.