A Study on IDS for preventing Denial of service attack using Outliers techniques

1.Ibrahim Salim.M
Research Scholar, Research and Development Centre,
Bharathiar University, Coimbatore, Tamil Nadu and
Assistant Professor,Department of Computer Applications,
MES College Marampally, Aluva,Kerala, India.
mes.ibrahimsalim@gmail.com

2. Dr.T.Abdul Razak
Associate Professor,Department of Computer Science,
Jamal Muhammed, College, Thiruchirappally,
Tamil Nadu , India
abdul1964@yahoo.com

Abstract—**Denial of service attack permits the intruders to access the network services thereby preventing the legitimate users to access the services. To overcome the deficits of the DoS attack, it is very essential to design an intrusion detection system. Intrusion detection system (IDS) is software that operates as a network security mechanism to protect the computer network system from attacks. With increasing number of data being transmitted gradually from one network to another, the IDS identify the intrusions in such large datasets effectively. Data mining is an efficient tool applied to outline the intrusion detection system and prevent the massive network data from the intruders. Outliers are patterns in data that do not match to a well-defined notion of normal behavior. Outlier detection aims to find patterns in data that do not conform to expected behavior. It is widely used for developing intrusion detection in cyber security. This paper presents the study of outlier detection technique and how it is used to develop the intrusion detection system to overcome the DOS attack.**

Keywords—DoSAttack; Intrusion Detection System; Data Mining; Outlier detection technique; Patterns

I. INTRODUCTION

Internet transforms the way of communication, style of conducting business, interacting with businesses and carrying out the regular operations. Internet services have been extended to all the traditional services such as banking transactions, medicine, education, research, entertainment defense and government services [1]. Progression in network technologies has provided an opportunity to the hackers and intruders to find the illegal ways to enter into a new system. One of the main threats formedbesides the computer network is the attack [2]thatrepudiates services to legitimate clients and users. The presence of secure network is essential to uphold the safety and security of various sites operating all the way through the internet.

A. Denial of Service Attack

Denial-of-Service (DDoS) attack is the attack in which the host's network elements are swamped with hugeamount of falsified attacking packets that are created from the large number _of machines [12]. A victorious attack permits the attacker to access to the host's machine, stealing of susceptible data and probably cause interruption and denial of service (DoS)[7] in some cases.

The main intention of the DoS attacks is to prevent legitimate hosts from using a service. The service can be either for free or paid. The attacker does not differentiate due to service fee. Special version of DoS attack is Distributed DoS attack, whose goal is to increase attack strength by using numerous maliciously misused computers. The goal is not to exploit the susceptible data but to create network congestion or to flood the application server by generating a large amount of traffic addressed to the host. DoSattacks have caused severe damage to network devices and services. In the earlier days it wasthe most common to execute these attacks at network and transport layer by flooding with ICMP or UDP messages.DoS attacks severely degrade the performance of the entire network. They enforceextensiveprocessing chores to the host by utilizing its system weakness or flooding[3]it with vast amount of ineffective packets.

B. Intrusion Detection System (IDS)

DoS attacks createsevere damages to the services running on the host machine. Hence, anwell-organized intrusion detection system to detect the DoS attacks is important to defend the online services. Intrusion detection system is a kind of security management system for computer networks. An ID system congregates and scrutinizes information from different areas within a computer network to identify the probable security infringes, which includes intrusions and misuse. IDSusesvulnerability assessment technology developed to assess the security of a computer network[5].

The major functions of the IDS are

- Monitor data transmission over the secured networks.
- Guarantee that the servers can contribute themselves to offer quality services with minimum delay in response.
- Detect attacks by evaluating certain features like arrival rate or header information.
- Examine the abnormal activity patterns.

978-1-4673-9916-6/16/$31.00 ©2016 IEEE

- Monitor system configurations and vulnerabilities.

C.*Classification of IDS*

In the IDS systems the detection process is deliberated in the network layer, transport layer and the application layer.

IDS may be categorized as host-based IDS and network-based IDS based on the information source[6].

- Host-based system: This type of IDS monitors the single machine or application and verifies the data that are traces by the operating system . [8]
- Network-based system: A network-based IDS examines a network area and analyses the traffic, which flows through the segment. The main advantage of this approach is the ability to monitor data and events without affecting host performance [4], [9].
- Hybrid system :Hybrid intrusion detection system is flexible and increases the security level. It merges IDS sensor locations and reports attacks[10]that are aimed at particular segments or entire network [11].

Signature based IDS and anamoly based IDS are the type of IDS which is classified based on type of analysis.

Signature based IDS is based on pattern matching techniques ,hence it works very much like antivirus software.It uses the signature database of the familiar attacks and attempt to match these signatures with the recorded data. the system raise an alert when it finds the appropriate match.

An anomaly-based IDS[13] build a reference statistical model of incoming traffic that provide the details of the normal behavior and usage patterns of the examined system and it uses the similarity metrics to compare the current input with the reference model .

This IDS can identify[14] the attack , if the examined traffic behavior does not match with the normal traffic pattern that is built using the training data set. The mismatching patterns are denoted as anomaly. This type of IDS has the ability to detect the unknown or new attacks as soon as it rises.

In misuse detection approach, an abnormal system behavior pattern is defined. This approach assumes that modeling an abnormal behavior is easy. Thus it defines the abnormal model and compares the analyzed data traffic [15] with the abnormal pattern. If any match is found then the system sends an alert message to inform about the attack .This IDS is bit similar to anomaly based IDS. However this IDS cannot newand more number of attacks.

D. Data Mining Techniques for IDS

The most important application of data mining technique is intrusion detection. This technique is used to develop the misuse approach based IDS and anomaly based IDS. Various processes like classification,association, clustering, grouping and outlier detection techniques are available to detect the intrusion. The purpose of each process is discussed below.

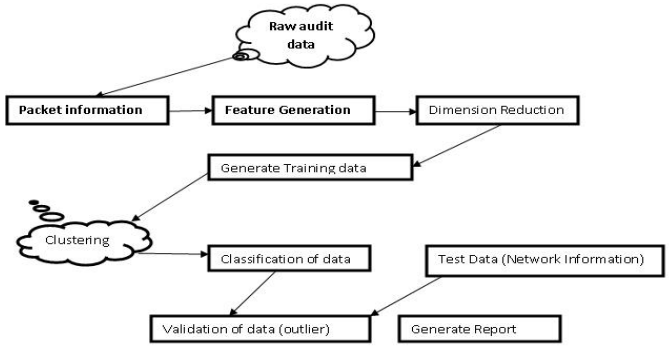
Classification:It is used to detect the individual attacks, It creates a classification of records. It produces high alarm rate. Boosting, a fine tuning techniques is used to reduce the problem of producing high alarm rate.

Association: illustrates the relationships within tuples.It is used to detect the mismatches or irregular arities when many tuples explore the unknown relationship , that has not happened previously.

Grouping is a technique that groups thetuples that exhibit similar properties according to described metrics. It can be used for general analysis similar to categorization, or for detecting outliers that may or may not represent attacks.

Clusteringmonitors the information system and raises alarms when security violations are founded.

Figure 1.1:Data mining Techniques to fabricate IDS Models



Outlier detection: It is a technique that findspatterns in data that do not match with the normal behavior [19]. By applying the clustering principle, outlier detection algorithms model the outliers and retrieve the noise set. The performance of outlier detection algorithm depends on how effective the clustering algorithm[20,21] is good in capturing the patterns and structure of the clusters.

The goal of this paper is to analysis associated research work using outlier technique for intrusion detection.

II. OUTLIER TECHNIQUE

Patterns in data that do not confirm to a well defined notion of normal behavior are called as outliers. Outlier detection focuses on to find patterns in data that do not match to a expected behavior. Applications of outlier technique are extensive in different requirements such as military surveillance, intrusion detections in cyber security, frauddetection [23] in financial systems etc. Showing variations from a usual system behavior, IDS is a better method for applying outlier detection

techniques. A dissimilar traffic pattern in a computer network means that a weak or hacked system [25] is forwarding data to an unauthorized system.

Classification of outliers can be done to three categories:

- Point outliers
- Contextual outliers
- Collective outliers

POINT OUTLIERS

When an independent data instance is considered as abnormal with reference to the remaining data then that particular instance is referred as point outlier. This is the basic and common type of outlier.

CONTEXTUAL OUTLIERS

When a data instance is abnormal in aspecific context then its referred as contextual or conditional outlier [22].The meaning of a context is added by the structure in the data set and has to be mentioned as a part of the problem formulation.Two sets of attributes are used:

Contextual attributes:They are used to determine the context for that instance.For example the Longitude and latitude of allocation are the contextual attributes in spatial data sets.

Behavioral attributes: The behavioral attributes define the non contextual characteristics of an instance,for example informing about the rainfall in a location is a behavioral attribute within a particular context. The abnormal behavior [27] is determined using the values for the behavioral attributes within a specific context. It is important in identifying contextual and behavioral attributes for a contextual outlier detection technique.

THE COLLECTIVE OUTLIERS:

When a set of related data instances is abnormal with regard to the entire data set ,then it is called as a collective outlier. The independent data instances in collective outlier may not be outliers by themselves, but their presence together as a combination is abnormal.

2.1 Operation mode of outlier techniques

The Outlier detection techniques can operate in one of the following three modes:

Supervised outlier detection: Techniques trained in supervised mode assume the availability of a training data set which has labeled instances for normal as well as outlier class. Typical approach in such cases is to build a predictive model for normal vs. outlier classes. Any unseen data instance is compared against the model to determine which class it belongs to. There are two major issues that arise in supervised outlier detection. First, the anomalous instances are few,as compared to the normal instances in the training data. Second, obtaining accurate and representative labels, especially for the outlier class is usually challenging. A number of techniques have been proposed [28], [29], [30] that inject artificial outliers in a normal data set to obtain a labeled training data set. Other than these two issues, the supervised outlier detection problem is similar to building predictive models.

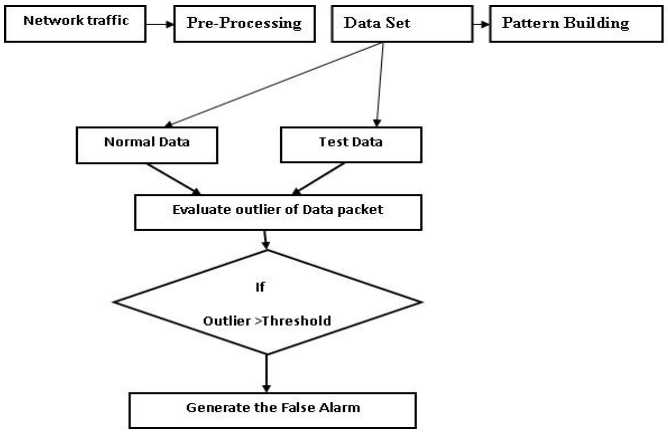
Semi-Supervised outlier detection: Techniques that operate in a semi-supervised mode, assume that the training data has labeled instances for only the normal class. Since they do not require labels for the outlier class, they are more widely applicable than supervised techniques. For example, in space craft fault detection [31], an outlier scenario would signify an accident, which is not easy to model. The typical approach used in such techniques is to build a model for the class corresponding to normal behavior, and use the model to identify outliers in the test data. A limited set of outlier detection techniques exist that assume availability of only the outlier instances for training [32]-[34]. Such techniques are not commonly used, primarily because it is difficult to obtain a training data set which covers every possible anomalous behavior that can occur in the data.

Unsupervised outlier detection: Techniques that operate in unsupervised mode do not require training data[33], and thus are most widely applicable. The techniques in this category make the implicit assumption that normal instances are far more frequent than outliers in the test data. If this assumption is not true then such techniques suffer from high false alarm rate. Many semi-supervised techniques can be adapted to operate in an unsupervised mode by using a sample of the unlabeled data set as training data. Such adaptation assumes that the test data contains very few outliers and the model learnt during training is robust to these few outliers.

III OUTLIER BASED APPROACH FOR IDS

Intrusion detection system has a great role for management of data effectively in a highly secured manner. To enhance this IDS is driven by the outlier based approach which is demonstrated in the below diagram.

3.1 Outlier based approach for IDS



The Figure 3.1.demonstrates the outlier approach in IDS. It requires a set of purely normal data to train the model.The Internet service provider (ISP) permits the normal data sets to this method generated by the set policies. Prior to observance the patterns are treated by anomalies .Outlier is considered as data point which is very different and the measurement is done with some computer based parameters from the rest of the data. By these data sets the outlier scheme works efficiently and deals with anomaly detection.

IV RELATED WORK

In IDS (Intrusion detection system) the outliers are of two types .The first method is the one which deviates significantly from others within their own network peripherals while the second type is the one whose patterns belongs to other network services other than their own service. It was also found that for finding intruders researchers have tried two methods either to model normal and subnormal data .Modeling both the normal and abnormal data permits the system to be tight on false positive and false negative as both the normal as well as abnormal patterns .Using only normal patterns allows the system to model to model the boundaries of normal data but due to the unknown nature of the boundaries of abnormal data ,it gives a possibility of alarming false positive also. Significant amount of the research works have pointed out that it is extremely difficult to find out outliers directly from high dimensional datasets, therefore most of the researches are moving towards with the reduction of the dimensionality of the dataset as a key task for better detection.

Different approaches for Outlier Detection are there, such as the Model based approach, Proximity-based approach and Angle-based approach. In the model based pattern, we can apply the model to represent normal data points, and can assume those points that do not fit or suit the model are outliers. Therefore, probabilistic tests based on statistical models, depth-based approaches and deviation-based approaches can be used for this outlier detection model. In Proximity-based approach, the spatial proximity of each object in the data space is examined and then we consider the object as an outlier if the proximity of an object deviates considerably from the proximity of other objects. Here, distance-based approaches and density-based approaches can be used for this outlier detection model. The key objective behind angle-based approach is that we measure the spectrum of pair wise angles between a given point and all other points. So, the outliers would be the points that have a spectrum featuring high fluctuation problems.

A method was outlined by Haystack [37] to assess an IDS method depending on the strategies of user and anomaly. This method detects various types of attacks like masquerade attacks, malicious use, leakage, service denial and access control of secured machines. The open source system called SNORT specifies the network based intrusion detection and prevention mechanism.

A standard report depending on analyzing the call sequences between intrusion detection and security adjacent to human system was developed by Forrest [38]. An attack is considered as the sequence deviation from normal profile sequence. This system works by using the previously gathered information and view table algorithm is implemented for significant learning program profiles.

In [39],An efficient intrusion detection method to detect the intrusion was proposed Anderson. Denning [43] developed an IDS with the mechanism using time- series, Markov chains, and statistics. The author deemed to treat the changes in the normal behavior of user as anomalous. Stanford Research Centre developed the futuristic mechanism which will include audit profiles of user's. The current status of the user can be monitored by the system. It will generate an alarm, if any change take places with user's activity when compared with audit profile of user.

SVM (Support Vector Machine) is applied to developan improved marking technique to identify the DDoS traffic with Time To Live (TTL) information at the routers. This technique was proposed by Lee[] , is very effective for managing malicious traffic and overseeing DDoS attack packets. For improving the band range, the SVM congestion signature is used by the , the entire network to filter malicious traffic. Hence path with DDoS attack can be possibly restricted by identifying the origin of DDoS attacks with a less number of marking packets. Major drawback of this method is requirement of additional memory for the router to support DDoS attack identification method.

A novel DDoS detection method based on hidden Markov models (HMMs) impose a technique for co reinforcement learning and distributed cooperation detection on source IP address to monitor the progress of the work. In the detection process, the detectors are distributed at intermediate network nodes or at frequencies of the new IP addresses to establish the normal traffic profile using near sources of DDoS attacks and HMMs. the cooperative reinforcement learning algorithm based on distributed multiple detector is exchanging information and computation is stored. This method proposed by Kim [23] is mainly efficient to progress the accuracy of the detector while processing with a huge sum of information.

In [40] the author came out with an approach to use outlier detection method by introducing random forests algorithm .Random forests are methods of un-pruned classification or regression trees. It is good in accuracy among the current data mining algorithms, especially for large datasets with many properties. Normal anomaly patterns are built over the network traffic datasets using subtractive clustering is proposed by

[41],and in parallel the built hidden markov model correlates the observation sequences and state transitions to predict the probable intrusion state sequence.

Unsupervised anomaly detection approach proposed in [41] is able to reduce false positives by classifying intrusion sequences .In [36] another unsupervised approach employs principal component analysis in order to detect changes in measurements of certain network traffic parameters. The issue in unsupervised detection is that there is given a large dataset where most of the elements are normal. On the other side their major benefit is the ability to process unlabeled data and find out intrusions. Onoccasionsunsupervised outlier detection methods may not brand malicious instances as an issue since the area of the feature space where they occur may be a dense one.

Lalane and broadle y [42.43.44]exanine unlabeled data for change detection by looking at user profiles and comparing the activity during an intrusion to the activity under a normal condition.

Ng et al[19] introduced a novel scheme of distance –based outlier detection approach,which is based on the nearest neighbor algorithm, which imlements a well defined metric to find outliers.This method is used to calculate the distance between eachpair of objects using a nested loop(NL) algorithm .The objects which are far away from the majority are signed as outliers[19].

Anomaly based intrusion detection using outlier subspace analysis is introduced by Kershaw et al[41].SPOT is implemented which is capable of quickly processing high dimensional streaming data analyzing its stream. It employs a window based time model that summarizes a decaying data which allows data to be processed timely and effectively. The normal behavior of a method is modeled using the specific set of system call combinations' sparse substrate Template is constructed using a group of subspaces to find outliers. To produce these subspaces a multi object genetic algorithm is used to produce these subspaces. Data arriving is mapped to a cell with low density derives a high abnormality value and are palced in a Outlier Repository. Thereforethis repository is used to determine outlier threshold which helps to find normal and intrusive traces.

Two phase framework for an outlier detection hase been introduced by Xiaoet al[46].The first learning phase consists of building a feature set of false positives which gets updated after a certain time frame and the threshold of true alert is calculated. In the next stage of online filtering, the outlier score of each new alert is compared with the value of threshold to find when its false positive .

Using proximities of network service type is done for anomaly based detection by Zhang et al. [38] .In their research, Pattern mining of network of netwokservices is done using random forest algorithm and have used concept of network services .K Means clustering to model normal patterns by Da et al. [36] is also used to find predicted attacks based on outlier factors with reference to statistical test.

Pareek et al[47] to model the behavior learning of internet have used SOMof internet using randomized parameters with weighted factors, and using Eucledian distance to obtain best matching for every parameter which gets updated on satisfying their model.

To reduce the dimensionality of the KDD dataset Huang et al [48] used PCA .Two types of outlier mining algorithms are used one base on similar coefficient sum and the second based on kernel density to define the anomaly set.Later the two algorithms are repeated many number of times.

Based on statistical method Taylor et al. [49] [50] derived a method based on statistical approach,it addresses the problems of monitoring high speed network traffic with the time limitations using only packet headers.

[49] [50] is a network intrusion system to detect misuse of intruders, it goes through the TCP packets with a low cost. It does clustering of normal network traffic.Changes or modifications of TCP header data from present clusters are used as a measure of search. It permits monitoring of high speed network traffic because once the normal pattern is constructed it reduces analysis complexity and use of less resource. Using a sampling method they have tested in the selected files of Darpa '98 and '99 dataset. On performing a cluster analysis they found 7 such clusters using Eucledian distance that represents normal samples, when both Euclidean distance and Mahalanobis is used as a method to find intrusions, They have found that false positives would be a massive problem with this tool and hence ,the significant level can be used as a tuning parameter in reflection to decrease the number of false positives.

V COMPARATIVE ANALYSIS OF DIFFERENT APPROACHES

False positive rate, Accuracy, Precision and Recall are the commonly used criteria for performance evaluation. They can be calculated as:

$$False\ Positive\ Rate(FPR) = \frac{False\ Positivee}{True\ Negative + False\ Positive} * 100$$

$$\text{True Positive Rate(TPR} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}} * 100$$

$$Accuracy = \frac{TP}{TP + TN + FP + FN} * 100$$

The number of malicious packets correctly classified as malicious is called as True Positive. False Positive (FP) is the number of normal traffic falsely classified as malicious. When the malicious traffic is classified as normal traffic then its called as False Negative (FN). True Negative (TN) is the number of genuine packets correctly classified as genuine.

Table 4.1.Comparative table of Performance analysis of different techniques used in IDS

The performance of every IDS technique differs in different scalable variables and each approach has an accuracy rate,FPR,TPR,Detection Rate. It is found that theOutlier Detection Algorithm has an highest accuracy rate in its performance when compared with other techniques.

Approach	Accuracy	FPR	DR
K-Means Clustering	75.41%	22.95%	66%
K-Medoids	76.72%	21.83%	62
OutlierDetection Algorithm	80.14%	21.83%	78
BIRCH Method	76.82%	18.16%	65
EM Clustering	78.06%	20.74%	63
Conceptual Clustering	76.41%	23.16%	64
Neural Network	79.17%	22.13%	81
Agglomerative Hierarchical Clustering	74.20%	21.46%	65
Divisive Hierarchical Clustering	73.24%	22.37	54
Hidden Markov models (HMMs	59	21	61
SVM	67%	4%	64

VI CONCLUSION

This paper surveys the different data mining techniques used to develop the IDS(Intrusion detection system).Table 4.1 describes the performance of different data mining techniques used to build the intrusion detection system. Among the various data mining methods its found that the results of outlier based is better. The performance is better in accuracy in data transmission and shows effective detection ratio. Many researchers have proved in developing the IDS by combining more than two approaches.The future focus of the research work is to develop an IDS based on Outlier detection approach to improve the accuracy ratio and Detection ratio in terms of detecting the malicious behaving nodes in the network.

REFERENCES

[1]G. Carl, G. Kesidis, R. R. Brooks, and S. Rai, "Denial-of-service attack-detection techniques," Internet Computing, IEEE, vol. 10

[2]Denning, D. E., "An intrusion detection model", IEEE Transactions on Software Engineering, CA,. IEEE Computer Society Press;1987

[3]V. Paxson, "Bro: A System for Detecting Network Intruders in Realtime," *Computer Networks*, vol. 31, pp. 2435-2463, 1999

[4]P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E.Vzquez, "Anomaly-based Network Intrusion Detection: Techniques,Systems and Challenges," *Computers & Security*, vol. 28,pp. 18-28, 2009

[5] Subramanirao Sridhar rao", SANS InstituteInfoSec Reading Room., "Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis",2011.

[6] J .X. Huang, J.Miao, Ben He, "High performance query expansion using adaptive co –training", Information Processing & Management, pp. 441–453, 2012.

[7] W. Lee, S.J. Stolfo, K.W. Mok, "A data mining framework for building intrusion detection models", in: Proceedings of IEEE Symposium on Security and Privacy, pp. 120–132, 1999.

[8] S. Axelsson, " Research in intrusion detection systems a survey", Chalmers University of Technology, Goteborg, Sweden, in: Tech. Rep.TR98-17,2000.

[9] S. Freeman, J. Branch, "Host-based intrusion detection using user signatures", in: Proceedings of the Research Conference RPI., 2002.

[10] D. Marchette, "A statistical method for profiling network traffic", in: Proceedings of Workshop on Intrusion Detection and Network Monitoring,pp. 119–128, 1999.

[11] Crosbie. M, E. H. Spafford,"Active defense of computer system agents", Technical Report CSD-TR- 95-008, Purdue Univ.West Lafayette, IN,1995.

[12] T.A. Longstaff, J.T. Ellis, S.V. Hernan, "Security of the Internet", in: F. Froehlich, A. Kent (Eds.), the Froehlich/Kent Encyclopedia of Telecommunications.Vol.15, pp. 231–254, 1998.

[13] Suresh Kumar, Anupama Chadha, "An Improved K-Means Clustering Algorithm: A Step Forward for Removal of Dependency on K", 2014 International Conference on

Reliability, Optimization and Information Technology -ICROIT 2014, India, Feb 6-8 2014.

[14]J.Han, M.Kamber ”Data Mining Concepts and Techniques”, in: ELSEVIER, Second Edition, 2006.

[15]Velmurugan, T., Santhanam. T ,” Computational Complexity between K-Means and K-Medoids Clustering Algorithms for Normal and UniformDistributions of Data Points”. Journal of Computer Science , pp 363–368, 2003.

[16] Lu, W., Tong, H... “Detecting Network Anomalies Using CUSUM and EM Clustering”. In: Proceedings of the 4thInternational Symposium on Advances in Computation and Intelligence, p. 297–308, 2009.

[17]Seetha,”Unsupervised Learning Algorithm for Color Texture Segmentation Based Multiscale Image Fusion”, European Journal of ScientificResearch 67 (4) 506–511, 2006.

[18]Chandola, V,” Anomaly detection: A survey”.ACM Computer society 41 (3) 1–58, 1998.

[19] Knorr,”Finding Intentional Knowledge of Distance-Based Outliers”.In Proceedings of the 25thInternational Conference on Very Large Data Bases, 211–222, 2009.

[20] J. Ryan, M.-J. Lin, R. Miikkulainen,”Intrusion detection with neural networks”, in: Proceedings of AAAI-97 Workshop on AI Approaches to Fraud Detection and Task Management, pp. 92–97,1997.

[21]J.Han, M.Kamber,”Data Mining Concepts and Techniques”, in: ELSEVIER, Second edition

[22] Song, X., Wu, M., Jermaine, C., and Ranka, S.”Conditional outlier detection”, IEEE Transactions on Knowledge and Data Engineering 19, 5, 631-645,2007

[23]Goldberger, A. L., Amaral, L. A. N., Glass, L.,Hausdorff, J. M., Ivanov, P. C., Mark, R. G., Mietus, J. E.,Moody, G. B., Peng, C.-K., and Stanley, H. E. 2000.PhysioBank, PhysioToolkit, and PhysioNet: Components of a new research resource for complex physiologic signals. Circulation 101, 23, e215 - e220. Circulation electronic Pages: http://circ.ahajournals.orgcgi/content/full/101/23/e215.

[24]Forrest, S., Warrender, C., and Pearlmutter, B. 1999. “Detecting intrusions using system calls: Alternate data models”,In Proceedings of the 1999 IEEE ISRSP. IEEE Computer Society, Washington, DC, USA, 133 - 145.

[25]Sun, P., Chawla, S., and Arunasalam, B. 2006. Mining for outliers in sequential databases. In SIAM International Conference on Data Mining.

[26]Noble, C. C. and Cook, D. J. 2003. Graph-based outlier detection. In Proceedings of the 9th ACM SIGKDD international conference on Knowledge discovery and data mining. ACM Press, 631 - 636.

[27]Sekar, R., Bendre, M., Dhurjati, D., and Bollineni, P.2001. A fast automaton-based method for detecting anomalous program behaviors. In Proceedings of the IEEE Symposium on Security and Privacy. IEEE Computer Society, 144.

[28] Theiler, J. and Cai, D. M. 2003. Resampling approach for outlier detection in multispectral images. In Proceedings of SPIE 5093, 230-240, Ed.

[29] Abe, N., Zadrozny, B., and Langford, J. 2006.Outlier detection by active learning. In Proceedings of the 12th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. ACM Press, New York, NY, USA, 504 - 509.

[30] Steinwart, I., Hush, D., and Scovel, C. 2005. A classification framework for outlier detection. Journal of Machine Learning Research 6, 211 – 232.

[31] Fujimaki, R., Yairi, T., and Machida, K. 2005. An approach to spacecraft outlier detection problem using kernel feature space. In Proceeding of the eleventh ACM SIGKDD international conference on Knowledge discovery in data mining. ACM Press, New York, NY, USA, 401 – 410

[32] Dasgupta, D. and Nino, F. 2000. A comparison of negative and positive selection algorithms in novel pattern detection. In Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics. Vol. 1.Nashville, TN, 125 - 130.

[33] Dasgupta, D. and Majumdar, N. 2002. Outlier detection in multidimensional data using negative selection algorithm. In Proceedings of the IEEE Conference on Evolutionary Computation. Hawaii, 1039 - 1044.

[34]Phoha, V. V. 2002. The Springer Internet Security Dictionary. Springer-Verlag.

[35] D. Kershaw, Q. Gao, and H. Wang, “Anomaly-Based Network Intrusion Detection Using Outlier Subspace Analysis: A Case Study,” in Advances in Artificial Intelligence, C. Butz and P. Lingras, Eds. Springer Berlin Heidelberg, 2011,pp. 234-239.

[36] W. Da and H. S. Ting,“Distributed Intrusion Detection Based on Outlier Mining,”in Proceedings of the 2012 International Conference on Communication,Electronics and Automation Engineering, G. Yang, Ed. Springer Berlin Heidelberg,2013, pp. 343-348.

[37]N. Devarakonda, S. Pamidi, V. V. Kumari, and A. Govardhan,“Outliers Detection as Network Intrusion Detection System Using Multi Layered Framework,” in Advances in Computer Science and Information Technology, N.Meghanathan, B. K. Kaushik, and D. Nagamalai, Eds. Springer Berlin Heidelberg,2011, pp. 101-111.

[38]ZHANG, J., ZULKERNINE, M. : Anomaly Based Network Intrusion Detection with Unsupervised Outlier Detection. Communications, 2006. ICC '06. IEEE International Conference on , vol.5, no., pp.2388-2393, June 2006 .

[39]H. P. Kriegel, P. Kroger and A. Zimek, “Outlier Detection Techniques,” inTutorial, 2010 SIAM International Conference on Data Mining (SIAM), 2010.

[40]J. McHugh, “Testing Intrusion Detection Systems: A Critique of the 1998 and 1999 DARPA Intrusion Detection System Evaluations As Performed by Lincoln Laboratory,” in ACM Transactions Information System Security, vol. 3, no. 4,Nov. 2000, pp. 262-294.

[41]D. Kershaw, Q. Gao, and H. Wang, “Anomaly-Based Network Intrusion DetectionUsing Outlier Subspace Analysis: A Case Study,” in Advances in Artificial Intelligence,

C. Butz and P. Lingras, Eds. Springer Berlin Heidelberg, 2011,pp. 234-239.
[42]T. Lane and C. E. Brodley. Sequence matching and learning in anomaly detection for computer security. In *Proceedingsof the AAAI-97 Workshop on AI Approaches to Fraud Detection and Risk Management*, pages 43–49. Menlo Park, CA:AAAI Press, 1997
[43]T. Lane and C. E. Brodley. Temporal sequence learning and data reduction for anomaly detection. In Proceedings of theFifth ACM Conference on Computer and CommunicationsSecurity, pages 150–158, 1998.
[44]T. Lane and C. E. Brodley. Temporal sequence learning and data reduction for anomaly detection. *ACM Transactions onInformation and System Security*, 2:295–331, 1999.
[45]Orair," Distance-based outlier detection: consolidation and renewed bearing". In: Proceedings VLDBEndow 3, 1-2, 1469–1480, 2007.
[46]F. Xiao and X. Li. 2008, "Using Outlier Detection to Reduce False Positives in Intrusion Detection," in IEEE IFIP International Conference on Network and Parallel Computing, 2008, pp. 26-33.
[47]V. Pareek, A. Mishra, A. Sharma, R. Chauhan, and S. Bansal,"A Deviation Based Outlier Intrusion Detection System," in Recent Trends in Network Security and Applications, N. Meghanathan, S. Boumerdassi, N. Chaki, and D.Nagamalai, Eds. Springer Berlin Heidelberg, 2010, pp. 395-401
[48] B. Huang,W. Li, D. Chen and L. Shi, "An Intrusion Detection Method Based on Outlier Ensemble Detection," in IEEE International Conference on Networks Security,Wireless Communications and Trusted Computing, 2009, pp. 600-603.
[49]C. Taylor and J. Alves-Foss, "NATE: Network Analysis of Anomalous Traffic Events, a Low-cost Approach," in Proceedings of the 2001 Workshop on New Security Paradigms, 2001, pp. 89-96.
[50]C. Taylor and J. Alves-Foss, "An Empirical Analysis of NATE: Network Analysis of Anomalous Traffic Events," in Proceedings of the 2002 Workshop on New Security Paradigms, 2002, pp. 18-26.