ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Review on Hybrid Intrusion Detection System

Ms.Nayana Dilip Sonje
PG Student,
Dept of Computer Engineering,
R.H.Sapat College of Engineering,
Nashik, Maharashtra, India.

Prof.S.R. Lahane
Assistant professor,
Dept of Computer Engineering,
R.H.Sapat College of Engineering,
Nashik, Maharashtra, India.

Abstract

This document gives formatting instructions for authors preparing papers for publication in the Proceedings of an International Journal of Advance Research in Computer Science and Management Studies. Net servers, info servers, cloud computing servers etc, are interconnected systems and they are currently below threads from network attackers. Mutually of commonest and aggressive suggests that Denial-of-Service (DoS) attacks cause serious effect on these computing systems. We introduce a denial of service attack finding system that uses multivariate correlation analysis (MCA) for correct network traffic characterization by the geometrical correlations between features of network traffic. Our MCA based denial of service attack finding system employs a principle of anomaly based finding in attack recognition. This makes our solution able of finding unknown and known denial of service attacks effectively by learning patterns of special network traffic just. Furthermore a triangle-area based method is proposed to speed up and to enhance the procedure of MCA. The effectiveness of our proposed detection system is measured using KDD Cup 99 dataset and the influences of both normalized data and non - normalized data on the performance of a proposed detection system are examined. The results show that our system performs two other prior implemented states of the art to handle in terms of finding accuracy.

Keywords:

Denial of Service, Multivariate correlation, network traffic, and anomaly based detection, triangle area, IDS, AD

1. Introduction:

DENIAL OF SERVICE (DoS) are one of the combative type of attack and approaching unsolicited behavior for online servers. Denial of service attacks severely decrease the availability of a sufferer, which can be a node, a host, a router or an entire network. They inflict intensive measurement tasks to the sufferer by taking advantage of its system vulnerability or flooding it with large amount of useless packets. The sufferer can be forced out of the service from a even several days to few minutes . This intent deep damages to a services running on the sufferer. Therefore, effective detection of Denial of service attacks is important to a protection of online services. Work on Denial of service attack finding is the main focuses on the development of network based discovery mechanisms. Discovery systems based on this mechanisms monitor traffic transmitting of a protected networks. This mechanisms can release the protected online servers from the convey and monitoring attacks that the servers can dedicate themselves to supply quality of services with minimum delay in response. Distributed opportunistic scheduling (DOS) is inherently more complicated than conventional opportunistic scheduling due to the absence of a central thing that knows the channel state of all stations [5]. Interconnected systems, such as net servers, web servers and database servers are now under threads from network hackers. As one of the common attack is Denial of Service (DoS) these attacks cause serious impact on the computing system [7]. Denial of Service (DOS) attacks are unlimited menace to internet websites and among the difficult security trouble in today Internet. The difficulty of Denial of service attacks has became well known, but it has been difficult to search the Denial of Service on the net. Distributed denial of service attack is a huge attack on a availability of services of a sufferer structure or network resources, published indirectly through many compromise computers on the net. Researcher have come up with more specific remedy to a DDoS problem [9]. With DOS, stations use random access to argue for the channel and upon winning a contention, they measure the channel conditions. After measuring a channel conditions the station only transmits if the channel quality is good; otherwise, it gives up the There are different Denial Of service Attack detection techniques proposed by the researchers over time to time which have some advantages over and vice-versa.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

There are many techniques used like K-map, combination of stateful and stateless signature with trace back technique, game-theoretic, Multivariate Correlation Analysis (MCA). Suseela T. Sarasamma, Qiuming A. Zhu, and Julie Huff [1] puts a new K-Map(Kohonen Net) multilevel hierarchical structure for an intrusion finding system is presented. Each step of the hierarchical map is organized as the simple winner take all K-Map.

One important advantage of this K-Map multilevel hierarchical is its calculation capability. Apart from other statistical inconsistency detection techniques such as K-means clustering or probabilistic analysis, nearest neighbor approach that engage distance measurement in a feature interval to recognize the outlines our request does not carry costly point to point calculations in organizing a data into clusters. One more advantage is network size reduced.

We use the grouping efficiency of the K-Map for detecting anomalies on selected dimensions of data set. Randomly selected data subsets that contain both the attacks and normal records from a KDD Cup data are used to train the hierarchical net. We use a assurance rate to label a clusters.

Then we use a test set from the same KDD Cup data set to test a hierarchical net. The paper[1] illustrate the multilevel hierarchical Kohonen Net or Kohonenself ordering map (K-Map) to implement an inconsistency based intrusion detection system (IDS sensor). We done our testing and training using the pre processed KDD Cup data set. Main objective was to detect different types of attacks as possible.

The experiment were done in two level. Firstly we used a single level winner takes all K-Map to do andevelopement of IDS. We can see in earlier serious limitations for a single level winner takes all K-Map in finding a large set of attacks and still keeping a low false positive rate [1].

The single level winner takes all K-Map is a useful method generally in the sense that it helps to group similar input vectors into clusters. However, it does not guarantee optimal separation of resulting clusters—refer Fig. 1(a) and (b), for example. There are two different types of objects.

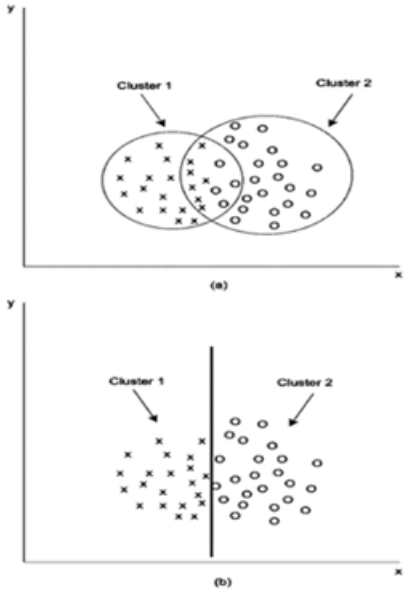


Fig.1. Effect of feature space dimensions on clustering

A simple winner takes all Kohonen Net consists of an input layer, a neurons layer and an output layer [1]. It only engage one neuron layer thus also call it a single level K-Map. The neurons layer consists of a set of neurons that can be visualized as arranged in a column—refer Fig. 2 for a graphical demonstration. Each neuron has an associated weight vector. The input layer serves to feed each neuron from a set of input vectors to the different neurons in the neurons layer. A input vector is attached to a neuron by its weight vector.

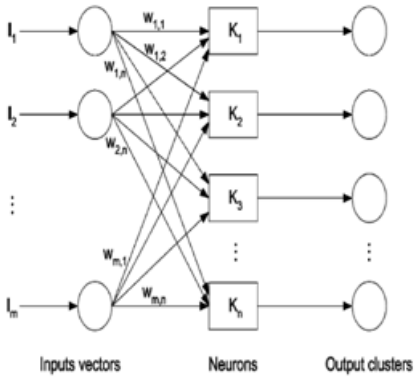


Fig.2. Single level winner takes all Kohonen map.

The output layer represents a set of clusters i. e. one for each neuron. The elements of an output cluster represent the input vector group that are closer to the neuron weight
.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The best matching neuron for an input vector is determined based on the dot product of the normalized weight vector and the normalized input vector of that neuron. This value is generally known as the neti. For all the neurons input vector is fed. The neuron gives the maximum value for is announced the winner or the best matching unit. In another way, only one neuron flame for a particular input vector. The finally result [1] from this is only one neuron flame at the output layer which make the algorithm implementation cost is low. John

Haggerty, Qi Shi and MadjidMerabti [2] , can combines both stateless and stateful signatures to provide early finding of the DoS attacks due to this enterprise network is protect. This paper is mostly focuses on how domain based way response to an attacks is used by mechanism to block traffic attack. This new solution is enables the blockage of the attack to be gradually propagated only through affected domains toward the attack sources. At the end the result[2] of attack is eventually narrow within its source domains, thus avoiding wasteful traffic attack overloading the network infrastructure.

This attempt also provides a real way of tracing back a source attack , without requiring the use of particular trace back methods and extra resources for their development. Ruiliang Chen, Jung-Min Park and Randolph Marchany [3], put mitigation of attack plan actively strangle traffic attack produced attacks in Distributed Denial of Service (DDoS).

In such paper presents Attack Diagnosis (AD), a new mitigation of attack scheme that adopts a divide and conquer technique. Packet marking and pushing concepts are combined in AD, and its architecture is in chain with the ideal DDoS attack countermeasure pattern for finding attack is performed near the packet filtering and sufferer node is executed close to the attack of sources.

Attack diagnosis is a reactive safety mechanism which is enabled by a sufferer node after a attack is finded. Mark the packet deterministically by instructing its upstream routers, the sufferer can back trace single attack source and command an attack diagnosis can enabled router close to a source for attack packets filter. This procedure isolates single attacker and strange it, which is repeated till upto the attack is mitigated. We also put an circulation to attack diagnosis called parallel

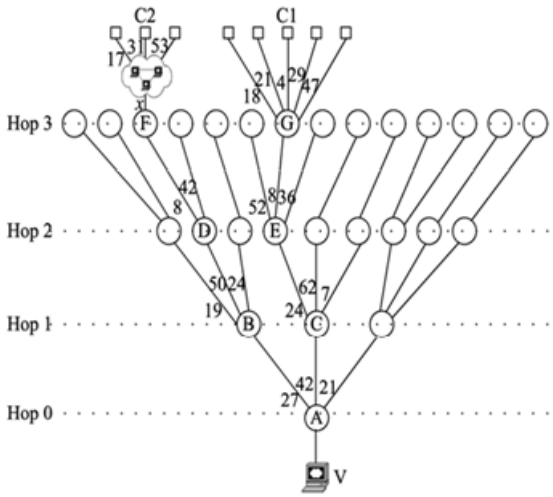


Fig. 3. An upstream tree of victim V

Parallel attack diagnosis that is capable of stranging traffic coming from a huge number of attacker simultaneously. Attack diagnosis and Parallel attack diagnosis are evaluated and analyzed using the lumeta's internet map, 6 degree complete tree model and skitter internet map. Both methods are shown to incur low false positive ratios and to be robust against IP spoofing [3]. Recognise attack diagnosis incapability to handle big portion attacks, we introduced their parallelized version, called parallel attack diagnosis. Parallel attack diagnosis is able of mitigating attack and tracing back traffic from many attackers simultaneously, thus enabling it to handle huge portion attacks. Our simulation and analysis results [3] indicate that attack diagnosis or parallel attack diagnosis has many advantageous features as it is reactive so as to incur limited overhead. It does not rely on signatures attack for filtering attack traffic. Next is robust against marking field forgeries and IP spoofing. It supports deployment in incremental.

Wanlei Zhou, WeijiaJia, Feilong Tang ,Song Guo, and Yong Xiang [4] , describe denial of service attack in distributed is a complex threat to the botnets and net are usually the engines behind them. By mimicking the traffic patterns of flash crowds the sophisticated bot masters try to disable finders This poses a complicated challenge to those who justify against distributed denial of service attacks. According to deep study of organization of current botnets and size, we found that as compared to the flows of flash attack the current attack flows are usually more same to each other. Based on this [4] we propose the algorithm of discrimination using the flow correlation coefficient as a similarity metric among suspicious flows.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We formulated the problem and represent theoretical proofs for the feasibility of the proposed technique of discrimination in theory. Our extensive experiments confirmed the demonstrated effectiveness and theoretical analysis of the proposed technique in practice. Albert Banchs, JoergWidmer, Andres Garcia Saavedra and Pablo Serrano [5], put game theory we address the problem of selfishness from a game-theoretic standpoint in DoS . They propose algorithm that satisfies the following properties: a) Wireless network is driven to the optimal point of operation when all the stations implement the algorithm and b) one or more selfish stations cannot obtain any gain by deviating from a algorithm.

The main theme of the algorithm is to react to the egostic station by using a more combative configuration that indirectly punishes this station. We plan a design that is multivariable control theory mechanism for punishment that is sufficiently strict to prevent the selfish behavior, yet not so severe as to render the system unstable. We conduct a game theoretic analysis based on repeated games to show the algorithm's effectiveness against a selfish stations. These results are confirmed by extensive simulations [5].

GautamThatte, UrbashiMitra, Fellow, and John Heidemann [6] , develops parametric technique to find network anomalies using contrast to other works requiring flow separation in only aggregate traffic statistics, even when the anomaly of total traffic is a small fraction . By adopting simple statistical models for background traffic and anomalous in the domain of time. One can forecast standard parameters in the real time, thus to avoid the need for manual parameter tuning or long trainingphase. A sequential probability ratio test is used by proposed bivariate parametric detection mechanism(bPDM) allowing for control over the false positive rate while examining the tradeoff between finding time and the potency of an anomaly.

Additionally, it uses both traffic-rate yielding a bivariate standards and packet-size statistics that ignore most false positives. The technique is analyzed [6] using the bit rate signal to noise ratio (SNR) metric, which is shown to be an powerful metric for inconsistency finding . The performance of the bPDM is calculated in three ways. First traffic generated synthetically provides for a controlled comparison of finding time as a function of the disconnected traffic level. Second the approach is shown to be able to find controlled attacks of abnormal attack over the Los Angeles, the University of Southern California (USC), campus network in varying mixes of real traffic. Third proposed algorithm achieves rapid finding of real denial of service attacks as determined by the replay of previously catured network traces. The technique implemented in this paper is able to find all attacks in these scenarios in a few seconds or less. S.Gomathi [7], give a easy example, a malicious host can continue transfer a radio signal in the order to interfere with reception to block any legitimate access to the medium.

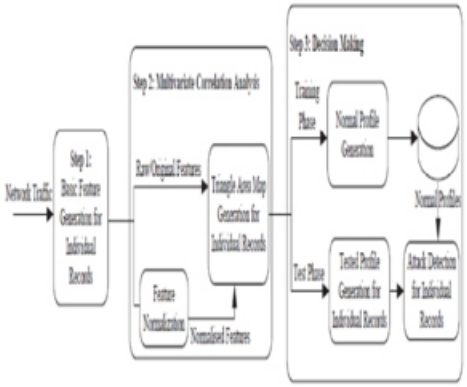
This is called the malicious nodes and the jamming are referred to as jammers. Jamming method [7] vary from simple ones based on the continuous transmission of interrupted signals to more stagy attacks that goal at exploiting the vulnerabilities of the particular protocol used. Denial of service attack finding system that uses multivariate correlation analysis (MCA) for correct network traffic characterization by extracting a geometrical correlations between features of network traffic .

The multivariate correlation analysis based Denial of service attack finding system employs the principle of anomaly based finding in attack recognition. This makes our solution able of finding unknown and known Denial of service attacks forcible by learning the sample appropriate network traffic only. R Nagadevi, P NageswaraRao, RameswaraAnand [8], explain about the results of multivariate correlation analysis on the distributed denial of service finding and suggests an example as a covariance analysis standards for finding signal to noise flooding attacks.

The imitation end results display that this technique is highly correct in finding malicious system traffic in distributed denial of service attack of various forces. This method can telling difference between attack traffic and ordinary. To be ensure this method can recognize even very tiny attacks only a small separate from usual behaviors. The linear difficulty of the techniques makes its presently finding practical.

The covariance sample in this document to some area verifies the correctness of (MCA) multivariate correlation analysis for distributed denial of service attack finding. Some open problem are fixed in this sample for further research.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal



The architecture [8] is divided into three levels or steps. First level is to generate the basic features for each single record. Second level is multivariate correlational analysis in which two operations can be done. First operation is raw features is provided for triangle map generation for each individual record and another operation is feature normalization. The last level is decision making. This decision making level is divided into two phase as training phase and test phase. DarshanLalMeenaDr.R.S.Jadon [9], put denial of service attacks are unlimited menace to internet websites and among the difficult security problems in today net. The problem of denial of service attacks has become known well but it has been difficult to detect the denial of service in the net. Distributed denial of service (DDoS) attack is a huge scale, coordinated attack on the availabilityof services of a network resources or sufferer system , launched indirectly through various compromised hosts on the net. Researchers have come up with more and more particular solutions to the distributed denial of service problem.

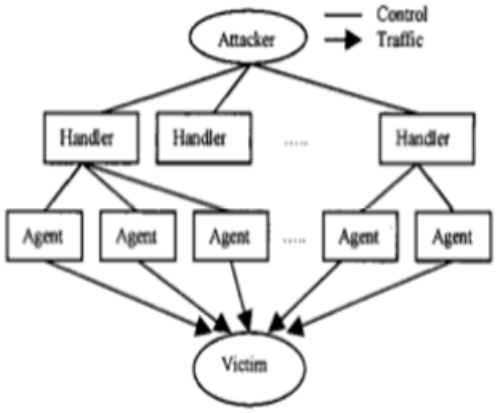


Fig. 5. Architecture of DDoS Attack

However present distributed denial of service attack tools keep status of improved and new attack methods are implemented. It is desirable to develop comprehensive distributed denial of service solutions to future and current distributed denial of service attack variants rather than to react with particular countermeasures. In order to help in this we carry a rough survey on the problem of distributed denial of service. We propose taxonomies of the potential and known distributed denial of service attack tools and methods.

Contiguous with this we discuss the defend challenges and issues and in fighting with such attacks. Based on the novel understanding of the problem we propose solutions classes to react and find survive to the distributed denial of service attacks. V. Jyothsna , V. V. Rama Prasad [10] , show anomaly based approaches are capable, signature based finding is preferred for mainstream development of the intrusion finding systems. As a diversity of anomaly finding methods were suggested that it is difficult to compare the weaknesses, strengths of these techniques.

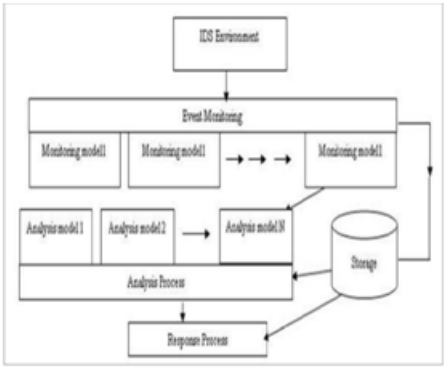


Fig. 5. Common Intrusion Detection Framework Architecture

The reason why industries don't favora anomaly based intrusion finding techniques can be well understood by validating the efficiencies of the all the techniques. To investigate this contribute, a current status of the performance habit in the field ofanomaly based intrusion finding is survey and reviewed fresh studies in this. The paper contains identification and summarization study [10] of the drawbacks of formerly surveyed works. Signature finding involves network traffic searching for a series of packet sequences or malicious bytes. The basic advantage of this method is that signatures are very easy to understand and implement if we know what network behavior we are trying to find.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

For example, we might use a signature that looks for accurate strings within exploit accurate overflow of buffer vulnerability. The incident generated by signature [10] based intrusion detection system can communicate the objective of the alert. As pattern matching can be done more efficiently on new systems so the power amount needed to perform this matching is minimum for a rule set. For example if the system that is to be secured only communicate via SMTP, DNS, and ICMP all other signatures can be avoided. Restrictions of these signature engines are that they only find attacks whose signatures are prior saved in database; a signature must be created for each attack; and new attacks cannot be found. This method can be easily deceived because they are only based on string matching and regular expressions. These mechanisms [10] only look for packets transmitting over wire within string. More over signatures fail to deal with attacks created by human or a worm with self-modifying behavioral characteristics, they work well against only the fixed behavioral pattern.

3. CONCLUSION:

In this way we have studied the existing approaches for detecting denial of service attack in distributed system. The multivariate correlation analysis based denial of service attack finding system which is powered by a triangle area based MCA technique and anomaly-based finding methods . The former method express a geometrical correlations hidden in single pairs of two distinct features within the every record of network traffic and offers more correct characterization for behaviors of network traffic. The latter technique facilitates our system to be able to differentiate both unknown and known denial of service attacks from proper network traffic. Disadvantage of this techniques are Time complexity more, also Results are not taken on real time dataset and False positive rate is more.

4. ACKNOWLEDGEMENT:

We would like to thank all the authors of different research papers referred during writing this paper. It was very knowledge gaining and helpful for the further research to be done in future.

REFERENCES:

1.S. T. Sarasamma, Q. A. Zhu, and J. Huff, "Hierarchica-Kohonenen Net for Anomaly Detection in Network Security," Systems, Man and Cybernetics, Part B: Cybernetics, IEEE Transactions on, vol. 35, pp. 302-312, 2005.

2.J. Haggerty , Qi Shi, "Early Detection and Prevention of Denial-of-Service Attacks: A Novel Mechanism With Propagated Traced-Back Attack Blocking" IEEE Transaction on, Vol. 23, 2005.

3.R. Chen, Jung-Min Park, R. Marchany, "A Divide-and-Conquer Strategy for Thwarting Distributed Denial-of-Service Attacks", IEEE Transactions, Vol. 18, 2007

4.R Nagadevi, P NageswaraRao, RameswaraAnand, "A New Way of Identifying DOS Attack Using Multivariate Correlation Analysis", International Journal of Computational Engineering Research (IJCER), Vol.04, 2014.

5.A. G. Saavedra, P. Serrano, J. Widmer, "A Game-Theoretic Approach to Distributed Opportunistic Scheduling Banch" , IEEE Transactions on, vol. 21, 2013.

6.G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.

7.S. Gomathi, "An Efficient Way of Detecting Denial-Of-Service Attack Using Multivariate Correlation Analysis", International Journal of Innovative Research in Computer and Communication Engineering (IJRCCE) Vol.2, 2014.

8.S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient," Parallel and Distributed Systems", IEEE Transactions on, vol. 23, pp. 1073 -1080, 2012.

9.DarshanLalMeena Dr. R.S.Jadon , "A Survey on Different Solutions to DDoS Attacks", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, 2014

10.V. Jyothsna, V. V. Rama Prasad, " A Review of Anomaly based Intrusion Detection Systems", International Journal of Computer Applications, Vol.28, 2011.