Machine Learning Techniques Used in Detection of DOS Attacks: A Literature Review

Niharika Sharma, Amit Mahajan, Vibhakar Mansotra
Department of Computer Science and IT, University of Jammu, Jammu and Kashmir, India

Abstract —Due to increasing complexity of systems, it is easier to compromise computer systems. Thus in order to detect attacks, Intrusion Detection Systems / Intrusion Prevention Systems is employed. Intrusion Detection Systems / Intrusion Prevention Systems is the most basic way to protect the network. IDS/IPS systems follow two different approaches on how to detect intruders: signature-based or anomaly-based detection. A signature-based IDS monitors packets on a specified network and then compares these packets against a set of signatures from known malicious threats. The anomaly-based detection technique centres on the concept of a baseline for network behaviour. Baseline can be considered as description of the type of network behaviour that can be accepted or is normal, any deviation from this baseline is considered as an anomaly. Therefore Anomaly based Intrusion detection uses machine learning techniques to detect whether a packet is intrusive or non-intrusive. The focal point of our study is to provide a systematic review of machine learning techniques used in dos attack detection.

Keywords — IDS/IPS, DOS attack, Machine Learning, Naïve Bayes, decision tree, SVM, ANN

I. INTRODUCTION

Due to increasing complexity of systems, it is easier to compromise systems. A defender is often expected to quickly access the situation and develop an appropriate defence strategy. The defender in this scenario is at weaker position because the attacker has ample amount of time to plan an attack whereas the defender has to immediately access the situation and act accordingly. Intrusion Detection Systems / Intrusion Prevention Systems are the most basic way to protect your own network. IDS detect attacks either using predefined, static signature or based on behaviour of users. Mostly IDS systems follow two different approaches on how to detect intruders: signature-based or anomaly-based detection. A signature-based IDS monitors packets on a specified network and then compares these packets against a set of signatures from known malicious threats. However this method is limited by the fact that it can only identify a limited amount of threats, e.g. generic, or extremely broad, signature. The anomaly-based detection technique centres on the concept of a baseline for network behaviour. Baseline can be considered as description of the type of network behaviour that can be accepted or is normal, any deviation from this baseline is considered as an anomaly.

II. BACKGROUND

WHY DOS ATTACKS?

According to recent reports by Kaspersky Lab fourth quarter of 2015 witnessed that resources in 69 countries were targeted by Botnet assisted attacks. Also fourth quarter saw the longest Botnet based DDoS attack which lasted for 371 hours i.e. 15.5 days approx. Attackers used IoT devices to carry out DoS attacks – for example, researchers found out that 900 CCTV cameras around the world were compromised and formed a botnet later on used for DDoS attacks. A new type of attack was detected by Kaspersky lab experts on web resources powered by the Word Press content management system (CMS), in which JavaScript code was injected into the body of web resources which then addressed the target resource on behalf of the user's browser. One such DDoS attack lasted 10 hours. Thus it is clear that the power of DoS attacks has not diminished with time. Hence it becomes important to detect and prevent such attacks.

DDoS ATTACKS

In "denial-of-service" attack an attackers attempt to prevent legitimate users of a service from using that service, such an attack results in multiple compromised systems. We outline the details of one such common attack for clarity. The TCP protocol usually uses a “handshake” method of establishing connection. In this process, node requesting Connectivity sends a synchronize (SYN) request to the required target to begin the handshake process. The target is required to respond to this request by sending an acknowledgement (SYN/ACK) package back. At last the node requesting connectivity sends another acknowledgement (ACK) back to the target to complete the handshake process, thus establishing a connection. In a TCP SYN attack an attacker(one or more) repeatedly sends SYN connection requests to a specific target, without complete handshake. As a result connection buffer of the target will be filled up with pending connections which will never be completed, and thus preventing it from answering new requests that may be valid.
TYPES OF DOS ATTACKS

DoS attack can be of various types some of them are explained under:

TCP SYN Flood: A SYN flood attack works by not responding to the server with the expected ACK code. An attacker can attack either by not sending the expected ACK back to the client requesting connection, or by spoofing the source IP address while sending SYN request, thus causing the server to send the SYN-ACK to an IP address which did not initiate SYN request, thus it will not send an ACK because it "knows" that it never sent a SYN request. The server will wait for the acknowledgement for some time, as simple network congestion could also be the cause of the missing ACK.

PING Flood: PING flood attack is simple type of DoS attack. In Ping flood attacker sends a series of ICMP Echo request ping packets to the target host on network, the target host sends ICMP reply packets that is ICMP Echo reply as a reply to the request. Due to this continuous Request and Reply packets the network becomes slow and as a result legitimate user have reduce speed network or some time become disconnected.

UDP Flood: Similar to Ping Flood, UDP flood is also type of DoS attack. In UDP flooding an attacker send UDP packet that contains the IP packets to target system with a main purpose of slowing down the target network. Due to slow speed, the target system is unable to handle authorized connections. Thus the server starts rejecting other request of UDP packets after UDP threshold is reached.

LAND DOS attacks: Local Area Network Denial attack is a DoS (Denial of Service) attack in which a special poison spoofed packet in send to a computer, causing it to lock up itself in a loop. This attack involves sending a TCP SYN packet with the target host's IP address as both source and destination to an open port. This causes the machine to reply to itself continuously.

The Smurf Attack: Smurf attack is a distributed denial-of-service attack where large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Most of the devices on a network will respond to this request by sending a reply to the victim's IP address, as a result victim's computer will be flooded with traffic. This can slow down the victim's computer to the point where it becomes impossible to work on.

DDOS attacks: In a distributed denial-of-service (DDoS) attack, multiple compromised systems attack a single target, thereby causing denial of service for users of the victimized system. A series of incoming messages to the target system forces it to shut down, as a result legitimate users denied of their services. In a typical DDoS attack, the attacker takes advantage of vulnerability in one computer system and makes it a DDoS master. The attack master (botmaster), identifies vulnerable systems and then infects them with malware. Eventually, the Botmaster instructs the infected or controlled machines to launch an attack against a specified target. A computer under the control of an attacker is known as a zombie or bot. A group of infected or controlled computers is known as a botnet or a zombie army.

III. MACHINE LEARNING TECHNIQUES USED IN DOS ATTACK DETECTION

Signature based IDS is a human dependent process as it requires several man hours to test, create and deploy those signature and again create new signature for unknown attacks. Thus it becomes necessary to offer a less human dependent system. Anomaly based IDS based on Machine Learning languages provides a solution to this problem, they help in implementing a system that can learn from data and provide prediction for the unseen data based on the learned data. For example, we could train machine learning system on incoming packets so that it can distinguish between intrusive and normal packet. Fig below shows some of the commonly used machine learning techniques for detection of DOS attacks.

<table>
<thead>
<tr>
<th>MACHINE LEARNING TECHNIQUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>DECISION TREES</td>
</tr>
<tr>
<td>SUPPORT VECTOR MACHINES</td>
</tr>
<tr>
<td>NAÏVE BAYES</td>
</tr>
<tr>
<td>ARTIFICIAL NEURAL NETWORKS</td>
</tr>
<tr>
<td>K-MEANS CLUSTERING</td>
</tr>
<tr>
<td>FUZZY LOGIC</td>
</tr>
<tr>
<td>GENETIC ALGORITHM</td>
</tr>
</tbody>
</table>

FIG:1 MACHINE LEARNING TECHNIQUES

DECISION TREES

In Decision tree learning a decision tree is used as a predictive model in which observations about an item are mapped to conclusions about the item’s target value. This predictive modelling approach used in data
mining and machine learning. In the process of decision analysis, a decision tree can be used to represent decisions and decision making visually and explicitly. In this algorithm, the data set is learnt and modelled. Therefore, whenever a new data item is given for classification, it will be classified accordingly learned from the previous dataset.[34] Decision Tree algorithm can also be used for DOS attack detection. Hoda Waguih[1], in his paper proposed an approach to detect DOS attacks, using classification techniques. The above approach lays its basis on classifying “normal” traffic against “abnormal” traffic in the sense of DoS attacks. The paper evaluates the performance of J48 decision tree algorithm for the detection of DoS attacks and then compares it with two rule based algorithms which are OneR and Decision table. Yi-Chi Wu et al.[2] designed a DDoS-detection system based on a decision-tree technique in which after an attack is detected, the system trace back to the attacker’s locations using a traffic-flow pattern-matching technique. A C4.5 classifier is used for detection of dos attacks. Dewan Md. Farid et al.[3] in their paper proposed a learning algorithm for anomaly based network intrusion detection system that distinguishes attacks from normal behaviours and identifies different types of intrusions using decision tree algorithm. Data set used is KDD99 benchmark network intrusion detection dataset. The classes in KDD99 dataset categorized into one normal class and four intrusion classes: probe, DOS, U2R, and R2L. Majed Tabash et al[4] proposed an approach in which decision trees and k-nearest neighbours classification techniques are to detect and classify Dos attacks using EGH dataset.

K-MEANS CLUSTERING

K-means clustering (MacQueen, 1967) is a method commonly used to automatically partition a data set into k groups. It proceeds by selecting k initial cluster centres and then iteratively refining them as follows: 1. Each instance di is assigned to its closest cluster centre. 2. Each cluster centre Cj is updated to be the mean of its constituent instances. The algorithm converges when there is no further change in assignment of instances to clusters.[5] Mangesh D. Salunke et al[6][8] proposed an architecture that captures packets. these packet are the manipulated according to the requirement such as feature selection, transformation etc. then k-means and naive bayes classification techniques are used to classify whether the packet is normal or is DOS attack. Xiaonian Zang et al[7] conducted an experiment mixed the simulated botnet traces with the normal Internet traffic by unifying the RTT extracted from real candidate traffic after filtering. Then the botnet C&C traffic are distinguished using hierarchical and K mean clustering algorithms. This preliminary experiment has shown the capability of the Hierarchical and K mean clustering in detecting botnet flows and provides a RTT adjustment method in mixing the botnet trace with the background normal internet traffic.

SUPPORT VECTOR MACHINES

Support Vector Machine (SVM) was initially proposed by Vapnik and since then has attracted a lot of attention in the machine learning research community. SVMs are set of related supervised learning methods used for classification and regression.[9]. Given a set of training examples, each marked as belonging to one of two categories, an SVM algorithm builds a model that predicts whether a new example falls into one of the two categories. Vipin Das et al.[10] in 2010 conducted an experiment to detect DOS attacks using RST(rough set theory) and SVM (support vector machines). Initially packets were captured from the network and RST was used to pre-process the data. The feature set selected by RST is sent to SVM model to learn and test respectively. Then the results are compared with PCA (Principal component analysis) and shows that RST and SMV could reduce false positive rate hence increasing the accuracy. T. Subbulakshmi et al[11] wrote a paper in which the main objective was to monitor the online network and automatically initiate a defence mechanism if any suspicious activity is encountered. Both non-spoofed and spoofed IP can be detected using this approach. The author uses Enhanced Support Vector Machines (ESVM) to detect Non spoofed IP’s and Hop Count Filtering (HCF) mechanism to detect spoofed IP’s These IP’s are used to initiate the defence process. Lanchester Law is used to calculate strength of the attack which is used to initiates the defence mechanism. Defence schemes such as Rate based limiting or History based IP filtering are automatically initiated to drop the packets from the suspected IP based on the calculated attack strength. Similar to [10] Rung-Ching Chen et al[12] wrote a paper in which RST and SMV were used to detect dos attacks with different feature set (obtained from RST) supplied to SVM. The focus of paper written by T.Subbulakshmi et al [13] was to create the Distributed Denial of Service (DDoS) detection dataset and detect them using the Enhanced Support Vector Machines. Using the generated DDoS dataset the Enhanced Multi Class Support Vector Machines (EMCSVM) is used for detection of the attacks into various classes. The performance of the EMCSVM is evaluated over SVM with various parameter values and kernel functions.

NAÏVE BAYES

Naïve Bayes is a simple technique for constructing classifiers: models that assign class labels to problem instances, represented as vectors of feature values, where the class labels are drawn from some finite set. Paper written by Kanagalakshmi,R et al.[14] proposed that use of Hidden Naïve Bayes (HNB) provides more accurate results than the traditional Naïve Bayes model. Hidden Naïve Bayes (HNB) model can be applied to intrusion detection problems (DOS attacks) that suffer from dimensionality highly correlated features and high network Data stream volumes. It is a data mining model that loosens the naive Bayes methods Conditional impartiality assumption. Mouhammad Alkasassbeh et al[15] in his paper collected new dataset that consist of DOS attacks in different network layers. DDoS attacks are detected using three techniques Multilayer perceptron(MLP), Naïve Bayes and Random Forest. MLP showed the highest accuracy rate (98.63%) as compared to other techniques. Jasreena Kaur Bains et al in [16] proposed an hierarchical layered approach for detection rate of attacks. Model used Naive bayes classifier with K2 learning process on reduced NSL KDD dataset for each attack class. In the proposed model every layer is trained to detect a single type of attack. The
outcome of one layer is passed on to another layer to increase the detection rate. In [17] R Vijayasarathy et al uses a Naive Bayesian(NB) classifier to design a system to detect DoS attacks. The work includes network modelling for two protocols – TCP and UDP. V. Hema et al [18] proposed an intrusion detection system for detection of DOS attacks against Domain Name Server (DNS) has been proposed. The proposed system consist of two parts: a statistical pre-processor and neural network classifier. The former extracts statistical feature and later classifies DOS attacks. At last, Three different neural networks are compared for classifying and detecting various types of DoS attacks. In a paper written by Madhav Kale et al [21] Resilient Back Propagation (RBP) is chosen as base classifier for research. This paper focused on improving the performance of the RBP classifier. The proposed classification algorithm, RBPBoost, is achieved by a combination of ensemble of classifier outputs and Neyman Pearson cost minimization strategy, for final classification decision. Detection accuracy and Cost per sample were the two metrics evaluated to analyse the performance of the RBPBoost classification algorithm. Results show that RBPBoost algorithm achieves high detection accuracy with fewer false alarms. Aim of this paper written by Mohammed Salem et al [22] was to determine if it is is possible for a firewall to analyse its own traffic patterns to identify attempted denial of service. Statistical analyses of firewall logs for a large network were carried out and a baseline determined. Estimated traffic levels were projected using linear regression and Holt-Winter methods for comparison with the baseline. The research proposes a Neural Network model for forecasting rejected traffic falling outside the projected level for the network under study that could indicate an attack. The results of the research were positive with variance from the projected rejected packet levels successfully indicating an attack in the test network. In [23] author Mohammad Masoud Javid et al proposed IDS, that uses supervised neural network to detect DOS intrusions in NSLKDD database. In the proposed IDS, author also used signature-based technique. IDSs is designed using the neural network that can identify different types of DoS attacks and designed a separate IDS for each one to detect that specific attack.

Fuzzy Logic

Fuzzy logic is derived from fuzzy set theory under which reasoning is approximate rather than precisely derived from classical predicate logic. By the help of fuzzy variables or linguistic terms, intrusion detection features can be viewed easily and decision of normal and abnormal activity in the network are based on its fuzziness nature that can identify the degree of maliciousness of a node. In [31] [35]. In [32] author N.Ch.S.N. Iyengar et al. proposed a fuzzy logic based defence mechanism that can be set with predefined rules by which, it can detect the malicious packets and takes proper counter measures to mitigate the DDoS attack. In the paper written by Stavros N. Shiaele et al [33] a method for DDoS detection by constructing a fuzzy estimator on the mean packet inter arrival times is proposed. The problem was divides into two challenges, the first being the actual detection of the DDoS event taking place and the second being the identification of the offending IP addresses. Also author managed to obtain results under a 3 sec detection window. In [24] the author R. Shamugavadi designed a fuzzy logic-based system for effectively identifying the intrusion activities within a network. Author used automated strategy for generation of fuzzy rules, which are obtained from the definite rules using frequent items. The experiments and evaluations of the proposed intrusion detection system were performed with the KDD Cup 99 intrusion detection dataset. In [25], author Vladimir et al proposed a detection and prediction mechanism against DDoS attacks in IEEE 802.15.4 using Fuzzy logic system. The main contribution of Fuzzy based detection and prediction system (FBDPS) was to detect the DDoS attackers by comparing the energy consumption of sensor nodes. The nodes with abnormal energy consumptions are identified as malicious attacker. Furthermore, FBDPS is designed to distinguish the types of DDoS attack according to the energy consumption rate of the malicious nodes.

Genetic Algorithms

Genetic Algorithms are another machine learning approach based on the principles of evolutionary computation. In other words A Genetic Algorithm (GA) is a programming technique that mimics biological evolution as a problem solving strategy. Genetic algorithm based intrusion detection system is used to detect intrusion based on past behaviour. A profile is created for the normal behaviour based on that genetic algorithm learns and takes the decision for the unseen patterns. Genetic algorithms also used to develop rules for network intrusion detection [34]. In [28] the author Anurag Andhare et al generates rules using Genetic algorithm (GA) based approach to detect DoS attacks on the system. Rule set is generated by training GA on KDD Cup 99 data set to detect attacks on the system. To generate a rule set, the algorithm considers different features in network connections of KDD Cup 99. In [29] author Mohammad Sazzadul Hoque et al proposed an Intrusion Detection System (IDS) which efficiently detects various types of network intrusion, by applying genetic algorithm (GA). A number of Parameters and the evolution processes for GA are discussed and implemented. This approach uses evolution theory to information evolution in order to filter the traffic data and thus
reduce the complexity. In [30] author Pankaj Salunkhe et al detects DOS attacks by using Genetic Algorithm (GA) based approach. GA is used to generate rules to detect DOS attacks. The GA is trained on KDD (Knowledge discovery and data mining) cup 99 dataset to generate a rule set that can detect DOS attacks. These rules are applied on IDS system which has a function of data encryption for protecting packets from intruders.

IV. CONCLUSIONS

After thorough review, it is concluded that network attacks are very dangerous and IDS/IPS does not cater to the latest attacks which are affecting the networks. Machine learning techniques are playing a vital role in accessing the severity of the attack and thus helping the organizations to take appropriate decisions to restrict such attacks. In future a comprehensive study will be carried out on the real time data collected from the university network using machine learning techniques. This will help to find the severity of the attacks over the university network, so that appropriate firewall rules will be applied to the network.

REFERENCES


[33] Stavros N. Shiaeles , Vasilios Katos , Alexandros S. Karakos , Basil K. Papadopoulos,’ Real time DDoS detection using fuzzy estimators,’ Elsevier 2 0 1 2
