CHAPTER 3

MODEL design FOR PREVENTING DDOS ATTACK IN PRIVATE CLOUD COMPUTING

1. **OVERVIEW**

This chapter will describe the proposed work of this research: model for preventing DDoS attack based on IDPS system. The main components of the model are DDoS intrusion detection system. Then the detection and prevention phase . In detection phase we have used PCA and LDA for data set classification that have three types of attack : UDP Attack, ICMP Attack, TCP Sync Attack and TCP PSH ACK Attack. With one million records of attacks with 13 features for all attack. In fact, the dataset came from real-world example of a DDoS attack with this characteristic is the CAIDA DDoS Attack 2007 dataset – popular dataset used by DDoS researchers containing approximately one hour of traffic traces from a DDoS attack

1. **THE MODEL DESGIN**

There are strong reasons to propose a new model for prevention based DDoS identification in Net-based system. The model can shown in figure 3.1, and figure 3.2

Figure 3.1 : the general architecture model



Figure 3.2: DDoS hypervisor IDPS cloud

**3.2.1 NETWORK TRAFFIC**

Securing a system from harmful disruptions, either from the system itself or the external attacks is an essential problem since the initial internet age. Usually, a system, especially those are characterized as a safety critical system employs a number of sensors to detect any influential parameters. The acquired value of parameters are than analyzed with particular techniques to determine a system under operation is always in a safe condition.

In case of securing computer network system, beside of keeping the system is at its optimal condition to serve the users, keeping the sensitive data from inappropriate or unauthorized users is also an important issue. In securing the system from any kind of intrusions some sensor like components play an important role. Instead of obtaining physical parameters, the sensors have a role in monitoring traffic across the network. Traffic monitoring is in general the responsibility of IDPS. It captures packets at particular time frame, namely every milliseconds then prevent it. The whole historical data is analyzed carefully to perform a kind of decision support system to detect any inappropriate access at nearly real time manner. From those captured suspicious IP’s IDPS extracts more detail information such as packet size, the origin of IP address, the attacked port number and also its packet type like ICMP, TCP and . In analyzing the traffic data, IDPS might look at the content of the packet to determine whether it contains any malicious code. Otherwise, it make use of any deviations from normal behaviors and profiles. The normal behaviors represent the normal or expected behaviors derived from previous regular activities, network connections, hosts or users over certain period of time.

On the other hand, by identifying deviation from the normal behaviors, the anomaly-based IDPS is able efficiently to detect a novel intrusion. However, it produces higher rate of false alarm. In the matter of traffic data analysis, some research works have previously been conducted in various approaches for various target. However, all of them were applied to the CIDA data set A number of incoming and outgoing packets from a certain port is a common parameter used in analyzing network traffic data where the basic architecture and a detail description of the system is explained.

Traditional packet-based IDS on cloud computing are time-intensive as they analyze all network packets. A state-of-the-art IDS should be able to handle a high volume of traffic in real time. Flow-based intrusion detection is an effective method for high speed networks since it inspects only packet headers. Anomaly-based intrusion detection is a well-known method capable of detecting unknown attacks

**3.2.1 Anomaly Knowledge Profile**

Building the profile of normal behavior and attempting to identify certain pattern or activity deviations from normal profile. Anomaly detection is used to find unknown attacks by using the concept of profiling normal behaviors. But, significant false alarm may be caused because it is difficult to obtain complete normal behaviors. Intrusion detection can be built upon multiple levels in a real computer network system. It will be a choosing the features that characterize the user or the system usage patterns in the best way, such that distinguishing abnormal activities from normal activities is done clearly.

During the early study on anomaly detection, the main focus was on profiling system or user behaviors from monitored system log or accounting log data –which has selected from referenced dataset that we have used

**3.2.3 Packet Capturing Model**

This will take in the incoming network traffic and capture packets for tcp, icmp and udp with all its flags.

**3.3 DDoS Intrusion Detection system**

DDoS Detection Model consists of three main parts

**3.3.1 Feature Extraction Model**

Feature Extraction Model Feature Extraction Model calculates the selected features for captured packets. We propose these features by observing the characteristics of DDoS attack packets. These features can be used to recognize and classify incoming attack packets and will be analyzed in Correlation Engine. Time-window are used as the unit to deal with packet’s features in this model. Experiments showed that these features contain significant information related to the presence of a DDoS attack. However, it takes in the network data and calculates the features for all the packets captured by the packet capturing module. Five different features are calculated like the average packet size, number of bytes, and number of packets, packet rate and bit rate.

**3.3.2 Traffic Aggregation Model**

As we know, DDoS attacks are distributed threats and attack packets are sent through multiple agents distributed on the internet. In reality, it is possible that packets captured from different Source IP addresses, are not recognized as attack packets while aggregation of packets sent from different sources to a specific destination makes a DDoS attack together. Therefore we proposed a Traffic Aggregation Model to aggregates incoming traffic from different sources to one specific destination and sends result table to Correlation Engine to detecting DDoS attack.

**3.3.3 Feature Selection**

Dimensionality reduction algorithms like PCA and LDA are used to select the features. PCA being a well-known algorithm analyses the covariance of each feature, which shown in figure 3.3. The dimensions are reduced further by LDA. LDA being a supervised classification technique provides more class separability .This further reduces the dimensionality of the feature set.



Figure 3.3: the proposed Feature Selection for IDS



Figure 3.4: the future set type

**3.3.3.1 PCA**

Karl Pearson invented the popular dimensionality reduction algorithm called Principal Component Analysis (PCA) in 1901. It is a desirable quality in image compression applications to minimize or reduce the redundancy of the input data(Patil & Mudengudi, 2011). PCA is a statistical analysis technique wherein the input data is projected onto eigenspace to increase the variance and reduce the variables with low eigenvalues. The mathematical representation of the computations is as follows:

Input (Training Set, Test Set)  
Output (Optimal Training Set, Optimal Test Set)

Compute Mean vectors for the input features dataset (

Mean

Step 1: Calculate the scatter matrix – Covariance Matrix

Step 2: Compute Eigen vectors and Eigen values

Step 3 :Sort the Eigen vectors in descending order ,

Step 4 :Project the principal components onto the input features dataset by using the below equation

Although we can use PCA to reduce the dimensions, our method will not lead to good results without having PCA pre-processing. This characteristic makes it possible for distance-based anomaly detection methods to keep their detection rates almost fixed while reducing the number of dimensions, which leads to less computational resources. In the proposed method, we use PCA to reduce the dimensions and transform to a new feature space, in which each feature is a combination of all the original features. As a result, we will have various values of one feature for different samples.

**3.3.3.2 LDA**

To extract the low-dimensional significant features, difference distance maps need to be generated to measure the difference between normal traffic and particular types of attack traffic, such as the difference between each pair of <Normal, Phfattack>, <Normal, Back attack> and <Normal,Apache2 attack>. Afterwards, LDA is employed to select the most signification features for each normal and attack pair based on the pre-generated difference distance maps. Finally, all of the selected features are integrated into a new significant feature set used for normal profile development and malicious behavior detection. For the selection of the most significant features, labeled training samples are required and randomly chosen from a normal sample dataset and various attack sample datasets.

1. Compute Mean vectors for the input features dataset (

Mean

1. Calculate the scatter matrices – within class(Sw) and between class(SB) matrices

M - Overall mean

1. Find linear discriminants by computing the eigen values for Sw-1 SB
2. Select the linear discriminants for the new feature set by sorting and choosing eigen vectors , with highest eigen values.
3. The new feature set obtained by the linear discriminants are then used to obtain transformed input dataset by following equation.

For the Normal Profile Development is utilized to detect the similarity between the normal behavior and new incoming packet. It is developed by using the normal training samples and the selected significant feature set.Without an appropriate criterion, it is hard to achieve a satisfactory detection performance. The larger the threshold value is, the less false positive alarm is generated. On the other hand, smaller threshold will in turn create a higher detection rate.

* + 1. **PCA and LDA FOR ALGORITHM SETTING**

Several variants of LDA have been investigated to address the vanishing of the within-class scatter under projection to a low-dimensional subspace in LDA. However, some of these proposals are ad hoc and some others do not address the problem of generalization to new data. Meanwhile, even though LDA is preferred in many application of dimension reduction, it does not always outperform PCA. In order to optimize discrimination performance in a more generative way, a hybrid dimension reduction model combining PCA and LDA is proposed T.he main goal is to enhance data discrimination that can be achieved with subspaces learned with either PCA or LDA alone. The learning mechanism differs from existing proposals in that it is guided by a hybrid model and thus addresses the problem of generalization to new data in a more direct way. In addition to the model, we developed computational strategies to estimate optimal subspaces

The problem using this model can be simply described as following: given a set of labeled training data from different classes and another set of unlabeled testing data from the same group of classes, identify each testing data relying the new model. Both sets consist of feature vectors in some

Step 1 : Compute Mean vectors for the input features dataset (

Mean

Step 2: Calculate the scatter matrix – Covariance Matrix

Step 3 : Compute Mean vectors for the principal components (

Mean

Step 4 : Calculate the scatter matrices – within class(Sw) and between class(SB) matrices

M - Overall mean

1. Find linear discriminants by computing the eigen values for
2. Select the linear discriminants for the new feature set by sorting and choosing eigen vectors , with highest eigen values.
3. The new feature set obtained by the linear discriminants are then used to obtain transformed input dataset by following equation

**3.3.4 OPTIMIZED FEATURE SELECTION USING ANTLION(ALO(**

Antlion optimization (ALO) is a bio-inspired optimization algorithm proposed by Mirjalili. The ALO algorithm mimics the hunting mechanism of antlions in nature. Antlions (doodlebugs) belong to the Myrmeleontidae family and Neuroptera order. They primarilyhunt in the larvae stage, and the adulthood period is for reproduction. An antlion larvae digs acone-shaped hole in the sand by moving along a circular path and throwing out sand with its huge jaw. After digging the trap, the larvae hides underneath the bottom of the cone and waits for insects/ants to become trapped in the hole. Once the antlion realizes that a prey is in the trap, it attempts to catch the prey. However, insects are typically not caught immediately and attempt to escape from the trap.

Artificial antlion. Based on the above description of antlions, Mirjalili uses the follow infacts and assumptions in the artificial antlion optimization algorithm :

• Prey (ants) move around the search space using different random walks;  
• Random walks are affected by the traps of antlions;  
• Antlions can build holes proportional to their fitness (the higher the fitness, the larger the  
hole);  
• Antlions with larger holes have a higher probability of catching ants;  
• Each ant can be caught by an antlion in each iteration;

• The range of random walks is decreased adaptively to simulat e sliding ants toward antlions;  
• If an ant becomes fitter than an ant lion, this mea ns that the ant is caught and pulled unde r  
th e sand by the ant lion;  
• An antlion repositions to the most recentl y caught prey and builds a hole to improve its  
chan ce of catching another prey after each hunt.  
Formally, the antlion optimization algorithm is given in Algorithm

Algorithm 1: Antlion optimization (ALO) algorithm

Input: Search space, fitness function, numbers of ants and antlions, number of iterations T Output: The elitist antlion and its fitness

1. Randomly initialize a population of ant positions Ant and a population of antlion positions Antlion.
2. Calculate the fitness of all the ants and antlions.
3. Find the fittest antlion; Elite.
4. t = 0.
5. while (t <=T)

foreach anti do

* Select an antlion using Roulette wheel.
* Slide ants toward the antlion as in Eq (2).
* Create a random walk for the Anti and normalize it, as shown in Eqs (4) and (5) for modeling trapping, Eq (6) for random walk, and Eq (8) for walk normalization
* End

6. Calculate the fitness of all ants.

7. Replace an antlion with its corresponding ant if the ant becomes fitter following Eq (1).

8. Update the elite if an antlion becomes fitter than the current elite.

10. t = t+1

end while

The antlion optimizer applies the following steps to an individual antlion:

1. Building a trap: a roulette wheel is used to model the hunting capability of antlions. Ants are assumed to be trapped in only one selected antlion hole. The ALO algorithm requires a roulette wheel operator for selecting antlions based on their fitness during optimization. This mechanism provides high chances to the fitter antlions for catching prey or ants.
2. Catching prey and re-building the hole: this is the final stage in hunting, in which the antlion consumes the ant. It is assumed that prey catching occurs when the ant becomes fit-ter (goes inside sand) than its corresponding antlion. The antlion has to update his position to the latest position of the hunted ant to increase its chance of catching new prey. Eq (1) reflects this process:

Where

t shows the current iteration

Shows the position of the antlion j at iteration t;

indicates the position of the ant i at iteration t; the antlion optimizer applies the following four operations to an individual ant:

|  |  |
| --- | --- |
| 1. Sliding ants toward antlion: antlions shoot sand toward the center of the hole once they realize that an ant is in the trap. This behavior causes the trapped ant that is attempting to escape to slide down. To mathematically model this behavior, the radius of the ants’ random walk hyper-sphere is decreased adaptively using Eqs (2) and (3). |  |

where:

* is the minimum of all variables at iteration t;
* I is a ratio, which is defined in Eq (3):

where:

* t is the current iteration;
* T is the maximum number of iterations;
* w is a constant defined based on the current iteration (w = 2 when t > 0.1T, w = 3 when
* t > 0.5T, w = 4 when t > 0.75T, w = 5 when t > 0.9T, and w = 6 when t > 0.95T). Basically, the constant w can adjust the accuracy level of exploitation.

1. Trapping in the antlion holes: by modeling the sliding of prey toward the antlion, the ant is trapped in the antlion’s hole. In other words, the walk of the ant becomes bounded by the  [position](#page5) of the antlion, which can be modeled by changing the range of the ant random walk toward the antlion position as in Eqs (4) and (5):

where:

* is the minmum of all variables at iterationt;
* is the maximum of all variables at iteration t;
* is the minimumof all variables for anti;
* is the maximum of all variables for ant I;
* represents the position of the antlion j at iteration t.
* Random walks of ant: random walks are based on Eq(6):

Where

* cumsum calculates the cumulative sum;
* T is the maximum number of iterations;
* t is the step of the random walk (iteration);
* r(t) is a stochastic function defined as:

Where rand is a random number generated with uniform distribution over [0,1]. To keep the random walks inside the search space, they are normalized using eq(8) (min-max normalization)

where

is the minimum random walk for variable i;

is the maximum random walk for variable i;

is the minimum of variable i at iteration t;

is the maximum of variable I at iteration t;

Elitism: to maintain the best solution(s) across iterations, elitism has to be applied. In this work, we consider that the random walk of an ant is guided by the selected antlion and by the elite antlion, and hence, the repositioning of a given ant follows the average of both random walks, as shown in Eq(9):

Where

is the random walk around the antlion selected using a roulette wheel;

is the random walk around the elite antlion

**Equation for Random walks of ants**

**For replacing antlion**

**Elitism:**



**3.4 DDoS Prevention System**

**3.3.5 ANN based Detection Classifier**

Detection Classifier – ANN : The antlion fitness of the ALO(output) is used to classify the normal traffic from attack traffic. The best fit antlion gets the highest fitness values. The ANN- feedforward neural network makes use of the antlion

**3.4.1 Reconstruct feature table with IPs, antiion fitness**



**3.4.2** ANN IPS classifier



3.4.3 Attack Traffic on IDPS

3.4.5 Filter attacking Source IP's

**3.4.6 UPDATE SUSPICIOUS IP'S TO ANOMALY KNOWLEDGE PROFILE**

An initial profile is generated over a period of time (typically days, sometimes weeks) sometimes called a training period. Profiles for anomaly-based detection can either be static or dynamic. Once generated, astatic profile is unchanged unless the IDPS is specifically directed to generate a new profile.

A dynamic profile is adjusted constantly as additional events are observed. Because systems and networks changeover time, the corresponding measures of normal behavior also change; a static profile will eventually become inaccurate, so it needs to be regenerated periodically. Dynamic profiles do not have b problem, but they are susceptible to evasion attempts from attackers. For example, an attacker can perform small amounts of malicious activity occasionally, then slowly increase the frequency and quantity of activity. If the rate of change is sufficiently slow, the IDPS might think the malicious activity is normal behavior and include it in its profile. Malicious activity might also be observed by an IDPS while it builds its initial profiles.

**Blacklists and Whitelists**

blacklist is a list of discrete entities, such as hosts, TCP or UDP port numbers, ICMP types and codes, applications, usernames, URLs, filenames, or file extensions, that have been previously determined to be associated with malicious activity. Blacklists, also known as hot lists, are typically used to allow IDPSs to recognize and block activity that is highly likely to be malicious, and may also be used to assign a higher priority to alerts that match entries on the blacklists. Some IDPSs generate dynamic blacklists that are used to temporarily block recently detected threats (e.g., activity from an attacker’s IP address). A whitelist is a list of discrete entities that are known to be benign. Whitelists are typically used on a granular basis, such as protocol-by protocol, to reduce or ignore false positives involving known benign activity from trusted hosts. Whitelists and blacklists are most commonly used in signature-based detection and stateful protocol analysis

Thresholds. A threshold is a value that sets the limit between normal and abnormal behavior. Thresholds usually specify a maximum acceptable level, such as x failed connection attempts in 60seconds, or x characters for a filename length. Thresholds are most often used for anomaly-based detection and stateful protocol analysis.

**Cloud Computing**

Cloud computing is the way to use computing resources as an utility. Both hardware and software can be delivered as a service over a network (typically the Internet).According to Ref. [43], there are two types of cloud: public cloud and private cloud.

* + 1. building cloud computing

A public cloud is designed to apply a pay-as-you-go manner to the general public to provide services. And a private cloud is usually used to deal with the inside data of an organization which are not open to the public. For example, Ref. shows that the IBM smart cloud can provide private cloud service by giving threat protection for every layer of virtual infrastructure, limiting access to critical data, tracking user access and getting virtual infrastructure reports.

1. **Chapter Summary**

This chapter has explained about the new proposed framework for

The purposes of behavior identification process are to analyze the operation of binary program using run time analysis and to observe target operation of

Next chapter will detail out the implementation process of the framework by using specific data for testing.

Patil, U., & Mudengudi, U. (2011). *Image fusion using hierarchical PCA.* Paper presented at the image Information Processing (ICIIP), 2011 International Conference on.