International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue1 | ISSN : 2456-3307

Identification of Peer-to-Peer Botnets in DDOS Attacks

S.Monisha*[1], K.Anitha[2]

*[1]Computer Science and Engineering, R.M.K Engineering College, Chennai, Tamil Nadu, India

[2]Computer Science and Engineering, R.M.K Engineering College, Chennai, Tamil Nadu, India

ABSTRACT

A Distributed denial of service (DDOS) is an coordinated attack generated by multiple computer systems attack a target (i.e) a server, or other network resource and cause a Denial of service (DOS)attack for users. A Botnet is a network of computers under the control of a Bot master. Each individual device in a botnet is referred as a bot. The most common application of botnet includes DDOS attack, Data theft and email spam. In existing approaches there is a difficult in testing the algorithm over more datasets, in order to examine the impact on performance of the nature of the system under attack, and the different behaviors of users surfing on the network. In this paper, we propose a Botnet detection technique by using this technique we can able to handle more datasets as well as we can also identify the bots in the network.To do this a bot scanner is used to scan the incoming file of the normal user if the incoming file is a malicious file then the bot scanner blocks that file and trace the IP address in order to identify botnet in the network.

Keywords:DDOS attack, Botnets,Bot Scanner,IP address.

I. INTRODUCTION

Network security is an activity designed to protect the network from unauthorized users. By securing our network we can safe our data. Effective network security controls the access to the network. It targets a variety of threats and stops them from entering or spreading in our network. It is a specialized field in computer networking that involves securing a computer network infrastructure. Network security is typically handled by a network administrator or system administrator who implements the security policy, needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work. In recent times, P2P has gained tremendous popularity. Most people share resources, programs, documents, movies and games using the system. A significant development during the recent past, made to the original P2P server facilitates the mounting of attacks. In P2P- based architecture, a seed list can be maintained with each host, and when a bot receives a message, it forwards it only to the private list of seeds. Botnets are group of computers which are connected to perform malicious activities such as spreading malware. Each individual system in botnet is referred as bots. These system have been attacked with malicious software that allows them to be remotely controlled.

Some botnets consist of more number of systems even millions of computers. Botnet is a short word for robot network.Like robots, software bots can be either good or bad. The bot doesn‘t always mean a bad piece of software, but most people refer to the type of malware when they use this word. If our system is under the control of a botnet, then it‘s infected with a type of malware(malicious software). The bot communicate a server or gets into contact with other neighbours bots and waits for instructions from the bot master who is controlling the botnet. This allows an attacker to control a large number of systems for malicious purposes. Computers in a botnet may also be infected with other types of attacks, like key loggers which record our financial information and send it to a remote server. Which makes a system part of a botnet is that it‘s being controlled remotely along with many other computers. The botmaster (Botnet creator)can decide what to do with the botnets, direct the bots(individual system in a botnet) to download more types of virus files, and even the bots can act together. You might become infected with a bot in the same way you‘d become infected with any other piece of virus file for example, by running expired software, using the extremely unsafe Java browser plug-in, or downloading and running software. In existing, they offer basically three contributions: 1)Introduce an abstract model for the aforementioned class of attacks, where the botnet emulates normal traffic by continually learning admissible patterns from the environment; 2)Devise an inference algorithm that is shown to provide a consistent (i.e., converging to the true solution as time elapses) estimate of the botnet possibly hidden in the network; and 3) we verify the validity of the proposed inferential strategy on a test-bed environment. Our tests show that, for several scenarios of implementation, the proposed botnet identification algorithm needs an observation time in the order to identify correctly almost all bots, without affecting the normal users activity. There is a difficult in testing the algorithm over more datasets, in order to examine the impact on performance of the nature of the site under attack.

How does DDOS attacks works

DDoS stands for Distributed Denial of service which means attacker send continuous virus file to the targeted system inorder to attack the target resource.The DDOS is a type of a DOS attack which means in a wireless network, a DOS attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources. The network environment lends itself to this type of attack, because it is so convenient for the attacker to direct multiple different messages to the target . In a DDoS attack, the incoming traffic attack the target user originates from many alternate sources potentially from more number of hackers or attackers. Therefore this kind of attack cannot be controlled by just blocking IP address of the attackers because it is difficult to differentiate the normal user traffic and the attacker traffic which is distributed across many areas. Due to the dramatic increase of DDoS attacks, network security defenders must focus on protecting the network community from two basic types of DDoS attacks: (i) network/transport layer DDoS attacks and (ii) application layer DDoS attacks.

1) Network or Transport Layer DDoS Attacks

The main target of this type of attacks is to overwhelm the network infrastructure consisting of servers, routers and switches by sending a large volume of attack traffic. These attacks can be generated by exploiting protocol weaknesses. Network/Transport layer attacks can be further categorized according to degree of automation, exploited attacks, types of attack networks used, attacks rates produced, target types and impacts of the attack.

2) Application Layer Attacks

Application layer DDoS attacks generally target the HTTP protocol with an objective to exhaust limited resources available to Web services. In comparison to network/transport layer attacks, these attacks consume lower bandwidth. The attacker usually customizes them to target a particular Web application by sending requests to tie up resources deep inside the affected network. To accomplish their malicious designs, such attackers require only limited network connections. Typically, such attacks are not trivial to identify because they look similar to legitimate traffic and the volume of traffic is also not too large.

II. RELATED WORK

In [1], They describe about the threats of distributed denial of service (DDoS) attacks have been increasing day-by-day due to rapid development of computer networks and associated infrastructure, and millions of software applications, large and small, addressing all varieties of tasks. Botnets cause a major threat to network security as they are widely used for many Internet fraud such as DDoS attacks, identity theft, email spamming, and click fraud. Botnet based DDoS attacks are trouble to the victim network as they can exhaust both network bandwidth and resources of the victim machine. This survey presents a comprehensive overview of DDoS attacks, their causes, types with a taxonomy, and technical details of various attack launching tools. In [2], Statistical approaches to DDoS attack detection and response which states the idea of the dangers postured by Distributed Denial of Service (DDoS) assaults on expansive systems, for example, the Internet, requests successful identification and reaction techniques. These strategies must be sent at the edge as well as at the center of the system. This paper presents strategies to distinguish DDoS assaults by registering entropy and recurrence arranged dispersions of chose bundle properties. The identification exactness and execution are dissected utilizing live movement follows from an assortment of system conditions running from focuses in the center of the Internet to those inside an edge organize. The outcomes show that these techniques can be powerful against current assaults and propose bearings for enhancing recognition of more stealthy assaults. In [3], Low- Rate DDoS Attacks Detection and Traceback by Using New Information Metrics which states about the low-rate distributed denial of service (DDoS) attack has significant ability of concealing its traffic because it is very much like normal traffic. It has the capacity to the current anomaly-based detection schemes. An information metric can quantify the differences of network traffic with various probability distributions. They innovatively propose using two new information metrics namely the generalized entropy metric and the information distance metric to detect low-rate DDoS attacks by measuring the difference between legitimate traffic and attack traffic. The proposed generalized entropymetric can detect attacks several hops at intially (three hops earlier while the order) than the traditional Shannon metric. The proposed information distance metric outperforms (six hops earlier while the order) the popular Kullback–Leibler divergence approach as it can clearly enlarge the adjudication distance and then obtain the optimal detection sensitivity.In [4], DDoS Attacks With Randomized Traffic Innovation: Botnet Identification Challenges and Strategies in this paper, they proposed an algorithm named BotBuster algorithm which detect bots effectively even in less then 1min to identify it without affecting the normal users‘ activity.In[5], Detecting BOT Victim in Client Networks which states about exploration in distinguishing bot casualty in customer systems. Botnets are accumulations of Internet has (bots) that, through malware disease, have fallen under the control of a solitary substance (botmaster).In [6], Novel Method for Intrusion Detection using Data Mining which states the Intrusion discovery is a fundamental segment of the layered PC security systems. It requires precise and proficient models for breaking down a lot of framework and system review information. The Authors propose a methodology which states about the Modern detection systems use sensor outputs available in the deployment environment to probabilistically identify the attacks [7].

III. IDENTIFICATION OF BOTNETS

We focus on a different type of botnet scan one performed under the command and control(C&C) of the botmaster, occurring over a well-delimited interval. It offers a detailed dissection of the botnet's scanning behavior, including general methods to correlate, visualize, and extrapolate botnet behavior across the global Internet.In Fig.1the botscanner is used which is implemented with coarse grained detection technique.In this technique initially it check the arriving file of the user.Each individual system is implemented with botscanner .When the file arrives the botscanner checks the file (i.e) it checks whether it is a bot file(virus file) or normal file. If it is a virus file the bot scanner determine this by checking each line of a source fileAfter checking the file the bot scanner block that file and forward that file immediately to admin .Then admin traces the IP address of the attacker thereby we can identify the bot and also we can avoid them in doing malicious activities .By implementing this kind of botnet detection technique in DDOS attack we can identify P2P botnets in DDOS attack and also we avoid transmitting virus files as soon as possible before they attacking normal users.

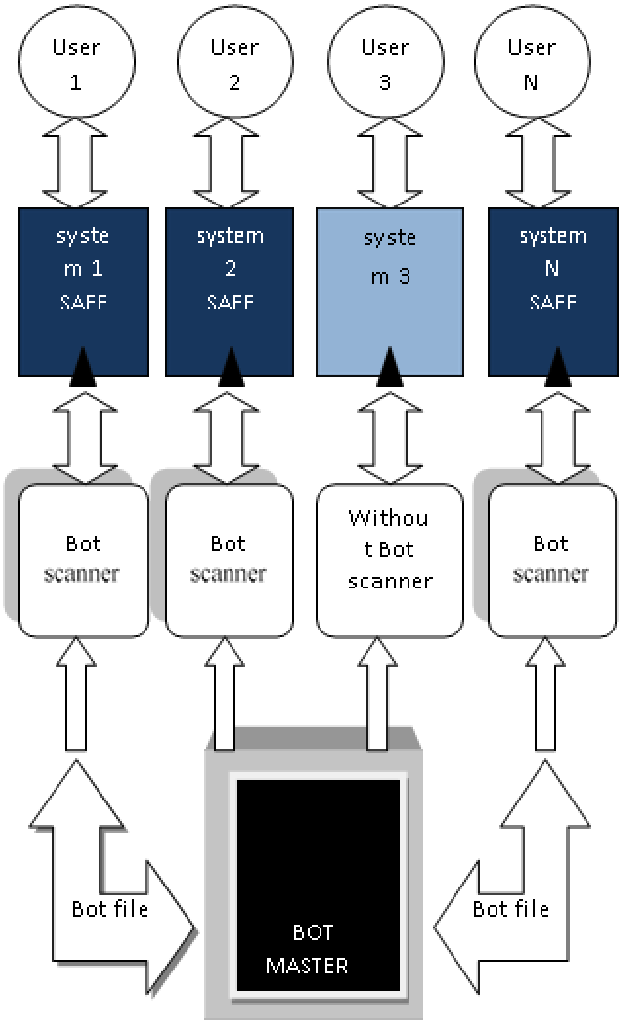

Figure 1. Architecture Diagram

Coarse-Grained Detection of P2P Bots

This technique is used to check the incoming files of the user .Each line of the file is checked. If it is detected as an infected file (i.e) if it contain viral code then it is blocked and the file is transmitted to admin then admin traces the IP address. By using this botnet detection technique we can able to identify stealthy P2P botnets, whose malicious activities are not observable. If the datasets are more, then it can also able to find botnets.

The transmission rate in a network is N(t)

(i.e) $$N(t)= S(\alpha,\lambda B)= \frac{\alpha \lambda B}{\alpha + \lambda B}$$

We design the windows for the project. These windows are used to send a message from one peer to another. We use the Swing package which is in Java to design the User Interface. Swing is a widget toolkit for Java to develope a code . It is part of Sun Microsystems' Java Foundation Classes (JFC) — an API for providing a graphical user interface (GUI) for Java programs. This component is responsible for detecting P2P clients by analyzing the remaining network flows. Here, the user receives a file from another peer system .Now the bot scanner is going to check the arriving file which is implemented with coarse grained detection technique which scan the incoming files of the user .

The user is a normal user then it is described as

$\sum t\to\infty\ n(normal(t)) =1$

The user is a bot user then it is described as

$\sum t\to\infty\ n(Bot(t)) =0$

If there is no normal users in a network then it is described as $B(1\to N) \approx R\ (\alpha,\lambda 1 + \lambda 2+\ldots\ldots.+\lambda\ N) = B$ bot

Then we upload required file from storage device to user account and send the file into destination account. We have different types of files such as data files, text files programming files, spreadsheet files and internet related files. Different types of files store different types of information. If the arrived file is a normal file then bot scanner allow that file to enter in to the user system .Or else if that file is an infected file then bot scanner block that file and does not allow that file to enter into the user system. By this way the bot file is detected and it is blocked by the admin and also bots are detected using Bot Detection Technique. Each of the obtained clusters of flows represents a group of flows with similar size. For each flow, we consider the set of destination IP addresses related to the flows in the clusters, and for each of these IPs. Here the admin cluster the IP address of the blocked file. Furthermore the blocked IP address system could not able to send a file again. From this we can find the IP address of the attacker. At last finally, we can protect the normal user from the attackers.

Table 1. Comparision Of Existing And Proposed Methods

S.No	Parameters	Our Approach (Coarse Grained Detection Technique)	Existing Approach (Botbuster Algorithm)
1.	Time required for identification of bots.	Within Fraction of Sec	Takes up to 1 min
2.	Normal User ratio in the network.	100% of normal users	100% of normal users
3.	Attackers ratio in the network.	100% ofAttackers	100% of Attackers
4.	Botnet identification ratio	98.9% of bots identified	90% of bots identified

If U1=U2 then it is composed only of normal user U1,U2 are the different users in the network.

When (t) increases, the ratio of attacks increase.

D(bot)=Bot(t)^Us(t)/B (i.e)D(t)denotes detected bots.

The transmission rate is denoted as N(t) .where N(t) is the time taken to transmits a file in a network.

N is the number of users in the network Bot(t) denotes bot .

Us(t) denotes User. N(t),Bot(t),Us(t)

```
N={1,2,………,N}
If N≠0 then
Select n1€N then
compare (n1U n2……….n)
If n1≠n2//Compares behavior of n1&n2 Select n1//Normal user
then compare( n2 U n3…..n)//Function gets executed
// upto n values Else
Print n =Bot
```

Here initially we have N number of users in the network,then the system checks whether the number of users is not equal to zero. If the number of user is not equal to zero.It starts processing or else it goes to end.Now select the initial user from the N which is n1 and it is compared with the other user n2 based on their network activity or file sharing between them.By comparing, the system will decide whether they are bots or not. If the comparison matches n1 is declared as bots and it is printed as a BOT or else it is declared as a normal user. Likewise ,the next user n2 is checked with the other user n3 and the function repeats until the value of n is equal to zero.

IV. EXPERIMENTAL RESULTS

The following graph shows the different experimental results

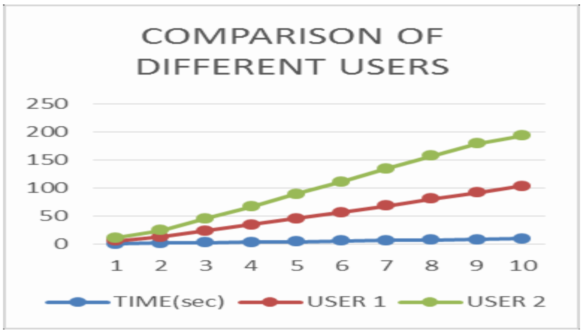

Figure 2. Comparison of users in a network

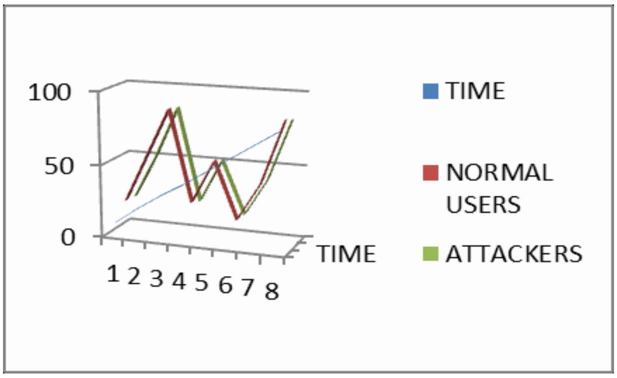

Figure 3. Botnet attacks

Figure 2. represents the different users ratio based on specified time(sec) in a network.Figure 3 denotes the probability of botnet attacks without the knowledge of the Victim(normal) user during certain period of time.Our approach can effectively detect those attacks using bot scanner.

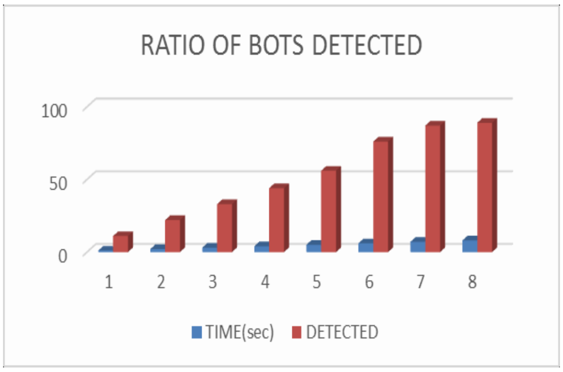

Figure 4. Ratio of bots identified

Figure 4. denotes the ratio of bots detected within specified period of time (sec) by detecting bots in the network we can avoid their malicious activities. Figure 5 describes IP address ratio traced by the admin these are the IP address of the bots.

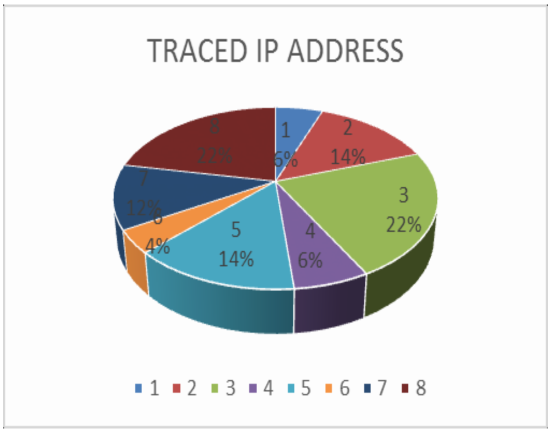

Figure 5. Ratio of IP Address traced

V. CONCLUSION

In this paper, we proposed a botnet detection technique which effectively detect the bot and protect the system from malicious attacks and also capable in supporting more datasets. The experimental result shows that this technique work effectively and stably .The proposed botnet detection formats other than text files such as (Image file, Audiofile,.etc)

VI. REFERENCES

[1]. N. Hoque, D. Bhattacharyya, and J. Kalita, Botnet in DDoS attacks: trends and challenges, IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2242-2270, fourth quarter 2015.

[2]. L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred,Statistical approaches to DDoS attack detection and response,in Proc. DARPA Information Survivability Conference and Exposition, Washington, DC, USA, Apr. 2003, pp. 303-314.

[3]. Y. Xiang,K. Li,and W. Zhou,Low-rate DDoS attacks detection and traceback by using new information metrics, IEEE Trans. Inf. Forensics and Security, vol. 6, no. 2, pp. 426-437, Jun. 2011

[4]. Vincenzo Matta,Mario Di Mauro,and Maurizio Longo, DDoS Attacks with

Randomized Traffic Innovation: Botnet Identification Challenges and Strategies, IEEE Transaction On Networking, August 2017.

[5]. Abinaya. E,Balamurugan. K,Detecting BOT Victim in Client Networks, IEEE Transaction On Networking ,Oct. 2016.

[6]. Sherish Johri , Novel Method for Intrusion Detection using Data Mining, IEEE Transaction OnNetworking nov.2015.

[7]. Z. Berkay Celik1, Patrick McDaniel1, Rauf Izmailov2, Nicolas and Ananthram Swami3 , Building Better Detection with Privileged Information, IEEE Transaction On Networking april 2011.

[8]. W. Stallings, Cryptography and Network Security: Principles and Prac- tice, 6th ed., Pearson, 2013.

[9]. J. Yuan and K. Mills, Monitoring the macroscopic effect of DDoS flooding attacks, IEEE Trans. Depend. Secure Comput., vol. 2, no. 4, pp. 324-335, Oct. 2005.

[10]. L. Li, J. Zhou, and N. Xiao, DDoS attack detection algorithms based on entropy computing, in Proc. ICICS 2007, Zhengzhou, China, Dec. 2007, pp. 452-466.

[11]. J. Luo, X. Yang, J. Wang, J. Xu, J. Sun, and K. Long, On a mathematical model for low-rate shrew DDoS,IEEE Trans. Inf. Forensics and Security, vol. 9, no. 7, pp. 1069-1083, Jul. 2014.

[12]. V. Matta, and P. Willett,Distributed detection with censoring sensors under physical layer secrecy,vol. 57, no. 5, pp. 1976-1986, May 2009.

[13]. M. Barni and B. Tondi,The source identification game: an information theoretic perspective, vol. 8,no. 3, pp. 450-463, Mar. 2013.

[14]. B. Kailkhura, S. Brahma, B. Dulek, Y. S Han, and P. Varshney,Distributed detection in tree networks: Byzantines and mitigation techniques, vol. 10, no. 7,pp. 1499-1512, Jul. 2015.

[15]. M. Mardani,G. Mateos,and G. B. Giannakis,Dynamic anomalography:tracking network anomalies via sparsity and low rank, vol. 7, no. 1, pp. 50-66, Feb. 2013.

[16]. M. Mardani,G. Mateos,and G. B. Giannakis,Recovery of low-rank plus compressed sparse matrices with application to unveiling traffic anomalies, vol. 59, no. 8, pp. 5186- 5205,Aug. 2013.

[17]. Y. Chen, K. Hwang, and W.-S. Ku, "Collaborative detection of DDoS attacks over multiple network domains," IEEE Trans. Parallel Distrib.Syst., vol. 18, no. 12, pp. 1649-1662, Dec. 2007.

[18]. G. Oke and G. Loukas, "A denial of service detector based on maximum likelihood detection and the random neural network," The Comput. J vol. 50, no. 6, pp. 717-727, 2007.

[19]. M. S. Fallah and N. Kahani, "TDPF: A traceback-based distributed packet filter to mitigate spoofed DDoS attacks," Security Commun.Netw., vol. 7, no. 2, pp. 245-264, 2013.