Improved framework for DDoS attack prevention in clustered environment

Rshma Chawla,

Assistant Professor, MMICT&BM, MMU, Mullana (Ambala*)*

Gurpreet Kaur

Assistant Professor, MMICT&BM, MMU, Mullana (Ambala*)*

Abstract

Distributed Denial of Service (DDoS) attack is large scale coordinated attack on the availability of services of a victim system or network resources. We proposed the problem of existing paper is high speed traffic measuring in DDoS attack. This problem is solved by transparency protocol. In existing paper it is just mentioned that it is measured through clustering, but we proposed that when it is divided into clustered traffic it is sent to transparent protocol. Transparent protocol works on the originality of data. In this source & destination address could be used as unique labels for the end system.

Keyword*: DDoS, Transparent protocol, clustering, flooding.*

Introduction

Denial of service attack programs have been around for many years with growth of internet they have increased. A DDoS streams do not have common characteristics as the currently available intrusion detection system (IDS). The aim of DDoS attacks is to make internet based services unavaible to its legitimate users. DDoS attacks is challenging for two reasons. First, the number of attacks involved in DDoS attacks is very large. If the volume of traffic sent by single attacker is small then the victim host is overwhelming. Second, attacker usually spoofs IP address, which is difficult to trace. Three types of flooding attacks are accessed in it TCP/SYN, UDP & ICMP. TCP SYN flood is a most dangerous of the DDoS attack .UDP flood attacks is to exploit the UDP services. UDP packets to different port of a target in random way. ICMP is a smurf attack which is used to put the target resources out of service that results in making the resource stagnate. DDoS attacks network follows two types of architecture. The agent handler architecture and internal relay chat. The agent–handler architecture for DDoS attack is comprised of clients, handler and agents. The attacker communicates with DDoS client system. The handlers are often software packages located through the internet that are used by client to communicate with the agent. The agent software is placed in the compromised system that finally carries out the attack. IRC communication channel is used to connect the client to agent. IRC ports can be used for sending commands to the agents. IRC channel as such channels tend to have large volume of traffic. DDoS defense mechanism approaches are three types of deployment source end, victim end and intermediate end.

Related work

A.Saidi [1] describes the conception of a multi-agent based intrusion prevention system that can apprehend these flooding attempts in distributed way. Three types of flooding DDoS attack SYN; UDP & ICMP are explained in it. The main features of DIDS are communication between its components and a fast analysis to assure a global view of the whole network and an efficient analyzer locally by distributing IDS tasks.

K Govinda [4] proposes a secure data transfer over cluster environment ensures composition of different traffic to handle DDoS attacks in cluster environment. This issue generally is in need of processing huge amount of data. The cloud computing is an extremely success full paradigm of service oriented and has revolutionized by the way computing infrastructure is abstracted and used.

Shahaboddin shamshiraband [2] proposes an IDS calling fuzzy and learning algorithm to protect wireless nodes within network and target nodes from DDoS attack to identify the attack patterned and take appropriate countermeasures .The FQL algorithm was trained and tested to establish its performance by generating attacks from the NSL-KDD. This paper discussed how DDoS attacks are launched in wireless network can be modeled through fuzzy Q-learning algorithm. The purposes of developing such models are included to evaluate whether resources of given system are vulnerable to certain types of attacks. The WSN model is represented in it. The aim of the proposed FQL is to obtain high detection accuracy with a low false alarm rate.

Saman taghavi zarger [6] presents that DDoS flooding attacks are one of the biggest concern of security. In this paper, it describes the DDoS flooding attack problem and attempts to combat it. They categorize the DDoS flooding attack & classify existing countermeasures based on where and when they prevent, detect and respond to flooding attack. An ideal comprehensive DDoS defense mechanism must take specific features to combat DDoS flooding attack both in real time and as close as possible to the attack sources some features are included in it.

Yuri demchenko [12] explains how the proposed model and SDLM SDI can be naturally implemented using modern cloud based infrastructures. The paper refers to different scientific communities to define requirement on data management access control and security. It analyzes the new challenges imposed in modern Q-science infrastructures by the emerging big data technologies. The main goal of the scientific infrastructure is to support the enterprise and operational procedure related to process monitoring and data processing. Cloud technology simplifies building of such infrastructure and provisions it on demand.

Guang Yao [3] proposes a lightweight and efficient framework for router based IP –spoofing filtering named SEFA. IP spoofing is well known security threat on the internet though there have been number of spoofing prevention mechanism due to the diversity of network. If taking into account the evolution of network. Even for a single network there is not always a solution applicable in practice. Operators may want to choose the solution exactly suitable for the network and demand a novel architecture to support spoofing filtering named SEFA (software defined filtering architecture). In route based IP spoofing filtering, SEFA should keep the router mostly unchanged. Operators do not want to offload all the functioning on router to SEFA. It should provide the minimal function set. They do not want to manage a full stack SDN controller.

Herodotus Herodotou [11] introduced starfish a self tuning system for big data analysis. Starfish builds on Hadoop well adapting to user needs and system workload to provide good performance automatically, without any need for users to understand and manipulate the many tuning krobs in Hadoop. Well Starfish is system architecture is guided by work on self tuning database system. Hadoop

is a MAD system that is becoming popular for big data analytics. An entire eco system of tools is being developed around Hadoop. A combination of factors contributes to Hadoop's Madness. First, copying files into the distributed file system is all it takes to get data into Hadoop. Then the Map reduce methodology is to interpret data at processing time not loading time. A system like Starfish is essential as Hadoop users continues to grow beyond companies like Face book, Yahoo etc. Hadoop now is a viable competitor to existing systems for Big data analytics.

Dilip Kumar G [7] surveys of DDoS detection methods are published .it highlights the open issues research challenges and possible solutions. The purpose of this paper is usually to put some order into existing defense methods to ensure that a greater perception of DDoS attack methods maybe accomplished and subsequent better efficient and effective algorithm techniques and procedures to combat these attacks could also be developed. The defense mechanisms like statistical, knowledge, soft computing are deeply explained in it. Defense architectures are divided into three classes: Source End, Victim End & Intermediate defense mechanisms are described in this paper.

T.Poonachandar [9] proposed DOS based adaptive & selective verification mechanisms are effective and efficient compared with the existing methods. Cloud clients can adapt efficiently to an attack by growing the request rate based on timeout windows to calculate attack rates. They conclude ASV advances the state of the art in bandwidth based DOS defense mechanisms by introducing cloud computing technology by using distributed adaptive solutions based on selective verification. It is shown that the effect of ASV on internet cross traffic is minimal and comparable to that of its native non-adaptive counterpart which represents no defense attack scenarios.

Manisha Sharma [13] describes cloud computing has generated a lot of interest and competition in the industry. It is an internet based service delivery model which provides internet based services, computing and storage for users in all market including financial, health care etc. In this paper we did systematic review on different types of clouds and security challenges that should be solved. Cloud security is becoming a key differentiator and competitive edge between cloud providers. This paper discusses the security issues arising in different types of clouds.

Monowar H.Bhuyan [10] presented an overview of DDoS attacks, detection schemes, research issues and challenges .The comparison of the existing detection mechanisms shows that most schemes are not capable of fulfilling all the requirements for real time network defense. Different performance parameters meet be balanced against each other dedicatedly and appropriately performance evaluation using DDoS tools data sets are fully elaborated in it. DDoS attack detection methods which are based on the architecture victim end & source end in network are discussed. The classify methods into major classes are also presented different strategies to evaluate performance of DDoS attack detection methods are described.

Abdullah H.alqahtani [8] concludes the design flaws of TCP/IP suite of protocol have been responsible for most of the attacks on the internet. It always requires security to be applied as an external layer to the TCP/IP suite and this approach causes various problems itself. It presents various attacks directed as TCP/IP and focused on the tools and defense mechanisms to identify the vulnerability that causes these attacks and ways to plug them. Networks sniffers and network analyzers are tools software/hardware used to sniff data flow through a connection .They work in passive mode and only tap into the connection to listen into the packet exchanged without alerting or redirecting some malicious packets. Wire shark, TCP/dump, Kismet, Ettercap are explained in it. IP spoofing & connection hijacking are described in it. IP spoofing involves maliciously creating TCP /IP packets using other IP addresses as source address with the aim to either conceal own identity. Routers use the IP address of destination and forward the packets to it.

Proposed Framework

This section proposes high speed traffic analysis for measuring in DDOS attack. The aim is to detect the DDOS attack at network site. It uses three basic components of IDS controller, analyzer, and response module.

Packets: It can be placed on a segment of a network. Any data like graphics, videos, audios etc that is shared over the network is sent in the form of segments is called packets.

Clustering traffic: According to nature of data stored in packets, these packets are categorized in different types of traffic that is busty traffic(BT),iterative traffic(IT),latency sensitive traffic(lST) and non real-time traffic(NRT).Very large files with huge transfer time is in busty traffic that consumes higher bandwidth and resources. Data that is essential and requires secure transfer is known as iterative traffic, e.g online banking transaction and real time chat messages. These files are smaller in size but require highly secured transfer protocols. Latency sensitive traffic attracts more flooding attacks due to its nature of high bandwidth consumption. Non real time traffic like emails that can be sent with delay categorized in non real time traffic.

Transparent protocol: The entire packet goes to transparent protocol that will check the flow of data. Transparency means originality. It cannot allow slowing down of the processing of normal packets. It could flow essentially unaltered throughout the network and their sources and destination addresses could be used as unique labels for the end system. It is the ability of a network to transport application information while altering or manipulating.e.g.Ipv6 packets cannot transport a payload of a maximum allowable size depending on the maximum transmission unit (MTU) of the relaying telecommunication infrastructure. If the application data generated is bigger than maximum transmission unit (MTU), it is fragmented at the sender side by the network layer process and transmitted in more IP packets delivered completely independently.

Event monitor: It is responsible of counter measure to an intrusion. The event monitor is responsible for all events. Event monitor detects such types or an event like message, alarm, and traffic regulations etc. If events have passive reaction, the system is called intrusion detection system. It audit the intrusion and others extrusion forwards to risk assessment. It warns to all extrusion data and tells about intrusion. It also tells that do not do any significant work because you are in risk. The Risk assessment sends the notifications to all extrusions through e mail or message queue. The audit data sends to server execution agents. The server execution agents have free senseless resource allocation. Other extrusions are in risk assessment that is defined by enabled IDS policies.

Using social networking media new attacks are generating day by day which are no one know about that so it difficult to attempt this framework. Another disadvantage is that it is time consuming. It takes lots of time to transfer the data.

Fig1 shows the said architecture

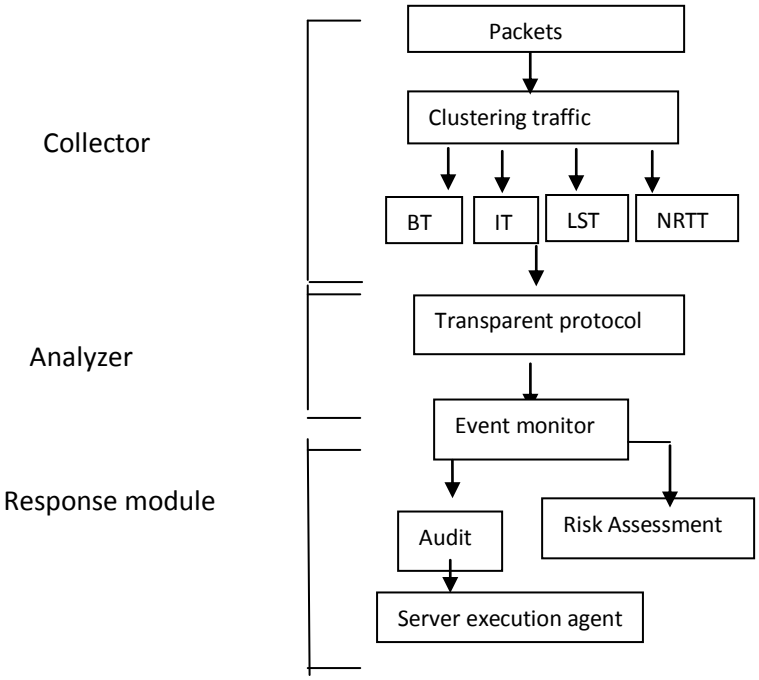

Fig1. Proposed framework of high speed traffic analysis of DDoS Attack

The proposed framework consists of three major modules that are collector, analyzer & response. The collector module is receiving node that collects incoming packets and then these packets are further classified based on the cluster traffic types that are busty traffic (BT), IT (), LST (), & NRTT (). Then these categorized packets are sent to Transparent Protocol in analyzer module in which data in these packets is treated on the basis of category, packets that contains bulk of data are treated with flow control protocols that ensures that packet is given high bandwidth to be transferred over the network. Packets that contain very essential data are treated with highest security protocols. Transparent protocol makes certain that every packet that passes through is clean and contains no malicious data. If any packet seems to be containing any harmful data or is not one of the selected categories, it stops the transfer of that packet and diverts it to event monitor. Event monitor further explores the content of packet received and send it for audit and risk assessment. If no policy against the packet is defined already, server execution agent creates a new security policy for the kind of packet received.

Open issues and challenges

The challenges impact the effectiveness of product and feasibility of their wide adoption.
1) During the rise of mobile device use, cloud computing is used &shared everything in social networking are being used.

2)The high volume & variety of data make it difficult to determine what is important, what should be collected, where it should be stored .some possible data sources include proxy logs, email Meta data, firewall logs, Ids logs, IPS logs.
3) The most notable assumption is that attack behavior is some, how different from normal traffic but attackers might hide their activities in normal traffic.
4) The high diversity of traffic on today's networks increases the challenge. There is an increasing amount of variability in network traffic that operators need to manage.
5) It is becoming more difficult to understand normal traffic and detect the important signal in the noise.
6) Lack of defense system benchmark. Researchers cannot compare actual performance of their solutions to exiting defenses.
7) Difficulty to large scale testing .This is currently impossible due to the large scale test beds, detailed and realistic tools that can support several thousand nodes.
8) Cross layer protocol which used in layers of network, it knows all the information about entire layers simultaneously.

References

[1] A. Saidi, A.Kartik, " A Multi-agent based Distributed Intrusion Prevention system against DDoS flooding attacks," Journal of Theoretical and Applied Information Technology, ISSN:1992-8645, Vol 59, No. 2, 20th Jan, 2014.

[2] Shahaboddin Shamshiraband, Nor Badrul Anwar, "Anomaly detection using Fuzzy Q-learning Algorithm," Acta Polytechnica Hungarica, Vol.11, No. 8, 2014.

[3] Guang Yao, Jun Bi, "Performing Software defined Route Based IP Spoofing Filtering with SEFA", 978-1-4799-3572-7/14©2014, IEEE.

[4]K. Govindra, E-Saththyamoorthy, "Secure traffic management in Cluster environment to handle DDoS attack," World Application Sciences Journal 32(9): 1828-1834, 2014.

[5] lovepreet kaur, abhinav bhandari,"DDoS attacks and various detection mechanisms", international journal for technology research I engineering vol 1, issue 9, May 2014.

[6] Saman Tagghavi Zarger, James Joshi and David Tipper, "A survey of Defense Mechanisms against distributed Denial of service (DDoS) flooding attacks, IEEE Communications Surveys and Tutorials, 15(4): 2046-2069, 2013.

[7] Dileep Kumar G, Dr C V Guru Rao,"A survey on defense mechaniary counting DDoS attack in the networking."International Journal of Advanced Research in Computer and Communication Engineering Vol 2, issue 07 July, 2013.

[8] Abdullah H. Algahtani, "TCP/IP attack, Defenses and Security Tools," International Journal of Science and Modern Engineering (IJISME), ISSN: 2319-6386, Volume-1 issue 10 Sep, 2013.

[9]T.Poonachandar, D.jaya prakash,"Denial of service (dos) attacks detection in cloud computing "Indian journal of research, volume: 2, issue 11, Nov 2013.

[10]Monowar H. Bhuyan, H.J.Kashyap, "Detecting Distributed Denial of service attacks methods, tools and future directions." Springs, (080933-7150, U.S.A. December 2012.

[11]Herodotus Herodotou, Harold Lim, "Starfish: A self-tuning system for Big Data Analysis."5th Biennial conference on innovative Data systems research (CIDR'II).Asilonar, California, U.S.A January 09-12-2011.

[12] Yuri G. Dantas, Vivek Nogam**,** "A selective Defense for Application Layer DDoS attacks," Federal University of Paraiba, Joao Pessoa, Brazil,2011

[13]Tripathi, Manisha Sharma, A mishra,"cloud computing security consideration "signal processing communication and computing (IPSCC), IEEE international conference 2011.