www.ijiarec.com

ISSN:2348-2079

Volume-6 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Local flow packet marking for network coding in manets

P. Vasanthakumar, Mrs. Umamaheswari A. M.E.

CSE, Department of CSE, Mahendra Engineering College

Assistant Professor, Department of CSE, Mahendra Engineering College

ABSTRACT

As in the case of DDOS attacks the attacker sends a large volume of malicious packets which later prevent the legitimate user to access the services, therefore our prime concern is to find out the no of packets being malicious in the legitimate requests and then mitigates them by an appropriate mechanism. In this paper an Analytical approach based on a mathematical equation which will be used to find out the no of packets being malicious under legitimate data packets and an algorithm which is a refined method of traditional hoop count inspection mechanism to mitigate the malicious packets which are coming along with the legitimate data from the attacker side and can pose a threat to the network performance.

Keywords: Ddos, Packets, Mitigate.

INTRODUCION

The existing network may connect multiple stub networks, which could make a single IP address to appear and have multiple valid hop-counts at the same time, which further require enchantment Some of them may have certain practical value, but they have to reconstruct the existing network and the routing instruments with great cast that DDoS attacks are posing a vital threat to the emerging Cloud Computing environment, its now become very essential to provide an effective mechanism that Mitigate these attacks. Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a victim computing system or network resource. When the operating system notices the high workload on the flooded service, it will start to provide more computing power to cope with the additional workload. The attacker can flood a single, system based address in order to perform a full loss of availability of the intended service. A Distributed Denial of Service (DDoS) attack is a large scale, coordinated attack on the availability of services of a victim system or network resource, launched indirectly through many compromised computers on the Internet. The services under attack are those of the "primary victim", while the compromised systems used to launch the attack are often called the "secondary victims". The use of secondary victims in performing a DDoS attack provides the attacker with the ability to wage a much larger and more disruptive attack, while making it more difficult to track down the original attacker. A Distributed Denial of Service (DDoS) attack uses many computers to launch a coordinated DoS attack against one or more targets [1-6].

Using client/server technology, the perpetrator is able to multiply the effectiveness of the Denial of Service attack. To keep in view the gravity of DDoS attack's and focus the research to provide a mechanism to mitigate these attacks by using an Analytical approach. The DDoS attacks on environment that warrant further research as the existing network may connect multiple stub networks which could make a single IP address to appear and have multiple valid hop-counts at the same time which further require enchantment in the our proposed algorithm HCI-MPR to check the

Author for correspondence:
CSE, Department of CSE, Mahendra Engineering College

credential of the sender for legitimate packets Secondly, so need a systematic procedure for setting the parameters according to the cloud environment for our proposed algorithm so that it shows effective results against real spoofed DDoS traffics. The data-compression techniques may interfere with latency requirements imposed by the application, as the nodes must wait to accumulate and aggregate received information. Some scenarios do not require support from all layers. Consider a Multi hop local positioning system based on hop-by-hop distance measurements to estimate the relative distance between an arbitrary node and an anchor node. The network layer and transport layer, used to handle the end-to-end data transmissions, are not required in this application. Consequently, these layers can be omitted [7-11].

LITERATURE SURVEY

"A Novel Attack Path Reconstruction Based on Packet Logging & Marking Scheme"

The internet is a worldwide network that combines millions local to global scope, private, public, academics, business, optical network technologies, government networks. It carries an expandable range of information resources and services which lead to bulk exchange of traffic over the Internet every day. This excessive popularity creates some troubles in the networks. Among them, Flash Crowd and Distributed Denial of Service (DDoS) attacks are the two major events. Web services need stability and security from these two concerns. There are some methods that can discriminate DDoS attack from flash crowd and trace the sources of the attack in huge volume of network traffic. However, it is difficult to detect the exact sources of DDoS attacks in network traffic when the Flash crowd event is also present. Due to the likeness of these two anomalies, the attacker can easily mimic the malicious flow into legitimate traffic patterns and defense system cannot detect real sources of attack on time. In this paper, entropy variation, a theoretic parameter, is used to discriminate DDoS attack from Flash Crowd and trace the sources of the DDoS attack. Entropy variation is a theoretic concept which is a measure of changes in concentration of distribution of flows at a router for a given time duration. The proposed strategy is effective and efficient, scalable that has several advantages like memory non intensive, minimum overhead in terms of resources and time, and independent of the traffic pattern.

DDoS attack shares some characteristics with flash crowd, but it's not the same. The server's internet connection is overloaded by both DDoS attack and flash crowd and result in partial or complete failure. Because of the vulnerability of the Internet, attackers can easily mix their traffic patterns in legitimate network traffic or hide attack flows into legitimate flows. Attack sources mimic to be legitimate users and send a large amount of malicious packets that can flood the target victim. This problem beat defense system and they cannot detect the attack sources in time. So it is necessary to discriminate legitimate flows from malicious flows.

"A hybrid approach to counter application Layer DDoS attacks"

Distributed Denial-of-Service (DDoS) attacks are a growing threat across the Internet, disrupting access to Information and services. Now days, these attacks are targeting the application layer. Attackers are employing techniques that are very difficult to detect and mitigate. This paper proposes a hybrid detection scheme based on the trust information and information theory based metrics. Initial filtering is based on the trust value scored by the client. Then the information based metric, entropy, is applied for final filtering of suspicious flow. The trust value for a client is assigned by the server based on the access pattern of the client and updated every time when the client contacts the server. The request from the client always includes this trust value to identify itself to the server. The Web user browsing behavior (HTTP request rate, page viewing time and sequence of the requested objects) of the client is captured from the system log during non-attack cases. Based on the observation, Entropy of requests per session is calculated and used for rate limiting the flow further. A scheduler is included to schedule the session based on the trust value of the user and the system workload. The detection mechanism

combines two algorithms to detect the sources of the attack.

1. Local flow monitoring algorithm and
2. IP trace back Algorithm.

This methodology reduces the operational workload; storage space required for routers, detection time and performs in terms of scalability that can be handled.

Distributed Denial-of-Service (DDoS) attacks are a dangerous hazard to the web. On the other hand, the memory less quality of the Internet routing technique makes it enormously solid to trace back to the source of these attacks. As a result, there is no successful and proficient technique to deal with this issue so far. In this paper, It recommend a novel efficient trace back technique for DDoS attacks that is based on entropy variations between ordinary and DDoS attack traffic, which is basically diverse from frequently used package marking techniques.

METHODOLOGY

In the proposed system a novel trace back method for DDoS attacks that is based on entropy variations between normal and DDoS attack traffic, which is fundamentally different from commonly used packet marking techniques. The PPM (Probilistic Packet Marking) or LFPM (Local flow Packet marking) trace back mechanisms and it outperform the available PPM and LFPM methods. Because of this essential change, the proposed strategy overcomes the inherited drawbacks of packet marking methods, such as limited scalability, huge demands on storage space, and vulnerability to packet pollutions. The implementation of the proposed method brings no modifications to current routing software. Both PPM and LFPM require updating on the existing routing nodes, which is extremely hard to achieve on the Internet. On the other hand, the proposed method can work independently as an additional module on routers for monitoring and recording flow information, and communicating with its upstream and downstream routers when the push-back procedure is carried out.

One of the most serious threats to the Internet, security is a DoS (Denial of Service) attack; where an attacker attempts to make a target host (called a victim) fail by sending a huge number of packets to the host. In particular, in recent years, a DDoS (Distributed DoS) attack, where there are many attackers scattered over the Internet, has become more prevailing. Such a DDoS attack can be represented by an attack tree, the leaves and the root of which are the attackers and the victim, respectively. Furthermore, the path along which an attack packet traverses from one attacker to the victim an attack path. A promising countermeasure against DoS/DDoS attacks is called the IP trace back. In IP trace back schemes, each router on attack paths, stores information about the paths on itself or on packets. Then the victim uses the information to recover the attack tree and to find out the attackers. IP traces back schemes are roughly classified twofold: probabilistic packet marking (PPM for short) protocols and logging ones. In PPM protocols, each router probabilistically writes path information onto the packets it receives. On the other hand, logging IP trace back protocols make each participating router sample packets, and store path information on itself IP trace back schemes are roughly classified into probabilistic packet marking (PPM) protocols and logging ones. PPM does not need storage resource of routers, although, it generally requires the victim to receive a large number of packets before he can reconstruct the attack tree.

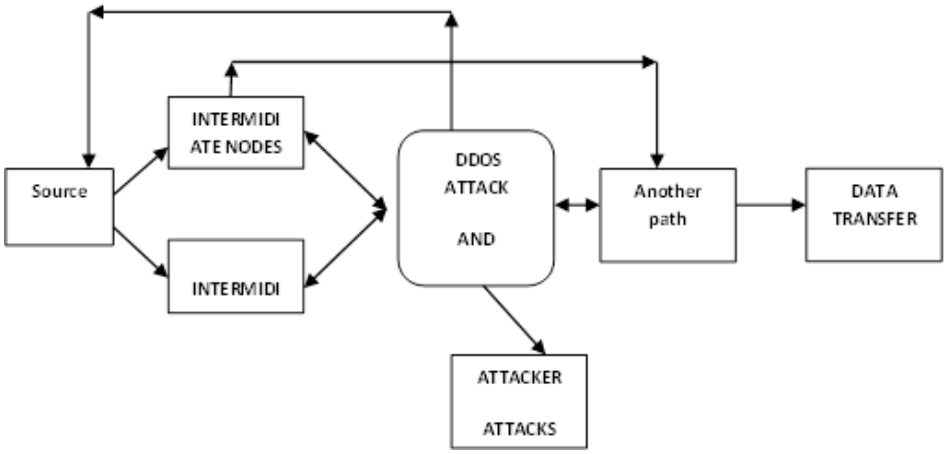

Fig 1.Architecture of Proposed System

RESULT AND ANALYSIS

Trace graph is a free tool for analyzing the trace files generated by ns2. Trace graph can support any trace format if converted to its own or ns2 trace format. Trace graph runs under Windows, Linux, and UNIX and MAC OS systems.

Some of the program features are as follows:

- 238 2D graphs: Trace graph supports drawing 238 different graphs depending upon different parameters in the 2 Dimensional area.
- 12 3D graphs: Trace graph supports 12 graphs in 3 Dimensions.
- Delay: This is the delay encountered between the sending and receiving of the packet.
- Jitter: This is the unwanted variation in the output.
- Processing Time: The time it takes for a node to process the input.
- Round Trip Time: The time required for a signal pulse to travel from a specific source to a specific destination and back again.
- Whole network, link and node graphs and statistics.
- All the results can be saved to text files, graphs can also be saved as JPEG and tiff.
- Any graph saved in a text file with 2 or 3 columns can be plotted.
- Script files processing to do the analysis automatically.

It sometimes hangs after displaying the graph in 3D. The reason why this tool was used in the simulation work is that there are not too many graphs plotting tools available in the market.

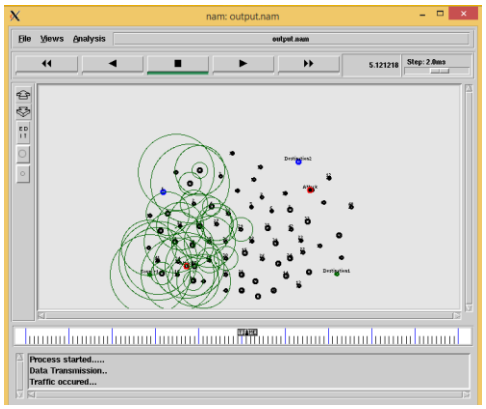

Fig .2 Find another Way And Resent Packet To Destination

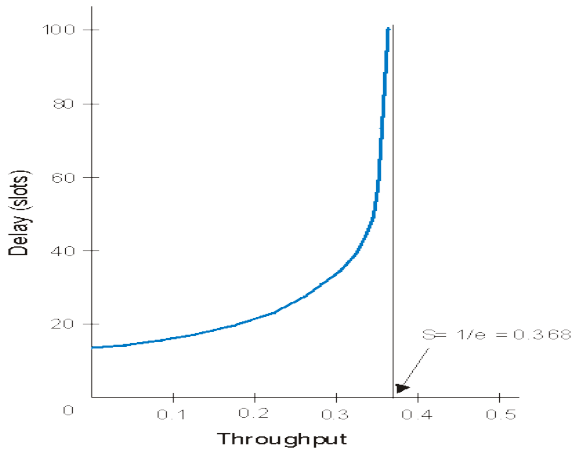

Fig.3 max throughput radio

CONCLUSION

Distributed Denial-of-Service (DDoS) attacks are a growing threat across the Internet, disrupting access to information and services. Now days, these attacks are targeting the application layer. Attackers are employing techniques that are very difficult to detect and mitigate. This paper proposes a hybrid detection scheme based on the trust information and information theory based metrics.

Initial filtering is based on the trust value scored by the client. Then the information based metric, entropy, is applied for final filtering of suspicious flow.

The trust value for a client is assigned by the server based on the access pattern of the client and updated every time when the client contacts the server. The request from the client always includes this trust value to identify itself to the server.

The Web user browsing behavior rate, page viewing time and sequence of the requested objects) of the client is captured from the system log during non-attack cases. Based on the observation, Entropy of requests per session is calculated and used for rate limiting the flow further.

A scheduler is included to schedule the session based on the trust value of the user and the system workload.

The future work implements the security level based data transmission on the network. It carries an expandable range of information resources and services which lead to bulk exchange of traffic over the Internet every day. This excessive popularity creates some troubles in the networks. Among them, Flash Crowd and Distributed Denial of Service (DDoS) attacks are the two major events.

REFERENCES

[1]. Chuchu Wu, Mario Gerla, and Mihaela van der Schaar,"Social norm incentives for network coding in MANETs", IEEE 2017, 2374-9660.

[2]. R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network infor- mation flow," IEEE Trans. Inf. Theory, 46(4), 2000, 1204–1216.

[3]. R. Koetter and M. Médard, "An algebraic approach to network coding," IEEE/ACM Trans. Netw., 11(5), 2003, 782–795.

[4]. S.-Y. R. Li, R. W. Yeung, and N. Cai, "Linear network coding," IEEE Trans. Inf. Theory, 49(2), 2003, 371–381.

[5]. S.-H. Lee, M. Gerla, H. Krawczyk, K.-W. Lee, and E. A. Quaglia, "Quantitative evaluation of secure network coding using homomorphic signature/hashing," in Proc. NetCod, Beijing, China, 2011, 1–10.

[6]. Z. Yu, Y. Wei, B. Ramkumar, and Y. Guan, "An efficient signature-based scheme for securing network coding against pollution attacks," in Proc. IEEE INFOCOM, 2008, 1409–1417.

[7]. J. Joy, Y. Yu-Ting, V. Perez, D. Lu, and M. Gerla, "A new approach to coding in content-based MANETs," in Proc. Int. Conf. Comput., Netw. Commun. (ICNC), Honolulu, HI, USA, 2014, 173–177.

[8]. S. Bhadra, S. Shakkottai, and P. Gupta, "Min-cost selfish multicast with network coding," IEEE Trans. Inf. Theory, 52(11), 2006, 5077–5087.

[9]. J. Price and T. Javidi, "Network coding games with unicast flows," IEEE J. Sel. Areas Commun., 26(7), 2008, 1302–1316.

[10]. Pragya Katiyar, U.Senthil Kumarn "Detection and Discrimination of DDOS Attacks from Flash Crowd Using Entropy Variations" 5(4), 2013.

[11]. "ETM: a novel Efficient Trace back Method for DDOS Attacks", 1(3), 2012.