Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.320 – 327

RESEARCH ARTICLE

PROTECTING PROXY BASED NETWORK FROM DDoS ATTACKERS WITH IP SPOOFING DETECTION

Yedu Krishnan.R
Department of Computer Science, Mahendra Institute of Technology, Mallasamudaram,
Tiruchengode, TamilNadu, India
yedukrishnan.r@gmail.com

A.Anbumani
Department of Computer Science, Mahendra Institute of Technology, Mallasamudaram,
Tiruchengode, TamilNadu, India
anbuinfo2006@gmail.com

Abstract: Distributed Denial of Service (DDoS) attacks along with IP spoofing is a major threat faced by networks. The problem is more complicated in case of proxy networks as it is difficult to identify the particular attacker node. A perfect novel server-side defense scheme is proposed to resist DDoS attack by identifying and blocking the particular attacker node along with provision for IP spoofing detection. A TSL-IP based HsMM algorithm and a Hop-count detection algorithm were proposed to detect attackers and spoofed IPs. The approach utilizes the TSL behavior of the requesting nodes to identify attacks and IP of the node as a unique identity to identify the particular attacker node, which makes the scheme more accurate than existing schemes. Soft control is a novel attack response method proposed in this work. It performs behavior reshaping that tries to converts a suspicious traffic into a relatively normal one before rudely discarding them. The Proposed variation in HTTP protocol supports for identifying which client is intruder rather than detecting the innocent web proxy. The TTL based filtering performs a mapping between IP addresses and their hop-counts to identify spoofed IP packets.

Keywords--DDoS, TTL, TSL, soft control, IP spoofing, Hop-count

I. INTRODUCTION

A proxy server, also known as a "proxy" or "application-level gateway", is a computer that acts as a gateway between a local network (e.g., all the computers at one company or in one building) and a larger-scale network such as the Internet. Proxy servers provide increased performance and security. A proxy server works by intercepting connections between sender and receiver. All incoming data enters through one port and is forwarded to the rest of the network via another port.

There are number of proxy-based networks today and there are many problems associated with these proxy- based networks. One of the main such problem is the DDoS attacks [13] in proxy-based networks. A Web proxy may be turned easily into an attacker by two steps: In the first step the attacker sends attack requests to a Web proxy and forces it to forward the attack requests to the origin server. In the second step the attacker disconnects connections between itself and with the proxy.

Security is of greater importance in proxy-based networks. Although most of the large-scale official proxies are usually configured to be secure, they cannot avoid being abused for the proxy based attacks. This type of attacks may bring new challenges to existing network security systems. Motivated by these issues, a novel resisting scheme is proposed to protect the origin server from web proxy-based HTTP attacks in this work. The proposed scheme is based on network behavior analysis. It maps a Web proxy’s TSL-IP behavior to a hidden semi-Markov model which is a typical double stochastic processes model. The output process of an HsMM [14] profiles the observable varying process of a proxy-to-server traffic which helps to identify attack behavior and by analyzing the IP it enables the detection and blocking of the particular attacker node.

TSL-IP based HsMM algorithm utilizes the TSL-IP behavior (Temporal and Spatial Locality behavior along with a unique client identity IP), which is processed to an HsMM chain. The hidden semi-Markov chain of an HsMM describes the transformation of a proxy’s internal behavior states that can be considered as the intrinsic driving mechanism of a proxy to server traffic. In such behavior model, detecting the abnormality of a Web proxy can be achieved by measuring the deviation between an observed behavior and the Web proxy’s historical behavior [15] profile. Long-term and short-term behavior assessment methods are proposed. Long-term behavior assessment provides warnings on a large scale whereas the short-term behavior assessment locates abnormal request sequences embedded in the proxy-to-server traffic. Here we propose a TSL based behavior analysis with IP based filtering to accurately detect the particular attacker client.

One of the main attacks which arise along with DDoS attacks is the IP spoofing [9][12][26]. When DDoS attacks in proxy-based networks arises along with IP spoofing the scene become worse and most of the detection mechanisms will fail. The mechanism described above will also fail in such case. So here we are integrating a perfect IP spoofing detection mechanism along with above described method to form a new scheme which perfectly defends DDoS attack along with IP spoofing. For IP spoofing filtering we use a Hop-count detection algorithm**.** This server side technology can be made implemented in large proxy-based networks. The proposed system will be able to be used as an efficient defending mechanism in the server –side against DDoS attack and IP spoofing in proxy-based networks.

II. RELATED WORKS

Traditional defense techniques focus on the network-layer DDoS attacks and use TCP and IP properties to discover attack signals arising. Since the HTTP-based DDoS attacks work on the application-layer and employ a new attack mechanism, the classical methods designed for the network-layer attack are no longer applicable. In such cases there is a need for application-layer DDoS detection mechanisms. However there are many schemes existing and some of them are as follows:

In [1], the clients are evaluated by a trust management mechanism, and then the application layer DDoS is mitigated by giving priority to good users. In [2], the zombies are identified by automatically changing puzzle, and then the HTTP requests of suspected hosts are blocked. In [3], a model is proposed to profile the normal access behavior based on four attributes of web page request sequences. The reconstruction error of a given request sequence is used as a criterion for detecting DDoS attacks. In [11], the flow correlation coefficient was used to measure the similarity among suspicious flows, and then the HTTP-based DDoS attacks from normal flash crowds were discriminated by the results of measurement. A traceback method was explored for the DDoS attacks based on entropy variations in [10]. In [17], user browsing behavior is applied to distinguish the anomalous HTTP requests from those of normal users. In [23], a multidimensional access matrix is defined to capture the traffic behavior of flash crowds and detect HTTP attacks that mimic or occur during the flash crowd event of a popular Web site.

All the above schemes are based on the assumption that the origin server is in direct contact with the clients. The case is true in normal networks but is not true in proxy-based networks. Hence based on the above mechanisms it is difficult to identify the particular attacker node (not the proxy) in a proxy-based network. In [24], the browsing behavior is utilized to form markovian chain using HsMM to identify abnormal proxy. This is a scheme meant for proxy-based networks. This scheme in [25] perfectly identifies the attacking proxy but fails to identify which client is the attacker. As a result sometimes this method will block innocent proxies. The scheme also fails to identify IP spoofing.

Some of the DDoS attacks, such as smurf [9] and Distributed Reflection Denial of Service (DRDoS) attacks [12], [26], are not possible without IP spoofing. Such attacks masquerade the source IP address of each spoofed packet with the victim's IP address. Overall, DDoS attacks with IP spoofing are much more difficult to defend. There are many router-based and host-based approaches to defend DDoS attacks along with IP spoofing. However, these router-based solutions require not only router support, but also coordination among different routers and networks, and wide-spread deployment to reach their potential. In contrast to the router-based approach, the host-based approach can be deployed immediately. Moreover, end systems should have a much stronger incentive to deploy defense mechanisms than network service providers. These host-based schemes will fail in case of huge proxy networks.

To overcome the demerits of above described schemes, we are proposing a perfect server side defense scheme which is capable to identify and defend the particular attacker nodes along with a perfect filtering mechanism to withstand the effects of IP spoofing. A hop-count based spoofing detection is used, which is perfect. Thus it can prevent DDoS attacks arising along with IP spoofing.

III. PROPOSED SYSTEM

The aim of the proposed scheme is to provide a security application which accurately detects and blocks DDoS attack creating nodes in a proxy-based network. The aim also extends to detect IP spoofing too. The application could be easily deployed in the origin server. Here we are proposing two main algorithms, a TSL-IP based HsMM algorithm for DDoS attack creating client detection and a Hop-count based algorithm for IP spoofing detection.

A. ALGORITHMS

A.1. TSL-IP BASED HsMM

```
Input : User request url ($U_i$)
Output : Attacker client (IP)

For each page $P_i$
    Get all possible links;
End For
    Group the possible links to sequence $X_i$;
    Insert $X_i$ to db;
For each url $U_i$
    For each sequence $X_i$
        If $U_i$ contains any of $X_i$;
            Add $U_i$ to separate sequence $S_i$;
        End If
    End For
End For
For each separate sequence $S_i$
    If length($S_i$) > Temporal/Spatial threshold
        Mark $S_i$ as attack url $A_i$;
    Else
        Delete $S_i$ from separate sequence;
    End If
End For
For each $U_i$ and $A_i$
    If source($U_i$)=source($A_i$)&$U_i$ contains any $A_i$;
        Identify source as attacker;
    Else
        Exceptional condition;
    End If
End For
```

A.2. HOP-COUNT BASED FILTERING

```
Input : Packet P and IP
Output : Status spoofed or not (G or B)
For each packet P:
    Extract the final TTL $T_f$ and the source IP address S;
    Infer the initial TTL $T_i$;
    Compute the hop-count $Hc=T_i-T_f$;
    Index S to get the stored hop-count $H_s$;
    If ($H_c!=H_s$)
        The packet is spoofed B;
    Else
        The packet is legitimate G;
    End if
End For
```

B. SYSTEM MODULES

B.1. TRAINING & DETECTION PHASE

The main step involved in the training phase is the attack learning. The attack learning is a complex process in which the request sequence characteristics are studied. The main characteristics here we take into account is the TSL or the Temporal and Spatial behaviors. The incoming requests are treated as queries which are then compared against each attack classes. The request is then assigned with the attack type that provides the best match using probability distribution. Then identify the temporal and spatial sequence and their distance.

During the comparison high priority is given to TSL behavior rather than normal behaviors. If any sequence found within the distance, that pattern is identified as an attack. If attack is found in the incoming request, then perform Temporal & Spatial Behavior Pattern Identifier analysis and organize incoming request as valid and invalid sequences.

B.2. SOFT CONTROL MECHANISM

This includes a soft control scheme which reshapes suspicious request sequence according to normal behavior. This process is done by partly discarding most likely malicious request instead of denying entire request sequence. This partly discarding is done based on a threshold value which is referred throughout. The request is cut into parts based on this threshold value in order to attain reshaping.

B.3. HTTP PROTOCOL EXTENSION

Design and implement a new HTTP protocol for detecting client based attack instead of Proxy based. Modify existing HTTP protocol by adding custom headers in HTTP protocol. These custom headers contain the IP of the client when forwarding from proxy server to server. So web server can group request from each client separately and easily detect attack based on client IP which is mandatory along with the request sequence.

B.4. ATTACKER CLIENT IDENTIFICATION

The Http protocol extension proposed above will make the IP of the system mandatory when a request is given from proxy to origin server. Due to this factor when an attack sequence is identified by the server based on our security application, it can also identify from which IP the attack is arising. Thus the attack creating client can be identified.

This method succeeds when normal DDoS attacks arise but when DDoS attacks arises along with IP spoofing this client identification fails. Hence we need to utilize an IP spoofing detection technique along with this. For that purpose we are using a hop-count based IP filtering too.

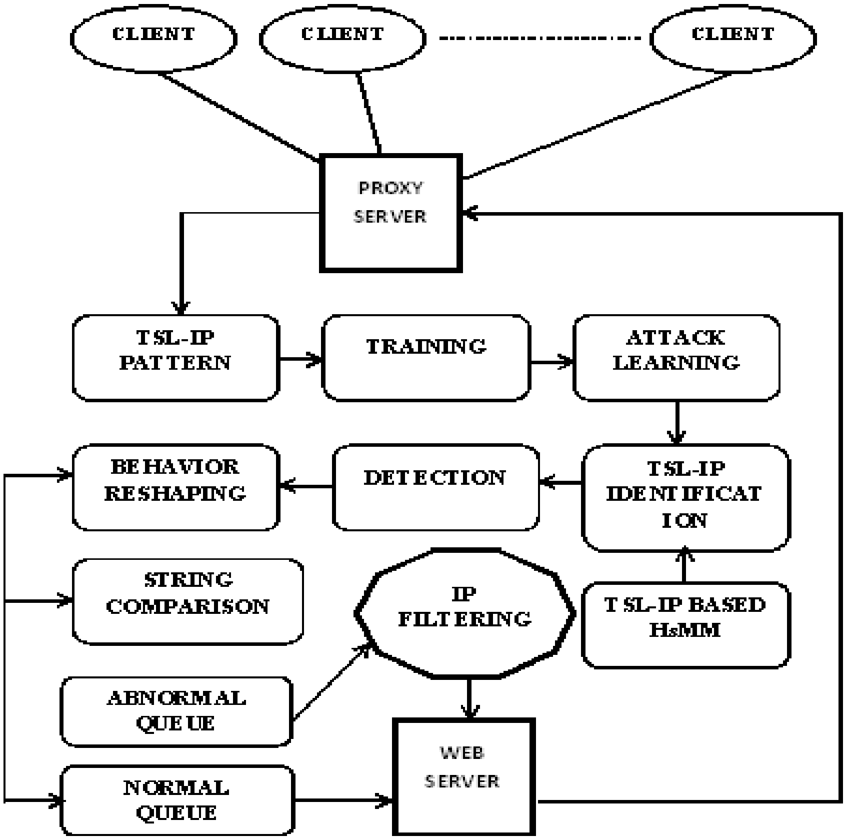

Fig.1. System Architecture

B.5. HOP-COUNT BASED FILTERING

The fundamental idea is to utilize inherent network information that each packet carries and an attacker cannot easily forge to distinguish spoofed packets from legitimate ones. The inherent network information we use here is the number of hops a packet takes to reach its destination: although an attacker can forge any field in the IP header, he cannot falsify the number of hops an IP packet takes to reach its destination, which is solely determined by the Internet routing infrastructure. The hop-count information is indirectly reflected in the Time-to-Live (TTL) field of the IP header, since each intermediate router decrements the TTL value by one before forwarding a packet to the next hop. A hop-count based filtering algorithm is proposed for this.

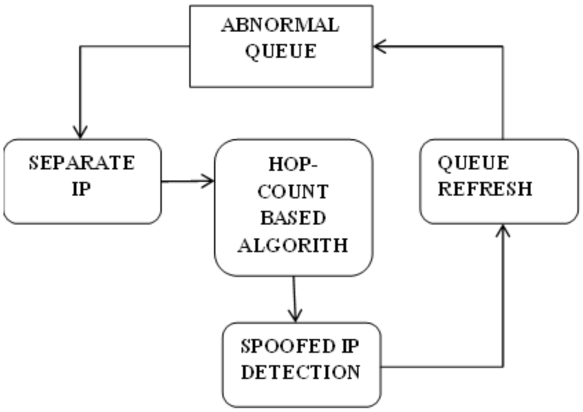

Fig.2. IP Spoofing detection

The idea behind hop-count filtering is that most randomly spoofed IP packets, when arriving at victims, do not carry hop-count values that are consistent with the IP addresses being spoofed. As a receiver, an Internet server can infer the hop-count information and check for consistency of source IP addresses. Exploiting this observation, HCF builds an accurate IP-to-hop- count mapping table. The table observation help to identify spoofed IPs. The attacker client IP identified above in B.5 is matched with the mapping table to identify whether it is spoofed or not. Hence it accurately defines the attacker client.

IV.CONCLUSION

The paper proposes a perfect novel scheme for defending DDoS attacks which arises along with IP spoofing. This can be easily deployed in origin servers and provides identification of not only the attacker proxy but also the particular attacker client. Sometimes IP spoofing causes innocent proxies and clients to be identified as attackers but here the IP filtering mechanism will result in an accurate detection of the DDoS attacker.

The hop-count based filtering is a time consuming and less accurate in case of huge traffic networks. In future researches has to be extended to find a more accurate filtering mechanism with less time consumption.

REFERENCES

[1] J. Yu, C. Fang, L. Lu, and Z. Li, “Mitigating Application Layer Distributed Denial of Service Attacks via Effective Trust Manage-ment,” IET Comm., vol. 4, no. 16, pp. 1952-1962, Nov. 2010.

[2] X. Ye, W. Wen, Y. Ye, and Q. Cen, “An Otpimal Based Mechanism for Defending Application Layer DDos Attacks,” Applied Informatics and Comm., vol. 227, pp. 388-396, 2011.

[3] S. Lee, G. Kim, and S. Kim, “Sequence-Order-Independent Network Profiling for Detecting Application Layer DDos At-tacks,” EURASIP J. Wireless Comm. and Networking, vol. 2011, no. 1, p. 50, 2011.

[4] Jaeyeon Jung, Balachander Krishnamurthy (2002), “Flash Crowds and Denial of Service Attacks: Characterization and Implications for CDNs and Web Sites” www 2002.

[5] Jian Pei,Jiawei Han,Behzard Mortazavi“Mining Acces Patterns Efficiently From Web Logs”, Simon Frazer University,Canada.

[6] Jie Yu , Chengfang Fang*y*, Liming Lu*y*, ZhoujunA “Lightweight Mechanism to Mitigate Application Layer DDoS Attacks.”

[7] John Ioannidis, Steven M. Bellovin,” Implementing Pushback: Router-Based Defense Against DDoS Attacks”.

[8] Kejie Lu, Dapeng Wu , Sinisa Todorovic (2007), “Robust and efficient detection of DDoS attacks for large-scale internet,” Computer Networks.

[9] Smurf IP denial-of-service attacks. CERT Advisory CA-98.01, 1998 [Online]. Available: http://www.cert.org/advisories/CA-98-01.html

[10] Shui Yu, *Member, IEEE,* Wanlei Zhou, *Senior Member, IEEE,* Robin Doss *Member, IEEE,*and *Weijia Jia, Senior Member, IEEE* (2010), “Traceback of DDoS Attacks using Entropy Variations” ,IEEE Transactions On Parallel And Distributed Systems.

[11] Shui Yu, Member, IEEE, Wanlei Zhou, Senior Member, IEEE,Weijia Jia, Senior Member, IEEE, Song Guo, Senior Member, IEEE,Yong Xiang, and Feilong Tang,(2012), “Discriminating DDoS Attacks from Flash Crowds Using Flow Correlation Coefficient”, IEEE Transactions On Parallel And Distributed Systems.

[12] S. Gibson, Distributed reflection denial of service Gibson Research Corp., Tech. Rep., Feb. 2002 [Online]. Available: http://grc.com/dos/

drdos.htm

[13]Tao Peng and Christopher Leckie and Kotagiri Ramamohanarao (2006), "Survey of Network-based Defense Mechanisms Countering the DoS and DDoS Problems," ACM Transactions on Computational Logic.

[14] Xiaobin Tan , Hongsheng Xi(2011) "Hidden semi-Markov model for anomaly detection", Applied Mathematics and Computation.

[15] XIE Yi and YU Shunzheng, "A Detection Approach of User Behaviors Based on HsMM", ITC19/ Performance Challenges for Efficient Next Generation Networks

[16] Yang Xiang, *Member, IEEE*, Ke Li, and Wanlei Zhou(2011), "Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics", IEEE Trnsactions on Information Technology.

[17] Yi Xie and Shun-Zheng Yu, (2009), "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors", IEEE/ACM Transactions on Networking.

[18] Yi Xie ,S.Tang and J.Hu,(2013), "Resisting web proxy-based Http attacks by temporal and spatial locality behavior," IEEE Transactions on Parallel and Distributed System.

[19] Yu Chen, *Member IEEE*, Kai Hwang, *Fellow IEEE*, and Wei-Shinn Ku, *Member, IEEE* "Collaborative Detection of DDoS Attacks over Multiple Network Domains" IEEE Transactions On Parallel And Distributed Systems.

[20] Amey Shevtekar, Karunakar Anantharam, and Nirwan Ansari(2005), " Low Rate TCP Denial-of-Service Attack Detection at Edge Routers", IEEE Communication Letters.

[21] Anirban Mahanti, Carry Williamson(2000)"Temporal Locality and its Impact on Web Proxy Cache Perfomance".

[22] Chia Yuan Cho, Juan Caballero, Vern Paxson (2004), "Insights from the Inside:A View of Botnet Management from Infiltration", Carnegie Mellon University ICSI.

[23] Y. Xie and S.-Z. Yu, "Monitoring the Application-Layer DDoS Attacks for Popular Websites," IEEE/ACM Trans. Networking, vol. 17, no. 1, pp. 15-25, Feb. 2009.

[24] P. Denning, "The Locality Principle," Comm. ACM, vol. 48, no. 7, pp. 19-24, 2005.

[25] Yi Xie, S. Tang, Y. Xiang, and J. Hu, "Resisting Web Proxy-Based HTTP Attacks by Temporal and Spatial Locality Behavior" july 2013.

[26] "An analysis of using reflectors for distributed denial-of-service attacks," ACM Comput. Commun. Rev., vol. 31, no. 3, pp. 38–47, Jul. 2001.