International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 4, Issue 4 (July-Aug, 2016), PP. 193-198

DEFENDING INIMITABLE ATTACKING HOST IN WEB-PROXY BASED TRAFFIC BY TSL BEHAVIOR

[1]Akhila K Raju, [2]Misha Ravi
[1,2,] Computer science and Engineering
Sree Buddha College of Engineering, Elavumthitta Pathanamthitta, India
[1]aakhilaa309@gmail.com

***Abstract*— Distributed Denial of Service (DDoS) attack is one of the most vulnerable threats that affect the client and server communication. The client can access services from server through different proxy server. Attackers can use this web proxy as an attacking tool by sending malicious requests to server through proxy. Defending such attacks by Web proxies is a tedious task. Here proposes a defending mechanism to resist web proxy-based DDoS attacks using the concept of Temporal and Spatial Locality (TSL) to access the behavior features of proxy to server traffic with the help of Hidden Semi Markov Model (HsMM). The existing methodology is based only on the proxy server behavior. In such cases, along with an attacking client the legitimate users also need to suffer with Denial of Service (DoS). A soft control scheme is proposed here, which is an attack response method that converts suspicious traffic into normal by behavior reshaping instead of discarding it. A Threshold Based Attack Detection (TBAD) algorithm for detecting actual attacking client rather than**
the innocent proxy by modifying the http protocol is included in this work. A session hijacking handler method is also implemented to find the session hijacking attacks. Thus, by the revised system a server can serve maximum legitimate users.

Index terms- **DDoS, proxy server, TSL, traffic analysis, attack detection, attack response.**

I. INTRODUCTION

In Internet, a DoS attack aims to disrupt the service provided by a network or server. It can be done in two ways; first method aims to collapse a system by sending one or more malicious packets that exploit software vulnerability in the victim system. The second method is to use large volume of unwanted traffic to occupy all the resources that could service legitimate users, which is more difficult to defend. If the traffic of a DoS attack comes from multiple sources, it is said to be Distributed Denial of Service (DDoS) attack. Now DDoS become one of the most vulnerable hazards to network system. Comparing with DoS attacks, the DDoS attack are more complicated and is a tedious task to detect them. The typical method is a network traffic flood DDoS attack to Web servers, in which multiple sources attack the particular target at the same time. Usually botnets are used to run these attacks. A DDoS attack can be throw in two steps. First, an attacker creates an attacking network that is distributed and includes a large number of compromised computers (zombies). Then, flood a huge amount of traffic towards victims. Second, through automated malicious codes, such as worms and allow the attacker to install DoS attacking programs that scan other hosts, install flood packets.

Proxy networks are used to protect applications against such DoS attacks. The aim is to hide the application behind a proxy network, thus preventing direct attacks on the application. The proxy server (fig 1.1) is the mediator between the client and server connection. A client connects to the proxy server, requesting different services such as a file, connection, web page, or other resources. Then the proxy server evaluates the request to simplify, control its complexity and decide to forward it to the server. A proxy server can be used as an attacking tool by the following ways: the attacker sends malicious requests to the proxy and forces it to send to the server; attacker drops the connection between itself and proxy server.

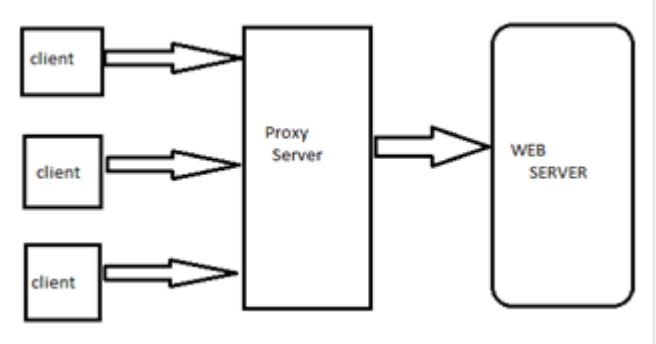

Figure 1.1: Proxy - Web Server Communications

The proposed system is based on network behavior analysis. It maps the access behavior of Web proxy to a hidden semi-Markov model (HsMM) which is a double stochastic processes model. The underlying process of the HsMM forms the semi-markov chain which describes the proxy server's internal behavior state transformation that forms the driving mechanism of a proxy to server traffic. Based on this model, detecting the

irregularity of a web proxy server can be accessed by calculating the difference between an observed behavior and the Web proxy's previous recorded behavior. A new soft-control scheme is proposed for attack response mechanism. It modifies the suspicious sequence into a relatively normal one by partly reshaping it, instead of denying the entire sequence of requests. Thus, it can protect the requests from the legitimate users to the greatest extent as possible from being provided with DoS.

II. LITERATURE SURVEY

Intrusion Detection System (IDS) is a security tool that is used to improve the security of data and network communication. IDS are mainly categorized into two, signature-based or anomaly-based [2]. Both systems are similar, main difference between them are in the concept of attack and anomaly. An attack is simply a sequence of task that makes the system security vulnerable. And, an anomaly is ‘‘an event that is suspicious from the perspective of security’’. A-NIDS (anomaly-based network intrusion detection systems) are emerging concept to protect systems and networks from vulnerabilities. This can be mainly grouped into three: statistical based, knowledge-based, and machine learning-based.

In statistical-based A-NIDS method, a profile is created which includes the network traffic behavior. This is based on the IP address, traffic rate, number of packets, etc. In the process of anomaly detection, current behavior is compared with the previously trained behaviour and checks whether it cross certain threshold value. The Knowledge-based techniques are one of the most commonly used approaches, in which the data is classified based on certain rules. Initially it consists of a training data, from which different classes and attributes are extracted. Then set of procedures and classification rules are deduced. Finally the data is processed. The machine learning scheme can be applied in different areas such as, Bayesian networks, neural networks, Markov models, Genetic algorithms, etc. It is based on explicit or implicit model that helps to categorize the pattern analysed.

Sequence-order-independent network profiling system mainly concentrates on the application-layer DDoS (App-DDoS) attacks [3]. The difference of App-DDoS with other conventional DDoS is that, it uses only trustful methods for attacks. An app-DDoS attack sends small packets only through trustful TCP connections such as HTTP and HTTPS and the real IP addresses are used for attacks. Since these attacks mimic the legitimate users, normal requests are indistinguishable from legitimate users. In order to detect App-DDoS this system uses the concept profiling the web browsing behaviour, thus the sequence order of web page can be used to detect such attacks. But the sequence order may vary according to individuals and browsing behaviours, here proposed a sequence order independent technique to profile the traffic behaviour.

Two new information metrics are used here to detect low-rate DDoS attacks [4]. They are generalized entropy metric and the information distance metric. Information metric helps to identify difference in traffic with different probability distributions. The limitations of existing includes: First, need to train the traffic behavior gradually. Second, they have high false-positive rate. Third, extracting features of normal behavior from vulnerable one is a tedious task. Shannon’s entropy and Kullback– Leibler’s divergence methods are legitimate methods to overcome these limitations. Also an IP trace-back analysis is proposed here. It is the ability to find the source of an IP packet without relying on the source IP field in the packet.

Flash crowd is an unexpected surge in visitors to a particular Web site, which is typically because of some newsworthy event that just took place. Here proposes a discriminating algorithm to differentiate DDoS attacks from flash crowd with the help of flow correlation method [5]. A flow correlation coefficient is used as a metric to measure the similarity between suspicious flows to differentiate DDoS attacks from genuine flash crowds. The proposed discriminating algorithm works independently for specific DDoS flooding attacks. Thus it is effective against unknown forthcoming flooding attacks.

A trace-back technique is used to detect DDoS attacks with the help of Entropy variations [6]. This entropy variation is based on the difference between the normal traffic and the DDoS attack traffic. IP trace-back policy is used here, two major methods for IP trace-back are: the probabilistic packet-marking (PPM) and the deterministic packet marking (DPM). Both of them require routers to mark each packet and they are vulnerable to hacking. Since IP trace-back must be free from packet pollution, the proposed method does not include packet marking. The packets that are moving through routers can be classified as flows, which are interpreted by the upstream router where a packet came from, and the destination address of the packet. If a DDoS is recognized, the victim identify the position of zombies by initially find which of its upstream routers are in the attack based on the flow entropy variations. Then it forwards the requests to their immediate upstream routers to identify the attacker sources. This process continues until it reaches the attack source. Advantages of this method include: it is free from the limitations of packet marking mechanism; it is efficient to detect packet flooding DDoS attacks.

Hidden Semi-Markov Model (HsMM) is an extension of Hidden Markov Model (HMM) is proposed here to describe the web browsing behaviours [7]. The underlying process of the HSMM forms the semi-markov chain. Each state in the markov chain has a variable duration that corresponds to the number of observations produced while in the state. HSMM is used in different fields such as, speech recognition, anomaly detection for network security, recognition of human genes in DNA, language identification, brain functional MRI sequence analysis, channel modelling, Internet traffic modelling, speech synthesis, image segmentation, etc. Here HSMM is used for anomaly detection on user browsing behavior; it depends on the structure of a website, which includes a large amount of web documents, hyperlinks, and the way the user accesses the webpages. A new efficient algorithm (M-algorithm) is also proposed here for implementation of the forward process of HSMM and detecting on-line App-DDoS attacks.

In the case of detecting App-DDoS for popular websites, a new technique is proposed based on document popularity [8]. The concept of spatial-temporal pattern is used for detection of

DDoS attacks. That is, an Access Matrix (AM) is defined to access the spatial-temporal patterns of normal traffic, and then HSMM is used to find the variations in AM and apply two analysis techniques for multidimensional data for HSMM. They are principal component analysis (PCA) and independent component analysis (ICA). PCA is based on based on converting large amount of variables into a smaller number of uncorrelated variables by detecting small number orthogonal linear combinations of the real variables which have the highest difference.

III. PROPOSED SYSTEM

The proposed system is based on the TSL behavior to filter the attack traffic from the aggregated proxy-to-server traffic, which is a new issue for the DDoS detection. The core TBAD algorithm for detecting actual attacking client rather than an innocent proxy by modify the http protocol is included in this work. The soft control scheme is proposed to improve the attack detection by reshaping the malicious request to normal rather than completely discarding it. Also the session hijacking handler is used to handle the session hijacking attacks.

A. Model Definition

The ultimate aim of the proposed system is to protect the origin server from the web proxy-based HTTP attacks. An assumption is made to simplify this problem; attack traffic is beginning from Web proxies instead of its real sources. The reason for taking this assumption is that, the victim server can only observe the proxies and the goal is to filter malicious traffic. A Web proxy's access behavior can be considered as a combination of certain external manifestations and intrinsic driving mechanisms. The external manifestations are able to monitor and they are usually controlled by the intrinsic driving mechanisms. These are not accurately obtained by the origin server but can be estimated by the observable features of proxy-to server traffic. HsMM can be used map the access behavior of web proxies; each hidden semi-Markov state represents a driving mechanism of a type of proxy-to-server traffic. The changes of driving mechanism can be identified by the transition between two different Markov states. The output of the proposed system should meet certain requirements: it must be independent of traffic intensity and gradually varying web contents and it must be able to obtain early detection. In order to meet these requirements the TSL behavior is used to access the features of proxy to server traffic.

B. System Design

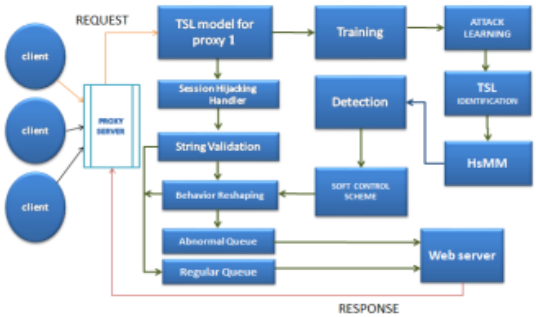

Figure 1.2: Architecture of proposed system.

The system architecture includes mainly three phases: Data extraction phase, Training phase, Detection phase. Normally the users request their files to web server through proxy. The detection system extracts a proxy's TSLs from its reference string and generates a TSL string. The complete sequence of requests is initially trained to the web server so that any attack sequence can be easily identified. The soft control scheme reshapes the abnormal string to normal. And the session hijacking handler identifies and handle the session hijacking attacks.

C. System Modules

This system includes mainly five modules namely, proxy server, web server, soft control, session hijacking handler, HTTP protocol modification. Initially develop a proxy server which act as proxy for client and provide interconnection between client and server. In the second module, create a web server which consists of three sub modules, they are; HTTP handler, training and detection. First, create a client server program for processing HTTP request. Second, create the training model by, learning the complete request sequence. Third, create a detecting system to find malicious requests using TSL behavior and checksum tracking. The third module is soft control scheme that is used to convert abnormal request to normal by partially discarding the request. Session hijacking handler is the forth module, which is a technique for finding and handling session hijacking attacks. The fifth module HTTP protocol variation, in which modify the HTTP protocol to identify the client based attacks, instead of proxy.

1) Proxy Server

Develop a proxy server system which acts as proxy for client. This server is used as the interconnection between client and web server. The client, for requesting resources from other services sends requests to an intermediary server that may be a computer system or an application; such a server is called a proxy server. A client may requests services, such as a file, connection, web page, or other resource available from various servers and the proxy server verify the request for simplification and controlling its complexity and then forward to the corresponding server. The steps involves for the creation of web proxy are:

- Create a server section for accepting connection from browser.
- Accept the connection.
- Read the web request from client.
- Establish the connection to web server.
- Send the request to web server.
- Read the response from server.
- Send the response to client.

2) Web Server

Develop an HTTP Server which contains the following modules:

a) HTTP Handler

Develop a client server program for processing HTTP request. The steps for creating the client server are:

- Create a server socket listen to port 8000.
- Read the request.
- Separate the url and checksum.
- Detect attack, if any.
- Otherwise, create the response.
- Send response to client.

b) Training

The training section is used to identify different request pattern to develop a training model. The important step involved in the training phase is the attack learning, which is a tedious task to access the characteristics of complete request sequences. The different possibilities of requests are obtained with the help of TSL behavior. A new iterative method based on the forward-backward algorithm is used here. The Forward-Backward algorithm is interference algorithm for hidden Markov models, computes the posterior marginal of all covert state variables given a chain of observations and state variables. It is used to refer to any algorithm belonging to the wide class of algorithms that make go on a sequence model in the forward-backward manner.

Algorithm: Forward and Backward
Input: sequence of states
Output: number of state process and observed processes
Forward, Backward (guessState, sequenceIndex)
if (sequenceIndex is past the end of sequence)
Return 1;
If (guessState, sequenceIndex)
== has been seen before, return saved result
Result = 0;
For each neighboring state n;
Result = result + (transition probability form quessState to n given observation
element at sequenceIndex) *
ForwardBackward(n,sequenceIndex + 1);
Save result; For (quessState, sequenceIndex)
Return result;

c) Detection

To detect the malicious request pattern a new algorithm is implemented here, which is called Threshold Based attack Detection (TBAD) algorithm. TBAD algorithm calculates the ΔT values, which gives the time distance between the current and previous request of a packet for a specific IP address. If this ΔT value of the IP frequency list exceeds the threshold value based on threshold settings, then the packets are dropped otherwise they are allowed to network for further processing of the HTTP request. And check whether the extracted IP address is in the IP address list; accordingly update the IP frequency list. If it is not able to find the checked IP address in the IP address list, then the new IP address and its arrival time are stored in the IP address list. Now, the ΔT value of two packets from same IP address and from different IP address is calculated. If the ΔT is less than 1 second, then the IP address is added to the IP frequency list. Otherwise the IP frequency list value for then the corresponding IP address is incremented by 1. For example, set the threshold value is 30, so it allows only 30 HTTP GET request. If the IP frequency list value of an IP address exceeds the limit, then the packets are dropped.

Algorithm: TBAD
Input: Network Traffic
IF (Outbound packets)
THEN
IF (Packet == HTTP GET)
THEN
Step 2: //Extract Parameters
// IP1, IP2, ... , IPn - remote IP address
// t1, t2, … , tn - Arrival time of packets
//IPAddrList - List of IP addresses
IPAddrList [IPn] [0] = in;
IPAddrList [IPn] [1] =tn;
Step 3: // ΔT - Difference in time between two instances of same IP address
// ΔT- Difference in time between two instances of different IP addresses
// N - Threshold value
//IPIncidenceList - IP Frequency List
ΔT = t2(IPAddrList[IPn][1]) - t1 (IPAddrList[IPn][1]);
IF (ΔT < 1 second)
THEN
IPIncidenceList [n] ++;
IF (IPIncidenceList [n] < N)
THEN
Allow packet to the network;
ELSE Drop packet;
END IF
END IF
ELSE
Allow packet to the network;
END IF
END IF

3) Soft Control

A "soft-control" scheme is implemented in this work for the attack response. This technique transforms the malicious sequences into a relatively normal one by partly discarding its most likely vulnerable requests instead of removing the complete sequences. Given a malicious reference string fw = {f1w,…, fTw of the wth time window, two auxiliary variables are defined: discard number (DNi) of requests generated by state i, global survival rate SRE = φ(BIw, μBI ; σBI)/ (μBI + 2σBI ,μBI. σBI). The behavior index (BI) and structure factor (SF) are two parameters for measuring the normality of proxy's behavior. The reshaping algorithm is shown below.

Algorithm: Reshape suspicious reference string
Require:
The abnormal reference string: f^w;
The hidden state process of f^w : x^w;
The BIw of f^w and its PDF $\varphi(x, \mu_{BI}, \sigma BI)$;
The Structure Factor: SF_i, i Ɛ IM;
Ensure: Reshape f^w and output: $\tilde{f}^w = \{\tilde{f}1^w, \ldots.., \tilde{\tilde{f}}T^w\}$
1: Calculate global survival rate SR_E;
2: Calculate final length of $\tilde{f}w$ by $\tilde{T}w = [Tw \cdot SRE]$;
3: **for** i = 1 to M **do**
4: $DN_i = 0$;
5: if $[\tilde{T}w \cdot SF^i] <= Num(i,w)$ **then**
6: $DNi = Num(i,w) - [\tilde{T}w \cdot SF^i]$;

7: **end if**
8: randomly mark DN_i requests of state i of f^w;
9: **end for**
10: Discard all marked requests of f^w;
11: Let $\tilde{f}w$ = fw and output $\tilde{f}w$;

4) Session Hijacking Handler

A session hijacking handler is implemented to identify and handling session hijacking attacks. The MITM attack is one of the session hijack attacks, in which an attacker intercepts all communications between the client and server. Now the flow of interaction is through the attacker, and the attacker is able to easily change the content. The target of these attacks is in the protocols that rely on the exchange of public keys to protect the communication.

5) HTTP Protocol Modification

Design and implement a new HTTP protocol for identifying the actual intruder client rather than the proxy server. Modifying the existing HTTP protocol is done by adding custom headers, with the help of MD5 algorithm. This algorithm creates a checksum value for each and every request from the client based on MAC address. Checksum is used for ensuring data that has not been corrupted, either accidentally or maliciously. Here it is calculated by applying MD5 algorithm to every request to the target server. The result is a string of hexadecimal digits which is unique to each request. Media Access Control (MAC) address is also called physical address; of a computer which is a unique identifier assigned to network interfaces for communications

in physical network segment. By using this checksum value, the web server can group request from each client separately and easily detect the attack based on this application ID and provides DoS accordingly.

IV. RESULTS

To defend inimitable attacking host in web proxy based traffic and to serve maximum legitimate users, initially create a sample website and trained the complete possible pattern of request to the server. This is done by the help of TSL behavior using forward and backward algorithm of HsMM. And then create an attack sequence generator in which a particular sequence is made to flood attack the server. That means this sequence is send to server which exceed the predetermined threshold value. At the same time create a random number of users that communicate with the server. The ultimate aim of this work is to identify the attacking host and no legitimate users will not suffer from this flood attack. Before attacking the server a checksum ID is created for each and every request using the MAC address with the help of MD5 Algorithm. This helps to easily find out the intruder client and decrease both the false negative ratio as well as the false positive ratio. The output of this thesis work is shown in fig 4.1, the zero percent false negative value shows that this

work can serve almost cent percent of legitimate users.

Figure 4.1: Output of the proposed system

The performance diagram of the proposed system is depicted in fig 4.2. In the existing system, both the false negative and false positive ratio increases as the number of attacking and non-attacking requests increases. But this work reduces both the false negative and false positive ratio.

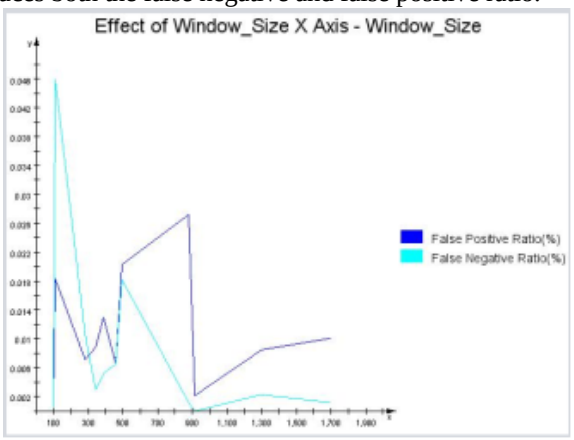

Figure 4.2: Performance Diagram

CONCLUTION AND FUTURE WORK

Web-Proxy based HTTP attacks are becoming one of the serious issues in the internet. The ultimate aim of this thesis was to give an effective solution for the detection and prevention of clients from unwittingly taking part in such attacks by filtering attack traffic from the aggregated proxy-to-server traffic. Some algorithms and techniques are used for discovering and protection such as, TBAD, HsMM, Forward-Backward algorithm, this focus on the traffic analysis and behavior analysis using Temporal and Spatial Locality behaviors. The Threshold Based Attack Detection (TBAD) helps to identify the actual intruder client rather than proxy server. And the implemented soft control scheme is successful in improving the detection performance by reshaping the suspicious request to normal request instead of discarding the entire request sequence. The detection performance of this work is better than the traditional statistical methods and it is independent of the traffic intensity and varying web contents. The major benefit of this thesis includes: it can detect the actual intruder client, thus there is no need to block the innocent proxy; the detection rate (DR), false positive rate (FPR) and false negative rate (FNR) are improved to meet the needs of practical applications, it provide early detection and the computational overhead is very low. Thus the revised

system is able to protect QoS of the legitimate users of the client system. The experiments can be further extended by implementing this work in other network topologies such as SDN, Adhoc networks, IoT, etc.

REFERENCES

[1] Yi Xie, S. Tang, Y. Xiang, and J. Hu, "Resisting Web Proxy-Based HTTP Attacks by Temporal and Spatial Locality Behavior", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 7, JULY 2013

[2] P. Garcia-Teodoro, J. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez," Anomaly-Based Network Intrusion Detection: Techniques, Systems and Challenges," Computers and Security, vol. 28, nos. 1/2, pp. 18-28, 2009.

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

[4] Y. Xiang, K. Li, and W. Zhou, "Low-Rate DDos Attacks Detection and Traceback by Using New Information Metrics," IEEE Trans. Information Forensics and Security, vol. 6, no. 2, pp. 426-437, June 2011.

[5] S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, "Discriminating DDos Attacks from Flash Crowds Using Flow Correlation Coefficient," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073-1080, June 2012.

[6] S. Yu, W. Zhou, R. Doss, and W. Jia, "Traceback of DDos Attacks Using Entropy Variations," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 3, pp. 412-425, Mar. 2011.

[7] Y. Xie and S. Yu, "A Large-Scale Hidden Semi-Markov Model for Anomaly Detection on User Browsing Behaviors," IEEE/ACM Trans. Networking, vol. 17, no. 1, pp. 54-65, Feb. 2009.

[8] 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.

[9] S.-Z. Yu and H. Kobayashi, "An Efficient Forward-Backward Algorithm for an Explicit-Duration Hidden Markov Model," IEEE Signal Processing, Letters, vol. 10, no. 1, pp. 11-14, Jan. 2003.

[10] A. Mahanti, D. Eager, and C. Williamson, "Temporal Locality and Its Impact on Web Proxy Cache Performance", Performance Evaluation, vol. 42, nos. 2/3, pp. 187-203, 2000.

[11] Udi Ben-Porat, Anat Bremler-Barr, Hanoch Levy, "Evaluating the Vulnerability of Network Mechanisms to Sophisticated DDoS Attacks".

[12] Alexander Afanasyev, Priya Mahadevany, Ilya Moiseenko, Ersin Uzuny, Lixia Zhang, "Interest Flooding Attack and Countermeasures in Named Data Networking", Proc. IFIP Networking, 2013.

[13] S. Triukose, Z. Al-Qudah, and M. Rabinovich, "Content Delivery Networks: Protection or Threat?" Proc. 14th European Conf. Research in Computer Security (ESORICS), pp. 371-389, 2009.

[14] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of Network-Based Defense Mechanisms Countering the Dos and DDos Problems", ACM Computing Surveys, vol. 39, no. 1, p. 3, 2007.

[15] Yi Xie, S.Yu, "Measuring the Normality of Web Proxies Behavior Based on Locality Principles", Network and Parallel Computing, volume 5245, pages 61-73, 2008.

[16] https://en.wikipedia.org/wiki/MD5.

[17] V. Almeida, A. Bestavros, M. Crovella, and A. de Oliveira, "Characterizing Reference Locality in the WWW," Proc. Fourth Int'l Conf. Parallel and Distributed Information Systems, pp. 92-103, 1996.

[18] Candid Wueest, "The continued rise of DDoS attacks", SECURITY RESPONSE, Version 1.0, October 21, 2014.

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

[20] http://en.wikipedia.org/wiki/Forward-backward algorithm.

[21] S. Yu, "Hidden Semi-Markov Models," Artificial Intelligence, vol. 174, no. 2, pp. 215-243, 2010.