A Distributed Approach to Defend Web Service from DDoS Attacks

Monika Sachdeva monika.sal@rediffmail.com
Assistant Proff./Department of Computer Science & Engineering
SBS College of Engineering & Technology,
Ferozepur, Punjab, India

GurvinderSingh gsbawa71@yahoo.com
Associate Proff./Department of Computer Science & Engineering,
Guru Nanak Dev University,
Amritsar, Punjab, India

Kuldip Singh kds56fec@riitr.ernet.in
Retd. Proff./Department of Electronics and Computer Engineering,
Indian Institute of Technology,
Roorkee, Uttrakhand, India

Abstract

Most of the business applications on the Internet are dependent on web services for their transactions. Distributed denial of service (DDoS) attacks either degrade or completely disrupt web services by sending flood of packets and requests towards the victim web servers. An array of defense schemes are proposed but still defending web service from DDoS attacks is largely an unsolvable problem so far. In this paper, DDoS defense schemes are classified into centralized and distributed and their relative advantages and disadvantages are explored. An ISP based distributed approach is a pragmatic solution to defend from DDoS attacks due to its autonomous control, more resources, and incremental scope. Traffic cluster entropy is conceptualized from source address entropy and the combination is used to detect various types of DDoS attacks against the web service. A framework is proposed which can detect the attack, characterize attack sources, and filter the attack packets as early as possible so as to minimize the collateral damage

Keywords: DDoS, Centralized Defense, Distributed Defense, Deployment, Detection, Response, Source Address Entropy, Traffic Cluster Entropy.

1. INTRODUCTION

Internet has changed the way traditional business models are operated. Web service is one of the most important facilities used by commercial and government organizations to perform their activities. However DDoS attacks against high profile sites in the recent past have manifested their devastating power and have raised unresolved issues related to Web security [1]. A lot of research [2][3][4][5] has been carried out to defend web service from DDoS attacks, but none of these schemes are able to handle DDoS attacks in a comprehensive manner. The stumbling barrier has been the vulnerabilities in the Internet infrastructure and the volume of legitimate looking attack traffic generated towards the web server which makes defense system itself susceptible against these attacks [6]. Due to sheer volume, most of these schemes crumble as their bandwidths, data structures and CPU cycles are exhausted in handling the spurious attack traffic only [7]. So the biggest need is to design a DDoS resistant scheme.

In this paper an emphasis is laid on use of distributed approach to defend web service from sheer volume of DDoS attack traffic by dividing computational overheads at multiple points so that the approach itself should be DDoS resistant. Since detection of DDoS attacks requires monitoring and analysis of complete traffic, so a technique, which can monitor and analyse traffic at distributed points, but actually behave as if the total traffic is monitored and analysed at single point, is good for DDoS attack detection [8]. Moreover characterization of attack traffic and then filtering also consumes computational resources, so they should also be distributed as far as possible. A framework is proposed in this paper to defend web service from DDoS attacks. It has following characteristics:-

1. Monitoring and analysis of traffic is distributed.
2. Complete traffic analysis for DDoS attack detection is carried out.
3. Defense is DDoS resistant so that automatic response may be generated.
4. Characterization of attack traffic is separately carried out from attack detection.
5. Filtering is done at distributed points.

An amalgamate approach of source address and traffic cluster entropy is used for attack detection. Kumar et al [8] formula has been used to compute entropies at one point collected from distributed points. The computed entropies are compared with base line entropies for signaling attacks. Characterization of attack traffic is based on finding new source addresses and cluster based on profiled traffic matrices. The attack signatures are communicated to the entry points so that they may be filtered without wasting core bandwidth.

The rest of the paper is organized as follows. Section 2 focuses on justifying distributed approach rather than centralized in a pragmatic manner. Section 3 discusses our detection approach. Section 4 explains proposed framework. Finally section 5 concludes our paper.

2. RATIONALE BEHIND DISTRIBUTED APPROACH

A comprehensive DDoS solution requires three effective modules namely traffic monitoring, traffic analysis, and attack traffic filtering [6] [8]. In a centralized solution all the modules are deployed at same place whereas voluminous and distributed nature of DDoS traffic demands a distributed DDoS solution because centralized solutions cannot handle high overheads of monitoring, analyzing and filtering. Components of distributed defense system are deployed at different locations and cooperate with each other to defend from the attacks. Compared with the centralized defense systems, distributed defense systems can discover and fight the attacks with more resources and at more than one point of the Internet. It is very difficult for the centralized defense system to detect the attack at the beginning. When the attacks are full-fledged, it becomes more difficult for defense system to resist the flooding. Moreover centralized defense systems are themselves more vulnerable to be attacked by hackers. The centralized defense systems are mostly deployed on the victim network because of economic reasons. Thus such defense systems are irresponsible systems which could only detect the attacks but cannot generate automatic alert and are also not able to filter the attack traffic themselves.

Distributed defense systems overcome the shortcomings of centralized and isolated defense systems. Deployed on all around the Internet, distributed defense systems can detect the attacks before they are launched by inspecting the traffic on many edge networks in which the computers are compromised by hackers. The most important and attractive feature of the distributed defense system is that the components in the distributed defense system can cooperate with each other to fight against DDoS attacks.

Centralized	Distributed
All the component modules are deployed at same place.	Whereas in distributed they are deployed at multiple places.
Highly Vulnerable and hence not robust against DDoS attacks.	Less Vulnerable and hence robust against DDoS attacks.
No cooperation and communication framework required.	Cooperation among various modules and proper communication framework required
Lesser resources are available for fighting against the attacks	More resources are available for fighting against the attacks
Mostly deployed at Victim site	Deployed at Victim-Core, Throughout the Internet and Victim-Source

TABLE 1: Centralized Vs Distributed defense

The advantage of distributed over centralized defense has been recognized in [9-11] [12]. A comparison of centralized Vs distributed is given in table 1.

Clearly distributed defense is the only workable solution to combat DDoS attacks. Some recently proposed defense systems use collaborating source-end and victim-end nodes [10], while others deploy collaborating nodes at the victim and core networks [13]. While they perform well against a variety of attacks, they do not completely handle the flooding DDoS threat. Specifically, source-victim defense systems fail to handle large attacks launched from legacy networks, while victim-core defense inflict high collateral damage to legitimate traffic. A few defense schemes combine defense nodes at all three locations [9] [11]. These defense mechanisms achieve higher effectiveness, but focus on a single approach to defense (e.g., a capability mechanism in [11], victim-hiding in [9]), which ultimately discourages integration with other defense approaches and wide deployment and hence are not practical. So a practical distributed defense mechanism which can have wide deployment is the need of the hour. Many distributed defense techniques are proposed in the literature. Distributed DDoS defense can be deployed at source, victim and intermediate, source-victim, and victim-intermediate networks.

Distributed defense techniques are likely to be the proper solution for handling the DDoS threat [14]. However, they are infrastructural solutions i.e. they span multiple networks and administrative domains and represent major undertakings of many Internet participants. Such systems are difficult to deploy and maintain. Further, the required cooperation of defense systems is hard to achieve due to distributed Internet management and strictly autonomous operation of administrative domains. Securing and authenticating the communication channels also incurs a high cost if the number of participants is large. In light of above said issues and Internet design vulnerabilities [3], a practical DDoS defense system deployment should have following important characteristics:

- Autonomous system i.e. whole defense location under one administrative control so that different defense nodes can collaborate in a secure manner.
- Large and infrastructure wise rich enough to handle high voluminous traffic from evenly distributed flood sources.
- Capability to evolve DDoS defense in incremental fashion.
- Sufficient financial motivation for value-added DDoS security service.

The Internet consists of thousands of Autonomous Systems (ASes) i.e., networks that are each owned and operated by a single institution. Usually each ISP operates one AS, though some ISPs may operate multiple ASes for business reasons (e.g. to provide more autonomy to administrators of an ISP’s backbones in the United States and Europe) or historical reasons (e.g. a recent merger of two ISPs) [15]. An ISP has total autonomy to collaborate defense nodes in a secure manner. Enough infrastructures can be provided for DDoS defense to handle high volume at ingress points. Moreover, once agreement is reached between various ISPs then inter co-operation among ISPs is also possible [16, 17]. Accordingly, there is scope of incremental DDoS defense. If a provider’s infrastructure is attacked (routers, DNS, etc.), all services to its customers fail, resulting in service level agreement (SLA) violations. Moreover, ISPs normally host most of the services available on the Internet. The cost of DDoS protection is insurance against catastrophic failures that would cost the business orders of magnitude more in terms of both revenue and negative customer relations. However, Cost-avoidance is not the only motivation to implement a complete DDoS solution in ISP domain. For the users, DDoS protection can also be offered as a value-added service that creates new revenue streams and provides competitive differentiation for ISPs. In nutshell, ISP level DDoS defense is most practical and viable at this stage. Though, longer term objective “how to achieve inter ISPs cooperation” still remains as the biggest challenge.

3. SOURCE ADDRESS AND TRAFFIC CLUSTER ENTROPY AS A DETECTION METRIC

Most of detection schemes in the literature fail to address a very important scenario comprising of legitimate increase in traffic called Flash events (FE) [18]. We have proposed an anomaly based approach to detect DDoS attack as well as to discriminate it from FE. Clearly first a base line behaviour of the system is required and then the same is compared with actual behaviour. If actual behaviour significantly deviates from normal behaviour then we raise an alarm for attack. Shannon entropy [19] has been used to conceptualize source address entropy [8][20] and traffic cluster entropy. The source address entropy and traffic cluster entropy are compared in different scenarios: normal and DDoS attacks, normal and flash, and flash with DDoS attack. Basic terminology and symbols used are explained below:-

Source IP address (src_IP):- A 4-byte logical address used in the packets to represent its source IP.

Traffic cluster (tc):- The traffic generated from same networks or administrative domains is defined as traffic cluster.

16-bit traffic cluster identifier ($tc16\_id$):- All the packets which share the same initial 16 bits of their src_IP are in same group called 16-bit traffic cluster. It is obtained by bit-wise AND operation of src_IP and 16-bit mask i.e. 255.255.0.0. A unique identifier assigned to such a traffic group or cluster is defined as 16-bit traffic cluster identifier.

24-bit traffic cluster identifier ($tc24\_id$):- All the packets which share the same initial 24 bits of their src_IP are in same group called 24-bit traffic cluster. It is obtained by bit-wise AND operation of src_IP and 24-bit mask i.e. 255.255.255.0. A unique identifier assigned to such a traffic group or cluster is defined as 24-bit traffic cluster identifier.

Source address entropy $H(src\_IP)$:- A metric that captures the degree of dispersal or concentration of distribution of a random variable is called sample entropy [8][20]. Let the random variable src_IP can take values $\{src\_IP_1, src\_IP_2, src\_IP_3, \ldots \ldots src\_IP_n\}$ in different packets. Let number of packets received per src_IP are $\{X_1, X_2, X_3, \ldots \ldots X_n\}$ respectively. Then as per Shannon criteria sample entropy is

$$H(src\_IP) = -\sum_{i=1}^{n} p(src\_IPi) \times log_2 \, p(src\_IPi) \qquad (1)$$

Here the probability of occurrence of src_IP i.e. $P(src\_IP) = \{p(src\_IP_1), p(src\_IP_2), \ldots\ldots p(src\_IP_n)\}$ is computed as $p(src\_IPi) = \frac{Xi}{S}$ where $S = \sum_{i=1}^{n} Xi$

Traffic cluster entropy $H(tc\_id)$:- Let the random variable tc_id can take values $\{tc\_ID_1, tc\_ID_2, tc\_ID_3, \ldots\ldots tc\_ID_m\}$ in different packets. Let number of packets received per tc_id are $\{Y_1, Y_2, Y_3, \ldots \ldots Y_m\}$ respectively. Then as per Shannon criteria traffic cluster entropy is

$$H(tc\_ID) = -\sum_{i=1}^{m} p(tc\_IDi) \times log_2 \, p(tc\_IDi) \qquad (2)$$

Here the probability of occurrence of tc_ID i.e. $P(tc\_ID) = \{p(tc\_ID_1), p(tc\_ID_2), \ldots\ldots p(tc\_ID_m)\}$ is computed as $p(tc\_IDi) = \frac{Yi}{S}$ where $S = \sum_{i=1}^{m} Yi$

Eq. (2) is used to compute 16-bit traffic cluster entropy $H(tc16\_ID)$ and 24-bit traffic cluster entropy $H(tc24\_ID)$ by finding 16-bit and 24-bit traffic clusters respectively.

In our approach, the packets destined to web server W_S are monitored at the point of presence PoPs of the protected ISP. PoPs of the ISP provide access of the Internet to its customers as well as are used for peering between ISPs. Packets are monitored in a short sized time window $\{t - \Delta, t\}$ to minimize memory overheads. Here Δ seconds is the size of time window. At time t, the monitoring process yields packets arrival distribution of src_IP and tc_id. Then the probability of occurrence of each src_IP and tc_ID i.e. $P(src\_IP)$ and $P(tc\_ID)$ are respectively computed. In the next step source address entropy $H(src\_IP)$ and traffic cluster entropies $H(tc16_ID)$and $H(tc24\_ID)$ are computed for the time window $\{t-\Delta,t\}$ as per flowchart in figure 3. The computed entropies with total number of packets are sent by every PoP to the PoP which connects web server to the protected ISP. Here cumulative source address and traffic cluster entropies are computed as per equation 3 and 4 given below.

$$H_S(src\_IP) = (1/S_f)\sum_{i=1}^{N} S_i\,(H_i(src\_IP) - \log(S_i)) + \log(S_f) \qquad (3)$$

$$H_S(tc\_ID) = (1/S_f)\sum_{i=1}^{N} S_i\,(H_i(tc\_ID) - \log(S_i)) + \log(S_f) \qquad (4)$$

If there is no significant increase in $H_S(src\_IP)$ as well as $H_S(tc16\_ID)$ and $H_S(tc24\_ID)$, it signifies legitimate traffic as during normal event number of traffic sources and network domains do not vary much. But during FE number of traffic sources increases however there less variation in network domains. So a significant increase in $H_S(src\_IP)$ but minor variations in $H_S(tc16\_ID)$ and $H_S(tc24\_ID)$ are the signs of FE. But if there is appreciable increase in $H_S(src\_IP)$ as well as in $H_S(tc16\_ID)$ and $H_S(tc24\_ID)$, it means DDoS attack has happened because a large number of zombies send traffic from different parts of the Internet belonging to different network domains. The flowchart for detection of attack is given in figure 4.

4. FRAMEWORK

The system architecture of the proposed approach is given in the figure 5. Three ISP are shown and ISP$_1$ is the protected ISP domain. ISPs contain many PoPs. These PoPs actually consist of interconnected edge and core routers [8]. PoPs are connected to customer domains via edge routers and are attached with each other through high bandwidth links between their core routers. Moreover ISPs are joined with each through peering via their PoPs [8] . So these PoPs are entry and exit points of the ISPs. The legitimate and attack traffic from ISP$_1$, ISP$_{2,}$ and ISP$_3$ are directed towards web server. Some of the customer domains have attack zombies as per figure 5. So customer domains generate legitimate, attack, or legitimate and attack traffic towards the web server. Through peering points legitimate and attack traffic from other ISPs enter protected ISP$_1$. The protected ISP$_1$ in the distributed framework shown in figure clearly indicates that at all the PoPs, we run traffic monitoring module, which not only separates source addresses from incoming packets but also classifies them into 16-bit and 24-bit traffic clusters. A time series analysis of this traffic is carried out at each PoP and computed entropy with total count of packets are sent to PoP connected to the server. Here anomaly based detection module runs which checks for presence of attacks using cumulative entropy computed using equation 3 and 4. The steps followed in distributed framework are given below:-

Step 1. Source IP address is detached from the incoming packet destined to protected web server at all the PoPs except at PoP Ps.

Step 2. Classification into 16-bit and 24-bit cluster is done at each PoP by using bit-wise AND operation of each source IP address with 255.255.0.0 and 255.255.255.0 respectively.

Step 3. A count is maintained for each source IP and 16-bit, 24-bit cluster in a time window $\{t-\Delta,t\}$.

Step 4. At the end of Δ seconds, source IP $H_i(src\_IP)$, 16-bit traffic cluster $H_i(tc16_ID)$and 24-bittraffic cluster $H_i(tc24\_ID)$ entropies are computed using equation 1 and 2 by all the PoPs where i=1 to N. Here N is number of PoPs.

Step 5. The computed entropies in step 4 are sent by all the PoPs to PoP Ps with sum S$_i$ of all the packets received at respective PoP where i=1 to N.

Step 6. At PoP Ps cumulative source IP $Hs(src\_IP)$, 16-bit traffic cluster $Hs(tc16_ID)$and 24-bit traffic cluster $Hs(tc24\_ID)$ entropies are computed using equation 3 and 4.

Step 7. Source IP $Hs(src\_IP)$, 16-bit traffic cluster $Hs(tc16_ID)$and 24-bit traffic cluster $Hs(tc24\_ID)$ entropies computed in step 6 are compared with baseline respective entropies. The detection procedure flags normal, flash event, and DDoS attack.

Step 8. In case DDoS attack is detected in step 7 then either 16-bit traffic cluster or 24-bit traffic cluster is selected as anomalous cluster for attack source characterization depending upon their entropy variation from threshold.

Step 9. Anomalous cluster is analysed to find new clusters which have not appeared earlier before detection of DDoS attack as they contain source IP of all zombies which are used for attack.

Step 10. A packet having information of all abnormal traffic clusters is made by PoP Ps which is communicated to all the PoPs which share the multicast group with PoP Ps.

Step 11. All the PoPs detach information of all abnormal traffic clusters from the packet communicated in step 10 and store the same in filter database as attack signatures.

Step 12. Each packet destined to protected web server is allowed to pass only after comparing it with attack signatures stored in filter database.

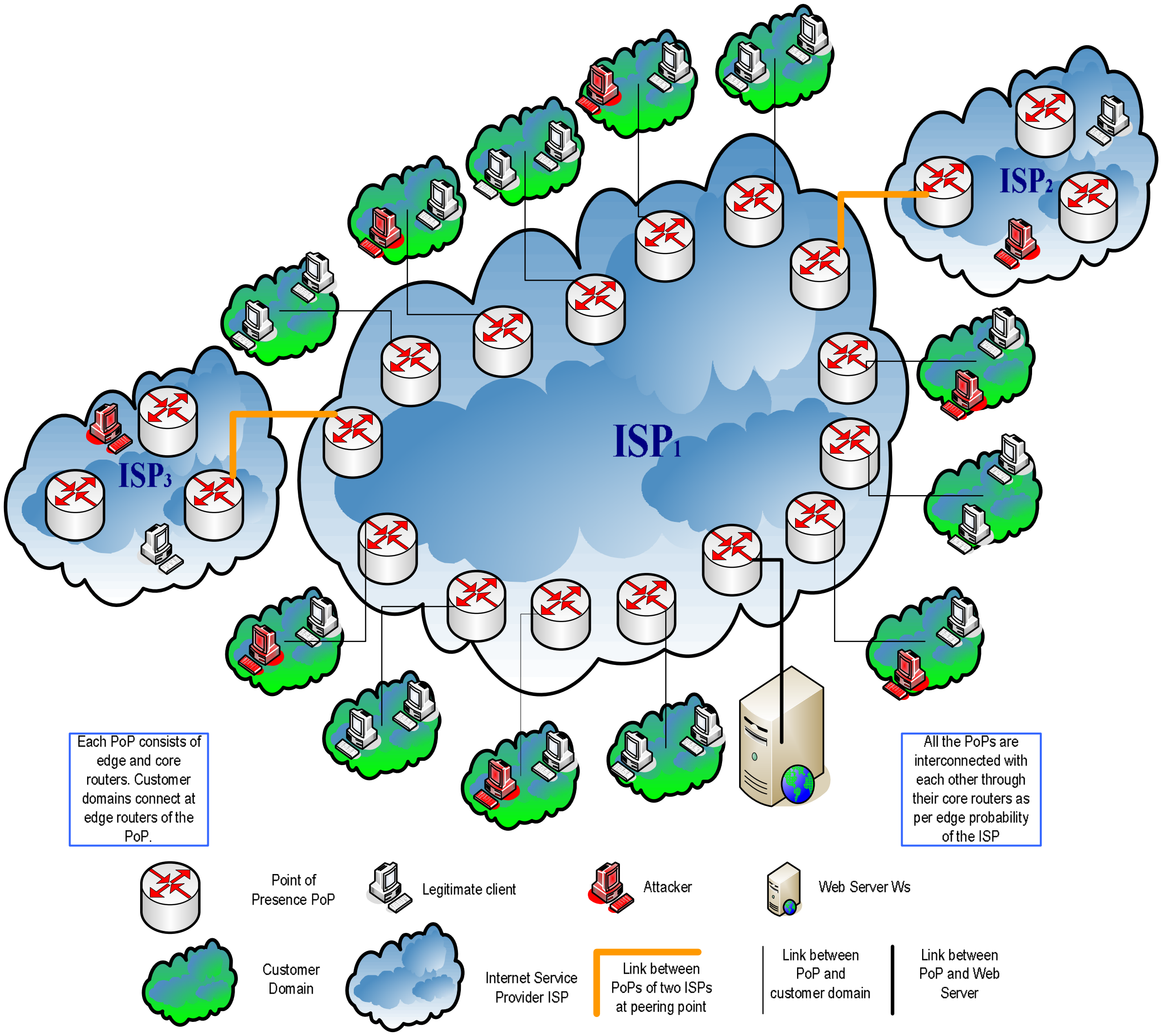
ISP2
ISP1
ISP3
Each PoP consists of edge and core routers. Customer domains connect at edge routers of the PoP.
All the PoPs are interconnected with each other through their core routers as per edge probability of the ISP
Point of Presence PoP
Legitimate client
Attacker
Web Server Ws
Customer Domain
Internet Service Provider ISP
Link between PoPs of two ISPs at peering point
Link between PoP and customer domain
Link between PoP and Web Server

FIGURE 1: System Architecture

Now the traffic reaching at PoP Ps drops significantly as attack traffic is getting filtered at PoPs only. As the attack traffic is dropped at PoPs only so is also does not consume expensive inner bandwidth of protected ISP. The innocent traffic cluster which were mixed by attackers in a crafty manner so as to hide their zombies also do suffer as only those traffic clusters are punished which have attack zombies. Hence collateral damage is also minimum in our approach. It is worth mention here that the different operations of the approach are carried at different points and hence there is no single computational point which can be attacked by the attacker.

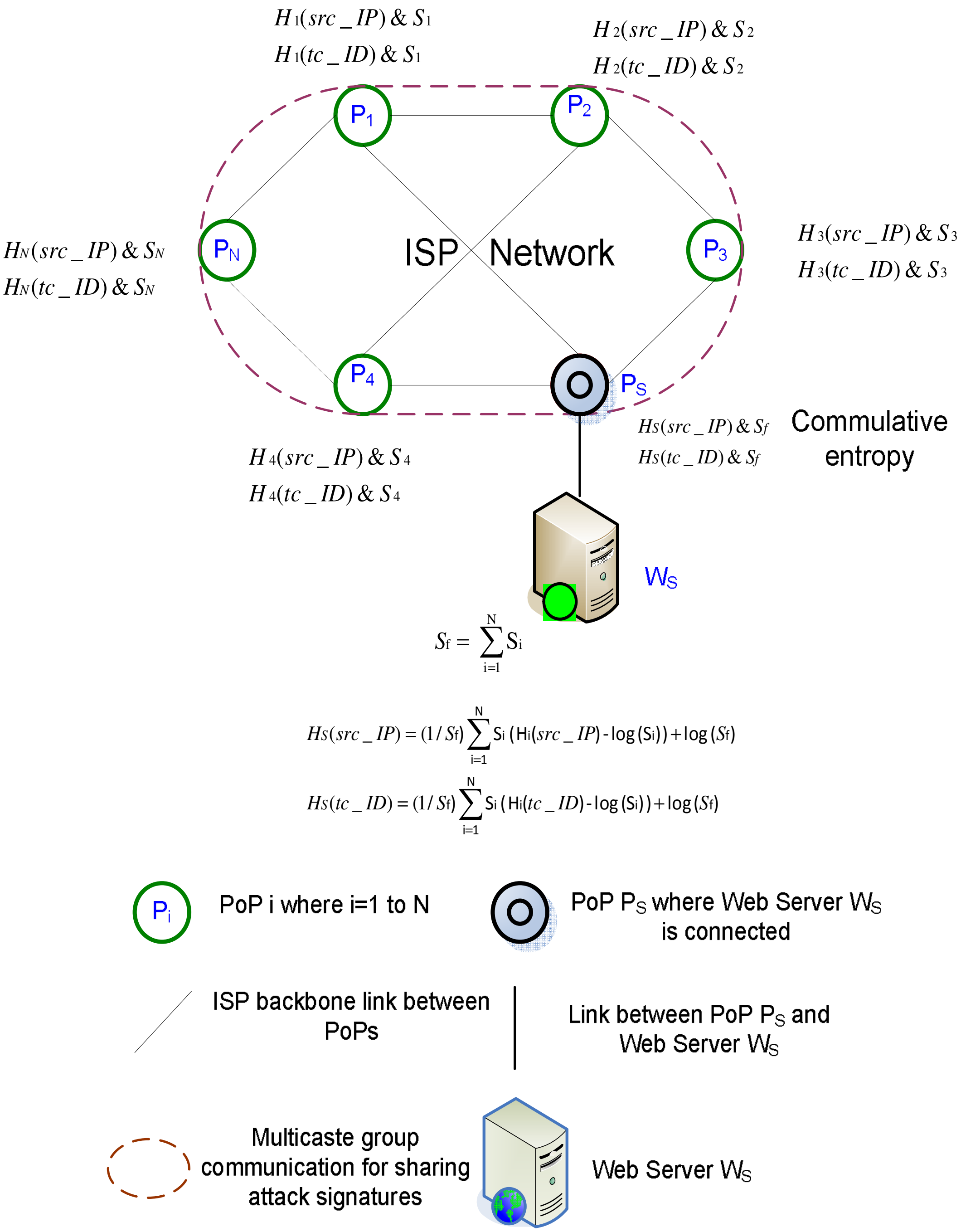
$H_1(src\_IP) \& S_1$
$H_1(tc\_ID) \& S_1$
$H_2(src\_IP) \& S_2$
$H_2(tc\_ID) \& S_2$
P_1
P_2
$H_N(src\_IP) \& S_N$
$H_N(tc\_ID) \& S_N$
P_N
ISP Network
P_3
$H_3(src\_IP) \& S_3$
$H_3(tc\_ID) \& S_3$
P_4
P_S
$H_S(src\_IP) \& S_f$
$H_S(tc\_ID) \& S_f$
Commulative entropy
$H_4(src\_IP) \& S_4$
$H_4(tc\_ID) \& S_4$
W_S
$S_f = \sum_{i=1}^{N} S_i$
$H_S(src\_IP) = (1/S_f)\sum_{i=1}^{N} S_i\,(H_i(src\_IP) - \log(S_i)) + \log(S_f)$
$H_S(tc\_ID) = (1/S_f)\sum_{i=1}^{N} S_i\,(H_i(tc\_ID) - \log(S_i)) + \log(S_f)$
P_i
PoP i where i=1 to N
PoP P_S where Web Server W_S is connected
ISP backbone link between PoPs
Link between PoP P_S and Web Server W_S
Multicaste group communication for sharing attack signatures
Web Server W_S

FIGURE 2: Distributed Framework

5. CONCLUSION AND FUTURE WORK

A distributed rather than centralized approach in ISP domain is the only pragmatic solution available against DDoS attacks as centralized approach suffers from single point failure bottleneck. Many defence schemes have used entropy but traffic cluster entropy combined with source address entropy is used to detect volume as well most of other intelligently crafted DDoS attacks. The proposed defence framework is comprehensive as it detects wide range of attacks, characterize attack sources and filter attack traffic. The computational burden is also distributed in such way as if amassed traffic is analysed at single point.

The future work of the paper is as below: -
An evaluation of traffic cluster entropy approach using NS-2 simulation test bed.
Implementation of distributed framework in NS-2 is there in line of sight.

6. REFERENCES

[1] M. Sachdeva, G. Singh, K. Kumar and K. Singh. "DoS Incidents and their impact: A review." The International Arab Journal of Information Technology IAJIT, ISSN: 1683-3198, Vol. 7, No. 1, January 2010, pp. 14-22.

[2] C. Douligeris and A. Mitrokotsa. "DDoS attacks and defense mechanisms: classification and state-of-the-art." Computer Networks, Vol. 44, No. 5, pp. 643–666, April 2004.

[3] J. Mirkovic and P. Reiher. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms." ACM SIGCOMM Computer Communications Review, Volume 34, No. 2, pp. 39-53, April, 2004.

[4] 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, Article 3, April 2007.

[5] M. Sachdeva, G. Singh, K. Kumar and K. Singh. "A Comprehensive Survey of Distributed Defense Techniques against DDoS attacks." International Journal of Computer Science and Network Security (IJCSNS), ISSN: 1738-7906, VOL.9 No.12, December 2009, pp. 7-15.

[6] J. Mirkovic. "D-WARD: Source-End Defense Against Distributed Denial-of-service Attacks." Ph.D. Thesis, University of California, Los Angeles, 2003

[7] K. Kumar, R.C. Joshi, and K. Singh. "An ISP Level Distributed approach to detect DDoS Attacks." Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications, ISBN: 978-1-4020-6265-0 (Print) 978-1-4020-6266-7 (Online), Springer Netherlands, DOI 10.1007/978-1-4020-6266-7, Pages 235-240, September 04, 2007.

[8] K. Kumar. "Protection from Distributed Denial of Service (DDoS) Attacks in ISP Domain." Ph.D. Thesis, Indian Institute of Technology, Roorkee, India, 2007.

[9] A. D. Keromytis, V. Misra, and D. Rubenstein. "SOS: An Architecture For Mitigating DDoS Attacks." IEEE Journal on Selected Areas in Communication, Vol. 22, No.1, pp. 176-188, 2004.

[10] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan. "CROSSACK: Coordinated Suppression of Simultaneous Attacks", Proceedings of DISCEX, pp. 2-13, 2003.

[11] X. Yang, D. Wetherall, and T. Anderson. "A DoS-limiting network architecture", Proceedings of ACM SIGCOMM, pp. 241-252, 2005.

[12] W. Shi, Y. Xiang and W. Zhou. "Distributed Defense Against Distributed Denial-of-Service Attacks", Proceedings of ICA3PP 2005, LNCS 3719, pp. 357-362,2005.

[13] G. Oikonomou, J. Mirkovic, P. Reiher, and M. Robinson. " A Framework for a Collaborative DDoS Defense", Proceedings of the 22nd Annual Computer Security Applications Conference, pp. 33-42, 2006.

[14] M. Robinson, J. Mirkovic, M. Schnaider, S Michel, and P. Reiher,"Challenges and principles of DDoS defense," ACM SIGCOMM, 2003.

[15] M. Caesar and J. Rexford. "BGP routing policies in ISP networks,"

[16] U. K. Tupakula and V. Varadharajan. "A controller agent model to counteract DoS attacks in multiple domains", Proceedings of Integrated Network Management, IFIP/IEEE Eighth International Symposium. pp.113-116, 2003

[17] S. Chen and Q. Song. "Perimeter-Based Defense against High Bandwidth DDoS Attacks." IEEE Transactions on Parallel and Distributed Systems, Vol. 16, No. 6, pp. 526-537, June 2005.

[18] G. Carl, G. Kesidis, R. R. Brooks, and S. Rai. "Denial-of-Service Attack - Detection Techniques." IEEE Internet Computing, Vol. 10, No. 1, pp. 82-89, Feb. 2006.

[19] C. E. Shannon and W. Weaver. The Mathematical Theory of Communication. University of Illinois Press, 1963.

[20] L. Feinstein, D. Schnackenberg, R. Balpuari, and D. Kindred. "Statistical Approaches to DDoS Attack Detection and Response" ,In Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03), Vol. 1, pp. 303-314, 2003.