A Comprehensive Survey of Distributed Defense Techniques against DDoS Attacks

Monika Sachdeva[1], Gurvinder Singh[2], Krishan Kumar[1], and Kuldip Singh[3]

[1]SBS College of Engineering & Technology, Ferozepur, Punjab, India
[2]Guru Nanak Dev University, Amritsar, Punjab, India
[3]Indian Institute of Technology, Roorkee, Uttarakhand, India

Summary
Distributed Denial of Service Attacks imposes a major threat to the availability of Internet services. Most of the applications like banking, trade, and e-commerce are dependent on availability of Internet. Defending Internet from these attacks has become the need of the hour. A typical DDoS defense comprises of three modules namely traffic monitoring, traffic analysis and traffic filtering. Based on placement of these modules, DDoS defense can be categorized into centralized DDoS defense and distributed DDoS defense. In centralized defense, all modules are placed on single point. Under severe DDoS attack, centralized defense itself succumbs to high volume of traffic. Hence it is itself vulnerable to DDoS attacks. In distributed defense, all of the defense modules are placed at different points and do not succumb to high volume of DDoS attack and can discover the attacks timely as well as fight the attacks with more resources. In this paper first important metrics are identified to evaluate distributed defense techniques. Then a comparative analysis based on identified metrics is done for existing distributed defense techniques. Research gaps are also highlighted in exiting techniques so as pursue research in this problem. Finally a generic defense methodology is proposed to combat DDoS attacks in automated manner.

Key words:
DDoS, Centralized defense, Distributed defense, deployment , detection ,response..

1. Introduction

In the present era, Internet has made all operations like e-commerce, banking, trade, social activities and mail discussions very easy. So an increasing number of critical services are motivated to use the Internet for daily operations. Thus Internet has come up as a critical resource whose disruption induces financial implications or even dire consequences on humanity. However Internet was fundamentally designed with functionality not security in mind, and it was indeed very successful in accomplishing this particular goal. It offers its participants fast, easy and cheap communication mechanisms, enforced with various higher-level protocols that ensure reliable and timely delivery of messages with certain level of quality of service. Technically Internet design follows the end-to-end paradigm. The end hosts deploy intelligence in terms of complex functionalities to achieve desired service guarantees, while the intermediate network which is full of resources provides the bare-minimum, best-effort service. Thus there is intelligence and resource asymmetry on the Internet. Such design opens several security issues that provide opportunities for various kinds of attacks on the Internet. Internet security includes aspects such as confidentiality, authentication, message integrity and non repudiation [1, 2].One of the main aspect of Internet security is availability. DDoS attacks pose a big threat to availability of services on the Internet.

According to the WWW Security FAQ [3] a DoS attack can be described as an attack designed to render a computer or network incapable of providing normal services. A DoS attack is considered to take place only when access to a computer or network resource is intentionally blocked or degraded as a result of malicious action taken by another user. These attacks do not necessarily damage data directly or permanently, but they intentionally compromise the availability of the resources. It renders a network, host, or other piece of network infrastructure unusable by legitimate users; especially it is against the frequently visited web sites of a number of high-profile companies [2] or governments. In Distributed Denial of Service (DDoS) attacks scenario, the attacks become coordinated and come from multiple sources at the same time [4], thus are even more devastating. In order to launch a DDoS attack, the attacker first scan millions of machines for vulnerable service and other weakness, then gain access and compromise these zombies or slave machines. These infected machines can recruit more zombies. When the assault starts, the real attacker hides the identity and sends orders to zombies to perform the attacks. The attackers are not going to thieve, modify or remove the information exchanged on networks, but they attempt to impair a network service, thus to block legitimate users from accessing the service. DDOS attacks can be classified into two broad categories: flooding attacks and vulnerability attacks [5]. Flooding DDoS attacks consume resources such as network bandwidth by overwhelming bottleneck link with a high volume of packets whereas vulnerability attacks use the expected

Manuscript received December 5, 2009
Manuscript revised December 20, 2009

behavior of protocols such as TCP and HTTP to the attacker's advantage. Vulnerability attacks can be addressed by fixing security holes in protocols whereas flooding DDoS attacks are one of hardest problem before security experts in present age as they exploit Internet architecture vulnerabilities which cannot be easily fixed.

A lot of work has been already done to combat DDoS attacks. An excellent review of existing techniques is available in [8-9][11][13][14][26]. However these review papers have not classified DDoS defense techniques based on placement of component modules which is very essential so as to devise robust solutions. In this paper an effort has been made to compare centralized and distributed DDoS defense and then distributed defense techniques are reviewed in a systematic manner. Research gaps in existing work are identified which provides directions for future work in this area.

In section 2, need of distributed defense is highlighted. Various key metrics to evaluate distribute defense techniques are identified in section 3. In section 4, existing distributed defense techniques are critically reviewed, research gaps in existing work are highlighted, and a comparative analysis of various distributed defense techniques based on key metrics is presented. In section 5, a generic methodology to counter DDoS attacks is proposed. Finally section 6 concludes the paper.

2. Need of Distributed Defense

A comprehensive DDoS solution requires three effective modules namely traffic monitoring, traffic analysis, and attack traffic filtering [6-7]. 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. And centralized defense systems themselves are 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 respond to the attacks, but not to stop the attacks.

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.

The advantage of distributed over centralized defense has been recognized in [8-10][33]. A summary of centralized Vs distributed is given in table 1.

Table 1: Centralized Vs Distributed defense

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

Clearly distributed defense is the only workable solution to combat DDoS attacks. Some recently proposed defenses use collaborating source-end and victim-end nodes [9], while others deploy collaborating nodes at the victim and core networks [11]. While they perform well against a variety of attacks, they do not completely handle the flooding DDoS threat. Specifically, source/victim defenses fail to handle large attacks launched from legacy networks, while victim/core defenses inflict high collateral damage to legitimate traffic. A few defenses combine defense nodes at all three locations [8][10]. These defenses mechanism achieve higher effectiveness, but focus on a single approach to defense (e.g., a capability mechanism in [10], victim-hiding in [8]), which ultimately discourages integration with other defenses 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.

3. Key Metrics to Evaluate Different Distributed Defense Techniques

Distributed Defense is the best way to combat DDoS Attacks. Traffic Monitoring, Traffic Analysis, and Traffic Filtering are the three main modules in any comprehensive

DDoS solution. Various metrics to evaluate different defense techniques are described below:

Deployment

The functionalities of defense nodes include detection of potential attack, alarm generating and multicasting, attack source finding, and attack traffic controlling. With regard to a deployment location, DDoS mechanisms can be deployed at the victim, intermediate, or source network. In Victim-Network Mechanisms, DDoS defense mechanisms is deployed at the victim network to protect this network from DDoS attacks and respond to detected attacks by alleviating the impact on the victim. Historically, most defense systems were located at the victim since it suffered the greatest impact of the attack and was therefore the most motivated to sacrifice some resources for increased security. Whereas in Intermediate-Network Mechanisms, DDoS defense mechanisms provide infrastructural service to a large number of Internet hosts. Victims of DDoS attacks can contact the infrastructure and request the service, possibly providing adequate compensation. Pushback and traceback techniques are examples of intermediate-network mechanisms. The goal of DDoS defense mechanisms deployed at the source network is to prevent customers using this network from generating DDoS attacks. Such mechanisms are necessary and desirable, but motivation for their deployment is low since it is unclear who would pay the expenses associated with this service.

Some approaches such as DefCOM [12], ACC [13] and ASSYST [14] deploy their nodes throughout the network. This deployment requires that every participating node must be able to perform the detection and traffic controlling functions, communicate and coordinate well with each other. It could raise the unnecessary traffic burden at the intermediate nodes. Moreover, it could not be the best place to detect the attack at the intermediate nodes. The best deployment is the mixture deployment at both source end and victim end. The reason for this deployment is that first, the victim end aggregates the most information for the detection and can achieve the most accurate detection true positive rate. Second, detecting preliminary attack signatures at source end allows the defense system to mitigate a DDoS attack at its initial phase. Third, the source end traffic controlling can protect the network's availability to a max degree because not only the victim but also the rest of network can be free of network congestion. But practically DDoS traffic is so low at sources that it is not easy to characterize attacks packets at the source. At victim end automation of real time response by generating alerts and collaborating with other defense nodes is difficult against high volume of DDoS attack traffic. Besides wide base of vulnerable machines on the Internet and distributed Internet control, global deployment at source is too difficult without explicit incentives. Moreover intermediate network is not owned by a single organization. So deploying defense modules in the Internet remains an important issue for a practical DDoS solution

Detection

There are different ways to detect attacks. In pattern matching, signatures of known attacks are stored in the database. Each communication is monitored and compared with database entries to discover occurrences of DDoS attacks. Occasionally, the database is updated with new attack signatures. The obvious drawback of this detection mechanism is that it can only detect known attacks, and it is usually helpless against new attacks or even slight variations of old attacks that cannot be matched to the stored signature. On the other hand, known attacks are easily and reliably detected, and no false positives are encountered. In anomaly detection, we have a model of normal system behavior, such as a model of normal traffic dynamics or expected system performance. The current state of the system is periodically compared with the models to detect anomalies. Approaches presented in provide examples of mechanisms that use anomaly detection. The advantage of anomaly detection over pattern detection is that unknown attacks can be discovered. However, anomaly-based detection has to address two issues:

1. Threshold setting. Anomalies are detected when the current system state differs from the model by a certain threshold. The setting of a low threshold leads to many false positives, while a high threshold reduces the sensitivity of the detection mechanism.

2. Model update. Systems and communication patterns evolve with time, and models need to be updated to reflect this change. Anomaly based systems usually perform automatic model update using statistics gathered at a time when no attack was detected. This approach makes the detection mechanism vulnerable to increasing rate attacks that can mistrial models and delay or even avoid attack detection.

Flooding DDoS attacks bring network anomaly such as the sudden surge of network traffic volume, increase of the packets with random source IP addresses, and asymmetric amount of packets associated with some network protocol such as TCP SYN. Detection and filtering is a straightforward approach to defend such attack. One of the main objectives of a successful distributed defense system is the fast and sensitive detection by using a fine granularity detection method. Though, detection of high rate flooding DDoS attacks is easy at the victim, but due to excessive DDoS traffic,

response is initiated manually in most of the cases. So a real time detection and automated response needs to be dealt more carefully at appropriate point of network where excessive traffic can be handled in a better manner. Moreover, selection of thresholds and their impact on detection accuracy needs to be analyzed properly so as to give meaningful direction to DDoS research [15].

Response

The goal of the attack response is to relieve the impact of the attack on the victim, while imposing minimal collateral damage to legitimate clients of the victim.

Rate-limiting and throttling are the most popular strategies used in the current distributed defense systems, such as in DefCOM [12], SOS [8], ACC [13], MANANet [16] and Throttle [11]. Because no defense systems can detect the attacking packets with 100 percent accuracy, it is advisable to limit the rate of high-bandwidth flows rather than to drop all the suspicious packets.

It also gives the defense system flexibility to adjust the limit to which the suspicious network traffic is suppressed. The disadvantage is that it allows a certain amount of attacking packets to pass through and some legitimate packets are either delayed or dropped. This will bring problems when rate limiting is deployed on the network in which there are resource-demanding applications (e.g. video stream) and the bandwidth is not big enough. However, currently there seems to be no better solutions unless the detection accuracy can be improved to a satisfying extent.

Security

A distributed defense system must be able to protect the information to be exchanged from being intercepted by the hackers. Current security mechanisms such as IPSec, PKI etc. are used to meet the requirement. The examples of security implement are highlighted in [17]. Some research has been done to deal with the denial of service problems in the security protocols [18-19]. An analysis of DDoS defense in terms of security is also done in [20] for controller agent model [21]. Here we do not specifically consider how to defend the security architecture because we assume the motivation of the DDoS attacks is to prevent the legitimate users from accessing the desired resources, but not to crash the security architecture, which is more difficult to achieve.

Robustness

Here robustness means the degree to which the distributed defense system itself can resist the attacks. When the distributed defense system is deployed and is known to the hackers, they will launch attacks to the distributed defense system so that the defense systems cause denial of service to protected systems. Although the distributed defense system is less vulnerable to such attacks than the centralized defense system, it is still possible that the distributed defense system fails due to the attacks targeting it. Unfortunately this issue is less concerned in the design of the current distributed defense system.

The concentration point of flooding DDoS traffic is victim so more attack evidence is also available near the victim. Detection of attack and characterization of attack sources can be done best near the victim. However, state monitoring and sophisticated analysis to capture all kinds of attack require higher computational complexity, which is vulnerability in case of high rate flooding DDoS attacks near the victim at single point. Distributed defense systems in which detection and characterization is done at single point, higher computational complexity vulnerability can really cripple detection system which is an integral part of whole distributed defense system.

4. Review of Existing Distributed DDoS Defense Techniques

A review of some of known distributed defense techniques is given below.

Pushback [22] enables routers to identify high-bandwidth aggregates that contribute to congestion rate limit them. If the congested router cannot control the aggregate itself, it requests its upstream neighbor's help in rate limiting. The performance of Pushback is good when attackers are collocated on a path separate from the legitimate traffic, otherwise it inflicts collateral damage. Further, Pushback cannot work in non-contiguous deployment and cannot detect attacks that do not congest core routers. By pushing the defense frontier towards attack sources, more legitimate traffic can be protected. An improved version of this pushback scheme called Selective pushback [23] sends pushback messages to the routers closest to the attack sources directly by analyzing the traffic distribution change of all upstream routers at the target. The benefit of this scheme is twofold. First, traffic distribution analysis can locate attack sources more accurately than purely volume-based approaches, especially during a highly distributed denial of service attack. Second, the pushback message can be sent to the routers closest to the attack sources directly, which can mitigate the attack damage more quickly than the original pushback scheme. But still accuracy of detection and deployment across multiple ISP domains remain big issues.

Tupakula et al. [21] propose a controller agent model to counteract DoS attacks within one ISP domain which

they later extended to multiple domains [24]. In this model, agents represent the edge routers and controllers represent trusted entities owned by the ISP. Once a target detects an attack, it sends a request to the controller, asking all agents to mark all packets to the target After checking the marking field, the target can find out which agent (edge router) is the entry point for the attack traffic. The target then sends a refined request to the controller, asking some particular agents to filter attack traffic according to the attack signature provided by the target. So attack traffic originating from zombies is filtered at ingress edges of the protected ISP, but legitimate traffic is allowed to enter the domain. In [24] designated controllers of multiple domains interact to decrease the impact of attack and Traceback the attack path till attack zombies. The main limitation of this model is that it uses third party detection for detecting and characterizing attack traffic.

This is a good model in terms of number of packets required to find ingress edges of attack, but attack signature should be as narrow as possible to lessen collateral damage. The communication required between victim and controller as well between agents and controllers should be first possible in state of DDoS and should also be confidential, authentic, integral and fresh. Moreover single point failure at controller due to DDoS attack centered at controller or intrinsic fault can really damage the whole scene. Also filtering techniques are used to stop the attack. Instead adaptive rate limit would be better if attack signatures are not accurate.

SOS [8] uses access points (SOAPs) close to source networks to verify legitimate users and send their traffic on the overlay to secret servlets that tunnel it to a distributed firewall protecting the victim. SOS offers good protection to the server but the traffic experiences a significant delay because it is routed on the overlay. SOS approach involves a variety of authentication and overlay routing mechanisms and suffers from routing related drawbacks. Moreover, if attackers can gain massive attack power, for example, via worm spread, all the SOAPs can be paralyzed, and the target's success will be disrupted..

Active Security System (ASSYST) [14] supports distributed response with non-contiguous deployment, with nodes equivalent to classifiers being deployed only at edge networks. CROSSACK [9] similarly forms a multicast group of defense nodes that are deployed at source and victim networks and cooperate in filtering the attack. Both [9] and [14] cannot handle attacks from legacy networks that do not deploy their defense mechanisms. Parameter Based Defense [25] constructs a multicast group at an ISP that rate limits an attack originated from one of its customer networks. It requires wide deployment and does not perform well in non-contiguous deployment. Yau et al. [11] propose a router throttle mechanism installed at the routers that are close to the victim. This defense system incorporates only victim-end and core defense mechanisms, and thus inflicts collateral damage to legitimate traffic. Some router based solutions consists of an overlay of routers with added functionality, which helps them trace and stop the attacks close to the source. Tracing is done using signatures assigned to each source network, and inflicts collateral damage on legitimate users that share a network with an attacker.

DefCOM [12] provides added functionality to existing defenses so they can collaborate in DDoS detection and response though a dynamically-built overlay. There are three types of DefCOM functionalities that are added to existing routers or defense nodes. A single physical node can host more functionality at a time. The functionalities are: (1) A classifier functionality is added to existing defenses that is capable of differentiating the legitimate from the attack traffic. A classifier marks packets recognized as legitimate with a HIGH-priority mark that guarantees priority handling by downstream DefCOM nodes. (2) A rate limiter functionality is deployed by routers. During an attack, a rate limiter runs a weighted fair share algorithm (WFSA) to prioritize traffic it forwards to the victim, and it rate limits this traffic to preserve victim's resources. (3) An alert generator functionality is added to defenses that can detect a DoS attack. An alert generator propagates the attack alert to other DefCOM nodes using the overlay. The alert contains the IP address of the attack's victim and specifies a desired rate limit, e.g., the size of the victim's bottleneck link. Extra infrastructure for overlay and cooperation at all points of the Internet are big concerns. Collateral damage depends upon accuracy of classifier.

Yau et al. [11] used router throttles to combat DDoS attacks against Internet servers. A proactive approach is followed in the sense that before aggressive packets can converge to overwhelm a server, routers along forwarding paths, regulate the contributing packet rates to more moderate levels, thus forestalling an impending attack. The basic mechanism is for a server under stress, to install a router throttle at an upstream router several hops away. The throttle limits the rate at which packets destined for server will be forwarded by the router. Traffic that exceeds the rate limit can either be dropped or rerouted to an alternate server. However, if the current throttle fails to bring down the load to below threshold, the throttle rate is reduced. On the other hand, if the server load falls below a low-water mark, the throttle rate is increased (i.e., relaxed). If an increase does not cause the load to significantly increase over some observation period, then the throttle is removed. The throttle rate is determined by two strategies: Just half or Farley equal (fair throttling) at all routers. The goal of the control algorithm is to keep the server load

within lower and upper thresholds whenever a throttle is in effect.

Here no pushback and response messages are required as in pushback technique [13][22]. Moreover in case of evenly distributed attackers, this approach yields better results as throttling is carried at k hops away, so concentrated good traffic near server is not dropped. In fact the effectiveness increases with value of k. Attackers can exploit communication part as no secure ways are used to send throttle messages in same and different domain. In case of meek slow rate attack, NPSR is very low. Control parameters should be set more dynamically and intelligently. Oscillations and more convergence time can also become bottleneck. Static selection of throttling routers can also become headache. Moreover no consideration of bandwidth, queue length of available links and routers between server and throttling routers/ingress points of ISP is considered in calculation of throttling rates as it is assumed that server is attached to backbone routers, so high bandwidth is available near server. Hence there is no chance of congestion of any link close to the server.

DiDDeM [26] uses a scalable mechanism to early detect the attack on the basis of congestion in cooperative domain. In this work, each domain is comprised of a single command and control server (c2) and a set of prefilters PFs/traffic monitors. The c2 acts as a server, located on a designated network node or router, to the PFs within the domain. The c2 provides the services of management of PFs; responses to attack detected and reported by PFs, and cooperation with adjacent domains. The c2 and PF work in correlation within the network and cooperative domain to rate limit the attack traffic as well as to traceback the attack source. Isotropic DDoS attacks can be combated provided they generate so much traffic that can cause congestion. Actually it is very difficult to have deployment of defense modules in multiple domains without any incentives from victim ISP domain. Moreover only aggressive attacks can be controlled. Slow rate and pulsing attacks cannot be defended.

Deployment, detection, response, security, robustness and implementation are some of the key issues for all distributed DDoS defense systems. A comparative analysis of various distributed defense schemes ACC [13] [22], SOS [8], Controller-agent [21][24][27], Throttling [11], DiDDeM [26], MANANet [16], CROSSACK [9], IDIP [28], ASSYST [14], and DefCOM [12] based on identified metrics is summarized in table 2.

Table 2.1: Summary of comparisons among distributed defense systems

	ACC [22]	**Controller-Agent [21]**	**Throttle [11]**
Deployment	Throughout the network	ISP domain	Routers close to victim
Detection	Congestion based	Third party Intrusion detection system	N/A
Response	Rate limiting	Dropping all packets	Rate limiting
Security	N/A	Analyzed in later versions	N/A
Robustness	Weak	Dynamic generation of Agent IDs	Weak
Implementat-ion	Difficult	Practical provided incentives are given to ISPs.	Difficult

Table 2.2: Summary of comparisons among distributed defense systems (contd.)

	DiDDeM [26]	**SOS [8]**	**MANANet [16]**
Deployment	Multiple ISP domains	Source/ Victim	Cooperative routers at the Victim
Detection	Congestion based	Filtering	PEIP
Response	Dropping all the packets till threshold is obtained	Rate Limiting	Rate Limiting
Security	N/A	IPSec	N/A
Robustness	----------	Moderate	Weak
Implementat-ion	Difficult	Difficult	Difficult

Table 2.3: Summary of comparisons among distributed defense systems (contd)

	CROSSACK [9]	**IDIP [28]**	**ASSYST [14]**
Deployment	Source/ Victim	Distributed groups	Throughout the network
Detection	Spectral analysis	Intrusion detection	Intrusion detection
Response	Dropping all packets	Dropping all packets	Dropping all packets
Security	CA	IPSec	N/A
Robustness	Weak	Weak	Weak
Implementat-ion	Easy	Easy	Difficult

Table 2.4: Summary of comparisons among distributed defense systems (contd)

	DefCOM [12]	D-DCFI [7]	Anjali et al. [32]
Deployment	Throughout the network	ISP domain	ISP domain
Detection	Traffic tree discovery	Flow based Entropy	Flow based Entropy
Response	Rate limiting	Filtering at edge routers of ISP domain	Autonomic dynamic honeypot redirection
Security	PKI	N/A	N/A
Robustness	Weak	Very Weak	Weak
Implementat--ion	Difficult	Very Easy	Difficult

Clearly there is no single defense mechanism which is good in all identified metrics. A distributed defense mechanism which detects and filters the low and high rate DDoS attacks at practically feasible locations on the Internet is required. Moreover detection as well characterization of attack traffic should be computationally feasible. At last there should not be manual intervention required for generating the response against DDoS attacks whereas an automatic filtering mechanism which can be triggered by detection and characterization module is the need of the hour.

5. Proposed Methodology

The validation of DDoS defense requires thousands of legitimate and attack nodes. Moreover different attack scenarios are also required to be tested. Keeping in view these requirements neither actual Internet nor experimental lab having required level of scalability is practically feasible. So a simulator which can emulate important protocols of Internet architecture is required for validation of proposed approach. The generic approach in fig. 1 makes use of NS-2 [29] as testbed because of following reasons: -

- NS-2 is a discrete event driven simulator used for wired cum wireless network research. Internet based applications are also event-driven in nature
- NS-2 is an open source tool and is extensible
- Wide use of NS-2 in research work as testbed for validation and performance comparison of different approaches.
- It has support for network protocols such as TCP and UDP, network traffic sources such as HTTP, FTP, Telnet, CBR, and Ping, router queue management mechanisms such as Drop Tail, RED and CBQ.
- Support for various servers and clients HTTP,FTP server and client is available with provision of trace driven simulations.
- A C++ user in NS can modify and/or create protocols, agents, and nodes etc. as per requirements of proposed approach.

First and foremost a Internet like topology needs to be generated using topology generators Inet[30], GTITM[31] etc. The topology generator produces a NS-2 compatible tcl file. Legitimate and attack traffic is attached either through traffic generators or after pre-processing of datasets for trace-driven simulations. Now in the network both attack and legitimate traffic flows from one point to another. The next phase involves monitoring of traffic at source/victim or intermediate network. The time stamped collection of packet headers at different points of topology help in analysis of traffic for detection. Time-series or packet window analysis of traffic using detection metric appropriate for DDoS attacks is done. Here chosen detection metric must be computationally efficient; otherwise traffic analysis component itself succumbs to the pressure of voluminous DDoS traffic. Moreover an anomaly based approach only is suitable for detection of novel attacks. So a detection model based on only legitimate traffic needs to be made which defines normal behaviour of the network. Detection thresholds needs to be computed based on ROC curves obtained at different values of tuning parameter. Once the attack is detected a characterization scheme helps in distinguishing attack packets from normal packets. The characterized attack traffic is then filtered at different points of the Internet using mitigation framework. Finally offline analysis of traffic traces obtained without attack, with attack and with defense on identified performance metrics helps in evaluation of specific proposed approach

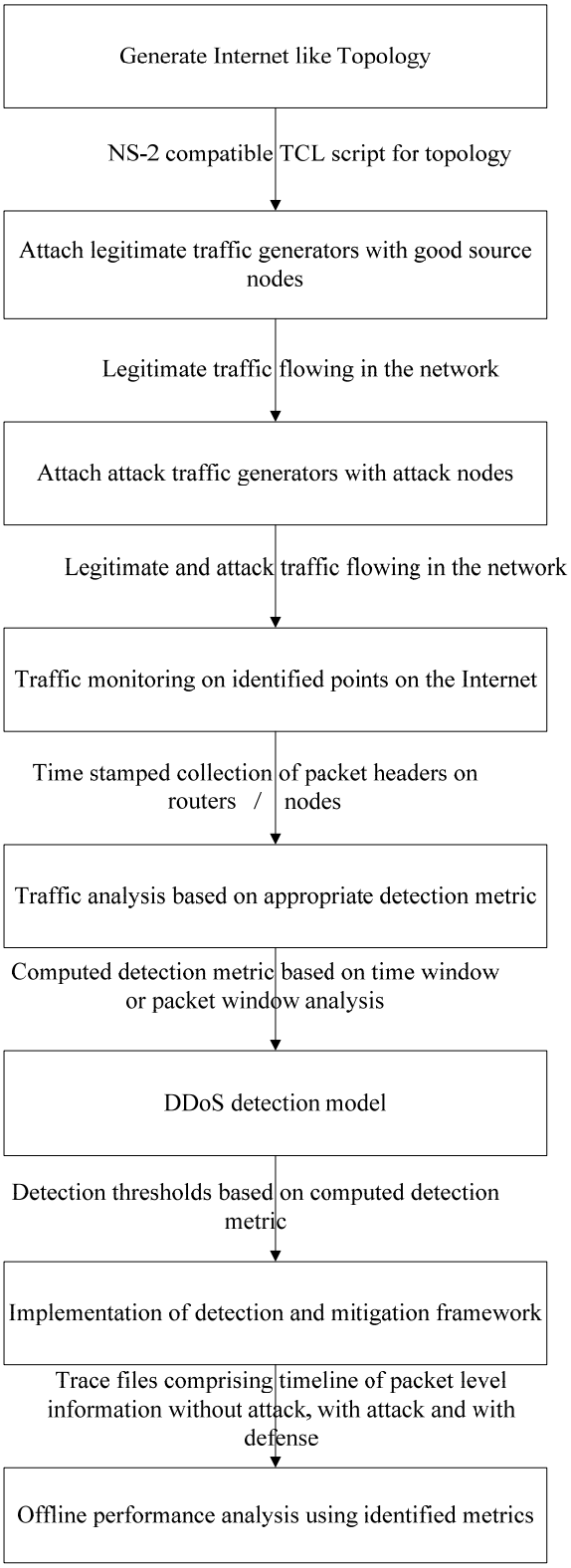

Figure 1: Generic Methodology for DDoS Defence

6. Conclusion

The major contributions of this paper are as follows:-

- A deep insight into need of distributed defense and its evolution.
- Identification of key metrics for comparing existing distributed defense techniques.
- Standings of distributed defense techniques in terms of identified metrics.
- Research gaps and scope for future work
- Generic methodology to pursue research in combating DDoS attacks

Drawbacks:-

Our review needs to be complemented with benchmark topology, legitimate and attack traffic generators, datasets and simulators which can be used for validation of proposed DDoS defense.

References

[1] McCumber, J. (1991). Information System Security: A Comprehensive Model. Proceedings of the 14th National Computer Security Conference. Baltimore. MD. USA.

[2] Kurose, J. and Ross, K. W. (2002). Computer Networking: A Top-Down Approach Featuring the Internet. pp 605-607. Second Edition, Addison Wesley.

[3] WWW Security FAQ. <http://www.w3.org/Security/Faq/wwwsf6.html>. Accessed 2007 Dec 9.

[4] Neumann, P. G. (2000). Denial-of-Service Attacks. Communications of the ACM 43(4): 136. xx

[5] Chena, L. C., Longstaff, T. A. and Carley, K. M. (2004). Characterization of defense mechanisms against distributed denial of service attacks. Computers & Security 23: 665-678.

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

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

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

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

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

[11] Yau, D. K. Y., Lui, J. C. S., Liang, F. and Yam, Y. (2005).Defending against distributed denial of service attacks with Max-Min fair server-centric router throttles. IEEE Transactions on Networking, Vol. 13. No. 1, pp. 29-42.

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

[13] Mahajan, R., Bellovin, S., Floyd, S., Paxson, V. and Shenker, S. (2002).Controlling high bandwidth aggregates in the network. ACM Computer Communications Review 32(3).
[14] Canonico, R., Cotroneo, D., Peluso, L., Romano, S. P. and Ventre, G. (2001). Programming Routers to Improve Network Security. Proceedings of the OPENSIG 2001 Workshop Next Generation Network Programming.
[15] Carl, G., Kesidis, G., Brooks, R. R. and Rai, S. (2006).Denial-of-Service Attack-Detection Techniques. IEEE Internet Computing, pp. 82-89.
[16] MANAnet DDoS White Papers, available at http://www.cs3-inc.com/mananet.html
[17] Shi, W., Xiang, Y. and Zhou, W.(2005).Distributed Defense Against Distributed Denial-of-Service Attacks. Proceedings of ICA3PP Springer-Verlag, LNCS 3719. pp. 357-362.
[18] Eronen, P. (2000). Denial of Service in Public Key Protocols. Proceedings of the Helsinki University of Technology Seminar on Network Security. xxx
[19] Leiwo, J., Nikander, P. and Aura, T. (2000). Towards network denial of service resistant protocols. Proceedings of the 15th International Information Security Conference. pp. 301-310.
[20] Tupakula, U. K. and Varadharajan, V. (2003).Analysis of automated model against DDoS Attacks. Available at: <http://citeseer.ist.psu.edu/664761.html.>
[21] Tupakula, U. K. and Varadharajan, V. (2003). A practical method to counteract denial of service attacks. Proceedings of the 26th Australasian Computer Science Conference, Volume 16, pp. 275-284.
[22] loannidis, J. and Bellovin, S. M.(2002).Implementing Pushback: Router-Based Defense against DDoS Attacks. Proceedings. of Network and Distributed System Security Symposium, Catamaran Resort Hotel San Diego, California.
[23] Peng, T., Leckie, C. and Ramamohanarao, K. (2002).Defending against distributed denial of service attack using selective pushback. Proceedings of the 9th IEEE International Conference on Telecommunications (ICT). pp 411-429. Beijing. China.
[24] Tupakula, U. K. and Varadharajan, V. (2003).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
[25] Chen, S. and Song, Q.(2005).Perimeter-Based Defense against High Bandwidth DDoS Attacks. IEEE Transactions on Parallel and Distributed Systems 16(6): 526-537.
[26] Haggerty, J., Shi, Q. and Merabti, M.(2005).Early Detection and Prevention of Denial-of-Service Attacks: A Novel Mechanism with Propagated Traced-Back Attack Blocking. IEEE Journal on Selected Areas in Communication. 23(10): 1994-2002
[27] Tupakula, U. K. and Varadharajan, V. (2004).Tracing DDoS Floods: An Automated Approach. Journal of Network and Systems Management 12: 111-135.
[28] Schnackenberg, D., Djahandari, K. and Sterne, D. (2000). Infrastructure for Intrusion Detection and Response. Proceedings of the DARPA Information Survivability Conference and Exposition, pp. 3-11.
[29] VINT Project U. C. Berkeley/LBNL, \NS2: network simulator," Available at http://www.isi.edu/nsnam/ns, 2006.
[30] Topology Project University of Michigan, \Inet: Internet Topology Generator,"Available at topology.eecs.umich.edu/inet/, 2006.
[31] GT-ITM Traffic Generator Documentation and tool, Available from: <http://www.cc.gatech.edu/fac/EllenLegura / graphs.html>.
[32] Sardana, A., Joshi, R. (2009). An auto-responsive honeypot architecture for dynamic resource allocation and QoS adaptation in DDoS attacked networks. Computer Communications. 32(12): 1384-1399.
[33] Shi, W., Xiang, Y., and Zhou, W. (2005). Distributed Defense Against Distributed Denial-of-Service Attacks. Proceedings of ICA3PP 2005, LNCS 3719, pp. 357-362.

Monika Sachdeva[1] has done B.Tech. Computer Science and Engineering from National Institute of Technology NIT, Jalandhar in 1997. She finished her MS Software Systems from BITS Pilani in 2002. Currently she is a Ph.D. student in Department of Computer Science & Engineering at Guru Nanak Dev University, Amritsar, Punjab, India. Her research interests include Web Services, Distributed Denial-of-Service, and Design and Analysis of algorithms.

Gurvinder Singh[2] has been a meritorious student throughout his academic career. He did his MCA from Guru Nanak Dev University, Amritsar GNDU, Amritsar in 1996. He finished his Ph.D. from GNDU, Amritsar in 2006. Currently, he is Reader in the Department of Computer Science & Engineering, GNDU, Amritsar. He has published over 40 research papers in International Journals and conferences. His general research Interests are in the areas of Parallel Computing and Computer Networks. Currently he is working on protection rom Internet Attacks.

Krishan Kumar[1] has done B.Tech. Computer Science and Engineering from National Institute of Technology NIT, Hamirpur in 1995. He finished his MS Software Systems from BITS Pilani in 2001. Recently in Feb. 2008, he finished his Ph. D. from Department of Electronics & Computer Engineering at Indian Institute of Technology, Roorkee. Currently, he is an Assistant Professor at SBS College of Engineering & Technology, Ferozepur, Punjab, India. His general research Interests are in the areas of Information Security and Computer Networks. Specific research interests include Intrusion Detection, Protection from Internet Attacks.

Kuldip Singh[3] received the B.E. (Electronics and Communication), M.E. (Electronics and Communication) and Ph.D. (Computer Engineering) degrees from University of Roorkee, Roorkee in 1968, 1970 and 1987 respectively. He is currently professor at Department of Electronics & Computer Engineering, Indian Institute of Technology Roorkee, India. His research areas are parallel processing, computer networking, bioinformatics, continuing education and human resource development.