CHAPTER 8

CONCLUSIONS AND SCOPE FOR FUTURE WORK

The growing number of DDoS incidents as well sophistication in DDoS attacks of present age poses undefeated challenges before security researchers. The main issues in defending against DDoS attacks are:-

- To detect all types of DDoS attacks reliably and accurately.
- To discriminate DDoS attacks from Flash events (FEs).
- To segregate attack traffic from legitimate traffic accurately.
- To react against huge volume generated by DDoS attacks in an automated manner with minimum collateral damage.

In this work, we have tried to address these issues in defending web service against DDoS attacks. The validation of the work has been done through simulation experiments in NS-2 test bed, trace-driven simulations in NS-2, analysis of real attack datasets, and emulation experiments on DETER test bed. The contributions of our work and future scope are summarized in subsequent sections.

8.1 Conclusions

I. An anomaly based detection approach which relies on both source IP address entropy and traffic cluster entropy has been proposed to not only capture variety of DDoS attacks but also to discriminate between DDoS attacks and FEs. The capability of entropy to summarize dispersion and skewness of traffic feature distributions has been used effectively in this work to detect various DDoS attacks. Moreover it has been widely observed in analysis of Internet traces, web logs and real datasets that a lot of machines send traffic towards web server during both DDoS attacks and FEs. But typical distribution of source IP addresses among few clusters during FEs, distinguishes FEs from DDoS attacks.

II. High rate skewed DDoS attacks, which completely disrupt services to legitimate clients, are detected reliably and accurately. In these attacks, few sources are used to send attack traffic at high rate towards server. Simulation
experiments are carried out at various attack strengths. CAIDA DDoS attack 2007 dataset has also been preprocessed and used in trace-driven simulation experiments. The sharp decrease in source address entropy below thresholds in all the experiments proved that the proposed approach is highly effective in detecting high rate skewed DDoS attacks.

III. Accurate detection of low rate Isotropic DDoS attacks, which slowly degrade services to legitimate clients, have always been a challenge for state-of-the-art detection approaches. The low rate DDoS attacks are simulated in our experiments by sending the same amount of traffic from each attack host as that of legitimate client without causing severe congestion at the bottleneck link in NS-2. The attack hosts are uniformly distributed in all the ISPs of the simulation topology. It has been found that both source address entropy and traffic cluster entropy cross their respective thresholds even though the total volume generated in not large enough.

IV. The proposed detection mechanism is adaptive to dynamic network environment. Traffic cluster entropy threshold is calibrated using receiver operating characteristics curve (ROC). An optimum value of traffic cluster entropy threshold has been computed so as to minimize false positives and negatives for the simulation environment. The evaluated metrics for detection are as follows:-

Detection rate : - 82%
False positive rate: - 20%
Precision : - 57%
F-measure : - 67%
Classification rate : - 80%

V. Most of the existing detection schemes including even source address entropy as detection metric have failed to address FE scenarios. The proposed detection approach exploits clustering behavior of sources in FEs and DDoS attacks. The source address entropy increases in both of the cases, but traffic cluster entropy increases beyond threshold only in case of DDoS attacks. In order to test the sensitivity of our detection approach, we have
increased number of new clusters in FEs from 0 to 80% and decreased number of new clusters from 100% to 2.5% in case of DDoS attacks. But still up to 35% new clusters in FE and up to only 4% new clusters in DDoS attacks, our approach is able to discriminate between FEs and DDoS attacks.

VI. DDoS attacks based on spoofing are also easily detected by our approach. MIT Lincon 2000 dataset has been analyzed in this work. It has a TCP flooding DDoS attack. The attack has started at 4873 seconds and finished at 4882 seconds i.e. duration of attack is 9 seconds. Empirical results are as below:-

Source address entropy without attack: - 3.32-3.45
Source address entropy during attack: - 9.93-13.72
Traffic cluster entropy without attack: - 1.88- 2.54
Traffic cluster entropy during attack: - 9.93-13.72

Clearly during DDoS attacks, all the attack sources belong to new clusters resulting in tremendous increase of source address entropy and traffic cluster entropy.

VII. Emulation experiments on DETER test bed have further strengthened our claim to use source address entropy and traffic cluster entropy as a detection metric on real hardware and operating system. The UDP flat, UDP rampup, UDP rampdown, UDP pulsing, and TCP flat attacks are launched with web traffic as background in different emulation scenarios. Flash traffic of the same strength is also mixed with legitimate web traffic in an another scenario. The rise in traffic cluster entropy in case of DDoS attacks and its stability in FEs clearly justify the supremacy of traffic cluster entropy as a metric to distinguish between FEs and DDoS attacks. Moreover an experiment methodology to systematically use DETER testbed resources in a convenient way has been provided to facilitate reserachers in the field of network security.

VIII. An ISP based distributed defense framework (DDF) is proposed as autonomy, adequate infrastructure, and viability of deployment in incremental fashion is possible in ISP domain. The deployment of various modules in ISP domain makes the approach pragmatic as defense modules
do not require whole Internet infrastructure to be modified and are independent in the sense that they can work in isolation though cooperation improves the results. Transit-stub model of GTITM Internet topology generator is adopted for creating topology consisting of eight ISPs domains. The victim server however is protected in single ISP domain only.

IX. The computational burden of proposed DDoS defense is distributed among all POPs of the protected ISP domain. There is no bottleneck point as for as computational complexity of deployed defense modules are concerned. It makes our distributed approach DoS-resistant.

X. The proposed approach to detect flooding DDoS attacks and filter attack traffic at ingress edges of the protected ISP domain generates an automated response against these attacks. Due to distributed functionality and better infrastructure to handle DDoS traffic at one hop upstream from victim network in ISP domain, our approach is successful in reacting to flooding DDoS attacks without manual intervention. The infrastructure however improves with tier level of the ISP.

XI. The detection approach in most of the existing schemes has high computational overheads. However the proposed entropy based detection approach has the capability to process the packets in OC3 range. Moreover monitoring, classification and entropy computation overheads are distributed among all ingress POPs of the protected domain so that POP connected to the protected server may be relieved to process huge volume of traffic near the server.

XII. Besides being computationally fast, the proposed approach is simple to implement as it is based on easily accessible information of source IP at ingress POPs of the protected ISP domain.

XIII. To objectively evaluate DDoS attack’s impact, its severity and the effectiveness of a potential defense, there is need of precise, quantitative and comprehensive DDoS impact metrics that are applicable to web services. We have identified web specific performance metrics from the literature. The degradation in web service due to DDoS attacks are quantified in terms of average response time and percentage of failed transactions at application level, throughput and percentage of link utilization at aggregate level, and
normal packet survival ratio (NPSR) and legitimate packet drop probability (LPDP) at packet level.

XIV. The filtering in the proposed defense framework is dynamic in two ways: (1) it triggers in state of attack only; (2) it adapts to change in attack sources used by attackers. POPs are able to process the packets at fast rates due to no look up and checking overheads in normal state. Even once attack is detected and attack sources are characterized using history based matrix, these overheads are distributed among all ingress POPs in addition to saving expensive core bandwidth. Moreover some attack tools keep on changing attack sources during attacks, so filter array population should be refreshed after every change. We have implemented this dynamism on the cost of attack status variable check whenever each time window starts.

XV. A comprehensive evaluation of proposed defense framework is carried out using web specific state-of-art experimental scenarios in NS-2 test bed. Performance metrics are compared in normal, attack, and with proposed defense control situations. The proposed defense is also compared with Pushback implemented on well known automatic queue management technique RED. The vast improvements in performance under proposed defense clearly manifest supremacy of the approach.

8.2 Scope for Future Work

This study is a small but significant step towards comprehensive defense against security attacks. It opens up a number of avenues for future work. An array of research issues which require thoughtful addressing are as follows:-

I. Monitoring and analysis of traffic are distributed so as to minimize computational overheads at any single point of the protected ISP domain. Moreover a small time window further reduces state monitoring overheads at each POP. But keeping in view practical deployment, traffic sampling without inducing bias and fast monitoring adapters can handle the traffic load in an improved manner. Better data structures like bloom filter can also be used to minimize storage complexity. Even packet-handling code can be optimized by eliminating floating point operations and achieving parallelism in clustering mechanism.
II. The information exchanged among POPs of the protected ISP domain in the proposed distributed defense framework is susceptible and can be intercepted by the hackers. Moreover, authentication of POPs is also not done before exchange of information. So the communication in distributed defense framework is vulnerable to passive and active attacks. Current security mechanisms such as IPSec, PKI, CA, Symmetric and Public key based authentication can be used to meet the requirements. Even security headers provided in IPv6 can be used to strengthen the framework against these attacks.

III. Current functionality of the proposed framework is limited to protected ISP domain only. However, it can be extended in multiple ISP domains using perimeter based approach or controller agent model proposed in the literature. The extended framework can be used for implementing filtering further upstream across multiple ISP domains.

IV. The identification of specific malicious flows for a particular ingress POP is not done in the proposed defense framework. A simple packet marking scheme can be used to characterize ingress POPs responsible for specific malicious flows. This will greatly reduce lookup overheads for filtering malicious flows at ingress edges of the protected ISP domain though at the cost of packet marking overheads.

V. The computation of cumulative entropy at POP connected to protected server relies on equations 4.9 and 4.10 to summarize entropies collected from all the POPs. Equation 4.9 is based on the assumption that set of flows observed at ingress POPs are mutually exclusive from each other. An analytical solution to remove this assumption can be beneficial to make proposed approach more practical and robust. Characterization of attack flows in a distributed manner and subsequently filtering malicious traffic near attack sources in multiple ISP domains are also our future goals.

VI. Though proposed history based characterization yield reasonable performance against DDoS attacks, yet sneaky attackers can falsely train our history to treat attacker’s sources as legitimate ones. As per literature, deviation in traffic cluster entropy can be effectively used to estimate
number of attack sources. The estimated number of attack sources can act as minimum threshold to find attack sources from the history matrix iteratively.

VII. DDoS attacks are launched using well coordinated and highly organized attack networks. The ISPs are also required to work in tandem for designing technical and economic models to achieve cooperation, in order to fight against the menace of DDoS attacks collaboratively.

VIII. An easy availability of user friendly attack tools and their source codes provide flexibility to attackers to create a variety of new attacks by error and trial. It is almost impossible to predict all attack variations and design defenses that will work for all cases. So the long term goal should be to design bugs free codes and fix the security holes in existing systems as early as possible.

IX. The number of DDoS defense techniques developed in recent past has grown in number but not in quality. The clear-cut proof for the same is growing number of DDoS incidents against popular sites. In order to strengthen the quality of research in the field, scalable test bed and freely accessible benchmarked attack datasets must be made available to the researchers. However the initiatives taken by Mirkovic et al. (2006) and her team in this regard are commendable and the whole research community in the field should propel their research efforts.