Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 85 (2016) 7 – 15

Procedia Computer Science

International Conference on Computational Modeling and Security (CMS 2016)

Trends in Validation of DDoS Research

Sunny Behal[a*], Krishan Kumar[b]

[a]Deptt of Computer Sci. & Engg, Shaheed Bhagat Singh State Technical Campus, Ferozepur-152004, India [b]Deptt of Computer Sci. & Engg, Shaheed Bhagat Singh State Technical Campus, Ferozepur-152004, India

Abstract

Over the last decade, attackers are compromising victim systems to launch large-scale coordinated Distributed Denial of Service (DDoS) attacks against corporate websites, banking services, e-commerce businesses etc. These attacks results in cripple down their services to legitimate users and cause huge financial losses. Numerous solutions have been purported to combat against these DDoS attacks but there is no impeccable solution to this challenging problem till date. Most of the existing solutions have been validated using experiments based on simulation but recently, the researchers have started using publically available real datasets for the validation of DDoS research. In this paper, the validation techniques used for DDoS research are investigated comprehensively and it is proposed to extend them with the inclusion of new validation technique of analyzing real datasets. A brief review of existing real datasets is presented to elucidate the trends in the validation of DDoS research.

Peer-review under responsibility of the Organizing Committee of CMS 2016

Keywords: DDoS; Intrusion; Flash Events; Datasets; Network Security

1. Introduction

DDoS attacks have become a serious cause of problem and security threat for the enterprises, banks etc. doing businesses over the Internet. These attacks have brought enormous financial losses to them over the years. According to CERT[1,2], "A DDoS attack is a malicious attempt from multiple systems to make computer or network resources unavailable to its intended users, usually by interrupting or suspending services connected to the Internet". There are number of evidences reported[1,3,4,5,6] which points out the severity of the DDoS problem. According to the survey conducted by Kaspersky lab in 2015[4], the average financial loss to the companies' suffering from DDoS attacks is in between $52000 to $440000. According to Q1 DDoS attack report 2015 by Arbor networks [5], the attackers are using three main types of DDoS attacks TCP SYN flood, DNS flood and Smurf attacks, out of which 76% are TCP SYN flood attacks, the 90% of the attacks are application layer attacks whereas 42% are of TCP State-Exhaustion attacks. The volume of traffic of such attacks have been amplified to around 400 Gbps in the year 2014 as compared to 100 Gbps in the year 2010. Even the number of DDoS attacks has also increased exponentially over the years[5]. According to Security watchdog report[6], the number of DDoS attacks have been increased by 240% in 2014.

* Corresponding author. Sunny Behal, Tel.: +1-91-82880-12007 Email address: sunnybehal@rediffmail.com

Peer-review under responsibility of the Organizing Committee of CMS 2016
doi:10.1016/j.procs.2016.05.170

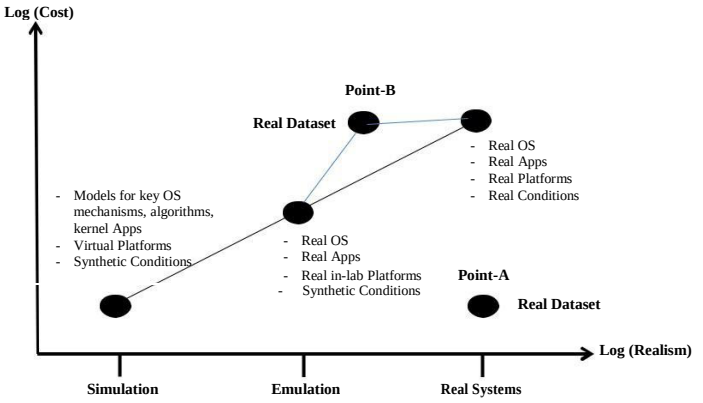

Fig. 1. Validation techniques used for DDoS related research

This is evident from this exponential increase in attack traffic that the attackers are continuously updating their skills, using advanced attack techniques to launch such huge amount of traffic and at the same time defeating the existing defense solutions. It has been observed that all of these DDoS attacks are launched now-a-days by using botnets [7]. These botnets are composed of millions of compromised machines which are controlled through some command and control server to flood enormous amount of data towards the victim[8]. The major contributions of this paper are :

- A review of validation techniques used for DDoS research.
- Addition of a new dimension of real datasets in the existing validation paradigms used for DDoS research.
- A review of publically available real datasets used for the validation of DDoS research on various identified attributes.
- Identification of the properties of a real datasets that would be more appropriate for the accurate validation of DDoS research.

The remainder of the paper is organized as follows. Section-II focuses on various validation techniques used for DDoS experimentation and their comparison. In section-III, a brief review of publically available real datasets on identified attributes is given and the last section concludes the work by highlighting the properties of an ideal realistic dataset that would be more appropriate for DDoS research.

2. Validation Techniques used for DDoS Research

Whenever a researcher proposes any novel detection or defense method in the field of network security, the proposed method has to be implemented in the form of a network based experiment for its evaluation and then it needs to be validated through available set of validation techniques. There are basically four approaches used for validation in network based experiments [9].

- **Mathematical models** are theoretical in nature. In such models, the given system, applications, platforms and conditions are modeled symbolically and then validated mathematically.
- **Simulation** provides a repeatable and controllable framework for network based experiments on a single com-puter system. A simulation based experiment is very easy to configure and manage. It gives flexibility to the programmers to do experiments in a rapid prototype and evaluation based environment so that many bad al-ternatives could be discarded timely before attempting a full implementation. Simulation use models of key operating system functions, kernel mechanisms, virtual platforms and synthetic conditions for experiments. Examples include NS2 [10], NS3[11], OMNET++[12], Qualnet3 [13], OPNET [14], CORE [15] etc.

Table 1. Comparison of validation techniques used for DDoS Research

Attributes	Simulation	Emulation	Real Systems	Real Dataset
Fidelity	Lowest	Moderate	Highest	Highest
Repeatability	Highest	Moderate	Lowest	Highest
Programmability	Highest	Moderate	Highest	Lowest
Extensibility	Highest	Moderate	Lowest	Highest
Research Functionality	Lowest	Moderate	Highest	Highest
Abstraction	Highest	Moderate	Lowest	Lowest
Type of Network Elements	Virtual nodes	Mixture of real and virtual nodes	Real nodes	Real nodes

- **Emulation** is an integration of simulation and real systems. In emulation, the real elements of an operating system and real applications are combined with unreal and simulated elements like soft network links, virtual intermediate nodes and unrealistic background traffic. However, emulation use soft routers for making connec-tions. The simulation runs in virtual simulated time whereas emulation runs in real time. Emulation technique has the concern of scalability factor as it is very di cult to extend the topology of computer systems beyond cer-tain limits and one can't make topology as large as of an Internet Service Provider (ISP) [16,17,18,19,20]. Examples include: NS3 [11], DETER[21], Emulab [22], WAN-in-Lab (WIL) [23] etc.
- **Real Systems** provide realistic network conditions, real operating systems, applications and platforms and is proven to be best for network based experimentations. However, there are some limitations of using real systems for experimentations like (a) change of network topology is not possible for a new experiment b) it is very unsafe to do live experiments with Internet worms, viruses etc. because they can easily escape from the experimentation setup and can damage the live network components and (c) the flooding based DDoS attacks can cause degradation of network links [19] . Examples include GENI [24], PlanetLab [25] etc.

Since the mathematical models are theoretical in nature, they can't be used for such network based experiments. The simulation technique can't execute real applications as it can approximate certain hardware and software functions only. The emulation provides a convenient way to use real hardware and applications, but its functionality is limited by the number of nodes, types of hardware, and di culty in configuration, management and reproducibility of exper-iments. The accuracy of simulation based experiments and their appropriateness for DDoS related research has been probed in recent times [9,26,19]. Real systems are ideal for validating network based research but they are limited in their functionality because of their complex nature. However, GENI[24], which is a real system based highly programmable networking testbed, has been in news recently. GENI is an attempt to interface all the existing popular testbeds like Emulab [22], PlanetLab [25] etc. into one integrated platform for executing real experiments at scale. The researchers are continuously working on solving the problems of real systems. The use of Software Defined Networking (SDN) [27],[28] is a promising approach which makes the networks highly scalable and programmable.

It has been investigated that real datasets have been used extensively for the evaluation and validation of DDoS re-lated research recently [19,20,29,30,31,32,33,34,35,36,37]. A real dataset is a live captured data which has been generated using realistic network conditions which includes real operating systems, applications and platforms. Alternatively, these datasets can also be synthetically generated in a closed lab environment using emulation based experimentation setups like NS3[11],Emulab[22], GENI [24]etc. Because of their extensive use for the validation of DDoS related research, it is proposed to add a new dimension into the existing set of validation techniques as revealed in Figure-1. Mathematical models are not shown in the figure because they are not used for network based real experiments. Two locations are identified where the real dataset validation technique can be added (shown in figure-1) depending upon whether we are using existing dataset or generating our own realistic dataset through real or hybrid experimentation. Further, all of these validation techniques including real datasets have been compared in Table-1 based on the generic properties of an ideal realtime network experimental setup viz: Fidelity, Repeatability, Programmability, Extensibility and Research Functionality [38,26,19,29]. The experimental setups like NS3[11],Emulab[22], GENI [24] etc. provide advanced facilities for

researchers to implement and evaluate DDoS detection and defense algorithms. Their generic properties are described briefly as follows:

- **Fidelity:** A network based experiment setup should possess fidelity criteria which mean reliability and depend-ability to the real networks. The fidelity dimension includes large topology having enough number of nodes, real routers, heterogeneous mixture of hardware and software, and real mix of link bandwidth capacities and delays.
- **Repeatability:** A network based experiment setup should possess the facility to save and repeat or reproduce experiments subjected to the same environmental conditions. However, the factors like Internet topology, avail-able bandwidth, enhancements in software and hardware, type of background traffic and attack traffic makes it very di cult to repeat an experiment using real systems.
- **Programmability:** A network based experiment setup should have the flexibility of using new customized net-work mechanisms for monitoring, filtering, detecting, adding or modifying router algorithms, realistic hetero-geneous hardware etc. However, use of software routers may add flexibility to the programmers.
- **Extensibility:** A network based experiment setup should have the provision to scale the topology of experiments in comparison to wild Internet. Experiments should be portable and should be accessed remotely.
- **Research Functionality:** In addition to control the hardware and software components of the experiments for the security based experiments, there is also need to facilitate technical and social environments for experiments like a wide variety of traffic and topology generators, diverse experimental profiles, latest tools for visualization and analysis of results etc.
- **Level of Abstraction:** Abstraction is the amount of complexity by which a system is viewed or programmed. The higher the level, the less detail and vice versa.
- **Type of Network Elements used:** This parameter states the type of network elements used in the experiment like real nodes, soft nodes or mix of both.

It has been observed from the comparison shown in the Table-1 that the simulation has lowest fidelity and research functionality whereas it is highest in case of real systems. The moderate values of emulation shows that it is a compromise between simulation and real systems. Each validation technique has its own merits and demerits. The real systems and real datasets are the best appropriate for validating and evaluating DDoS related research. As real systems based experiments are very complex and di cult to handle, the focus of researchers is shifting towards the use of publically available real datasets.

3. Review of Real Datasets used for DDoS Experiments

Recently, most of the DDoS related researchers have started using publically available real datasets for the valida-tion of their approaches [19,20,29,30,31,32,33,34,35,36,37]. However, the appropriateness of the selected dataset for the approach to be validated remains an open issue. According to Bhuyan et. al. [39], it is very crucial to select a suitable dataset for the validation of any proposed DDoS attack detection technique. The captured network trace should contain the mixture of realistic background traffic and attack traffic in appropriate proportion, and should not be biased towards specific type of traffic[37]. However, it is very di cult to ensure appropriate mixture of normal and attack traffic in a real experiment driven dataset because there is no known formula to model Internet traffic correctly[55].

There are number of real datasets which are publically available and have been used extensively for the DDoS related research. These real datasets are summarized below:

- **FIFA World Cup Dataset 1998:** This dataset records the requests sent to the football world Cup's website during the time period April - July 1998. Overall 1,352,804,107 requests were received by the website.

The stored log files were originally in the Common Log Forma but to ensure the privacy of each individual that visited the website, the client IP addresses are pseudonymised and replaced with a unique identifier.[48]

- [illegible]
- **MIT Lincoln Laboratory LLSDDoS Dataset 1998:** This laboratory is the store house of tcpdump network traces data that has been captured in realtime. For example, LLDOS 1.0 dataset records a DDoS attack run by an inexperienced attacker whereas LLDOS 2.0.2 dataset records a DDoS attack launch by a stealthier attacker. The data of all 5 attack phases of a DDoS attack has been recorded in which the attacker firstly do network scanning in initial phase and then compromise the hosts by exploiting the sadmind vulnerability of solaris Operating system. Then it downloads the mstream DDoS software which is a trojan based malicious program and launch the DDoS attack [40].
- **KDD cup Dataset 1999 :** The KDD Cup 1999 dataset was generated for the 3rd International Knowledge Discovery and Data Mining Tools Competition(KDD99). This dataset is extensively used for malware related research. But its scope of usage is very limited. Mainly it is used for the evaluation of signature based IDS's only. It is not appropriate for evaluating DDoS detection, Flash Events and DDoS defense methods[41].
- **UCLA Dataset 2001:** This dataset contains packet traces collected during August 2001 by Network research lab. It contains records of UDP flood traffic having 1001B long packets. The attack is aborted at the end of the trace and proceeds with legitimate connections[42].
- **CAIDA DDoS Attack Dataset 2007:** This dataset contains the traffic traces of a flooding DDoS attack for the period of around one hour. The aim of attack was to consume the computing resource of the targeted server. However, IP addresses are pseudonymised, their payloads and non-attack traffic has been removed from the dataset for security reasons which limits the usability of this dataset. This dataset found its application in detecting low rate stealthy as well as high rate flooding DDoS attacks [43].
- **Waikato Internet Trace Storage Project Dataset 2009**: This is another widely referenced dataset for DDoS related research[1]. In this dataset, IP addresses are not actual and has been modified , the headers of transport layer and payload of UDP packets are removed for security reasons [44].
- **DARPA DDoS attack dataset 2009:** This is the latest DDoS attack based dataset from MIT Lincoln laboratory. The captured traffic contains a SYN flood DDoS attack on one target and background traffic. The DDoS traffic comes from about 100 di erent IPs. These hosts were used to launch a malware DDoS attack on a non-local target [45].
- **TUIDS DDoS Dataset 2012:** this dataset was prepared using TUIDS testbed archietecture with a Demilitarized zone (DMZ), consists of traffic from 5 di erent networks inside Tezpur University Campus. The attackers are placed in both wired and wireless networks with reflectors and the target placed inside the internal network. This dataset has also find its application in detecting low rate stealthy as well as high rate flooding DDoS attacks [46].
- **Booter DNS Dataset 2014:** This dataset is used to detect DNS based reflection and amplification DDoS attacks. This dataset is the record of DNSSEC-signed domains which includes traffic from around 70% of all active domains [47].

Today, the major thrust area in the field of DDoS is to distinguish attack traffic from similar looking Flash Events (FE) traffic [37]. FE traffic occurs when a server experiences an unexpected increase in requests from the legitimate clients. The Flash Events (FEs) have some common characteristics with DDoS attacks such as a substantial increase in the incoming network traffic, the overloading of the servers providing the services, and a degradation in the delivery of service [49]. It has been observed from the comparison as shown in Table 2 that there are only two datasets available for detecting FE traffic which are quite obsolete as there is enormous change in behavior of traffic, users and Internet services over the years and the same datasets can't be used as benchmark for validating present-day detection method-ologies. In DDoS research, only CAIDA [31,37,50,51,49,52], DARPA [53,51] and TUIDS [31] datasets are extensively used, the other datasets MIT Lincoln's LLSDOS 1.0 and 2.0[32,50], UCLA [49] and Waikato [44] are used rarely because they are quite obsolete as cleared from their year of generation. In KDD Cup 1999 dataset, it is very di cult to discriminate the attack traffic from the background traffic as the dataset is not properly labeled. TUIDS

Table 2. Comparison of publicly available real DDoS datasets

Year	Dataset	Dataset Category	Dataset Scope	Traffic Type	Traffic capturing Layer	IP Address
1998	FIFA World Cup [46]	Real	Flash	HTTP	Application	Mapped
1998, 1999, 2000	MIT Lincoln Laboratory LLSDDoS 1.0 and LLSDDoS 2.0.1 [40]	Synthetic	DDoS	TCP	Transport	Actual
1999	KDD Cup [41]	Real	Flash, DDoS	TCP	Transport	Mapped
2001	UCLA [42]	Synthetic	DDoS	UDP	Transport	Mapped
2007	CAIDA [43]	Real	DDoS	ICMP	Network	Mapped
2009	Waikato Internet Trace Storage Project [44]	Synthetic	DDoS	UDP	Transport	Actual
2009	DARPA 2009 DDoS Attack [45]	Synthetic	DDoS	TCP	Transport	Actual
2012	TUIDS [46]	Synthetic	DDoS	ICMP, UDP, TCP	Network, Transport	Actual
2014	Booter [47]	Real	DDoS	DNS	Application	Actual

dataset is recently been gaining popularity in the field of DDoS research but is synthetically generated. Booter DNS dataset is the latest addition in this list but it contains DNS queries traffic only.

There are number of limitations of these publically available datesets which limits their usage for validating DDoS research.

- the presence of asymmetric traffic.
- short length of the captured network traces.
- pseudonymised IP addresses that makes the understanding of traffic context very difficult.
- the model of legitimate user's behavior till date is not known, and hence not properly captured.
- low rate stealthy attacks that are di cult to detect, are not captured.
- most of the available datasets capture network layer traffic, hiding the application specific details.
- FE datasets are obsolete.
- failure of existing DDoS detection and defense approaches as attackers are moving from high volume, easily noticed attacks to low volume stealthy attacks.

It is evident from these limitations that these publically available datasets lacks key characteristics of the network traffic and thus are not appropriate for the validation of DDoS research. For the evaluation of any DDoS attack detection method, the availability of such realistic traffic dataset that possess mixture of appropriate attack traffic, non-attack traffic and normal background traffic, is the need of the hour. An ideal realistic dataset must possess the following properties.

- **Real source and destination IP addresses.** In order to simulate real time traffic scenarios, it is required that the clients must make valid TCP connections with the target server and accesses real pages on the server, which is possible only when both the client and server IP addresses are real.

- **A wide range of random source IP addresses.** The network traffic initiating from a wide range of IP addresses forms the key characteristic of the network dataset. It is required that actual attacks and FE traffic should be generated making use of a wide range of IP addresses.
- **Actual packets with valid headers.** To ensure the realistic nature of the traffic generated and captured , it is desirable that packets must have valid headers.
- **Appropriate mixture of normal and attack traffic.** To effectively evaluate any DDoS attack technique, the network traffic has to be generated with a appropriate mixture of normal legitimate and malicious attack traffic.

The properties of real datasets mentioned above are idealistic and are very di cult to achieve by real systems experimentation alone. Real systems suffer from a number of problems as mentioned earlier. They need to be augmented with emulation based techniques for better results as done by Fico et. al [54]. More reasonable results in DDoS research can also be obtained if the operational data from known networks become available for research purpose. A few researchers have performed real experiments in recent times [20,37,56]. Calvet et. al. [20] observe the behavior of Waledac botnet in a real time environment and access the performance of mitigation scheme against its P2P infrastructure. Sajal et.al. [37] developed a realtime traffic generation testbed framework for synthetically generating di erent types of realistic DDoS attacks, FEs and other benign traffic traces. Spognradi et. al.[56] did the analysis of real netflow datasets captured in the ExTrABIRE project of Italy for large scale traffic anomaly detection. Yuan et.al. [53] supervise the network traffic on the edge routers of local area network and measure the flow entropy metric to detect traffic anomalies. On the similar grounds, focusing on realtime experiment setups to enable the validation of DDoS research against real traffic at large scale, is the need of the hour. The researcher community should now change their focus from traditional simulation based experiments and analyzing publically available obsolete datasets to real scalable experiments.

4. Conclusion

Many solutions have been proposed to detect, prevent or mitigate DDoS attacks in literature. Most of these solutions have been validated using experiments based on simulation, emulation, real systems and analysis of publically available real datasets. Each of these validation techniques has their own merits and demerits but recently, real datasets are extensively used as an alternative to existing validation techniques of DDoS related research. It has been observed from the comparison of various publically available real datasets that there is no appropriate dataset avail-able for validating the DDoS research. Most of the available real datasets are obsolete, some of them lack required characteristics of network traffic and most of the above real datasets are not make available to the research community for security reasons. So, it is concluded that the trend of DDoS research is shifting towards scalable real experiments and there is need to generate realistic datasets. Our future work is to develop such a scalable real testbed for the generation of realistic datasets. It would surely be going to help the research community to develop more accurate detection and defense mechanisms to tackle the ever growing threat of DDoS attacks.

References

1. CERT, . The cert website http://cert.europa.eu/static/whitepapers/cert-eu-swp/ddosfinal.pdf. 2015.
2. Zhang, Y., Liu, Q., Zhao, G.. A real-time ddos attack detection and prevention system based on per-ip traffic behavioral analysis. In: Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on; vol. 2. IEEE; 2010, p. 163–167.
3. Silicon, . The silicon angle website http://siliconangle.com/blog/2013/08/26/5-notorious-ddos-attacks-in-2013-big-problem-for-the-internet-of-things/. 2013.
4. Report, K.. The kaspersky report 2015. 2015. URL: http://business-reporter.co.uk/2015/01/29/firms-face-financial-loss-ddos-att

5. Arbor, . Arbor network ddos attacks report http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5405-arbor-networks-records-largest-ever-ddos-attack-in-q1-2015-ddos-report. Tech. Rep.; Arbor Networks; 2015.
6. Watchdog, S.. The international business times http://www.ibtimes.co.uk/ddos-attacks-rises-by-240-2014-1442813.2014. URL: http://www.ibtimes.co.uk/ddos-attacks-rises-by-240-2014-1442813.
7. Wang, F., Wang, H., Wang, X., Su, J.. A new multistage approach to detect subtle ddos attacks. Mathematical and Computer Modelling 2012;55(1):198–213.
8. Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. 2012.
9. Ali, K.. Algorizmi: A Configurable Virtual Testbed to Generate Datasets for O ine Evaluation of Intrusion Detection Systems. Ph.D. thesis; 2010.
10. NS2, . The network simulator 2 http://www.isi.edu/nsnam/ns/. 2015. URL: http://www.isi.edu/nsnam/ns/.
11. NS3, . The network simulator 3 http://www.nsnam.org/. 2015. URL: http://www.nsnam.org/.
12. OMNET++, . The network simulator http://omnetpp.org/. 2015. URL: http://www.omnetpp.org/.
13. Qualnet, . The qualnet network simulator http://web.scalable-networks.com/content/qualnet/. 2015. URL: http://web.scalable-networks.com/content/qualnet/.
14. Chertov, R., Fahmy, S., Shro , N.B.. Emulation versus simulation: A case study of tcp-targeted denial of service attacks. In: Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006. 2nd International Conference on. IEEE; 2006, p. 35–326.
15. Ahrenholz, J., Danilov, C., Henderson, T.R., Kim, J.H.. Core: A real-time network emulator. In: Military Communications Conference, 2008. MILCOM 2008. IEEE. IEEE; 2008, p. 1–7.
16. White, B., Lepreau, J., Stoller, L., Ricci, R., Guruprasad, S., Newbold, M., et al. An integrated experimental environment for distributed systems and networks. ACM SIGOPS Operating Systems Review 2002;36(SI):255–270.
17. Guruprasad, S., Ricci, R., Lepreau, J.. Integrated network experimentation using simulation and emulation. In: Testbeds and Research Infrastructures for the Development of Networks and Communities, 2005. Tridentcom 2005. First International Conference on. IEEE; 2005, p. 204–212.
18. Mirkovic, J., Fahmy, S., Reiher, P., Thomas, R.K.. How to test dos defenses. In: Conference For Homeland Security. 2009, p. 103–117.
19. Schmidt, D., Suriadi, S., Tickle, A., Clark, A., Mohay, G., Ahmed, E., et al. A distributed denial of service testbed. In: What Kind of Information Society? Governance, Virtuality, Surveillance, Sustainability, Resilience. Springer; 2010, p. 338–349.
20. Calvet, J., Fernandez, J.M., Bureau, P.M., Marion, J.Y., et al. Large-scale malware experiments: Why, how, and so what? In: Proceedings of the 2010 Virus Bulletin Conference (VB). 2010, .
21. DETER, . The deter testbed http://www.deter-project.org/. 2015.
22. Emulab, . The emulab network testbed http://www.emulab.net/. 2015.
23. Lee, G.S., Andrew, L.L., Tang, A., Low, S.H.. Wan-in-lab: Motivation, deployment and experiments. In: Proc. PFLDnet. 2007, p. 85–90.
24. Elliott, C.. Geni-global environment for network innovations. In: LCN. 2008, p. 8.
25. Peterson, L., Bavier, A., Fiuczynski, M.E., Muir, S.. Experiences building planetlab. In: Proceedings of the 7th symposium on Operating systems design and implementation. USENIX Association; 2006, p. 351–366.
26. Mirkovic, J., Wei, S., Hussain, A., Wilson, B., Thomas, R., Schwab, S., et al. Ddos benchmarks and experimenter's workbench for the deter testbed. In: Testbeds and Research Infrastructure for the Development of Networks and Communities, 2007. TridentCom 2007. 3rd International Conference on. IEEE; 2007, p. 1–7.
27. Yeganeh, S.H., Tootoonchian, A., Ganjali, Y.. On scalability of software-defined networking. Communications Magazine, IEEE 2013; 51(2):136–141.
28. Kim, H., Feamster, N.. Improving network management with software defined networking. Communications Magazine, IEEE 2013; 51(2):114–119.
29. Hussain, A., Schwab, S., Thomas, R., Fahmy, S., Mirkovic, J.. Ddos experiment methodology. In: Proceedings of the DETER Community Workshop on Cyber Security Experimentation; vol. 8. 2006, .
30. Ozcelik, , Brooks, R.R.. Deceiving entropy based dos detection. Computers & Security 2015;48:234–245.
31. Bhuyan, M.H., Bhattacharyya, D., Kalita, J.. An empirical evaluation of information metrics for low-rate and high-rate ddos attack detection. Pattern Recognition Letters 2015;51:1–7.
32. Ma, X., Chen, Y.. Ddos detection method based on chaos analysis of network traffic entropy. Communications Letters, IEEE 2014; 18(1):114–117.
33. Shiaeles, S.N., Katos, V., Karakos, A.S., Papadopoulos, B.K.. Real time ddos detection using fuzzy estimators. computers & security 2012;31(6):782–790.
34. Detection Of Application Layer DDos Attacks Using Information Theory Based Metrics; vol. 10. 2012.
35. Hermenier, F., Ricci, R.. How to build a better testbed: Lessons from a decade of network experiments on emulab. In: Testbeds and Research Infrastructure. Development of Networks and Communities. Springer; 2012, p. 287–304.
36. Wu, Y.C., Tseng, H.R., Yang, W., Jan, R.H.. Ddos detection and traceback with decision tree and grey relational analysis. International Journal of Ad Hoc and Ubiquitous Computing 2011;7(2):121–136.
37. Bhatia, S., Schmidt, D., Mohay, G., Tickle, A.. A framework for generating realistic traffic for distributed denial-of-service attacks and flash events. Computers & Security 2014;40:95–107.
38. Benzel, T., Braden, R., Kim, D., Neuman, C., Joseph, A., Sklower, K., et al. Experience with deter: a testbed for security research. In: Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006. 2nd International Conference on. IEEE; 2006, p. 10–pp.
39. Bhuyan, M.H., Kashyap, H.J., Bhattacharyya, D.K., Kalita, J.K.. Detecting distributed denial of service attacks: Methods, tools and future directions. The Computer Journal 2013;7:031.
40. MIT, . The mit lincoln laboratory llsddos 1.0 dataset https://www.ll.mit.edu/ideval/data/2000/llsddos1.0.html. 1998.
41. KDD, . The kdd cup dataset http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html. 1999.

42. UCLA, . The ucla network traces dhruba k bhattacharyya/publication/262297993packet and flow based network intrusion dataset. 2001. URL: http://www.lasr.cs.ucla.edu/ddos/traces/.
43. CAIDA, . The caida ddos attack dataset http://www.caida.org/data/passive/ddos-20070804dataset.xml. 2007.
44. WAIKATO, . The waikoto internet trace storage project dataset https://labs.ripe.net/datarepository/data-sets/the-waikato-internet-traffic-storage-wits-passive-datasets. 2009.
45. DARPA, . The darpa ddos attack dataset. 2009. URL: http://www.isi.edu/ant/traces/DARPA2009DDoSattack-20091105.README.txt.
46. TUIDS, . The tuids dataset dhruba k bhattacharyya/publication/262297993packet and flow based network intrusion dataset. 2014.
47. Booter, . Dns and dnssec dataset www.simpleweb.org/wiki/traces. 2014.
48. FIFA, . The fifa world cup dataset http:// ita.ee.lbl.gov/html/contrib/worldcup.html. 1988.
49. Rahmani, H., Sahli, N., Kamoun, F.. Distributed denial-of-service attack detection scheme-based joint-entropy. Security and Communica-tion Networks 2012;5(9):1049–1061.
50. Xiang, Y., Li, K., Zhou, W.. Low-rate ddos attacks detection and traceback by using new information metrics. Information Forensics and Security, IEEE Transactions on 2011;6(2):426–437.
51. Lee, K., Kim, J., Kwon, K.H., Han, Y., Kim, S.. Ddos attack detection method using cluster analysis. Expert Systems with Applications 2008;34(3):1659–1665.
52. Bhatia, S., Mohay, G., Tickle, A., Ahmed, E.. Parametric di erences between a real-world distributed denial-of-service attack and a flash event. In: Availability, Reliability and Security (ARES), 2011 Sixth International Conference on. IEEE; 2011, p. 210–217.
53. Tao, Y., Yu, S.. Ddos attack detection at local area networks using information theoretical metrics. In: Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on. IEEE; 2013, p. 233–240.
54. Ficco, M., Avolio, G., Palmieri, F., Castiglione, A.. An hla-based framework for simulation of large-scale critical systems. Concurrency and Computation: Practice and Experience 2015;.
55. Paxson, V., Floyd, S.. Wide area traffic: the failure of poisson modeling. IEEE/ACM Transactions on Networking (ToN) 1995;3(3):226–244.
56. Spognardi, A., Villani, A., Vitali, D., Mancini, L.V., Battistoni, R.. Large-scale traffic anomaly detection: Analysis of real netflow datasets. In: E-Business and Telecommunications. Springer; 2014, p. 192–208.