Scalable DDoS Mitigation System for Data Centers

Zdenek MARTINASEK

Department of Telecommunications, Faculty of Electrical Engineering and Communication,
Brno University of Technology, Technicka 12, 616 00 Brno, Czech republic

martinasek@feec.vutbr.cz

DOI: 10.15598/aeee.v13i4.1531

Abstract. *Distributed Denial of Service attacks (DDoS) have been used by attackers for over two decades because of their effectiveness. This type of the cyber-attack is one of the most destructive attacks in the Internet. In recent years, the intensity of DDoS attacks has been rapidly increasing and the attackers combine more often different techniques of DDoS to bypass the protection. Therefore, the main goal of our research is to propose a DDoS solution that allows to increase the filtering capacity linearly and allows to protect against the combination of attacks. The main idea is to develop the DDoS defense system in the form of a portable software image that can be installed on the reserve hardware capacities. During a DDoS attack, these servers will be used as filters of this DDoS attack. Our solution is suitable for data centers and eliminates some lacks of commercial solutions. The system employs modular DDoS filters in the form of special grids containing specific protocol parameters and conditions.*

Keywords

Data center, DDoS, protection.

1. Introduction

Nowadays, the risk of cyber-attacks that are aimed at government, companies, news media or end users represents a real threat. According to the studies realized annually, the most commonly used techniques of cyber-attacks are DoS (Denial of Service) and SQL (Structured Query Language) injection (It is a statistic of actually realized attacks). DoS attacks can be simply divided into two basic types [1]: *Flooding attacks* and *Logical attacks*. In *Flooding DoS attacks*, an attacker sends a large amount of traffic to consume CPU (Central Processing Unit) or the bandwidth of the victim. The DoS attack consumes the resources of the victim's server or network in order to degrade a performance or cause a server crash. Flooding attacks take advantage of the weaknesses of the communication protocols such as TCP (Transmission Control Protocol) [2], [3], UDP (User Datagram Protocol) [4], [5], ICMP (Internet Control Message Protocol)[6], FTP (File Transfer Protocol) [2], SIP (Session Initiation Protocol) [7] or HTTP (Hypertext Transfer Protocol) [8]. *Logical attacks* use weaknesses in applications or software used at the victim's side. The attacker sends only a few messages that abuse the weaknesses of the software in order to disable or crash the target machine. The DoS attack is usually performed by a network node (e.g. a personal computer) seized by the attacker [1]. These network nodes are called zombies or botnets and they are not completely under the control of the attacker. It causes that the attack consists of large quantities of requests (usually hundreds or thousands), what can be realized from all over the world. The attacker creates a necessary infrastructure of botnets simply by using Trojan horses or other malware, that are running on the infected network nodes. Distributed Denial of Service attacks are performed by multiple nodes. Currently, the infrastructure of botnets is getting bigger and ready to attack anytime. More details about DDoS attacks can be found in survey papers [9], [10].

In practice, DDoS attacks have different use cases and targets. We summarize these observations in the following points:

- *Denial of Service* - it represents a classic usage of DDoS attacks. The competing companies are usually the target in this use case and the attacker wants to cause large financial losses and impair the company's reputation. Government networks and media servers are another typical target of these attacks.
- *Masking of cyber-attacks* - in this case, the attacker uses a DDoS attack to mask the "true" at-

tack that focuses on obtaining specific sensitive information (e.g. the attacker knows a bug in the system and he intends to take advantage of that). Under normal circumstances, the attack realized would be easily detectable but within the massive DDoS attack, it is extremely difficult to identify this attack. Hence, the attacker has enough time to take advantage of the bug. It usually takes several days to go through all logs to disclose the hidden attack. The target of these attacks can be almost anyone (companies, government networks, media servers, the banking sector and end users).

- *Extortion* - in this case, the victim must pay the attacker certain amount of money under the threat of DDoS attack.

1.1. State of the Art

From the available security reports that analyze the network traffic, one can obtain more detailed information about DDoS attacks that have been realized within a certain time period. Important information are the distribution of individual attacks, duration, intensity and target of attack [11], [12], [13], [14]. Based on this information, we can conclude the following facts:

- The distribution of DDoS attack types changes really quickly in response to the protection implemented. For example, SynFlood was the most widely used attack earlier but nowadays it is replaced by DNSFlood because a lot of users have already implemented SynFlood protection.
- Security reports confirmed the balance of DDoS attacks targeted at applications and network infrastructure.
- Attackers use increasingly more sophisticated DDoS attacks that combine different techniques of DDoS. One example is a large UDPFlood combined with a slow HTTPFlood [15].
- Intensity of DDoS attacks is rapidly increasing [16], [17]. For example, the average intensity of one DDoS attack was 3.92 Gbps in the first quadrant of 2014, in the second quadrant, the average intensity was 12.42 Gbps. Hence, we can suppose the permanent increase of the attack intensity.

One can cast doubts on the detachment of information provided because these reports are made by producers of DDoS protection. However, we can confirm the same facts from information provided by data service providers from the Czech Republic (Providers of data services are victims of DDoS attacks, therefore, providing correct data is in their own interest). In the Czech Republic, the DDoS attacks demonstrated their effectiveness in 2013. The media servers (iDNES.cz, IHNED.cz, Lidovky.cz, Seznam.cz etc.), servers of mobile operators (T-Mobile, Telefonica O2 etc.) and bank servers (CSOB, Komercni banka, Ceska sporitelna etc.) were targets of the attacks successively. During these attacks, end users could not send and receive electronic mails, make payments in Internet banking and payment terminals did not work. The statistics of data center WEDOS and Nethost confirm that the important thread lies in increasing intensity of DDoS attacks. In 2013, these data centers detected attacks with intensity around 3 Gbps, at the beginning of 2014, the attacks had intensity of 6 Gbps and in the middle of the year the attacks had intensity of 20 Gbps.

Generally, it is really difficult to defend against these types of attacks because they do not target specific vulnerabilities of the systems. Academia and industry have made tremendous efforts to defend DDoS attacks [10], [18]. In the first step, DDoS attacks are recognizable and classifiable by detecting anomalies in network traffic based on machine learning [19]. In the second step, the illegitimate traffic is dropped. A simple approach is based on the black and white lists [20]. An interesting method that tries to mitigate DDoS attacks by an offensive approach was presented [21]. Techniques based on packet marking require a huge amount of packets to be monitored [22], [23]. In our research, we focus on basic defense techniques that are based on secure network infrastructure [24], [25], [26]. The most important element of the infrastructure is IPS (Intrusion Prevention Systems).

On the market, several IPS solutions can be found that detect and eliminate quite well the DDoS attacks on the network infrastructure. The following list shows the most known and used solutions: DDoS protection (F5), DefencePro (Radware), DDoS protection (Prolexic Technologies), Pravail Availability Protection System (ARBOR Networks) and ADS series (NSFOCUS Information Technology). Commercially available solutions contain several principal lacks that make impossible their wide application. Main lacks can be summarized as follows:

- High acquisition price - all commercial solutions mentioned above are very expensive. The economic cost is the main reason why most of the smaller entities are unprotected (Valid for the Czech Republic). From a simple calculation of the number of DDoS attacks per year, the cost of the IPS device, operating costs, the time when the device is active, it follows that it is an inefficiency investment.
- Impossibility of the DDoS protection sharing - for these systems, it is not possible to share the DDoS protection for more entities, because producers have know-how and they prevent sharing

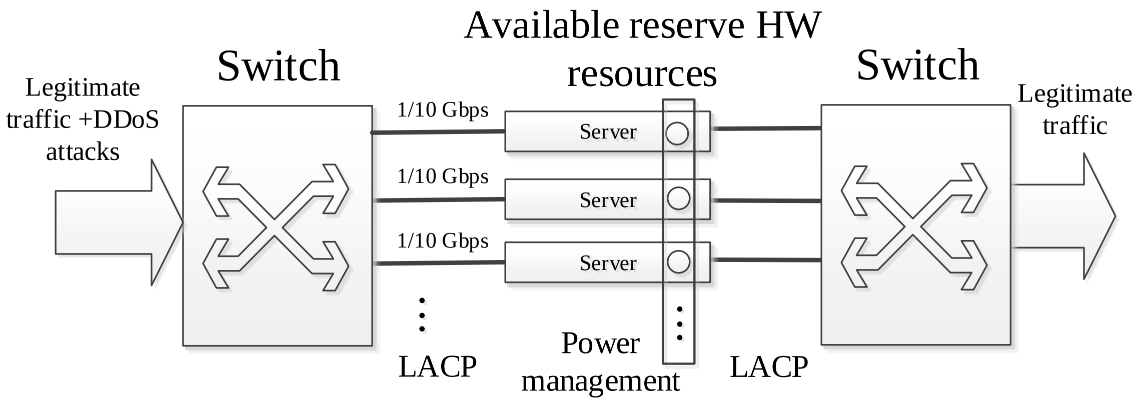

Fig. 1: Block diagram of the system proposed.

by license (in fact, these devices are not designed for sharing).

- Problem of redundancy solution - it is not possible to realize redundancy without buying an additional equipment.
- Maximum throughput limitation - this is the critical disadvantage. These commercial devices are limited by the maximum speed of the interface (e.g. 10 Gbps) and the throughput cannot be increased linearly (one can combine multiple devices, but the price is multiplied). Based on the current state, the average intensity of DDoS attacks exceeds the speed of 10 Gbps more than two times. A modular DDoS protection system that would allow to increase the filtering capacity linearly is completely missing.
- Commercial solutions are not suitable for data centers.

Recently, many companies such as Incapsula, Defense.net, Prolexic DDoS Mitigation Services, Verisign DDoS Protection Services, CloudFlare Enterprise, Nexusguard have offered DDoS protection as a service based on the cloud. The cloud based DDoS protection can be less expensive for certain types of the clients (small/medium companies), nevertheless, the detection and mitigation of DDoS attacks can take longer due to the routing. Therefore, it is desirable to develop DDoS solution with the following properties: cheap solution, possibility to increase the filtering capacity linearly, suitability for data centers, scalable, and easy-to-manage.

1.2. Our Contribution

This short paper reports some preliminary results and the main ideas of our ongoing project. The main goal of our project is to propose and implement a scalable software DDoS protection that eliminates the lacks of the commercially available solutions. Our research and key observations are strongly focused on applicability in data centers because the research is conducted in cooperation with the commercial company Nethost. The company operates data center with more than 800 servers and 2.500 VPS (Virtual Private Server). Our main intention is to realize an anti-DDoS system where it is possible to increase throughput (filtering capacity) linearly and acquisition costs are really small. At the beginning of the article, we have presented a critical analysis of the existing IPS systems and our motivation. Based on the main facts, we propose our DDoS solution that eliminates these lacks. We illustrate the main ideas using the main functional components of the system.

2. System Proposal

The key observation of system proposed is based on the free availability of redundant hardware resources that can be effectively used to eliminate (filter) DDoS attacks. Data centers have to modernize their hardware resources practically every year, therefore they have plenty of reserve hardware that has a sufficient computing power. For example, the company Nethost has reserve hardware in the price of 260 000 $ at present. The main idea is to develop a DDoS defense system in the form of portable software image that can be installed on the reserve hardware resources (servers). During a DDoS attack, these servers will be used as

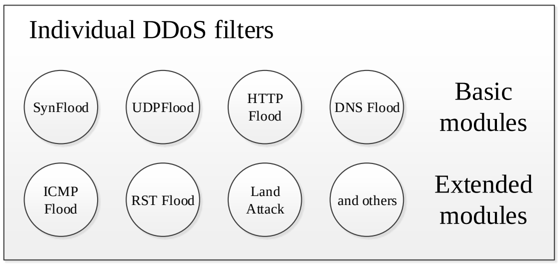

Fig. 2: Block diagram of the DDoS filters implemented.

filters of this DDoS attack. The block diagram of the system proposed is depicted in Fig. 1.

Reserve servers that contain the installed image of the defense system, will be connected to the switch (or bridge, it will be decided later based on benchmark test realized during the project) using 1 Gbps or 10 Gbps ports. By default, the defense system proposed (a filter of DDoS) is turned off and it consumes no energy. During the DDoS attack, the required number of servers will be connected using the power management system and the required amount of traffic will be filtered using the LACP (Link Aggregation Control Protocol). For example, we connect two servers using 10 Gbps ports, therefore the proposed system will be able to filter legitimate traffic within the DDoS attack that exceeds 12 Gbps. After DDoS termination, the servers will be turned off in order to save operating costs or special software modules will be activated to accelerate proxy, to perform security tests or to run a virus scan.

The defense system proposed includes filtering modules specialized that are targeted at the specific types of DDoS attacks. This modularity allows easy and fast modification, reaction and supplementation. The modular scheme also allows to eliminate the different combination of DDoS attacks in a simple manner. We assume that the system will always contain basic filters such as SynFlood, UDPFlood, HTTPFlood and DNSFlood corresponding with the most commonly used DDoS attacks. Furthermore, the system will contain filtering modules extended for other types of DDoS attacks (we assume ICMPFlood, FloodRST etc.) that will be gradually implemented. Block diagram of the individual filtering module is depicted in Fig. 2.

The entropy traffic models, time series analysis and static analysis of data traffic are included in our research to detect the DDoS attacks. We do not consider the behavioral analysis methods because we intend to avoid the problems associated with learning phase (necessary learning, inaccuracy patterns, re-learning if network configuration is changed, etc.). The individual filters are implemented in a form of special grids that effectively eliminate specific DDoS attacks (grids respond to specific protocol parameters or conditions according to the protocols RFC (Request For Comments)). In fact, this implementation represents an improved state analysis of individual protocols.

The proposed modular system in the form of the portable image is based on virtualization, therefore it is possible to involve all available computing capacity to filter DDoS attacks. Theoretically, one can filter any amount of the traffic depending on the available computational resources. The key advantage lies in the linear increase of filtering capacity in response to the current state of the DDoS attacks. This is the main advantage in comparison with commercial systems. The scalable defense system reduces the costs by using own hardware, i.e. the system represents a more convenient solution in terms of investment and liquidity for a large number of end users. We summarize the main advantages of the system proposed in the following points:

- The system allows linear increasing of the filtering capacity.
- The software solution is suitable for data centers (shared DDoS protection has influence on big number of end users).
- The system is implemented on several individuals nodes, therefore in case of failure, one will lose only one part of the filtering capacity (redundant solution).
- Effective usage of available hardware resources.
- Low price.
- Modularity enables quick reaction to new DDoS attacks and to protect against combination of attacks.

3. Conclusion

This paper reports some preliminary results and the main ideas of our ongoing project, that aims to develop a scalable DDoS mitigation system, which is suitable for data centers. The main idea lies in utilization of redundant hardware resources to eliminate the DDoS attacks. We believe that the system proposed reaches sufficient filtering capacity by combination of software and hardware to meet the needs of data centers. The main advantages of the system are the linear increasing of the filtering capacity, sharing of DDoS protection and low price.

Future work of our research is the implementation and testing of the system proposed. Firstly, we want to focus on benchmark testing of filtering capacity. Subsequently, we will focus on the research and testing of individual filtering modules.

Acknowledgment

Research described in this paper was financed by the National Sustainability Program under grant LO1401. For the research, infrastructure of the SIX Center was used.

References

[1] SRIVASTAVA, A., B. B. GUPTA, A. TYAGI, A. SHARMA and A. MISHRA. *Advances in Parallel Distributed Computing - A recent survey on DDoS attacks and defense mechanisms*. Berlin: Springer, 2011. ISBN 978-3-642-24036-2.

[2] WANG, H., D. ZHANG and K. G. SHIN. Detecting SYN flooding attacks. In: *Proceedings of IEEE Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2002)*. New York: IEEE, 2002, pp. 1530–1539. ISBN 0-7803-7476-2. DOI: 10.1109/INFCOM.2002.1019404.

[3] KIM, M. S., H. J. KONG, S. C. HONG, S. H. CHUNG and J. W. HONG. A flow-based method for abnormal network traffic detection. In: *Network Operations and Management Symposium, 2004*. Seoul: IEEE, 2004, pp. 599–612. ISBN 0-7803-8230-7. DOI: 10.1109/NOMS.2004.1317747.

[4] LAU, F., S. H. RUBIN, M. H. SMITH and L. TRAJAKOVIC. Distributed denial of service attacks. In: *IEEE International Conference on Systems, Man, and Cybernetics, 2000*. Nashville: IEEE, 2000, pp. 2275–2280. ISBN 0-7803-6583-6. DOI: 10.1109/ICSMC.2000.886455.

[5] SOMMER, R., D. BALZAROTTI and G. MAIER. *Recent Advances in Intrusion Detection*. Berlin: Springer, 2011, pp. 161–180. ISBN 978-3-642-23644-0.

[6] LIMWIWATKUL, L. and A. RUNGSAWANG. Distributed denial of service detection using TCP/IP header and traffic measurement analysis. In: *IEEE International Symposium on Communications and Information Technologies (ISCIT 2004)*. Sapporo: IEEE, 2014, pp. 605–610. ISBN 0-7803-8593-4. DOI: 10.1109/ISCIT.2004.1412917.

[7] AKBAR, M. A., Z. TARIQ and M. FAROOQ. A comparative study of anomaly detection algorithms for detection of SIP flooding. In: *2nd International Conference on Internet Multimedia Services Architecture and Applications (IMS 2008)*. Bangalore: IEEE, 2008, pp. 1–6. ISBN 978-1-4244-2684-3. DOI: 10.1109/IMSAA.2008.4753934.

[8] CHELSEA, A. *Generated anomaly pattern for HTTP flood protection*. US Patent 7617170. Patented 2009.

[9] MIRKOVIC, J. and P. REIHER. A taxonomy of DDoS attack and DDoS defense. *ACM SIGCOMM Computer Communication Review*. 2004, vol. 34, no. 2, pp. 39–53. ISSN 0146-4833. DOI: 10.1145/997150.997156.

[10] PENG, T., C. LECKIE and K. RAMAMOHANARAO. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*. 2007, vol. 39, no. 1, pp. 1–42. ISSN 0360-0300. DOI: 10.1145/1216370.1216373.

[11] Global application & network security report 2013. *RADWARE*. 2013.

[12] BAO, X. and H. HONG. NSFOCUS DDoS threat report 2013. *NSFOCUS Information Technology*. 2013.

[13] Prolexic quarterly global DDoS Attack Report Q1-Q4. *AKAMAI*. 2013.

[14] Global application & network security report 2014. *RADWARE*. 2014.

[15] HANSEN, R. Slowloris HTTP DoS. *Hackers.org* [online]. 2014. Available at: `http://ha.ckers.org/slowloris/`.

[16] Distributed denial of service trends report. *VERISIGN*. 2014.

[17] PLXsert's Q4 2014 state of the internet–Security Report. *AKAMAI*. 2014.

[18] ZARGAR, S. T., J. JOSHI and D. TIPPER. A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks. *IEEE Communications Surveys & Tutorials*. 2004, vol. 15, no. 4, pp. 2046–2069. ISSN 1553-877X. DOI: 10.1109/SURV.2013.031413.00127.

[19] JALILI, R., F. IMANI-MEHR, M. AMINI and H. R. SHAHRIARI. Detection of Distributed Denial of Service Attacks Using Statistical Preprocessor and Unsupervised Neural Networks. *Information Security Practice and Experience*. 2005, vol. 3439, iss. 1, pp. 192–203. ISSN 0302-9743. DOI: 10.1007/978-3-540-31979-5_17.

[20] KANG, S. H., K. Y. PARK, S. G. YOO and J. KIM. DDoS avoidance strategy for service availability. *Cluster Computing*. 2013, vol. 16, no. 2, pp. 241–248. ISSN 1386-7857. DOI: 10.1007/s10586-011-0185-4.

[21] WALFISH, M., M. VUTUKURU, H. BALAKRISHNAN, D. KARGER and S. SHENKER. DDoS defense by offense. In: *Proceedings of the 2006 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM 2006).* New York: ACM, 2006, pp. 303–314. ISBN 1-59593-308-5. DOI: 10.1145/1159913.1159948.

[22] BELENKY, A. and N. ANSARI. On deterministic packet marking. *Computer Networks.* 2007, vol. 51, no. 10, pp. 2677–2700. ISSN 1389-1286. DOI: 10.1016/j.comnet.2006.11.020.

[23] SEVAGE, S., D. WETHERALL, A. KARLIN and T. ANDERSON. Practical network support for IP traceback. *ACM SIGCOMM Computer Communication Review.* 2000, vol. 30, no. 4, pp. 295–306. ISSN 0146-4833. DOI: 10.1145/347057.347560.

[24] PATEL, C. M. and V. BORISAGAR. Survey On Taxonomy Of Ddos Attacks With Impact And Mitigation Techniques. *International Journal of Engineering Research & Technology.* 2012, vol. 1, no. 9, pp. 1–8. ISSN 2278-0181.

[25] JAIN, A. and A. K. SINGH. Distributed denial of service (DDoS) attacks-classification and implications. *Journal of Information & Operations Management.* 2012, vol. 3, no. 1, pp. 136. ISSN 0976-7754.

[26] LOUKAS, G. and G. OEKE. Protection against denial of service attacks: A survey. *The Computer Journal.* 2010, vol. 53, no. 7, pp. 1020–1037. ISSN 1020-1037.

About Authors

Zdenek MARTINASEK Received M.Sc. (Ing.) at the Department of Telecommunications at the Faculty of Electrical Engineering and Communication at Brno University of Technology in 2008. He received Ph.D. at the same Department. He also helps to cover pedagogically Master's program course. The area of his professional interests is cryptography, power analysis, sensors and modern data communication.