Network Parameters Applicable in Detection of Infrastructure Level DDoS Attacks

Ivan Cvitić, Dragan Peraković, *Member, IEEE,* Marko Periša, and Mario Musa

***Abstract* — Distributed denial of service attacks represent continuous threat to availability of information and communication resources. This research conducted the analysis of relevant scientific literature and synthesize parameters on packet and traffic flow level applicable for detection of infrastructure layer DDoS attacks. It is concluded that packet level detection uses two or more parameters while traffic flow level detection often used only one parameter which makes it more convenient and resource efficient approach in DDoS detection.**

***Keywords* — traffic flow, network packets, network security, resource availability, anomaly detection**

I. Introduction and related research

Distributed denial of service (DDoS) are coordinated attacks by a large number of terminal devices in the function of degrading the quality of an information and communication service or other resources or completely disabling access to it. Given the simplicity of their implementation, these attacks have been steadily increasing over the past ten years. The consequences of DDoS attacks have the potential of business continuity disruption, loss of credibility and ultimately financial loss. Particularly important are new information and communication environments such as critical infrastructure management, smart cities, traffic management systems and autonomous vehicles with the use of the concepts of Internet of Things and Cloud Computing, where unavailability of the service with financial losses can adversely affect the safety of people. More frequent application of information and communication technologies and services in these environments requires a high level of service availability. As a consequence, the negative impact of DDoS attacks and the damage caused by such attacks are growing.

Ivan Cvitić, PhD student, Department of information and communication traffic, Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia (phone: 385-1-2457943 e-mail: ivan.cvitic@fpz.hr).

Dragan Peraković, Department of information and communication traffic, Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia (phone: 385-1-2457915 e-mail: dragan.perakovic@fpz.hr).

Marko Periša, Department of information and communication traffic, Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia (phone: 385-1-2457914 e-mail: marko.perisa@fpz.hr).

Mario Musa, PhD student, Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia (e-mail: maro.musa@lutrija.hr).

TABLE 1: PARAMETERS USED IN DDOS DETECTION

Research	*Packet / traffic flow level*	*Selected parameters*	*Number of parameters*	*Used method*	*Detection accuracy*
[1]	packet	source IP addresses, ID, sequence number, source/destination port numbers	5	Artificial neural network	98%
[2]	packet	packet arrival time, source IP address, destination IP address, protocol, packet length	5	Artificial neural network	82,1% - 95,6%
[3]	packet	Time to Live (TTL), source IP addresses	2	Support vector machines / Multilayer perceptron	98,42% - 99,39%
[4]	packet	protocol, destination port, number of connections, packet length	4	Fuzzy Q-learning	88,77%
[5]	packet	number of packets, number of bytes	2	Multivariate data analysis	97,53% - 98,6%
[6]	packet	source IP addresses, source country, source port, destination port, protocol, SYN flag, ACK flag, RST flag, packet length, TTL, time interval between two packets	11	Decision tree / Naive Bayes	98% - 99%
[7]	traffic flow	packet interarrival time	1	Function approximation methods for Hurst parameter estimation	50% - 100%
[8]	traffic flow	number of packets in time	1	Naive Bayes	85% - 95.93%
[9]	traffic flow	flow count	1	Fast entropy	N/A

978-1-5386-3073-0/17/$31.00 ©2017 IEEE

Given the negative effects of DDoS attacks, there is a need to explore methods and ways of detecting them. The most common detection methods are based on detecting anomalies in network traffic due to the ability to recognize new and currently unknown attack patterns.

By analyzing the previous, relevant researches carried out in the area of development of the DDoS detection methods, table 1 was generated. Researches using network packets and traffic flow parameters for the purpose of DDoS attack detection where analyzed. Included researches provide approximately the same detection accuracy. The table contains parameters used for detection purposes, total number of used parameters, detection method, detection accuracy, and level at which detection is performed (packet level or traffic flow level).

The table shows the frequent use of particular parameters such as source and destination IP addresses [1], [2], [9] and source and destination ports and protocol [1]. The parameters used depend on the type of DDoS attack that is being detected, but also on the methods used for detection and are significantly different depending on the research.

The aim of this research is to provide insight and synthesis of packet and traffic flow network parameters that can be used to develop new DDoS attacks detection models.

II. Taxonomy of DDoS attacks

Network based attacks are identified as anomalies of network traffic [10]. Anomalies are network traffic patterns that differ in relation to previously defined patterns of normal traffic.

TABLE 2: TAXONOMY OF DDOS ATTACKS BASED ON TCP/IP LEVEL

Denial of service attack		
Single source denial of service attack (SSDoS)	**Distributed denial of service attack (DDoS)**	
	Infrastructure level	**Application level**
	TCP SYN	HTTP GET
	UDP Flood	
	UDP Fragment	HTTP POST
	NTP	
	TCP ACK	PUSH
	DNS	
	ICMP	HEAD
	SSDP	

Denial of Services implies a general class of network-based attacks targeting the availability of information and communication resources. The DoS attack implies one source that generates traffic to the destination in order to exploit its capacity limitation and causing the unavailability of the information and communication resource. Technological development, encompassing the development of devices with greater network processing capabilities, reduces the effectiveness of DoS attacks. This implies that one device has no ability to generate sufficient traffic that would result in congestion at the destination. For the purpose of increasing the amount of traffic that is directed towards the attack goal, DDoS attacks are being applied. In DDoS attacks multiple devices are coordinated with the aim of directing a large amount of traffic to the desired destination [11].

DDoS attacks can be divided depending on the TCP / IP (Transmission Control Protocol / Internet Protocol) layer targeted by the generated traffic as shown in table 2. Therefore, they are divided into those directed to the infrastructure layer (data and network) and directed to the application layer [12]. The SYN flag represents one of six possible TCP header flags (ACK, SYN, URG, FIN, RST, and PSH) whose function is to synchronize sequential packet numbers when initiating a TCP session, and it is often used for implementation of DDoS attack. Except the SYN (which is the most common variation of DDoS attack according to [13]) and other TCP header flags table 2 shows other protocols or protocol parameters that were used in DDoS attacks based on infrastructure and application layer.

According to [13] attacks are more often directed towards the infrastructure TCP / IP layer. The share of such attacks is 99.43%, while the application attack share is 0.57% [14]. The reason for the presented relationship is potentially the result of less complexity of implementing infrastructure-based DDoS attacks compared to application-based. The above shows the need for intensive research and development of methods of detection of an infrastructure-based DDoS attacks.

III. Applicable parameters in the detection of infrastructure level DDoS attack

Since the first occurrence of DDoS attacks, numerous methods have been developed for detecting it. Detection methods can be segmented into two primary classes. The first class includes pattern-based methods. The above methods are based on the comparison of incoming traffic with pre-defined profiles and samples of known network anomalies corresponding to DDoS attack. The primary deficiency of the said detection class is the inability to identify new, unknown attacks [15].

The second class of detection methods implies detection of anomalies in network traffic. The advantage of this class of methods and the reason for their frequent use is the ability to detect so far unknown attacks. The working principle of anomalies based detection methods is the comparison of incoming traffic with previously defined normal traffic according to certain parameters of network packets or traffic flow [16]. Selection of parameters to be used is a key component for achieving an effective system of DDoS attacks detection. According to [17] number of used parameters must be as low as possible and it is necessary to use parameters that have the greatest impact when detecting network traffic anomaly.

A. Source and destination IP address parameters

The source and destination IP addresses represent one of the required packet header parameters and are often used as DDoS attack detection. Examples of using these parameters are seen in the research [1], [2], [9] shown in table 2. Research [18] uses the destination IP address as a parameter for calculating entropy based on which the TCP SYN DDoS attack is detected. In mentioned research, the destination IP address is the target address and represents a constant causing entropy drop during the attack.

B. Protocol and packet length parameters

Although often use in various research such as [2] and [4], protocol as a parameter do not have major impact on detection of DDoS attacks. For example TCP SYN DDoS attack use the TCP protocol like most of the other packets representing legitimate traffic. Unlike protocol, packet length parameter have great impact on DDoS detection possibilities. Attack packets often have similar or equal lengths. That characteristic can be used in entropy based DDoS detection [18].

C. Time to live parameter

Time to live (TTL) is a packet header field that preserves value representing the number of nodes packet passed from source to destination. This parameter can be used for detection of spoofed IP address often used in DDoS attacks [3], [19].

D. Number of packets parameter

Number of packets is a parameter often used in detection of UDP based DDoS attacks [5], [20], [21], [22]. According to [22] even though UDP does not provide confirmation about delivery, in legitimate UDP application mechanism is implemented for ensuring that the other party is receiving or sending packets. Mentioned implies that, under normal circumstances the packet rate in one direction is proportional to the packet rate in other direction.

E. TCP header flag parameter

Header flags of TCP packet header is often used for DDoS attack on infrastructure level so number of research are using this parameter in its detection [6], [23]. Example of such attack is TCP SYN DDoS flood where attacker is taking advantage of TCP handshake process shown in Fig. 1. In shown scenario attacker initiates TCP handshake process by sending TCP packet with SYN flag. Destination server allocates large number of DDoS attackers' defined amount of resources and response with TCP packet containing SYN ACK flag. Instead of finishing TCP handshake process, attacker gives no response and destination server keeps allocated resource. With large number of DDoS attackers it is possible to use entire server capacity causing its unavailability for legitimate users.

Use of TCP packet header flag parameter can be seen in research [23] where the CUSUM algorithm (common algorithm in statistics processing) is detecting change in sent and received TCP packets with SYN flag.

Research [18] also uses mentioned parameter entropy calculation. During DDoS attacks entropy of SYN flag parameter is in decline because of continuous repetition of TCP packets with active SYN flag.

F. Parameters on traffic flow level

Traffic flow is defined as the unidirectional series of IP packets containing the same source IP address, source port, destination IP address, destination port and protocol [24]. Aggregated flows have a larger number of packet information that reduces the amount of monitoring data which is why traffic flow parameters are often used in DDoS detection [9]. Flow count is one of the used parameters in DDoS detection seen in [9]. In aforementioned research fast entropy is calculated of flow count for each connection. Another parameter on traffic flow level used is number of packets in time seen in [8]. Collected traffic samples are then transformed in matrices using discrete Fourier transform and discrete wavelet transform. Given matrices are then used for developed naïve classifier method.

IV. Discussion and Conclusion

This paper presented parameters on packet and traffic flow level that can be used in detection of infrastructure layer DDoS attacks. Identified parameters do not represent the final list but only those that authors find relevant trough actual scientific literature analysis.

From presented research it can be concluded that packet based detection requires aggregation of multiple features for efficient detection. Current stand in research is that number of used parameters needs to be as low as possible. But with development of IC technologies which supports higher speed of traffic processing it is, or will be in near future possible to use larger number of traffic parameters for real time detection of DDoS attack.

DDoS detection based on traffic flow requires considerably less parameters (most often one) for developing efficient DDoS detection model. According to aforementioned traffic flow based detection presents more convenient approach which will require less processing resources currently resulting in more efficient DDoS detection.

In future work it is planned to use identified parameters in development of new, efficient detection model that will be able to detect the infrastructure layer DDoS attacks.

References

[1] A. Saied, R. E. Overill, and T. Radzik, "Artificial Neural Networks in the Detection of Known and Unknown DDoS Attacks: Proof-of-Concept," in Neurocomputing, vol. 430, Elsevier, 2014, pp. 309–320.

[2] D. Perakovic, M. Perisa, I. Cvitic, and S. Husnjak, "Artificial neuron network implementation in detection and classification of DDoS traffic," TELFOR J., vol. 9, no. 1, pp. 26–31, Nov. 2017.

[3] G. Preetha, B. S. K. Devi, and S. M. Shalinie, "Autonomous agent for DDoS attack detection and defense in an experimental testbed," Int. J. Fuzzy Syst., vol. 16, no. 4, pp. 520–528, 2014.

[4] S. Shamshirband, N. B. Anuar, M. Kiah, and S. Misra, "Anomaly Detection using Fuzzy Q-learning Algorithm," J. Intell. Fuzzy Syst., vol. 11, no. 8, pp. 5–28, 2014.

[5] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, “Botnet in DDoS Attacks: Trends and Challenges.,” IEEE Commun. Surv. Tutorials, vol. 17, no. 4, pp. 2242–2270, 2015.

[6] E. Balkanli, J. Alves, and A. N. Zincir-Heywood, “Supervised learning to detect DDoS attacks,” in 2014 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2014, pp. 1–8.

[7] U. Premarathne, U. Premaratne, and K. Samarasinghe, “Network traffic self similarity measurements using classifier based Hurst parameter estimation,” in Proceedings of the 2010 5th International Conference on Information and Automation for Sustainability, ICIAfS 2010, 2010, pp. 64–69.

[8] R. F. Fouladi, C. E. Kayatas, and E. Anarim, “Frequency based DDoS attack detection approach using naive Bayes classification,” in 2016 39th International Conference on Telecommunications and Signal Processing (TSP), 2016, no. June, pp. 104–107.

[9] J. David and C. Thomas, “DDoS Attack Detection Using Fast Entropy Approach on Flow- Based Network Traffic,” Procedia Comput. Sci., vol. 50, pp. 30–36, 2015.

[10] V. Chandola, A. Banerjee, and V. Kumar, “Anomaly detection,” ACM Comput. Surv., vol. 41, no. 3, pp. 1–58, 2009.

[11] K. G. Dileep, G. C. Rao, M. K. Singh, and G. Satyanarayana, “A Survey on Defense Mechanisms countering DDoS Attacks in the Network,” Int. J. Adv. Res. Comput. Commun. Eng., vol. 2, no. 7, pp. 2599–2606, 2013.

[12] B. Singh, K. Kumar, and A. Bhandari, “Simulation Study of Application Layer DDoS Attack,” in 2015 International Conference on Green Computing and Internet of Things (ICGCIoT), 2015, pp. 893–898.

[13] D. Peraković, M. Periša, and I. Cvitić, “Analysis of the IoT impact on volume of DDoS attacks,” in XXXIII Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – PosTel 2015, 2015.

[14] Akamai, “Akamai’s State of the Internet - Security (Q1-2017),” 2017. [Online]. Available: https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-state-of-the-internet-report-q1-2017.pdf.

[15] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, “Network Anomaly Detection: Methods, Systems and Tools,” IEEE Commun. Surv. Tutorials, vol. 16, no. 1, pp. 303–336, 2014.

[16] J. Mirkovic and P. Reiher, “A taxonomy of DDoS attack and DDoS defense mechanisms,” SIGCOMM Comput. Commun. Rev., vol. 34, no. 2, pp. 39–53, 2004.

[17] D. K. Bhattacharyya and J. K. Kalita, DDoS Attacks: Evolution, Detection, Prevention, Reaction and Tolerance. Boca Raton, USA: CRC Press, 2016.

[18] S. Sharma, S. K. Sahu, and S. K. Jena, “On selection of attributes for entropy based detection of DDoS,” in 2015 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2015, 2015, pp. 1096–1100.

[19] G. U. Devi, M. K. Priyan, E. V. Balan, C. G. Nath, and M. Chandrasekhar, “Detection of DDoS Attack using Optimized Hop Count Filtering Technique,” Indian J. Sci. Technol., vol. 8, no. 26, pp. 1–6, 2015.

[20] C. Zhang, Z. Cai, W. Chen, X. Luo, and J. Yin, “Flow level detection and filtering of low-rate DDoS,” Comput. Networks, vol. 56, no. 15, pp. 3417–3431, 2012.

[21] K. Zeb, B. AsSadhan, J. Al-Muhtadi, and S. Alshebeili, “Anomaly detection using Wavelet-based estimation of LRD in packet and byte count of control traffic,” in 2016 7th International Conference on Information and Communication Systems (ICICS), 2016, pp. 316–321.

[22] G. Alexandru, S. Raj, and R. Marc, “Classification of UDP Traffic for DDoS Detection,” in LEET’12 Proceedings of the 5th USENIX conference on Large-Scale Exploits and Emergent Threats, 2012, pp. 7–7.

[23] B. Yang and X. Wang, “Selection of parameter for SYN flood source-end detection,” in Proceedings of 2011 International Conference on Electronic and Mechanical Engineering and Information Technology, EMEIT 2011, 2011, pp. 106–109.

[24] C. Zhang, Z. Cai, W. Chen, X. Luo, and J. Yin, “Flow level detection and filtering of low-rate DDoS,” Comput. Networks, vol. 56, no. 15, pp. 3417–3431, 2012.