# A DDoS Detection Algorithm Based on Chaos Using Density of Maxima

Josimar Tavares, Ewerton M. Salvador, Alisson V. Brito

Centro de Informática – Universidade Federal da Paraíba (UFPB)
josimartaf@gmail.com, ewerton@ci.ufpb.br, alisson@ci.ufpb.br

**Abstract:** In this paper, a technique is presented to analyze and detect anomalies in network data flows. The Density of Maxima is used to measure the chaotic behavior of network traffic in order to detect DDoS attacks. The experiments were performed using data containing synthetic traffic created with the JMeter tool, real data from the World Cup 1998, CAIDA 2007 and DARPA 2009 DDoS Malware datasets. All tests demonstrated the effectiveness of the technique in identifying when the attacks occurred, as well as in separating regular from DDoS traffic.

**Keywords:** *network traffic analysis; chaos theory; density of maxima; network security.*

## 1. Introduction

Among the security issues of the Internet, one that stands out is the Distributed Denial of Service (DDoS) attack. This kind of attack aims to disrupt services on the victims, partially or entirely preventing them from functioning. According to the Kaspersky Lab's Global IT Security Risk Survey of 2017, 50% of enterprises claim that the frequency and complexity of DDoS attacks targeting organizations are growing every year [1].

Attacks of this type are usually related to the use of botnets, which are the primary tools for conducting DDoS attacks. Nowadays, the traffic generated by DDoS attacks has reached the terabytes scale. Three of the major DDoS attacks known to date are the following: the attack against Google, which registered a traffic of 2.54 Tbps; the attack against the Microsoft Azure Cloud, which peaked 2.4Tbps of traffic; and the attack against Amazon, which registered 2.3Tbps of traffic [2].

Among other relevant DDoS incidents, one can cite the attack against the GitHub website, which had a traffic record of 1.3 Terabits per second (Tbps) [3]. The Mirai Internet of Things (IoT) botnet attack occurred in 2016 and exceeded 600 Gbps of traffic [4]. Renowned companies (e.g. Twitter, Spotify, and Amazon) also had problems because of DDoS attacks on their services for almost two hours on Oct 21, 2016. The revenue loss due to DDoS attacks has touched to $209 million in the first quarter of 2016, compared to $24 million for all of 2015 [5].

In addition to causing immediate and visible operational problems, many companies also claim that DDoS attacks are being used to cover up other types of incidents, leading to severe financial damage and reputation. Respondents claimed that DDoS attacks were serving as a smokescreen to cover up other attacks such as malware infection, data leakage, network intrusions, and financial thefts [1].

One of the main difficulties in dealing with DDoS attacks is that the attacking devices usually have fake IP and MAC addresses (spoofed), hiding the source of the disruption. Because of this enormous amount of connections, it is challenging to differentiate legitimate users from connections generated by attackers.

Several difficulties need to be handled when the DDoS and regular traffics are mixed. Non-standard ports, disguised ports, and network address translation (NAT) additionally increase the difficulties during classification [6].

This problem motivated new approaches to tackle these types of attacks, such as network traffic analysis together with other tools like Chaos Theory and Time Series. Some research approach methods that use DDoS attack detection implemented software and hardware platforms with Field Programmable Gate Arrays (FPGA). This type of device requires less than one microsecond to classify a sample of incoming traffic as an attack or a regular one [7].

The literature points out that a signal related to network traffic presents a chaotic behavior [8]. Thus, this chaotic behavior can be used to detect DDoS attacks [9-10], or to implement network intrusion detection systems [11]. Some works use temporal series analysis [12], while others use artificial neural networks [13]. All of those works use the Lyapunov Exponent technique to measure the chaotic behavior for identification of anomalies in network traffics.

In this work, a technique called Network Analysis based on Chaos using Density of Maxima (NAC-DM) is presented. NAC-DM is based on the fact that the density of peaks of a signal is related to its chaotic behavior [14]. Thus, a computationally simple approach that counts the number of peaks per time is successfully applied to detect DDoS attacks in network traffics.

## 2. Related Work

Currently, there are already in the literature some works that use chaos characterization technique to detect DdoS attacks. These papers are briefly presented in this section.

Khan, Ferens and Kinsner [11] apply chaos theory to measure the complexity of Internet packages in order to determine whether they are regular or anomalous. The work [9] uses an algorithm for detecting DDoS attacks using the ARIMA (Autoregressive Integrated Moving Average). This algorithm requires the IP address of the devices and the number of transmitted packets per minute. Chonka, Singh, and Zhou [8] have developed an algorithm that uses network self-similarity theory to

differentiate DDoS flood attack traffic from legitimate network traffic.

Wu and Chen propose an improvement to the technique introduced in a previous work [13]. The DDoS detection algorithm is improved based on the NADA (Network Anomaly Detection Algorithm).

Differently from the strategy adopted in this research, these related works use the Lyapunov Exponent technique along with other techniques, such as neural networks or time series models.

## 3. Experiments

Some data sets were used to validate the NAC-DM technique: (1) synthetic traffic using JMeter [15], which is a traffic-generating tool, (2) Fifa World Cup 98 data, and public datasets with DDoS attacks, such as (3) CAIDA 2007, and (4) DARPA 2009 DDoS Malware.

### 3.1 Synthetic Traffic with JMeter

The primary purpose of the JMeter tool was to generate HTTP traffic in a controlled manner [15]. The experiment allowed to explore different scenarios than the ones presented in third parties data sets. Using JMeter, it is possible to configure the number of users, data traffic, and specify attacks.

Another experiment simulating traffic on a Web server under DDoS attack was performed using Jmeter [15]. 2-hour traffic was generated with five simulated users performing HTTP requests to the webserver. Another device was used to perform DDoS attacks on the same server. Even though it is only one device, a large number of requests were made in comparison to regular traffic, as one can observe in Figure 1(a).

During the traffic generation, two attacks lasting 5 minutes each were configured against the webserver. The first attack occurred at 1800 seconds after the beginning of the traffic generation, and the second attack started after 4200 seconds. The values computed for NAC-DM are presented in Figure 1(b). There are two signals in the same plane, the first one (in red) represents the original signal plus the two attacks and the second one (in blue) is the regular traffic excluding the attack signals. As we can see, the values between X=60 and X=69 represent the interval between the beginning and the end of the first attack. Likewise, the values between X=141 and X=149 mark the beginning and the end of the second attack.

### 3.2 FIFA World Cup'98

*1) Experiment 1*

In this experiment, we analyzed real traffic data from FIFA World Cup ‘98, choosing May 3rd, 1998 (source: http://ita.ee.lbl.gov/html/contrib/WorldCup.html) as our analysis target.

A copy of the traffic generated by the DDoS attack was made, in order for it to be inserted into the original traffic at two different places. The original signal (blue), and the signal modified by the attack (red) are presented in the same chart (Figure 2(a)). The NAC-DM technique was used in both signals, and the obtained results can be seen in Figure 2(b). In this experiment, the attacks started at 7200 and 14400 seconds after the traffic started, and both lasted for about 5 minutes. The values of X = 240 and X = 481 correspond to the beginning of both attacks.

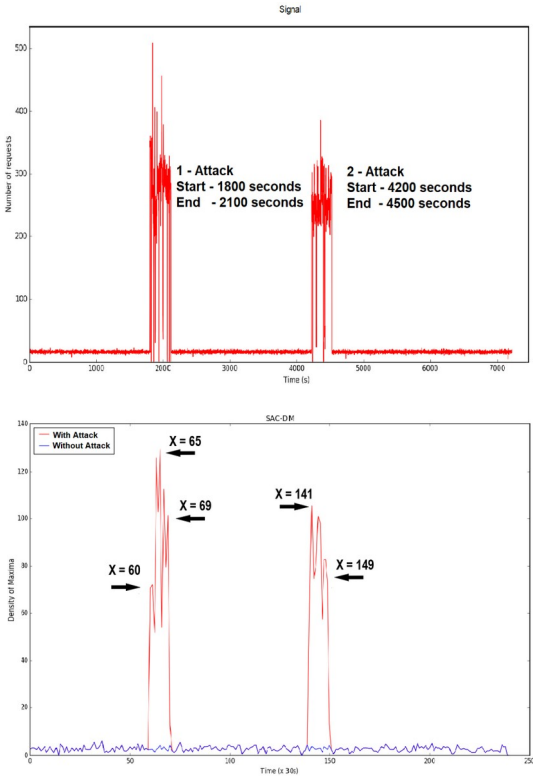


Figure 1. Signals in experiment with JMeter: (a) Original signal, (b) values of NAC-DM.

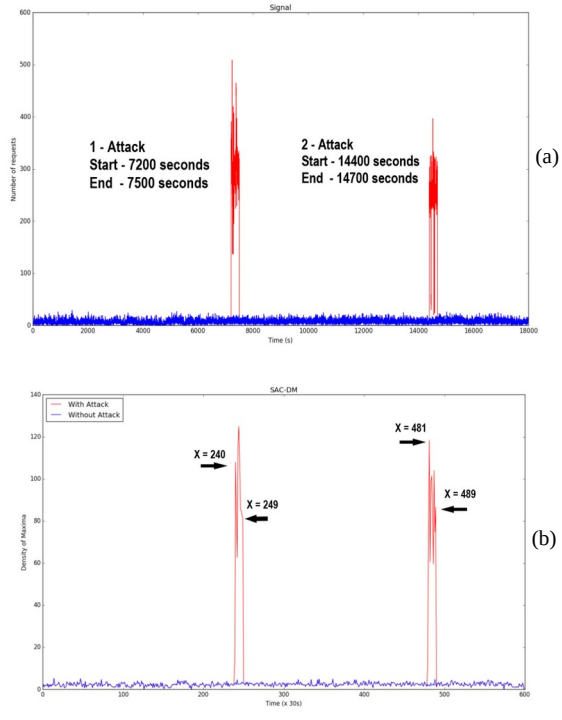


Figure 2. Results from World Cup, experiment 1: (a) Signal, (b) NAC-DM.

*2) Experiment 2*

This experiment aimed to observe the behavior of the algorithm in real traffic. Because of this, we looked for an interval in the traffic trace where access peaks occurred as the result of legitimate usage of the network. The selected day in the traffic trace was June 30th, 1998, where two decisive games at different times occurred. The second game had a high number of requests, but there were no attacks [16].

The results can be seen in Figure 3. The detection algorithm identified no attacks, which demonstrates that the technique is not only capable of detecting DDoS attacks, but also capable of not detecting false attacks.

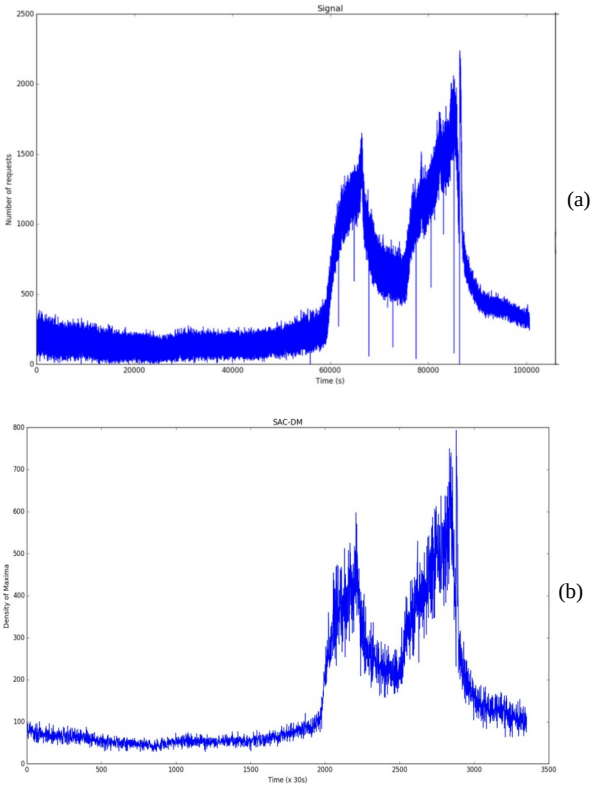


Figure 3. Results from World Cup, experiment 2: (a) Signal, (b) NAC-DM.

### 3.3 Datasets from CAIDA and DARPA

The datasets CAIDA 2007 [17] and DARPA 2009 DDoS Malware [18] are well known in the network analysis community. The dataset used by CAIDA 2007 in this experiment was the same used in [19]. The algorithm identified the beginning of the attack at X=54, as seen in Figure 4(a). This value corresponds to the value of X=1620, as seen in Figure 4(b).

Concerning the dataset from DARPA 2009, as it contains only 330 seconds, the sample size was configured to 5 seconds (instead of 30 as in previous experiments). The algorithm detected the attack at X=11 and at X =65, as seen in Figure 5(a). Both values correspond to the two attacks present on the signal, which started around 55 and 329 seconds, as seen in Figure 5(b). In other words, the NAC-DM showed peaks while the attacks occurred.

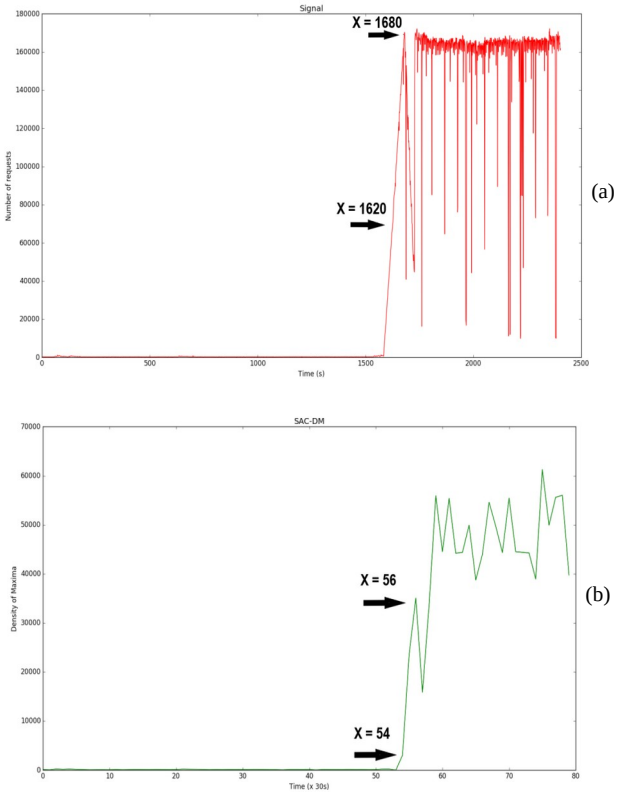


Figure 4. Analysis of dataset from CAIDA 2007: (a)Signal, (b)NAC-DM.

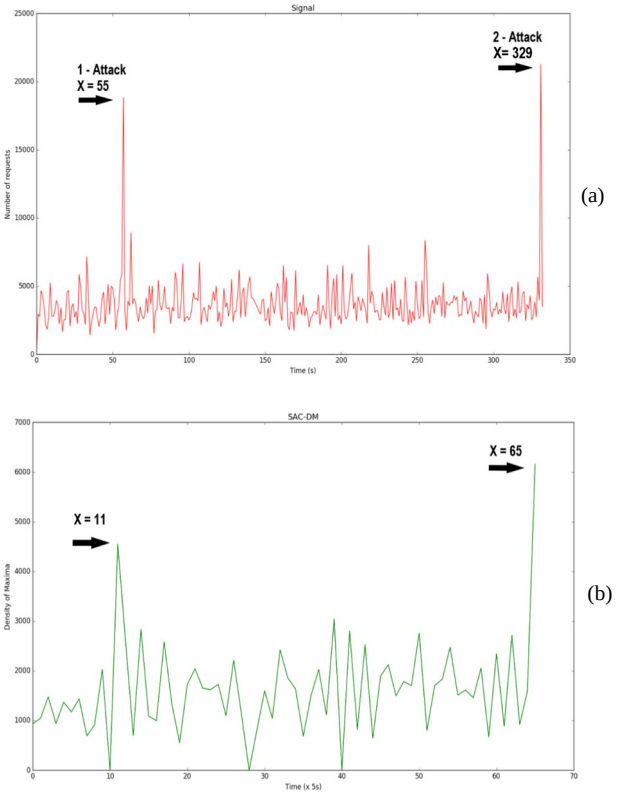


Figure 5. Analysis of dataset from DARPA 2009: (a)Signal, (b)NAC-DM.

## 4. Conclusion

In this work, a DDoS attack detection algorithm was presented based on the Chaos, using the Density of Maxima. The results obtained during the experiments were satisfactory, and confirmed the ability of the algorithm to detect attacks. In Table 1, the accuracy rate of the algorithm is presented. For all the scenarios, the accuracy rate was 100%.

One of the scenarios evaluated FIFA WC'98-2, a dataset without any DDoS attacks. However, there were two peaks due to a large number of access by legitimate users during the event. The algorithm did not detect any attacks on the dataset, which resulted in no false positive. It makes clear its capability to distinguish a legitimate peak of traffic from a peak caused by a DDoS attack.

Table 1: Accuracy of results from experiments.

| Dataset | Attacks | Detection | Precision |
|---|---|---|---|
| JMeter | 02 | 02 | 100% |
| FIFA WC'98 - 1 | 02 | 02 | 100% |
| FIFA WC'98 - 2 | 00 | 00 | 100% |
| CAIDA 2007 | 01 | 01 | 100% |
| DARPA 2009 | 02 | 02 | 100% |

## Bibliography


[1] K. Lab (2017) Kaspersky lab research shows ddos devastation on organizations continues to climb. Kaspersky Press Release. Online: https://usa.kaspersky.com/about/press-releases/2017_kaspersky-lab-research-shows-ddos-devastation-on-organizations-continues-to-climb

[2] Cimpanu, C. (2021) Microsoft said it mitigated a 2.4 tbps ddos attack. *The Record*. Online: https://therecord.media/microsoft-said-it-mitigated-a-2-4-tbps-ddos-attack-the-largest-ever/

[3] Akamai (2018) Memcached reflection attacks: A new era for DDoS. Online: https://www.akamai.com/uk/en/multimedia/documents/brochure/memcached-reflection-attacks-launch-a-new-era-for-ddos-brochure.pdf

[4] KrebsOnSecurity (2016) Krebsonsecurity hit with record ddos. Blog KrebsOnSecurity. Online: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/

[5] Behal, S.; Kumar, K. (2017) Detection of ddos attacks and flash events using information theory metrics–an empirical investigation. *Computer Communications* 103(C): 18-28. DOI: 10.1016/j.comcom.2017.02.003

[6] Deka, R.; Bhattacharyya, D.; Kalita, J. (2019) Active learning to detect ddos attack using ranked features. *Computer Communications* 145: 203-222. DOI: 10.1016/j.comcom.2019.06.010

[7] Hoque, N.; Kashyap, H.; Bhattacharyya, D. (2017) Real-time ddos attack detection using fpga. *Computer Communications* 110: 48-58. DOI: 10.1016/j.comcom.2017.05.015

[8] Chonka, A.; Singh, J.; Zhou, W. (2009) Chaos theory based detection against network mimicking ddos attacks. *IEEE Communications Letters* 13(9): 717-719. DOI: 10.1109/LCOMM.2009.090615

[9] Nezhad, S.; Nazari, M.; Gharavol, E. (2016) A novel dos and ddos attacks detection algorithm using arima time series model and chaotic system in computer networks. *IEEE Communications Letters* 20(4): 700-703. DOI: 10.1109/LCOMM.2016.2517622

[10] D. Y. e. a. Zhi-jun Wu, Jin Lei (2013) Chaos-based detection of ldos attacks. *Journal of Systems and Software* 86(1): 211-221. DOI: 10.1016/j.jss.2012.07.065

[11] Khan, M.; Ferens, K.; Kinsner, W. (2014) A chaotic measure for cognitive machine classification of distributed denial of service attacks. In: Proc. 2014 IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing, pp. 100–108. DOI: 10.1109/ICCI-CC.2014.6921448

[12] Wu, X. and Chen, Y. (2013) Validation of chaos hypothesis in NADA and improved DDoS detection algorithm. *IEEE Communications Letters* 17(12): 2396-2399. DOI: 10.1109/LCOMM.2013.102913.130932

[13] Chen, Y.; Ma, X.; Wu, X. (2013) DDoS detection algorithm based on preprocessing network traffic predicted method and chaos theory. *IEEE Communications Letters* 17(5): 1052-1054. DOI: 10.1109/LCOMM.2013.031913.130066

[14] Bazeia, D.; Pereira, M.; Brito, A.; Oliveira, B.; Ramos, J. (2017) A novel procedure for the identification of chaos in complex biological systems. *Scientific Reports* 7: a44900. DOI: 10.1038/srep44900

[15] Abbas, R.; Sultan, Z.; Bhatti, S. (2017) Comparative study of load testing tools: Apache JMeter, HP LoadRunner, Microsoft Visual Studio (TFS), Siege. *Sukkur IBA Journal of Computing and Mathematical Sciences* 1(2): 102-108. DOI: 10.30537/sjcms.v1i2.24

[16] FIFA, (2019) 1998 world cup france. FIFA. Online: https://www.fifa.com/worldcup/archive/france1998/matches

[17] CAIDA (2009) Center for applied internet data analysis (caida). Center for Applied Internet Data Analysis (CAIDA),Online: http://www.caida.org/data/passive/ddos-20070804dataset.xml.

[18] Manaf Gharaibeh (2009) Darpa-2009 intrusion detection dataset report. Colorado State University. Online: http://www.darpa2009.netsec.colostate.edu/

[19] Behal, S.; Kumar, K. (2016) Trends in validation of DDoS research. *Procedia Computer Science* 85: 7-15. DOI: 10.1016/j.procs.2016.05.170