Application of Machine Learning Techniques to Distributed Denial of Service (DDoS) Attack Detection: A Systematic Literature Review.

Sergio Armando Gutiérrez, John Willian Branch

Grupo GIDIA, Departamento de Ciencias de la Computación y la Decisión
Universidad Nacional de Colombia
Medellín
Email: {saguti—jwbranch}@unal.edu.co

Keywords: Network Security, DDoS attack detection, SLR, Systematic Literature Review.

Abstract

This paper presents an approximation to state of art in application of some machine learning techniques to the field of Distributed Denial of Service (DDoS) attack detection. From a structured mapping study, relevant papers were selected, and later they were reviewed to detect the type of attacks they address, the techniques providing best performances and the techniques which present evidence to be conceived and used in distributed environments.

1 Introduction

Denial of Service (DoS) Attacks are not a new concern on the field of Computer Security. In mid nineties decade, they became a very effective attack method. Later, with the wide adoption of Internet, threats such as viruses, trojans and worms appeared, taking DoS to a higher scale, producing the so-called Distributed Denial of Service (DDoS) Attacks.

A DDoS attack is a type of Denial of Service where multiple coordinated devices are used to launch an attack towards one or more targets. The ultimate goal of DDoS is to exhaust processing and connectivity resources of the targets to avoid that legitimate users access the services provided by computer platforms, thus causing a partial or total unavailability. Because of the many-to-one dimension that poses this type of attacks, they are generally very powerful and devastating. Scientific community forecasts that the disruptive power of DDoS attacks, their sofistication and damage capacity tends to increase in a very high rate, becoming a very critical threat for modern and emergent internet services [1, 2, 3, 4, 5]. Development of adequate solutions to detect and prevent this devastating attacks, and to minimize the damage they can provoke becomes an important task for scientific community.

In this paper, an approximation to state-of art from a Systematic Literature Review in application of Machine Learning to DDoS Attack detection is presented. Machine Learning can be defined as the ability which can be exhibited by a computer program to learn and improve its future execution from the results of previous execution. In other words, the ability to improve its performance over the time.

Machine learning aims to answer many of the same questions as statistics or data mining. However, unlike statistical approaches which tend to focus on understanding the process that generated the data, machine learning techniques focus on building a system that improves its performance based on previous results. In other words systems that are based on the machine learning paradigm have the ability to change their execution strategy on the basis of newly acquired information [6].

This paper is organized as follows. Section 2 describes the methodology used to perform the Literature Review, the search parameters used, the research questions and the inclusion and exclusion criteria used to produce the literature mapping and identify the papers to be reviewed. Section 3 presents the detailed Literature Review on the selected paper, and the answers to proposed research questions. Finally, Section 4 presents the conclusion of this Literature Review and future work that can be derived from it.

2 Methodology

For this paper, the methodology of Systematic Literature Review introduced by Kitchenham et al [7] was used. A previous mapping was performed to identify the most relevant Machine Learning techniques used for DDoS attack detection to focus the review.

For paper retrieval, SciVerse SCOPUS [http://www.scopus.com] was used. This is because SCOPUS has a wide coverage, with access to several of the most important scientific databases as ACM, IEEE, Elsevier, among other, simplifying in that way the search process. The main interest in the searching was DDoS attack detection, so the search string used was (“DDoS Attack Detection”) OR (“Distributed Denial of Service Attack Detection”). The search was configured to retrieve works between 2008 and 2012, on the field of Computer Science, and the types of publications retrieved were Journal Articles, Review Articles, and Conference articles. No other filters were applied.
2.1 Research questions

For the guidance of literature review, three research questions were defined:

- **RQ1**: What types of DDoS Attacks have been addressed with detection based on Machine Learning techniques?
- **RQ2**: What of the Machine Learning techniques included in the review present the best performance, regarding the reduction of false detections (False positivies and false negatives)?
- **RQ3**: What of the techniques included in the review are reported to be used in distributed environments, or included in collaborative detection implementations?

There are two main interests in choosing these research questions. One is the interest in detecting what types of attacks are being studied with more detail. Literature reports that detection of attacks related to transport and network protocols has had more interest, but attacks targeted to application protocols are not still a widely explored research topic [8][9][10][11].

The other interest is identifying how much attention is put in attack detection for distributed computational environments, and in development of collaborative approaches for attack detection. Because of the nature of DDoS attacks, distributed and large scale, and because of the emergence of computing paradigms such as Cloud Computing, distributed solutions and collaborative approaches appear to be promising solutions to face this kind of attacks [12][13][14][15].

2.2 Inclusion and exclusion criteria

Some rules were defined to select the relevant papers from the whole universe retrieved at search time. These criteria were applied to select among the downloaded works, to decide which to review or which to discard.

For the mapping previously performed to identify the Machine Learning techniques to be reviewed in detail, papers whose main topic would be Distributed Denial of Service Attack Detection were included, and papers written in english. On the other side, the works not having DDoS detection as main topic, written in other languages different than english and the ones which could not be downloaded or gotten after requesting them to the authors were discarded and not included for further study.

2.3 Preliminary Results

After performing the search with the keywords and parameters previously mentioned, SCOPUS retrieved 405 papers.

From these 405 papers, 345 were downloaded or obtained from direct request to the authors. The other 60 papers were discarded directly by one or several of the exclusion criteria defined.

Then, after applying the inclusion and exclusion criteria on the 345 remaining papers, 141 papers were selected, and classified for further analysis.

From this universe of 141 papers, after a mapping study, 54 papers were identified to present approaches for DDoS Attack Detection, using mainly Machine Learning techniques.

Further classification was performed on these 54 papers, and the most used techniques were detected; these were Cumulative Sum - CUSUM Algorithm (11 papers), Support Vector Machines - SVM (5 papers), Principal Components Analysis - PCA (4 papers) and Neural Classifiers (4 papers)

In the next section, detailed revision of these works is presented, focused in answering the proposed research questions.

3 Detailed Literature Review

In this section, the detailed literature review is presented. In the first part, the review of the selected papers is discused; the papers are grouped by the technique they use. In the second part, the proposed research questions are answered.

3.1 Literature Review

3.1.1 Cumulative SUM (CUSUM) Algorithm

Wei et al [15] present a mechanism for detection of DDoS attacks aimed to TCP protocol on Kernel based Virtual Machines (KVM) [17]. They focus in studying the relationship that should be kept between starting and ending packets associated to TCP connections. Their approach shows high performance regarding detection time, and refers to have almost 0% of false detections. It presents a scalability issue because information of the connection is stored in hash tables, what might induce performance degradation if tables have high number of records.

Nosrati et al [18] address the detection of DDoS attacks in Internet Multimedia Subsystem, specifically in relation to REGISTER operation (the action a device performs to authenticate and inform itself its location within the network to a control entity) of Session Initiation Protocol (SIP). They present a variant of CUSUM named adaptive z-score CUSUM; this adaptive variant has the capacity to adapt itself to changes which could occur in the traffic (In this case, quantity of REGISTER messages), for example, for connection restablishment. Their approach presents a low detection time, and a False Rate Alarm near to 6%. It is a simple approach, which could be adapted to be used in other application cases.

Yi et al [19] present a mechanism to analyze per IP behavior. A profile of the sending and receiving traffic of every IP address in the network is created. Then, that profile is evaluated to decide whether it meets normal behavior, or whether it indicates an anomaly. The presented approach analyzes metrics of messages related to TCP protocol, and also ICMP and DNS messages. It is conceived to be deployed at so-called leaf routers, that is to say, routers which interconnect particular network segments. The presented results show times in the order of minutes for detection, which for some application scenarios could be inconvenient. Also, although it is thought to be used at leaf routers to protect smaller network segments, it might have scalability issues for high number of users, and it is not clear
whether present limitations in environments using dynamic IP assignments.

Du and Nakao \[20\] present Mantlet, a complete solution for DDoS attacks, covering Anti-Spoofing (False source IP Addresses), detection and mitigation. The detection component of Mantlet uses CUSUM to detect anomalies in the ratio between sent and received packets. A very important feature of the presented solution is that it generalizes the detection, covering besides TCP packets also UDP packets. Thus, it covers a wider spectrum of Transport Layer. Mantlet shows a very low rate of false alarms, and the capacity to reduce detection times as the attack intensity increases; it implies that for stealth attacks (low rate attacks), performance might drop.

Salem et al \[21\] propose an approach for Flooding DDoS attacks using a variation of CUSUM named Multi Channel Non Parametric (MNP). This solution covers a wide spectrum of network protocols, being able to detect TCP, UDP and ICMP based attacks. The justification in using a non parametric version is because of the high variability of network traffic and the lack of consensus on relevant features to monitor on it. This work does not present detailed results on detection time or false detections rate.

Leu and Li \[22\] present an Intrusion Prevention System with detection features based on CUSUM. Their approach presents detection time around 1.3 secs, and detection accuracy of 98.4%; low rates of false positives (3.2%) and false negatives (0%).

Zhou et al \[23, 24\] present an approach for attack detection starting from a P2P network built for detection. Devices organize themselves in a P2P network, detection is performed locally at end host via CUSUM algorithm, and at occurrence of abnormalities, they are broadcasted to other nodes in the network. With this information, similarity of abnormalities is detected. Detection rate for this approach is as high as 96%, and false positives as 9.3%.

He et al \[25\] present a scheme for bandwidth estimation for detection of DDoS. The main idea of this solution is that during a DDoS attack, available bandwidth is depleted. This approach presents a 100% detection rate and low detection times.

Finally Berral et al \[26\] present and adaptive approach for detecting flooding attacks. They combine CUSUM for anomaly detection with other Machine Learning techniques such as Naive Bayes for traffic classification. This approach presents 95% of accuracy, no false positives, and only false negatives.

3.1.2 Support Vector Machines

Choi et al \[27\] present an approach based in the concept of Timeslot Monitoring Model. This technique operates monitoring and producing profiles from user activity in predefined intervals, to detect whether a given profile corresponds to normal or attack activity, when that activity is executed by an automatic tool. This approach fits to detection of application layer protocols although it was tested specifically with HTTP protocol; It shows 100% of accuracy when 2 intervals for monitoring are used.

3.1.3 Principal Component Analysis

Bharati et al \[31\] present a framework based on PCA for detection of application layer DDoS attacks, specifically, those based on HTTP traffic. It works by building profiles from browsing activity of users. This framework presents very low attack detection time, in comparison to other existing methods; no information on false positives is provided.

Liu et al \[32, 33\] present a solution combined of PCA and Sketches for detection in a distributed way. It is able to perform detection of anomalies both at the user side and at a central point, usually the Network Operation Center. Although results are not presented in detail, from graphics provided by authors is possible to note that the proposed approach has very low false detections rate, and it has low detection times.

Finally, Li et al \[34\] present a solution using PCA based on the concept of spatial correlation; this is, relations which can be established from studying similarities which present the traffic flows associated to attack, when directed towards the target. This solution shows more than 80% accurate detections, with only 0.1% of false positives. It is important remark the distributed nature of this solution, understanding the very own distributed nature of the attacks under study.

3.1.4 Neural classifiers

Raj Kumar et al \[35\] present an approach based on an ensemble of neural classifiers, on the idea that by combining classifiers, it is possible to reduce the overall error. Applied to detection of TCP, UDP, ICMP and HTTP based attacks, it presented a 98% of accurate detections, and around 3% of false positives.

Li et al \[36\] present an approach based on LVQ Neural Networks; they present results showing 99.7% of accurate detections, with around 0.3% of false positives; results with this kind of neural network are shown to be better than the ones obtained with back propagation neural network.
With DDoS attacks, it is possible that approaches be highly distributed, so, because of this fact and because of the fact that approaches with capabilities of collaboration, distribution and even mobility combined with machine learning and other techniques could provide better performance.

As future work from this review, exploring more recent papers (up to date) and deeper analysis of experimental results of reviewed papers is proposed.

3.2 Answering research questions

In this part of the section, answers to the proposed research questions are provided.

Regarding RQ1, most of the reviewed works show to be focused in low level DDoS attacks; IP, TCP and UDP based attacks is the most commonly analyzed attack type. Anyway, some of the authors address the problem of application based attacks, which are more complex to detect because of the high variability of attack patterns that can appear on traffic associated to them. Specifically the works referenced in [13] (SIP - IMS), [19] (DNS), [27] (HTTP), [31] (HTTP), [35] (HTTP), [37] (DNS) present approaches for application layer attack detection. Particularly, in the case of HTTP, is usual to model the attack as variations on normal user activities profiles.

In relation to RQ2, the review of the selected works allows to see that the best performances are provided with implementations of SVM (30) and LVQ Neural networks (36). It is important to clarify that there were some papers which did not present explicitly their results, so it might be possible to have approaches which would have better results to these referenced.

Finally, regarding RQ3, most of the works present centric solutions, to be used near to victim device. There are references of distributed approaches in [23, 24] and [34].

4 Conclusions and Future Work

An approach to state of art in application of Machine Learning to DDoS Attack detection was presented via Systematic Literature Review. From a structured procedure for reviewing papers, it was detected that an important topic to be researched is detection of application layer based protocols. Reviewed authors who have worked on this topic usually mention the wide quantity of literature which can be found regarding low level (Transport and network layers) DDoS attacks; IP, TCP and UDP based attacks is the most commonly analyzed attack type. Anyway, some of the authors address the problem of application based attacks, which are more complex to detect because of the high variability of attack patterns that can appear on traffic associated to them. Specifically the works referenced in [13] (SIP - IMS), [19] (DNS), [27] (HTTP), [31] (HTTP), [35] (HTTP), [37] (DNS) present approaches for application layer attack detection. Particularly, in the case of HTTP, is usual to model the attack as variations on normal user activities profiles.

In relation to RQ2, the review of the selected works allows to see that the best performances are provided with implementations of SVM (30) and LVQ Neural networks (36). It is important to clarify that there were some papers which did not present explicitly their results, so it might be possible to have approaches which would have better results to these referenced.

Finally, regarding RQ3, most of the works present centric solutions, to be used near to victim device. There are references of distributed approaches in [23, 24] and [34].

References


