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

# Sergio Armando Gutierrez; John Willian Branch

## 2013

This paper presents an approximation to state of art in application of some machine learning techniques to the field of Distributed Denial of Service attack detection

# 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.

# Study subjects

**405 papers**

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

# Findings

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%)

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

# Scholarcy Highlights

* Denial of Service (DoS) Attacks are not a new concern on the field of Computer Security
* A Distributed Denial of Service (DDoS) attack is a type of Denial of Service where multiple coordinated devices are used to lauch an attack towards one or more targets
* A previous mapping was performed to identify the most relevant Machine Learning techniques used for DDoS attack detection to focus the review
* 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 - CUmulative SUM (CUSUM) Algorithm (11 papers), Support Vector Machines - SVM (5 papers), Principal Components Analysis PCA (4 papers) and Neural Classifiers (4 papers)

# Scholarcy Summary

## Introduction

Denial of Service (DoS) Attacks are not a new concern on the field of Computer Security.

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.

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 provocate becomes an important task for scientific community

## Methods

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.

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

## 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.

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)

## Conclusion

An approach to state of art in application of Machine Learning to DDoS Attack detection was presented via Systematic Literature Review.

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 in contrast to literature on Application Layer attacks.

Another important detected issue is that, there are techniques providing good performances, increasing accuracy, reducing detection times and avoiding false detections is always a goal to achieve in detection techniques.

Tsai, “Web botnet detection based on flow information,” in ICS 2010 - International Computer Symposium, pp. 381–384, 2010

# Contributions

Conclusions and Future WorkAn 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 in contrast to literature on Application Layer attacks.Another important detected issue is that, although there are techniques providing good performances, increasing accuracy, reducing detection times and avoiding false detections is always a goal to achieve in detection techniques. Besides, an important challenge arises in relation to application of detection techniques on high speed networks, which are everyday more common.Collaborative and distributed detection is a topic deserving more attention. Because of the emergent trend on cloud and grid computing environments, platforms and services tend to be highly distributed, so, because of this fact and because of the very own nature of DDoS attacks, it is possible that approaches [1] C.-M. Chen, Y.-H. Ou, and Y.-C. Tsai, “Web botnet detection based on flow information,” in ICS 2010 - International Computer Symposium, pp. 381–384, 2010.

# Future work

Section 3 presents the detailed Literature Review on the selected paper, and the answers to proposed research questions. Section 4 presents the conclusion of this Literature Review and future work that can be derived from it.

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.

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

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 in contrast to literature on Application Layer attacks.