Traditional Machine Learning: Identifying Predictive Feautures of DDOS Attacks and Correlation with Botnet Activity

Casandra Newsom   
*Business Cybersecurity Management West Virginia University*Morgantown, USA  
cn00034@mix.wvu.edu

Benjamin McGavin  
*Business Cybersecurity Management West Virginia University*Morgantown, USA  
bpm00015@mix.wvu.edu

Julia Ossey  
*Business Cybersecurity Management West Virginia University*Morgantown, USA  
jo00044@mix.wvu.edu

***Abstract*—** In today’s cybercrime environment, Distributed Denial-of-Service (DDoS) attacks are becoming more prevalent. DDoS attacks are a major cybersecurity threat where attackers overwhelm a target system with additional traffic to disrupt its services. Botnets are often used to amplify

and distribute these attacks, making them more potent and harder to mitigate. In this paper, we aim to utilize traditional machine learning algorithms pattern detection capabilities to identify predicate features of DDoS attacks and explore any correlations to botnet activity. This approach based on the performance metrics below suggests a successful outcome of using traditional machine learning algorithms in establishing a detection system to identify future DDoS attacks on a target system.

Keywords—DDoS, botnet, machine learning, cybersecurity

# Introduction and related work

As DDoS attacks increase worldwide so will the need for an accurate detection system to alert target systems of a potential attack.

Research other papers on topic.

This paper focuses on DDoS activity as it relates to Internet of Things (IOT) and the possible correlation between DDoS attack and botnet activity. This paper seeks to answer the following questions:

1. What are the key network features that serve as indicators or predictors of future DDoS attacks targeting IOT devices?
2. Does botnet activity have any correlation to DDoS attacks? If so, how?

The results of our research indicated that traditional machine learning algorithms such as Logistic Regression, Random Forest and SVM identified high performance.

# Approach

## Data Collection

## Pre-processing

## Feature Extraction

## Classification

# experiments and analysis

## Authors and Affiliations

## Identify the Headings

## Figures and Tables

#### Positioning Figures and Tables: Place figures and tables at the top and bottom of columns. Avoid placing them in the middle of columns. Large figures and tables may span across both columns. Figure captions should be below the figures; table heads should appear above the tables. Insert figures and tables after they are cited in the text. Use the abbreviation “Fig. 1”, even at the beginning of a sentence.

1. Table Type Styles

| Table Head | Table Column Head | | |
| --- | --- | --- | --- |
| Table column subhead | Subhead | Subhead |
| copy | More table copya |  |  |

1. Sample of a Table footnote. (*Table footnote*)
2. Example of a figure caption. (*figure caption*)

# conclusion and future work

# References

The template will number citations consecutively within brackets [1]. The sentence punctuation follows the bracket [2]. Refer simply to the reference number, as in [3]—do not use “Ref. [3]” or “reference [3]” except at the beginning of a sentence: “Reference [3] was the first ...”

Number footnotes separately in superscripts. Place the actual footnote at the bottom of the column in which it was cited. Do not put footnotes in the abstract or reference list. Use letters for table footnotes.

Unless there are six authors or more give all authors’ names; do not use “et al.”. Papers that have not been published, even if they have been submitted for publication, should be cited as “unpublished” [4]. Papers that have been accepted for publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation [6].

1. G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. *(references)*
2. J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.
3. I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.
4. K. Elissa, “Title of paper if known,” unpublished.
5. R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.
6. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, “Electron spectroscopy studies on magneto-optical media and plastic substrate interface,” IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].
7. M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

**IEEE conference templates contain guidance text for composing and formatting conference papers. Please ensure that all template text is removed from your conference paper prior to submission to the conference. Failure to remove template text from your paper may result in your paper not being published.**