Critical Review of Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm

Jay Hunter (45776182)

ENGG1600

14/09/21

1 CONTENTS

2 INTRODUCTION

2.1 PURPOSE

The goal of this critique is review *Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm* written by researchers at the *Beijing University of Posts and Telecommunications* in the context of applicability in Critical Infrastructure Systems (CIS) operated by private and state entities. Distributed Denial of Service (DDoS) attacks are a form of cyber-attack where the victim network is incapable of sending or receiving network communication as the targeted network controller is overloaded by a flood of superfluous network requests made by the attacker. According the *Presidential Policy Directive*, Critical Infrastructure Systems are systems "… considered so vital to [a population] that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters…" (Dawson et al., 2021). A DDoS attack on CIS would cause said system has the potential to not only prevent the communication within a CIS network but also shut the system down entirely if the controller is sufficiently overloaded (Polat et al., 2020).

2.2 OVERVIEW OF THE PAPER

Researchers Yonghao Gu, Kaiyue Li, Zhentan Guo, and Yongfei Wang from the Beijing University of Posts and Telecommunications wrote *Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm* in 2019. In their paper, they propose the following argument, the two major machine learning algorithms currently presented, supervised algorithms require either copious amounts of prelabelled data to train, unsupervised models rely on local optimal leading to poor detection rates, and both utilise too many features for detection which can lead to worse performance and higher resource use. The researchers propose a semi-supervised weighted k-means Hadoop-based hybrid feature selection algorithm. They hypothesis this would require fewer labelled data sets for training whilst maintain accuracy. They also present a density-based initial cluster centre selection method as a second hypothesis in solving the issue of outliers and local optimal k-means clustering. The proposed algorithm is then used on multiple datasets, separately, for training then verification of their hypothesis (Gu et al., 2019).

2.3 BACKGROUND

2.3.1 Cyber Security Requirements and Constraints for Critical Infrastructure Systems

Security researchers who focus on Critical Infrastructure Systems agree to properly secure their systems protective methods must be active not passive (Dawson et al., 2021; Gunduz & Das, 2020; Ramotsoela et al., 2019; Tuptuk et al., 2021). Methods of achieving active protection are not. In the scope of defending CIS from DDoS attacks, K. Demir suggests Multipath-TCP (MPTCP) method which would systematically change open port numbers on a CIS's Wide Area Measurement System (WAMS). If an attack were to occur, they MPTCP method would open additional ports and direct the traffic away from the CIS controller (Demir & Suri, 2017). N. Bawany proposes a framework to protect Software Defined Networks called SEcure and AgiLe (SEAL). This framework was developed to be used on SDNs in a smart city's entire network, from water treatment to parking spacing. It was made to be scalable proactive depending on the criticality of the system it is protecting (Bawany & Shamsi, 2019). John O'Raw and his team propose making industrial WANS SDNs themselves and making Industrial Internet of Things (IIoT) inaccessible through the plant's WAN (O'Raw et al., 2019).The prior suggestions though different in methodology, share similar features. They require little financial resources to implement, minor or no computational overhead, are highly effective, and are currently implementable in Critical Infrastructure Systems with minor changes to its overall operation. These features are the constraints presented by protecting Critical Infrastructure Systems. This is further shown by the industry's response to an Amendment Draft currently before Australian Parliament.

Currently before Australian Parliament is the *Security Legislation Amendment (Critical Infrastructure) Bill 2020*. This Bill received 129 submissions from over 1,000 individuals during a three-week period of consultation (Department of Home Affairs, 2021). Of the 129 submissions, a common question of what additional financial commitments may be needed by an entity to adhere to this bill and when those commitments would be due (au Domain Administration, 2020; Australian Banking Association, 2020; Dickens, 2020; Queensland University of Technology, 2020; Vizza, 2020). All subsectors under the branch of Critical Infrastructure need to consider the cost of developing new and maintaining existing security systems. In this process, the entities which operate the CIS must classify and prioritise the most impactful attacks on their respective infrastructures (Rodofile et al., 2019). Cyber security is not limited to the impacts of DDoS attacks, and the systems developed to prevent attacks and mitigate damage need to efficient and cost-effective to operate (Poppensieker, 2019). Though a DDoS attack can temporarily shut down a Critical Infrastructure System, the attack itself generally lasts about a day. Cyber-attacks with similar intentions but different methodology can last must longer and cause more systematic damage and financial loss (Thompson, 2021).The recent May 7th ransomware attack on Colonial Pipeline and the Stuxnet worm, named 'the World's first digital weapon' are examples of attacks which have inflicted more damages alone than a DDoS attack current has (Kushner, 2013; Mehrotra, 2021; Osborne, 2021; Wade, 2021; Write, 2021; Zetter, 2014).

2.4 Hypothesis

The financial cost to deploy and maintain the proposed Distributed Denial of Service Detection algorithm from the Beijing University of Posts and Telecommunications is disproportionally high to the efficacy of the algorithm in comparison to others.

3 Critique

3.1 Accuracy is Misleading

The present algorithm's results after being tested on multiple datasets appear impressive. The detection rate (RR) is high, false positive rate (FP) is low. These results are passed through a TOPSIS method to calculate T(RR, FPR) (Fitness of the function) where the smaller the value is, the better the feature subset is at detecting attacks. Table 4 of the paper outlines the results of their algorithm and compare it other DDoS detection algorithms. The algorithm's success is due to the four algorithms presented in the paper. The first three algorithms pre-process the data to prepare it for the fourth and final algorithm title SKM-HFS. The first algorithm uses the Hadoop framework to pre-process the data by normalising the data and determining their RSD with *Equation 3* in the paper. The RSD is defined as the ratio of average Sum of Squared Errors (of a k-means method) to cluster Distance. The RSD values are processed through a TOPSIS method in ascending order for feature selection. The following two algorithms are the crux of why their presented algorithm provide accurate values (Gu et al., 2019).

Algorithm 2 is their solution to the following disadvantages of utilising k-means algorithms; k-means provide equal weighting to all clusters within a dataset. To mitigate this, algorithm 2 of the paper calculates the Euclidian distances between each point in the dataset as the radius, sorted in ascending order. *Algorithm 3* uses the radius found in *Algorithm 2* with its respective datapoint and arranges those pair in descending order based on their density. If a maximum density is not unique, it takes the mean of all datapoints and returns that as a dataset. The final algorithm, SKM-HFS, is used to train data with the data provided in *Algorithm 2* and the data provided through *Algorithm 3* for its initial cluster selection (Gu et al., 2019).

As stated, the accuracies presented by the researcher in *Table 4* appear impressive; but there are two major issues with the information presented. The values presented are not standard for machine learning accuracy. An F1 score is a measure of a model's overall accuracy given a dataset using the harmonic mean of the precision and recall where a perfect score is 1 (100%) (Wood, 2021).It presents the *true* accuracy of a test. The second issue is the complex methodology required to achieve these results when compared to simpler machine learning models utilising entropy convey otherwise. Researchers from Gazi University present F1 scores at a minimum of 88.45% in their comparison between Support Vector Machines (SVM), K-Nearest Neighbour (KNN), Artificial Neural Networks (ANN), and Naïve Bayes (NB) algorithms when using entropy in their detection method. The minimum presented accuracy is 91%, which too appears more impressive than the 88.45% F1 score to readers unfamiliar with the metric definitions (Polat et al., 2020). In comparison the worst accuracy presented for SKM-HFS is 98.86% when used on the CICIDS dataset (Gu et al., 2019).This performance metric is misleading to the audience to the efficacy of the SKM-HFS algorithm.

Dr Ramotsoela and his team reported a F1 result of 90.61% when tested on the BATADAL dataset for their presented ensemble technique, developed to replace density-based algorithms for DDoS attacks. Though it did not outperform density-based algorithms during their testing phase, this algorithm did not require as much pre-processing of data as the comparison algorithms and it was as resource intensive as its competitors in CIS DDoS detection (Ramotsoela et al., 2019). Two research groups, one lead by Dr Koay from the University of Waikato and the second a review of paper lead by Dr Geetha, found the entropy algorithm, feature selection, and window size for reading traffic data are more important than the machine learning algorithm itself (Geetha & Thilagam, 2021; Koay et al., 2019). If the pre-processing of training data is better indicator to an machine learning models detection F1 score, and the model itself does not require significant resources to accurately detect and prevent DDoS attacks on Critical Infrastructure Systems. SKM-HFS's complexity in training and resource requirements for implementation are disproportionate to its ability in comparison to competing models.

3.2 DDoS Attacks Are Volume-Based

Cyber security has been shown to be increasingly important to businesses, research done by the Florida Atlantic University presented business relationships between suppliers and customers deteriorate within two years of a cyber-attack (Thompson, 2021; Wang, 2020). Distributed Denial of Service (DDoS) attacks are one of the most common cyber-attacks according to Cisco Systems (CISCO Systems, 2021). Cyber security researcher, Stefano De Blasi, and Cloudflare state preparing and executing DDoS attacks are becoming increasingly simple (Blasi;, 2020; Cloudflair, 2021b). In September 2017 Google had mitigated a DDoS attack which reached 2.54 terabits per second (Tbps), In February of 2020, Amazon prevented a 2.3Tbps attack and in August of the same year, the New Zealand stock exchange was halted for four consecutive days due to a DDoS attack (Cimpanu, 2020; Cloudflair, 2021a; Editors, 2020; Farrer, 2020). Though the attacks on Google and Amazon were prevented the sheer volume of the traffic could overwhelm any system if it was successfully implemented. If either of these companies had used the SKM-HFS algorithm as suggested by the researchers, the volume itself would overwhelm the cluster computers needed to detect the attack. The Hadoop-based framework required for this algorithm, itself runs on cluster computers requiring a minimum of 2GB of Random Access Memory (RAM) to process each bit of data (Hodge et al., 2016; Hortonworks, 2014). Using the current largest recorded DDoS at 2.54Tbps, each computer in the cluster would need a minimum of 317.5 gigabytes (GB) of RAM to process the data, excluding the requirements for operating system (OS) overhead and requirements of other parts of the algorithm. This framework is not suited for live DDoS detection. SKM-HFS's minimum requirements to protect a Critical Infrastructure System are incredibly high. To reasonably cost-manage the model running on a system would be to utilise server farms which scale to need. These services are provided by both Google and Amazon who have shown to be capable of mitigating previously unseen records in DDoS attacks. By that point, to minimize cost and maximize the protection, an entity could utilise services offered by those companies to protect their systems, rending the SKM-HFS redundant. From a business perspective, the cost of building each individual server, maintaining, and powering them would be a larger financial burden than proved systems whose pricing scales to need.

4 CONCLUSION

The financial commitment to deploy and maintain the SKM-HFS algorithm presented by Dr Gu and his team at the *Beijing University of Posts and Telecommunications* is disproportionately high compared to its ability to detect an oncoming DDoS attack on a Critical Infrastructure System. Researchers have shown that the methods of training and reading the data are more indicative of success than the algorithm utilised. Given this, entities looking to protect their Critical Infrastructure Systems should seek other models for comparable protection at a fraction of the cost.

This algorithm and the methodologies presented would be better used in forensic analysis of prior DDoS attacks to further the abilities of more efficient algorithms in the future. It would be suggested that any further work done on the SKM-HFS algorithm be to reduce its resource requirements and improve its efficiency. It is also suggested that the researchers publish their F1 results alongside their accuracy as not to potentially mislead the readers.

5 References

au Domain Administration. (2020). *Submission in response to the Exposure Draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020* au Domain Administration. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS057-CISoNS-auDA.PDF

Australian Banking Association. (2020). *Security Legislation Amendment (Critical Infrastructure) Bill 2020*. A. B. Association. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS081-CISoNS-AustralianBankingAssociation.PDF

Bawany, N. Z., & Shamsi, J. A. (2019). SEAL: SDN based secure and agile framework for protecting smart city applications from DDoS attacks. *Journal of network and computer applications*, *145*, 102381. https://doi.org/10.1016/j.jnca.2019.06.001

Blasi;, S. D. (2020, 10/11/2020). Work Smarter, Not Harder: The Evolution of DDoS Activity in 2020. *Digital Shadows*. https://www.digitalshadows.com/blog-and-research/the-evolution-of-ddos-activity-in-2020/

Cimpanu, C. (2020, 16/10/2020). Google says it mitigated a 2.54 Tbps DDoS attack in 2017, largest known to date. *ZDNet*. https://www.zdnet.com/article/google-says-it-mitigated-a-2-54-tbps-ddos-attack-in-2017-largest-known-to-date/

CISCO Systems. (2021). *What Are the Most Common Cyber Attacks?* CISCO Systems. https://www.cisco.com/c/en_au/products/security/common-cyberattacks.html

Cloudflair. (2021a). *Famous DDoS attacks | The largest DDoS attacks of all time*. https://www.cloudflare.com/en-au/learning/ddos/famous-ddos-attacks/

Cloudflair. (2021b). *How to DDoS | DoS and DDoS attack tools*. Cloudflair. https://www.cloudflare.com/en-au/learning/ddos/ddos-attack-tools/how-to-ddos/

Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. *Land Forces Academy review*, *26*(1), 69-75. https://doi.org/10.2478/raft-2021-0011

Demir, K., & Suri, N. (2017). *Towards DDoS Attack Resilient Wide Area Monitoring Systems* Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy. https://doi.org/10.1145/3098954.3103164

Department of Home Affairs. (2021). *Protecting Critical Infrastructure and Systems of National Significance* Department of Home Affairs Website: Australian Federal Government Retrieved from https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-critical-infrastructure-systems

Dickens, N. (2020). *AIP SUBMISSION ON THE EXPOSURE DRAFT SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020*. A. I. o. Petroleum. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS019-CISoNS-AustralianInstituteofPetroleum.PDF

Editors. (2020, 26/08/2020). New Zealand stock exchange halted by cyber-attack. *BBC News*. https://www.bbc.com/news/53918580

Farrer, M. (2020, 28/08/2020). New Zealand stock exchange disrupted by fourth 'offshore' cyber attack. *The Guardian*. https://www.theguardian.com/world/2020/aug/28/new-zealand-stock-exchange-disrupted-by-fourth-offshore-cyber-attack

Geetha, R., & Thilagam, T. (2021). A Review on the Effectiveness of Machine Learning and Deep Learning Algorithms for Cyber Security. *Archives of computational methods in engineering*, *28*(4), 2861-2879. https://doi.org/10.1007/s11831-020-09478-2

Gu, Y., Li, K., Guo, Z., & Wang, Y. (2019). Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm. *Ieee Access*, *7*, 64351-64365. https://doi.org/10.1109/ACCESS.2019.2917532

Gunduz, M. Z., & Das, R. (2020). Cyber-security on smart grid: Threats and potential solutions. *Computer networks (Amsterdam, Netherlands : 1999)*, *169*, 107094. https://doi.org/10.1016/j.comnet.2019.107094

Hodge, V. J., O'Keefe, S., & Austin, J. (2016). Hadoop neural network for parallel and distributed feature selection. *Neural Networks*, *78*, 24-35. https://doi.org/https://doi.org/10.1016/j.neunet.2015.08.011

Hortonworks. (2014). *Cluster Planning Guide*. https://docs.cloudera.com/HDPDocuments/HDP2/HDP-2.0.6.0-Win/bk_cluster-planning-guide/bk_cluster-planning-guide-20140120.pdf

Koay, A., Welch, I., & Seah, W. K. G. (2019). (Short Paper) Effectiveness of Entropy-Based Features in High- and Low-Intensity DDoS Attacks Detection. In N. Attrapadung & T. Yagi (Eds.), *Advances in Information and Computer Security, Iwsec 2019* (Vol. 11689, pp. 207-217). https://doi.org/10.1007/978-3-030-26834-3_12

Kushner, D. (2013, 26/02/2013). The Real Story of Stuxnet. *IEEE Spectrum*. https://spectrum.ieee.org/the-real-story-of-stuxnet

Mehrotra, W. T. K. (2021, 04/06/2021). Hackers Breached Colonial Pipeline Using Compromised Password. *Bloomberg News*. https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

O'Raw, J., Laverty, D., & Morrow, D. J. (2019). 2019 IEEE 5th World Forum on Internet of Things (WF-IoT). In (pp. 70-75): IEEE.

Osborne, C. (2021, 12/05/2021). Colonial Pipeline attack: Everything you need to know. *ZDNet*. https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

Polat, H., Polat, O., & Cetin, A. (2020). Detecting DDoS Attacks in Software-Defined Networks Through Feature Selection Methods and Machine Learning Models. *Sustainability*, *12*(3), 1035. https://www.mdpi.com/2071-1050/12/3/1035

Poppensieker, D. C. J. M. K. T. (2019). *Perspectives on transforming cybersecurity*. K. Company. https://www.mckinsey.com/~/media/McKinsey/McKinsey%20Solutions/Cyber%20Solutions/Perspectives%20on%20transforming%20cybersecurity/Transforming%20cybersecurity_March2019.ashx

Queensland University of Technology. (2020). *Response to the exposure draft of the Security Legislation Amendment (Critical Infrastructure) Bill 2020*. Q. U. o. Technology. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS051-CISoNS-QUT.PDF

Ramotsoela, D. T., Hancke, G. P., & Abu-Mahfouz, A. M. (2019). Attack detection in water distribution systems using machine learning. *Human-centric computing and information sciences*, *9*(1), 1-22. https://doi.org/10.1186/s13673-019-0175-8

Rodofile, N. R., Radke, K., & Foo, E. (2019). Extending the cyber-attack landscape for SCADA-based critical infrastructure. *International Journal of Critical Infrastructure Protection*, *25*, 14-35. https://doi.org/10.1016/j.ijcip.2019.01.002

Thompson, R. O. N. (2021, 28/05/2021). Cyber attacks can shut down critical infrastructure. It's time to make cyber security compulsory. *The Conversation*. https://theconversation.com/cyber-attacks-can-shut-down-critical-infrastructure-its-time-to-make-cyber-security-compulsory-160991

Tuptuk, N., Hazell, P., Watson, J., & Hailes, S. (2021). A Systematic Review of the State of Cyber-Security in Water Systems. *Water*, *13*(1), 81. https://www.mdpi.com/2073-4441/13/1/81

Vizza, S. A. T. (2020). *SECURITY LEGISLATION AMENDMENT (CRITICAL INFRASTRUCTURE) BILL 2020 EXPOSURE DRAFT BILL SUBMISSION*. https://www.homeaffairs.gov.au/reports-and-pubs/files/critical-infrastructure-consultation-submissions/EDS094-CISoNS-AustralianInformationSecurityAssociation.PDF

Wade, S. S. M. (2021, 26/05/2021). Colonial Pipeline forked over $4.4M to end cyberattack – but is paying a ransom ever the ethical thing to do? . *The Conversation*. https://theconversation.com/colonial-pipeline-forked-over-4-4m-to-end-cyberattack-but-is-paying-a-ransom-ever-the-ethical-thing-to-do-161383

Wang, C. H. J. H. M. J. K. L. (2020). The Impact of Customer’s Reported Cybersecurity Breaches on Key Supplier’s Relationship-Specific Investments and Relationship Duration. *SSRN*, 1-61. https://doi.org/http://dx.doi.org/10.2139/ssrn.3544245

Wood, T. (2021). What is the F-Score? https://deepai.org/machine-learning-glossary-and-terms/f-score

Write, A. (2021, 25/06/2021). Stuxnet: The Threat of Tomorrow Unveiled. *The Cove*. https://cove.army.gov.au/article/icymi-stuxnet-the-threat-tomorrow-unveiled

Zetter, K. (2014, 11/03/2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. *Wired*. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/