EFFICIENCY OF MACHINE LEARNING METHODS IN THE DETECTION OF DDOS ATTACKS

ENGG1600

JAY HUNTER (45776182)
UQ CYBER

0 ABSTRACT

Distributed Denial of Service attacks have been increasing in volume and occurrence over the last decade. An attack on a Critical Infrastructure System could lead to the death of people during the shutdown of the system. Given this, it has become a priority to defend Critical Infrastructure Systems against Distributed Denial of Service attacks. Current methods of prevention through machine learning algorithms have focused heavily on the accuracy of their algorithms whilst neglecting the costs associated with implementing them. To counter this, Support Vector Machines, k-Means, Random Forrest, and k-Nearest neighbour algorithms have been tested without modification to compare results and give insight to how applicable the algorithms are to real-world defence. The results found that current research has provided little improvement in the accuracy of the algorithms without requiring immense computational power.

1 INTRODUCTION

According the *Presidential Policy Directive*, Critical Infrastructure Systems (CIS) 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). Distributed Denial of Service (DDoS) attacks are one of the most common cyber-attacks according to Cisco Systems (CISCO Systems, 2021). 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. 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). 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).

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). This is highlighted by submissions to Australian Parliament on *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 enquiry was 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).

Researchers developing Machine Learning DDoS attack detection algorithms for CIS have focused on the accuracy of their algorithms rather than their applicability in industry. Researchers at the Beijing University of Posts and Telecommunications presented the *SKM-HFS* algorithm in their 2019 paper *Semi-Supervised K-Means DDoS Detection Method Using Hybrid Feature Selection Algorithm* (Gu et al., 2019). Though the algorithm was shown to be

accurate, its framework would require 317.5 gigabytes (GB) minimum for each computer in the cluster to process the current largest DDoS attack of 2.54Tbps (Hortonworks, 2014). This makes the algorithm prohibitively expensive for an entity to implement and maintain.

1.1 Research Question

Has the research and development of Machine Learning based DDoS detection algorithms shown improvement in either accuracy or time required to process network traffic? If so, are these improvements still viable for an entity to utilise in their Critical Infrastructure System?

1.2 Overview of this Paper

Section 2 is an outline of related work, definitions of selected algorithms, defines entropy, and performance metrics used to test algorithm viability. *Section 4* outlines the methodology used for executing the comparison algorithms and collect the required data. *Section 4* Compares the results found to current related work.

2 Related Work

2.1 Performance Metrics

Five measurement values used to determine the efficacy of a machine learning (ML) algorithms. Accuracy is used to determine how well a model can identify patterns and relationships in the data provided to it. Precision is a measurement of the true positives identified by the algorithm. It is used when trying to minimise the number of false positives in an algorithm. Recall is used as an indicator of false negatives in an algorithm. F1 is the harmonic mean between precision and recall, often used to evaluate the retrieval capability of a system. A perfect algorithm has a score of 1. F2 is an extension of F1, where an increase in β denotes that recall is more important to an algorithm than precision.

Table 1: Value Definitions

Accuracy	The proportion of true positives (TP) and true negatives (TP) with false positives (FP) and false negatives (FN).	$A = \frac{\text{TP} + \text{TN}}{TP + TN + FP + FN}$
Precision	The fraction of correct answers in total answers.	$\text{P} = \frac{\lvert\text{TP} \cap \text{Total Samples}\rvert}{\lvert\text{TP}\rvert}$
Recall	The fraction of correct answers.	$R = \frac{\lvert\text{TP} \cap \text{Total Samples}\rvert}{\lvert\text{Total Samples}\rvert}$
F1	F1 is the harmonic mean of precision and recall. It shows how sensitive method is in a binary test.	$F_1 = 2 \cdot \frac{\text{Precision} \cdot \text{Recall}}{Precision + Recall}$
F2	Provides a higher weight to recall than precision. Used when attempting to correctly classify as many samples as possible.	$F_2 = (1 + \beta^2) \cdot \frac{\text{Precision} \cdot \text{Recall}}{(\beta^2 \cdot Precision) + \text{Recall}}$

2.2 SUPPORT VECTOR MACHINE

2.2.1 Definition

Support Vector Machine (SVM) is a supervised machine learning algorithm which can be used for both classification and regression challenges. However, it is mostly used in classification problems. In addition to performing linear classification, SVMs can efficiently perform a non-linear classification using what is called the kernel trick, implicitly mapping their inputs into high-dimensional feature spaces.

2.2.2 Current Research

Dr K.S Sahoo and his team present three permutations of the SVM algorithm, N-KPCA+GA+SVM, KPCA+GA+SVM, and PCA+GA+SVM for DDoS detection in their paper *An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks*. These permutations were methods of training the ML algorithm and prepressing the data. They tested their permutations on two DDoS testing datasets, KDD'99 and NSL-KDD. Each algorithm was tested on both algorithms three times. (Sahoo et al., 2020).

Shideh Yavary Mehr and Byrav Ramaurthy from the University of Nebraska-Lincoln presented their paper *An SVM Based DDoS Attack Detection Method for Ryu SDN Controller* at the *15th International Conference on Emerging Networking Experiments and Technologies*. They present a novel DDoS detection system for SDN Controllers using Python and Ryu. In this system, a SVM classifier detects DDoS attacks and alters the SDN controller which then blocks the malicious packets. Their method was shown to allow the network to continue its network communication after 80 seconds with the network returning to normal communication after 120 seconds. The total reduction of effects from DDoS attacks is presented to be 36% (Mehr & Ramamurthy, 2019).

2.3 K-NEAREST NEIGHBOUR

2.3.1 Definition

In classification, k-Nearest Neighbour (KNN) algorithms assign a class to data based on features most common to each data point and their 'neighbours'.

2.3.2 Current Research

Researchers Shi Dong and Mudar Sarem in their paper *DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks* presented a novel concept of utilising the degree of attack (DDADA) with KNN to detect DDoS attacks. This concept is a utilises the gain of the attack, measured by the flow of data, within a given timeframe and compares it to a threshold. If that threshold is reached, a DDoS attack has occurred. (Dong & Sarem, 2020).

Researchers from the *Nanjing University of Posts and Telecommunications* show in their paper *Efficient DDoS Detection Based on K-FKNN in Software Defined Networks* their modification to the standard KNN algorithm, K-FKNN, is better at detecting DDoS attacks. Result are shown in *Table 1* (Xu et al., 2019).

2.4 RANDOM FOREST

2.4.1 Definition

Used for classification, Random Forest (RF) construct a plethora of decision trees during the training phase of the model. When the model is then implemented, data passed through it is processed through the decision trees to an end value.

2.4.2 Current Research

Researchers from the University of Brawijaya presented DDoS Attack Early Detection and Mitigation System on SDN using Random Forest Algorithm and Ryu Framework at the *8th International Conference on Computer and Communication Engineering*. They present the use case for utilising a separate Software Defined Network with a Random Forest classifier (RF-SDN) which dynamically classifies traffic based on the flow of the data. The results presented show that CPU usage is reduced by 44.9% when compared to current protection software with an accuracy of 98.38% (Nurwarsito & Nadhif, 2021).

Researchers at the Rajshai University of Engineering and Technology present two novel Internet of Things (IoT) security algorithm in their paper *DDoS Attack Detection in IoT Networks Using Learning Models Combine with Random Forest as Feature Selection*. Tests were conducted on the CICIDS2017. The RF-MLP algorithm scored a 99.58% for F1 values with a 99.26% recall. The second algorithm, RF-CNN scored 99.63% for F1 values and 99.34% in precision. The methods presented were designed to use hardware resources conservatively and outperformed their comparison algorithms (Farukee et al., 2021).

2.5 K-MEANS

2.5.1 Definition

K-means clustering (KM), clusters data by a specified k value. Data is then randomly allocated to these clusters. The algorithm then randomly selects a centre and begins optimising the positions of the data until the cluster has either stabilized or a defined number of iterations has been reached.

2.5.2 Current Research

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 presented a novel Hadoop-based KM algorithm, SKM-HFS. It was tested over four datasets, DARPA, CAIDA, CICIDS, and Real-World and presented a mean accuracy of 99.33% across all four sets. It has a major issue of requiring cluster-computers with a minimum of 320GB of RAM. Not ideal for any real-world situation (Gu et al., 2019).

DDoS Detection and Defense Mechanism for SDN Controllers with K-Means was presented by Dr Cui and his team at the *13th International Conference on Utility and Cloud Computing (UCC)*. In this presentation they propose the utilisation of K-Means clustering to filter malicious packets in an SDN. Their method of using a KM algorithm to alter a switch show to mitigate the effects of a DDoS attack with CPU usage 3 seconds into an attack and returning to normal after 7 seconds. It achieved this by using the entropy of the network traffic as an indicator of an attack rather than labelling potentially malicious IP addresses (Cui et al., 2020).

2.6 SHANNON ENTROPY

Entropy has been shown to be an effective pre-processing technique for the detection of both high and low intensity DDoS attacks (Koay et al., 2019). There are many variations of entropy calculation. Shannon Entropy is the basis of these variations and is the focus of many papers on the subject (Kalkan et al., 2018; Koay et al., 2018; Liu et al., 2019). It is calculated with the following formula:

$$H(X) = -\sum_{i=1}^{n} P(x_i) \log P(x_i)$$

This summation is the average level of the information through a system. Through the calculation of this average, machine learning algorithms can efficiently identify when network traffic is rapidly moving from the average and identifies a DDoS attack (Gunduz & Das, 2020; Ramotsoela et al., 2019). This is done through windows. Windows are time frames in either nanoseconds or seconds for which the average network traffic is calculated (Koay et al., 2019; Sahoo et al., 2018).

3 METHODOLOGY

Four machine learning algorithms were chosen: Support Vector Machine, k-Nearest Neighbour, Random Forest, and k-Means to be tested on the DDoS attack dataset, Electra Modbus (Perales Gomez et al., 2019). Electra Modbus is a relatively new attack dataset which is to be used for DDoS detection for Smart Grid Critical Infrastructure Systems. These critical infrastructure systems are part of the current advance in electrical grid critical infrastructure, gaining connectivity to the internet. Electra Modbus is designed to assist researchers in developing protection systems for such systems.

Electra Modbus has labels for all network traffic in the dataset. For the purposes of this experiment, all machine learning algorithms are supervised. That is, during the training phase, the algorithms are told whether the traffic that it is processing is malicious or not through the given labels. The selection of specific parts of a dataset (I.P. Address, MAC Address, Type of Connection, ect) is called feature selection (Koay et al., 2018; Li et al., 2018). The effect of feature selection was not investigated as there were not enough unique datapoints for the features provided by the Electra Modbus dataset. *Figure 1* presents a diagram of how the data was tested.

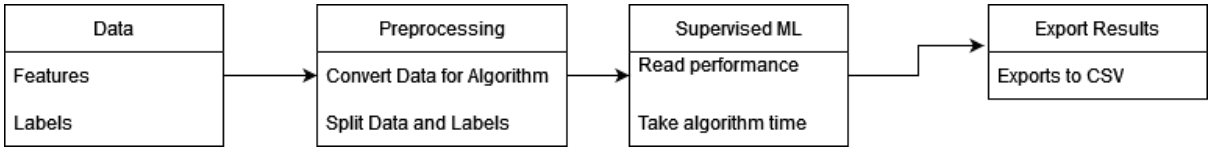

Figure 1: Testing Diagram

The data was tested in four ways. First, the data was tested without any modification (N). The next three times, the data was tested with Shannon Entropy with window sizes of 0.01 seconds (W1), 0.1 seconds (W2), and 1 second (W3). The effect of entropy on algorithm results presents a better insight to how effective the algorithms would be if implemented in a critical infrastructure system as the network traffic through the algorithm will not be consistent.

Each of the four machine learning algorithms were tested for their Accuracy, Precision, Recall, F1, and F2 values on the Electra Modbus dataset to determine their performance. The first three steps of *Figure 1* were repeated 5,000 times and the means were taken before the

results were exported to a CSV. By the law of large numbers, the means of these algorithms are closest to their true mean. To prevent the algorithms from being skewed to the dataset, each time this process was repeated, the algorithms were reset and retrained.

4 RESULTS AND DISCUSSION

There are multiple common issues present among the comparison algorithms (from *Section 2)* presented in *Table 2*. Most were missing the process time of their algorithms on their respective datasets. Precision, Recall, and F1 values are missing from many papers or are included as visual graphs with no exact values. This missing information makes direct testing of hypothesis and algorithm effectiveness. This further exemplifies the issue of transparency present in current research for Machine Learning based DDoS detection. This lack of transparency makes direct comparisons between prior work and the values obtained difficult. Because of this, inferences and generalisations need to be made for comparison.

The result obtained from the testing, shown in *Table 2*, appear to convey there has been little improvement in the effectiveness and applicability of machine learning algorithms in current research. The SKM-HFS algorithm shows the most improvement when compared to the four tested k-Means algorithms. However, this improvement came at a large computational cost as mentioned in *Section 2.5.2*. For the KPCA+GA+SVM, KPCA+GA+SVM, and PCA+GA+SVM algorithms, presented by K.S Sahoo exact values were not presented for precession and recall, with bar-graphs in their place. Because of this, no exact values have been included in *Table 2*. From exact values given, there appears to be a moderate increase in accuracy, but it is uncertain if this also increased processing time. Support Vector Machine has been shown to be the slowest algorithm of the four with the slowest being SVM-N. Entropy appears to have produced better processing times but the accuracy of the algorithms decreased at each window interval. Random Forest and k-Nearest Neighbour appear have had no considerable improvements in any of the performance metrics.

The low performance of the k-Means algorithms is likely due to how the algorithm groups the datapoints. This is exemplified by the results shown for KM-W1, KM-W2, and KM-W3. The datapoints provided by the Shannon Entropy windows have likely been grouped together for classification. This grouping has not properly identified DDoS attacks from normal traffic. This may be fixed with a larger dataset, which could be investigated further.

The times of the algorithms on the Electra Modbus dataset aligns well with research which has been focused on IoT devices. The K-Means clustering method discussed in *Section 2.5.2*, developed by Dr Cui is an example of improvement in time, resource use, and detection rate. Though the paper did not present any of the performance metrics outlined in *Section 2.1*, the KM algorithm developed was made to be a classifier for a detection algorithm. The researchers also presented a low CPU usage for DDoS detection and attack prevention. The results are not reproducible or testable, as the hardware used for testing is not given.

Table 2: Results

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	F2-Score (%)	Time (s)
SVM-N	93.74	92.61	93.74	0.92	0.92	14.97
SVM-W1	86.55	86.60	86.55	0.84	0.94	3.01
SVM-W2	89.65	89.00	89.65	0.88	0.88	3.21
SVM-W3	80.30	78.78	80.30	0.77	0.77	3.89
KNN-N	99.38	99.40	99.38	0.99	0.99	0.66
KNN-W1	98.08	98.05	98.08	0.98	0.98	0.20
KNN-W2	98.37	98.31	98.37	0.98	0.98	0.20
KNN-W3	98.75	98.74	98.75	0.98	0.98	0.19
RF-N	99.99	99.99	99.99	0.99	0.99	1.81
RF-W1	99.87	99.87	99.87	0.99	0.99	0.83
RF-W2	99.89	99.89	99.89	0.99	0.99	1.02
RF-W3	99.91	99.91	99.91	0.99	0.99	1.27
KM-N	13.35	42.54	13.35	0.18	0.27	1.04
KM-W1	13.11	40.23	13.11	0.17	0.25	0.46
KM-W2	13.18	43.00	13.18	0.17	0.25	0.37
KM-W3	12.91	39.66	12.92	0.17	0.25	0.63
N-KPCA+GA+SVM	95.72					
KPCA+GA+SVM	95.30					
PCA+GA+SVM	93.44					
DDADA	98.70	98.50	98.70	0.98		
K-FKNN		97.50	98.50	0.98		
RF-SDN	98.38					
RF-MLP	99.58	99.26	99.90	0.99		
RF-CNN	99.63	99.34	99.34	0.99		
SKM-HFS	99.33					

5 CONCLUSION AND RECOMMENDATIONS

The results found from the testing appear to show there has been little improvement in Machine Learning based algorithms for DDoS detection. This, however is a large generalisation. The issue relates closer to a lack of transparency in how performance metrics are made and what they exactly are. This issue is furthered by comparing algorithms on different datasets. The random forest and k-Nearest Neighbour algorithms appear to be better than prior work but this disingenuous. The dataset itself may have problems in its creation. This problem is rarely discussed in papers comparing their results to prior papers.

Future work on this problem would be to take the methodology presented in *Section 3* to obtain the performance metrics outlined in *Section 2.1* on the same datasets used in related works. The results found by the same algorithms on different datasets could then be generalised to present the most optimal machine learning detection algorithm. As it currently stands, where improvements appear to exist in current research, there is too little presented data and information in methodology to reliably reproduce results given.

6 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

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/

Cui, J., Zhang, J., He, J., Zhong, H., & Lu, Y. (2020). 2020 IEEE/ACM 13th International Conference on Utility and Cloud Computing (UCC). In (pp. 394-401): IEEE.

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

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

Dong, S., & Sarem, M. (2020). DDoS Attack Detection Method Based on Improved KNN With the Degree of DDoS Attack in Software-Defined Networks. *Ieee Access*, *8*, 5039-5048. https://doi.org/10.1109/access.2019.2963077

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

Farukee, M. B., Shabit, M. S. Z., Haque, M. R., & Sattar, A. H. M. S. (2021). DDoS Attack Detection in IoT Networks Using Deep Learning Models Combined with Random Forest as Feature Selector. In M. Anbar, N. Abdullah, & S. Manickam, *Advances in Cyber Security* Singapore.

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

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

Kalkan, K., Altay, L., Gur, G., & Alagoz, F. (2018). JESS: Joint Entropy-Based DDoS Defense Scheme in SDN. *IEEE journal on selected areas in communications*, *36*(10), 2358-2372. https://doi.org/10.1109/JSAC.2018.2869997

Koay, A., Chen, A., Welch, I., & Seah, W. K. G. (2018). 2018 International Conference on Information Networking (ICOIN). In (pp. 162-167): IEEE.

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

Li, J. D., Cheng, K. W., Wang, S. H., Morstatter, F., Trevino, R. P., Tang, J. L., & Liu, H. (2018). Feature Selection: A Data Perspective. *Acm Computing Surveys*, *50*(6), Article 94. https://doi.org/10.1145/3136625

Liu, Z., He, Y., Wang, W., & Zhang, B. (2019). DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN. *China communications*, *16*(7), 144-155. https://doi.org/10.23919/j.cc.2019.07.012

Mehr, S., & Ramamurthy, B. (2019). Proceedings of the 15th International Conference on emerging networking experiments and technologies. In *Conference on emerging Networking Experiments and Technologies* (pp. 72-73): ACM.

Nurwarsito, H., & Nadhif, M. F. (2021). 2021 8th International Conference on Computer and Communication Engineering (ICCCE). In (pp. 178-183): IEEE.

Perales Gomez, A. L., Fernandez Maimo, L., Huertas Celdran, A., Garcia Clemente, F. J., Cadenas Sarmiento, C., Del Canto Masa, C. J., & Mendez Nistal, R. (2019). On the Generation of Anomaly Detection Datasets in Industrial Control Systems. *Ieee Access*, *7*, 177460-177473. https://doi.org/10.1109/ACCESS.2019.2958284

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

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

Sahoo, K. S., Puthal, D., Tiwary, M., Rodrigues, J. J. P. C., Sahoo, B., & Dash, R. (2018). An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. *Future Generation Computer Systems*, *89*, 685-697. https://doi.org/https://doi.org/10.1016/j.future.2018.07.017

Sahoo, K. S., Tripathy, B. K., Naik, K. S., Ramasubbareddy, S., Balusamy, B., Khari, M., & Burgos, D. (2020). An Evolutionary SVM Model for DDOS Attack Detection in Software Defined Networks. *Ieee Access*, *8*, 1-1. https://doi.org/10.1109/ACCESS.2020.3009733

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
Xu, Y., Sun, H., Xiang, F., & Sun, Z. (2019). Efficient DDoS Detection Based on K-FKNN in Software Defined Networks. *Ieee Access*, *7*, 160536-160545. https://doi.org/10.1109/ACCESS.2019.2950945