ISSN 2278-3091
Volume 9, No.3, May - June 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse215932020.pdf
https://doi.org/10.30534/ijatcse/2020/215932020

Application Layer Denial of Services Attack Detection Based on StackNet

SAMI SMADI[1],MOHAMMAD ALAUTHMAN[2], OMAR ALMOMANI[3], ADEEP SAAIDAH[4], FIRAS ALZOBI[5]

[1]Department of Information System and Networks, The World Islamic Science & Education University, Jordan, sami.smadi@wise.edu.jo
[2]Department of Internet Technology, Zarqa University, Jordan, malauthman@zu.edu.jo
[3]Department of Information Security, The World Islamic Science & Education University, Jordan, omar.almomani@wise.edu.jo
[4]Department of Information System and Networks, The World Islamic Science & Education University, Jordan, adeeb.saaidah@wise.edu.jo
[5]Department of Information System and Networks, The World Islamic Science & Education University, Jordan, firas.alzobi@wise.edu.jo

ABSTRACT

Denial of Services (DoS) Attack is one of the most advanced attacks targeting cybercriminals. The DoS attack is designed to reduce the performance of network devices by performing their intended functions. In addition, the confidentiality, reliability and quality of data can be compromised by DoS attacks. In this paper, a new model is introduced that detects network traffic and varies type of application layer DoS attacks. The proposed model usesStackNet architecture which consists of three-layer that works in the feed-forward method. The results showed that the proposed model had a high accuracy level of 99.3% in the measurement of application-layerDoS attacks.

Key words: DoS Attack ,IDS, StackNet, Machine learning.

1. INTRODUCTION

The widespread use of the Internet and exponential development of connectivity and computer networks increase and cause catastrophic harm to cybercriminals activities in the target networks. DoS attacks are one of the quickest attacks to be conducted with tremendous network infrastructure impacts and severe organizational losses. Cyber-attacks are also extended depending on the network influence and financial losses.

A network attack is any mechanism or tool used to attempt to harm the network security of computer networks [1-9]. Attackers consider several different stages in order to perform attacks, starting with the attacker's initial motivation and the final attack execution [1, 10-13]. The most attractive type of attack is a DoS.This research concentrates on detecting attacks, in particular, DoS floods and brute-force attacks. DoS attacks are widely used in the areas TCP-SYN attacks, UDPflooding attacks, ICMPEcho assault, HTTP flood attacks, slowloris and slowpost attacks. DoS flooding attacks are most commonly associated with DoS flooding attacks.

There has been a lot of comprehensive research on the financial losses caused by DoS attacks. In 2016, the total losses of approximately $1,5 million for 651 individuals in five different categories (revenue losses, technical assistance expense, operational disruptions, lost user efficiency and Damage to assets of information technology).These losses were reported by the Ponemon Institute[4, 14-18]. In 2017, 49% of organization experience a DDoS attack [19]. In consequence, many companies wish to protect their networks against multiple attacks that could cost them massive losses through computer network security services

The Simple Network Management Protocol (SNMP) is a common protocol for the management of internet-based network devices with the TCP/IP series. SNMP is a User Datagram Protocol (UDP) application layer protocol. It is used for network computer setup and collection of information such as Standard PCs, Switches, Servers and routers[20].Many recent intrusion detection studies rely on raw packet data to assess the safety status of computer systems and networks, which lead to considerable processing and slowing identification [21].

As already stated, the SNMP supports variables corresponding to system-level traffic information. The information can be passively tracked from network devices and can be used to identify network behaviour, thereby using it for network anomaly detection[20].A Management Info Base (MIB) is a machine network database that manages objects. SNMP regularly funds MIB. Since the SNMP[21] is

standardized and implemented on every network computer, we have therefore chosen the SNMP as a protocol for network attack-detection to add to the quality of the MIB statistics to be conveniently gathered for analysis. The fine-grassed data generated by the MIB for anomaly detection allows users to escape some of the obstacles of network intrusion detection.

Any malicious behaviour that occurs can affect a particular MIB attribute in some way. Therefore, SNMP-MIB data is a source of anomaly detection indicators that can make network anomaly detection more reliable.Proper SNMP-MIB variables have to be chosen because no single variable can capture all network anomalies.In order to enhance the detection model the number of MIB variables involved need to be minimized[21-24].

An IDS is an excellent protection tool for DoS attacks. The concept behind the DoS threat was to apply a data flood to a given system to prevent computer operators from doing what they required. Moreover, it impairs access by registered users to machine services.

A DoS attack can be divided into two primary strategies:Firstly, through using the vulnerable network servers, computers and protocol. Secondly, exploiting a large number of spoofed source addresses. This paper used a StackNet model in which various DoS attacks were identified by a collection of SNMP variables and an assumed data set.

This paper is organized as follows: Section 2 introduces manyprevious studies in the field of identity network anomaly, which highlights the DoS attacks on SNMP-MIB datasets. Section 3 addresses the model suggested for this contribution. The experimental results of this approach are described in Section 4. Finally, Section 5 addresses the conclusion of the model presented and future work.

2. RELATED WORK

Different strategies were used in the literature to detect DoS attacks, such as Machine Learning (ML), knowledge-based, and statistical[25]. Every approach suggested has different problems and limitations. For example, statistical methods are not capable of knowing the normal distribution of network packets with certainty.Network events are examined against defined rules or patterns of attack in knowledge-based approaches, as attackers change their techniques, the knowledge base fails to identify new attacks[26]. Machine training techniques are good because they do not require any prior knowledge of data distribution, but it is one of the key challenges for machine learning to determine the best feature set[25]. Based on the previous discussion, in this paper, a machine learning paradigm is used. Several researchers in the past decade have extensively studied the identification of anomalies and computer network attacks. The majority of the current network anomalies and detection of network attacks are based on network traffic analysis (e.g. delay, packet number, IPProtocol, ports, network flow, and so on). Another tool for finding network anomalies is the SNMP MIB.

C. Rahmaniet al. developed a proactive detection approach usinga statistical method for detecting DDoS attacks [27]. The framework has been developed using the SNMP variable based on MIB variables. Four MIB variables have been obtained from four different categories, IP, ICMP, TCP and USP. DDoS attacks showed high efficiency in their experiments.Once a contrast between the standard and the attack runs of the MIB values was made, the attack signatures were detected. If that signature were located in the Network Management System (NMS), an attack occurred.

Q. Wu and Z. Shao haveutilized an Auto-Regressive (AR) approach for time series data using five MIB category, and they have performed a sequential network anomaly test[28]. The experiments conducted in a real-time scenario usingSmurf, SYN, ICMP floods and UDP attacks,these attacks were used to assess their detection method.

In[29], an SNMP MIB data traffic anomaly detection system was developed, which included the four interface category MIB variables. The proposed method was tested using two types of DoS attacks, such as SYN Flood and Smurf. They noticed that this approach was able to effectively detect flood attacks.

S. Rao and S. Rao introduced an easy and fast intravenous sensing algorithm using the correlation of the SNMP-MIB features, in particular for the detection of traffic attacks by floods[30]. For attack detection,sixteen MIB features from six classes were identified. The efficiency of the proposed detection algorithm was checked using TCPSYN, ICMP floods and UDP. They have demonstrated that their work can accurately detect all types of assaults with very low FPs and FNs rates.

J. Yu et al. and Bao et al. proposed a machine learning systems to detect network intrusion using SNMP-MIB dataset[21, 31]. Fast and low weight systemswere proposed, which detects and classifies SVM-based floods. 13 SNMP MIB variables were collected in actual experiments, consisting of four MIB sets includesUDP, IP, TCP and ICMPat of 15-second time-window intervals. The systems proposed for the attack detection of severalattacks types were built in a hierarchical SVM structure: TCP-SYN and UDP, as well as ICMP floods.

G. Al-Naymat et al.[32] have proposed amachine-learning technique to detect network attacks and abnormalities based on SNMP-MIB data sets. The SNMP-MIB has proven to be an effective strategy for identifyinganenormous number of different kind of DoS via using three algorithms: Multilayer perceptron, Random-Forest and Adaboost. These algorithms were used for various MIB groups (ICMP, IP, TCP and UDP).The selected algorithms have achieved diverse group-based accuracy. High accuracy was obtained by applying the

Random-Forest algorithm to the IP category with 100% rates and 99.93% rates when using the interface cluster.

A hybrid method for capturing and detector of malicious traffic has been suggested by Al-Kasassbeh[33].A neural network has been used to build the classification model. The proposed model achieved high precision in the identification and detection of Malicious Traffic at a low false-negative rate at a rate of 98.3%.

Sharma et al.[34]showed that the analysis of the volume could not detect sorts of network abnormalities entirely. Researchers have been able to analyze network anomalies using services such as the SNMP, DNS and Network Time Protocol. Moreover, NfDump machine learning was used for storing and processing network packets.

R. Suganya[35]has adopted a new hybrid approach through the incorporation of two approaches (misuse-based and network detection) to permit the frame-built for traffic detection and attacks without any prior knowledge. The idea behind this approach is that legitimate and malicious traffic should be classified and segregated in order to use regular traffic during anomaly detection. The authors were able to detect attacks with an appropriate system, as the hybrid module found that network attacks are detected more easily than isolated methods (network malfunctions and anomaly detections).

Namvarasl and Ahmadzadeh have implemented a new IDSmethodusingmachine-learning and SNMP[36]. In the proposed approach, DoS and DDoS attacks are detected and estimated in real-time. Based on three submodules, the authors developed their approach. Initially, the MIB features were taken from a variety of categories (C4.5 and Ripper). The detection technique for intruders was set to a selected DoS attack vector where four MIB classes (ICMP, TCP, IPand UDP) were allocated a set of 66 variables.

Based on the previous studies, our contributions in this paper are twofold. Firstly, design a new detection model for the DoS attacks that overwhelmed the existing models. Secondly, to overcome the disadvantage of using a single classifier in the previous models, a StackNet model has been used in order to increase the classification accuracy or minimize regressor failure. In this study, the accuracy of the model suggested has been evaluated and mapped using normal and general datasets with 34 MIB variables.

3. Application layer DoS attack detection approach

This section is divided into three main sections, starting from a short summary of the used dataset. The second section clarified StackNet classifiers in their entirety for classifying the dataset and determining whether legitimate traffic or attack occurs. Lastly, the evaluation metrics are listed with the results and discussions.

3.1. SNMP-MIB Dataset

Al-Kasassbeh et al. create sufficient datasets to resolve resource constraints in previous data sets [37]. In order to test the SNMP for network abnormality behaviour, they have implemented a robust SNMP-MIB data set. SNMP-MIB data have been obtained by the authors using a number of DoS and brute-force attacks. The data set collected contains 34 MIB variables comprising 4,998 records. The classes of the MIB are called ICMP, IP, TCP, UDP and Socket.SNMP-MIB datasets were used in this study for the assessment and implementation of the detection approach. The set of data we based on contains 4,998 records of six major types of attacks such as UDP, ICMP Echo, HTTP, TCP-SYN, Sloloris and Slowpost. as shown in Table 1.

Table 1: Traffic type and number of generated records

No.	Traffic Label	Traffic count
1	Normal	600
2	ICMP-Echo Attack	632
3	TCP-SYN Attack	960
4	UDP Flood Attack	773
5	HTTP Flood Attack	573
6	Slowloris Attack	780
7	Slowport Attack	480
8	Brute Force Attack	200

3.2. StackNetClassifiers

StackNet[38] is a machine learning technique that behaves as a feed-forward neural network. StackNetuses the stacked generalization of Wolpert[39] at several levels to increase the classification accuracy or minimize regressor failure. Similar tobackward propagation in the training phase, StackNet is designed iteratively one layer per layer (using stacked generalization) and each layer uses the final goal.

There are two separate StackNet modes: Firstly, each level uses the predictions of only one previous layer explicitly, and Secondly, each layer uses the predictions of all prior levels

including the restacking mode input layer. StackNet is typically better than the best single-layer layout. Their performance remains based on a combination of strong and various single models, to make the best of this meta-modelling methodology.

The proposedStackNet model is shown in Figure 1. The model contains three layers, and 11 models are composed. Such models include one regressor of the Bayesian ridge [40]; four regressors of random forests[41]; three regressors of extra-trees[42]; one regressor boosting grade[43]; one regressor kernels[44]; and one regressor slope. The first layer

is equipped with one linear regressor and five ensemble-based regressors; the second with one linear regressor and two ensembles, and the third with only one linear regressor. The predictions from all previous layers, including the input one, are used for each layer.

3.3. Evaluation Metrics

The model output was calculated employing a variety of well-known criteria, such as accuracy, precision, the area under the
roc curve, and detection rates. The efficiency of the classifier has been calculated according to the matrix of confusion:

1. $$Accuracy = \frac{TP+TN}{TP+FN+TN+FP} \quad (1)$$

   Where FP, TN, TP and FN represent False Positive, True Negative, True Positive, and False Negative, respectively.

2. **Detection rate (TPR)**, also called recall, indicates the percentage of malicious instances that were predicted as malicious[45].

$$TPR = \frac{TP}{TP+FN} \quad (2)$$

3. **False-positive rate (FPR)** is the ratio of items incorrectly classified as an attack to all items that belong to normal and can be written as:

$$FPR = \frac{FP}{FP+TN} \quad (3)$$

4. **Precision** indicates the percentage of instances correctly classified as a positive instance**.**

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

5. The Curve area (AUC) is an output metric for classification problem at different threshold settings. ROC is a probability curve, and AUC is the degreeof separability measure. It shows how much model is able to differentiate between classes. The higher the AUC, the stronger the 0s as the 0s and 1s as the 1s are expected[46].

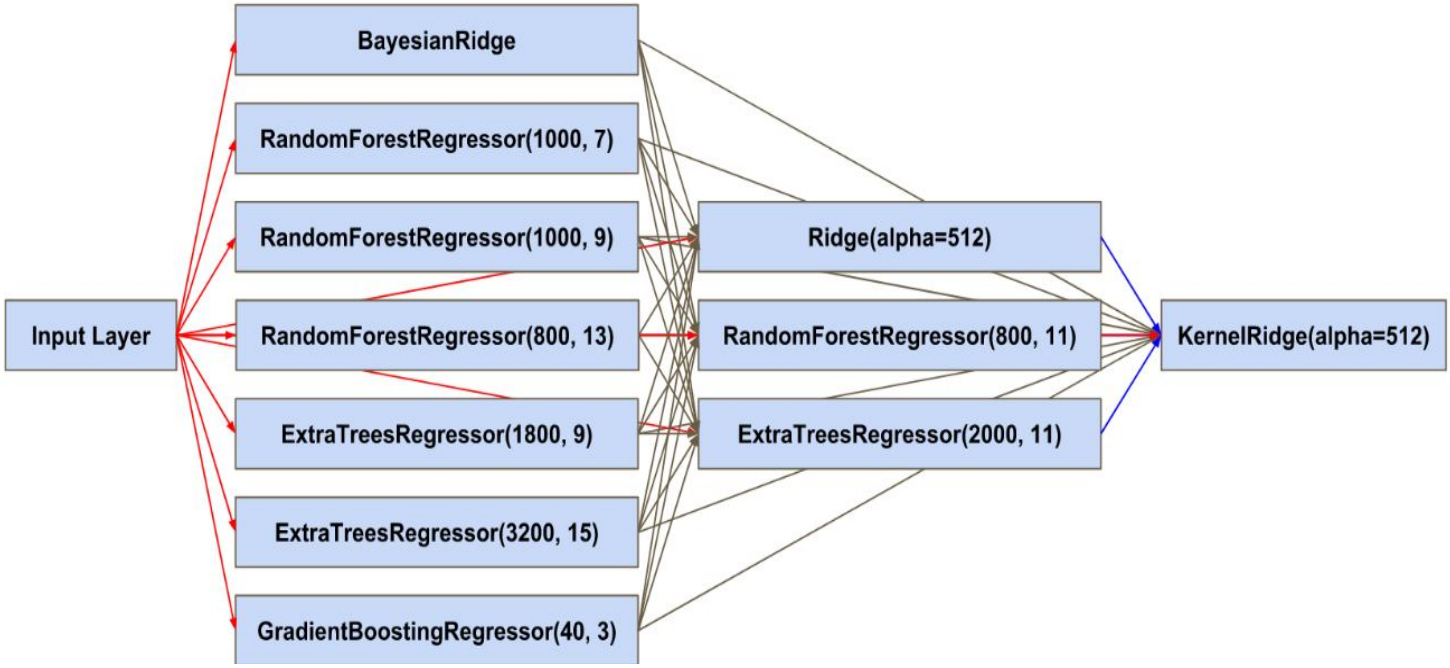

Figure 1: The architecture of the proposed StackNet[47] for DoS attack detection

3.4. Results

The tests and performance were measured using the 64-bit Intel ® CoreTM i7 processor with a Windows 10 8 GB of RAM. The results of the proposed model relied on the MIB dataset referred to above in the previous section. The techniques of classification were then applied individually to each group. Table 2 displays the ability of different classifiers to detect DoS in terms of accuracy, TPR, FPR, precision, F-measure, AUC, and RMSE. The results show that the StackNet outperform other classifiers in terms of all metrics.

As shown in Table 2, the adapted approach achieves higher performance compared with other machine learning algorithms. However, we conduct our experiments using machine learning algorithms that used for IDS, such as Decision Tree Classifier[48], SVM [49]**,** K-Neighbors Classifier [50]**.** The accuracy of the proposed model is 99.38% which is better than other classification algorithms, as shown in Figure 2. In addition, as shown in Figure 3, the approach proposed achieves the best AUC performance in comparison with other machine methods.

Table 2: Experimental results

Classifiers	Accuracy	TPR	FPR	Precision	F-measure	AUC	RMSE
SVM	0.90134	0.91291	0.18364	0.97333	0.94216	0.86464	0.09866
KNN	0.95657	0.96703	0.1202	0.98335	0.97512	0.92342	0.04343
Decision Tree	0.98719	0.98719	0.00841	0.99385	0.99272	0.97326	0.01281
StackNet	0.9938	0.9938	0.00455	0.99749	0.99647	0.98854	0.0062

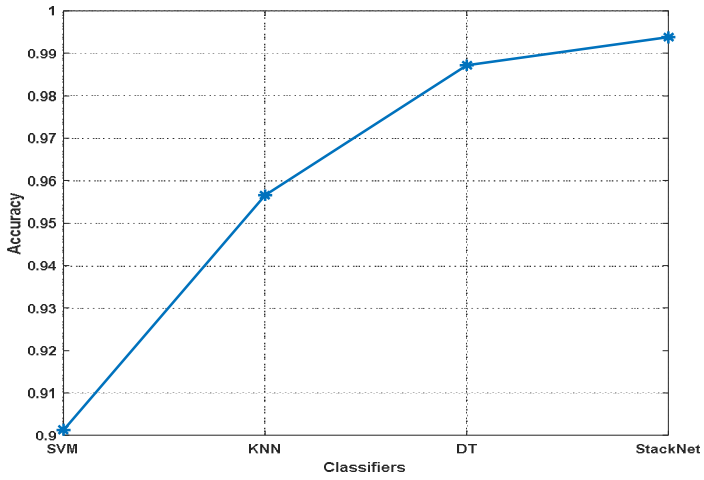

Figure 2: Accuracy of the proposed model in comparison with other classification algorithms

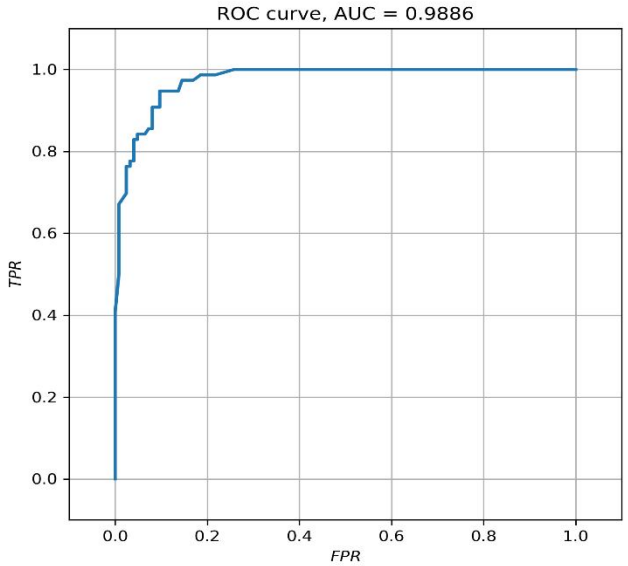

Figure 3: Area under ROC

Table 3 shows outcomes and comparison of the proposed model with those of previous work; the DoS attacks were mainly collected from SNMP-MIB [37] and MIB variables. The results show that the detection mechanisms based on machine learning outperform other techniques as the detection model can adapt its detection rules based on new attacks behaviour, as seen in the collected dataset. Moreover, the proposed model based on StackNet can achieve even a higher result since the model built using StackNet that encompasses a list of classifiers can overpass the short comes of any single classifier.

Table 3: Comparison of our approach with previous studies

Author	Technique	Classifier	Dataset	Results
Al-Kasassbeh[33]	Machine Learning	ANN	SNMP-MIB [37]	Accuracy 98.38%
C. Rahmani et al. [27]	Statistical	None	MIB variables extracted from real-time traffic	Fitted value 90.59% for UDP flood, SYN flood, ICMP flood and

				Smurf attacks
T.P. Vuong et al. [51]	Knowledge-Base	DECISION TREES	MIB variables extracted from real-time traffic	Accuracy 93.81%
Kirichenko et al. [52]	Knowledge-Base	Random Forest	SNMP-MIB [37]	TPR 92.2%
Proposed Approach	Machine Learning	StackNet	SNMP-MIB [37]	Accuracy 99.3%FPR 0.4%

4. CONCLUSION

Data filtering is essential to protect networks from various forms of attack that destroy sensitive data and cause severe losses for organizations. Several techniques for detecting network anomalies have therefore been implemented so that the network system will operate normally without any interference or data interruption. It was noticed in this paper that StackNet handles all DoS attacks efficiently. Further, improve their ability to detect all and new types of attack types, the SNMP-MIB variables should be improved for future work.

REFERENCES

1. Alauthman, M., et al., *An efficient reinforcement learning-based Botnet detection approach.* Journal of Network and Computer Applications, 2020. **150**: p. 102479. https://doi.org/10.1016/j.jnca.2019.102479
2. Ammar, A., et al., *An Online Intrusion Detection System to Cloud Computing Based on Neucube Algorithms.* International Journal of Cloud Applications and Computing (IJCAC), 2018. **8**(2): p. 96-112.
3. Alauthaman, M., et al., *A P2P Botnet detection scheme based on decision tree and adaptive multilayer neural networks.* Neural Computing and Applications, 2018. **29**(11): p. 991-1004. https://doi.org/10.1007/s00521-016-2564-5
4. Al-Kasassbeh, M., et al., *Feature Selection Using a Machine Learning to Classify a Malware*, in *Handbook of Computer Networks and Cyber Security: Principles and Paradigms*, B.B. Gupta, et al., Editors. 2020, Springer International Publishing: Cham. p. 889-904.
5. Alieyan, K., et al., *DNS rule-based schema to botnet detection.* Enterprise Information Systems, 2019: p. 1-20.
6. Alauthman, M., et al., *Machine Learning for phishing Detection and Mitigation.* Machine Learning for Computer and Cyber Security: Principle, Algorithms, and Practices, 2019: p. 26. https://doi.org/10.1201/9780429504044-2
7. Alieyan, K., et al. *Botnets Detecting Attack Based on DNS Features.* in *2018 International Arab Conference on Information Technology (ACIT)*. 2018. IEEE.
8. Alnawasrah, A., et al. *Fast flux botnet detection framework using Adaptive dynamic evolving spiking neural network algorithm*. in *2018 9th International Conference on Information and Communication Systems (ICICS)*. 2018.
9. Alkasassbeh, M. and M. Almseidin, *Machine Learning Methods for Network Intrusion Detection.* International Journal of Computer and Information Engineering, 2018. **12**(8): p. 614-619.
10. Almomani, A., et al., *An Online Intrusion Detection System to Cloud Computing Based on Neucube Algorithms.* International Journal of Cloud Applications and Computing (IJCAC), 2018. **8**(2). https://doi.org/10.4018/IJCAC.2018040105
11. Alauthman, M., *An efficient approach to online bot detection based on a reinforcement learning technique*. 2016, Northumbria University.
12. Al-Qerem, A., et al., *Network-Based Detection of Mirai Botnet Using Machine Learning and Feature Selection Methods*, in *Handbook of Research on Multimedia Cyber Security*. 2020, IGI Global. p. 308-318.
13. Al Ashhab, Z., M. Anbar, and M. Mahinderjit, *S., K. Alieyan and WI Abu Ghazaleh, Detection of HTTP Flooding DDoS Attack using Hadoop with MapReduce: A Survey*. International Journal of Advanced Trends in Computer Science and Engineering, 2019. **8**(1). https://doi.org/10.30534/ijatcse/2019/12812019
14. Ray, D.E., et al., *2016 Cost of Data Breach Study: Global Analysis*, in *Valuing Data: An Open Framework*. 2018, Ponemon Institute LLC Bradley Beach, NJ. p. 1-8.
15. Al-Nawasrah, A., et al., *A Survey of Fast Flux Botnet Detection With Fast Flux Cloud Computing.* International Journal of Cloud Applications and Computing (IJCAC), 2020. **10**(3): p. 17-53.
16. ALAUTHMAN, M., *Botnet Spam E-Mail Detection Using Deep Recurrent Neural Network.* International Journal, 2020. 8(5).

https://doi.org/10.30534/ijeter/2020/83852020

17. Alauthman, M. and G. Albesani, *Application-Layer Dos Attack Detection Using Machine Learning.* Proceedings Book, 2019: p. 58.
18. Al-Kasassbeh, M., et al., *Detection of IoT-botnet attacks using fuzzy rule interpolation.* Journal of Intelligent & Fuzzy Systems, 2020. **Preprint**: p. 1-11.
19. Almousa, M., *Analyzing Cyber-Attack Intention for Digital Forensics Using Case-Based Reasoning.* International Journal of Advanced Trends in Computer Science and Engineering, 2019. **8**: p. 3243-3248. https://doi.org/10.30534/ijatcse/2019/92862019
20. Thottan, M. and C. Ji, *Anomaly detection in IP networks.* IEEE Transactions on signal processing, 2003. **51**(8): p. 2191-2204.
21. Yu, J., et al., *Traffic flooding attack detection with SNMP MIB using SVM.* Computer Communications, 2008. **31**(17): p. 4212-4219.
22. Hwoij, A., M. Al-Kasassbeh, and M. Al-Fayoumi, *Detecting Network Anomalies using Rule-based machine learning within SNMP-MIB dataset.* arXiv preprint arXiv:2002.02368, 2020.
23. Alkasassbeh, M.S. and M.Z. Khairallah, *Network Attack Detection With SNMP-MIB Using Deep Neural Network*, in *Handbook of Research on Intrusion Detection Systems.* 2020, IGI Global. p. 66-76.
24. Manna, A. and M. Alkasassbeh. *Detecting network anomalies using machine learning and SNMP-MIB dataset with IP group*. in *2019 2nd International Conference on new Trends in Computing Sciences (ICTCS)*. 2019. IEEE.
25. Sharafaldin, I., et al. *Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy*. in *2019 International Carnahan Conference on Security Technology (ICCST)*. 2019. IEEE. https://doi.org/10.1109/CCST.2019.8888419
26. Bhuyan, M.H., et al., *Detecting distributed denial of service attacks: methods, tools and future directions.* The Computer Journal, 2014. **57**(4): p. 537-556.
27. Rahmani, C., M. Sharifi, and T. Tafazzoli. *An exprimental analysis of proactive detection of distributed denial of service attacks.* in *Proceedings of the IIT Kanpur Hacker's Workshop (IITKHACK04)*. 2004.
28. Wu, Q. and Z. Shao. *Network anomaly detection using time series analysis.* in *Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services-(icas-isns' 05)*. 2005. IEEE.
29. Garber, L., *Denial-of-service attacks rip the Internet.* Computer, 2000(4): p. 12-17.
30. Rao, S. and S. Rao, *Denial of Service attacks and mitigation techniques: Real time implementation with detailed analysis.* This paper is from the SANS Institute Reading Room site, 2011.
31. Bao, C.-M. *Intrusion detection based on one-class svm and snmp mib data*. in *2009 Fifth International Conference on Information Assurance and Security*. 2009. IEEE.
32. Al-Naymat, G., M. Al-Kasassbeh, and E. Al-Harwari, *Using machine learning methods for detecting network anomalies within SNMP-MIB dataset.* International Journal of Wireless and Mobile Computing, 2018. **15**(1): p. 67-76.
33. Alkasassbeh, M., *A novel hybrid method for network anomaly detection based on traffic prediction and change point detection.* arXiv preprint arXiv:1801.05309, 2018. https://doi.org/10.3844/jcssp.2018.153.162
34. Sharma, R., A. Guleria, and R. Singla, *Characterizing Network Flows for Detecting DNS, NTP, and SNMP Anomalies*, in *Intelligent Computing and Information and Communication*. 2018, Springer. p. 327-340.
35. Suganya, R., *Denial-of-Service Attack Detection Using Anomaly with Misuse Based Method.* International Journal of Computer Science and Network Security, 2016. **16**(4): p. 124-128.
36. Namvarasl, S. and M. Ahmadzadeh, *A dynamic flooding attack detection system based on different classification techniques and using SNMP MIB data.* International Journal of Computer Networks and Communications Security, 2014. **2**(9): p. 279-284.
37. Al-Kasassbeh, M., G. Al-Naymat, and E. Al-Hawari, *Towards generating realistic SNMP-MIB dataset for network anomaly detection.* International Journal of Computer Science and Information Security, 2016. **14**(9): p. 1162.
38. Michailidis, M., *Stacknet, meta modelling framework*. 2017.
39. Wolpert, D.H., *Stacked generalization.* Neural networks, 1992. **5**(2): p. 241-259.
40. MacKay, D.J., *Bayesian interpolation.* Neural computation, 1992. **4**(3): p. 415-447.
41. Breiman, L., *Random forests.* Machine learning, 2001. **45**(1): p. 5-32.
42. Goetz, M., et al., *Extremely randomized trees based brain tumor segmentation.* Proceeding of BRATS challenge-MICCAI, 2014: p. 006-011.
43. Friedman, J.H., *Greedy function approximation: a gradient boosting machine.* Annals of statistics, 2001: p. 1189-1232.
44. Ghahramani, Z., *Probabilistic machine learning and artificial intelligence.* Nature, 2015. **521**(7553): p. 452.
45. Smadi, S., N. Aslam, and L. Zhang, *Detection of online phishing email using dynamic evolving neural network based on reinforcement learning.* Decision Support Systems, 2018. **107**: p. 88-102. https://doi.org/10.1016/j.dss.2018.01.001

46. Smadi, S., et al. *Detection of phishing emails using data mining algorithms*. in *2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA)*. 2015. IEEE.
47. Kao, P.-Y., et al., *Predicting Fluid Intelligence of Children using T1-weighted MR Images and a StackNet.* arXiv preprint arXiv:1904.07387, 2019.
48. Safavian, S.R. and D. Landgrebe, *A survey of decision tree classifier methodology*. IEEE transactions on systems, man, and cybernetics, 1991. **21**(3): p. 660-674.
49. Nagunwa, T., et al. *A Framework of New Hybrid Features for Intelligent Detection of Zero Hour Phishing Websites*. in *International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)*. 2019. Springer.
50. Sarkar, M. and T.-Y. Leong. *Application of K-nearest neighbors algorithm on breast cancer diagnosis problem*. in *Proceedings of the AMIA Symposium*. 2000. American Medical Informatics Association.
51. Vuong, T.P., et al. *Decision tree-based detection of denial of service and command injection attacks on robotic vehicles*. in *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*. 2015. https://doi.org/10.1109/WIFS.2015.7368559
52. Kirichenko, L., T. Radivilova, and V. Bulakh, *Machine learning in classification time series with fractal properties.* Data, 2019. **4**(1): p. 5. https://doi.org/10.3390/data4010005