A Study On Existing Challenges In Safeguarding Networks From Intruders And Malicious Invasions With Adaptive Solutions

P. Ramachandran ,
Research Scholar ,PG and Research ,Department of Computer Science
J.J.College of Arts and Science (Autonomous), Pudukkottai.
Dr. R. Balasubramanian
Ph.D, Research Guide and Professor, PG and Research ,Department of Computer Science, J.J.College of Arts and Science (Autonomous)
Pudukkottai.

Abstract:

Internets and Networks have been growing steadily over the years but have grown exponentially in the recent decade due to a variety of reasons. For Example, the growth of social media, e-commerce, Internet based video channels, online education and many more. Though at the outset, everything looks fine, these networks face a major challenge in terms of security and cyber attacks which have also been evolving along with internet growth. Cyber attacks have grievous consequences and disastrous effects on networks. Malwares are primary weapons in such attacks on networks. They exploit existing networks vulnerabilities or utilize emerging technologies. Provisioning networks with security is a major challenge. Thus, effective malware defence mechanisms are the need for the hour. This highlights various studies that have been proposed in securing networks with possible safeguarding solutions. This paper also highlights various datasets used in network intrusion proposals.

Keywords: *Malware, Intrusion detection system, NSL_KDD, KDD Cup 99, Network security, Machine learning, deep learning*

Article Received: 18 October 2020, Revised: 3 November 2020, Accepted: 24 December 2020

Introduction:

Internet is an indispensable element of current computer systems generating internet traffics that are often voluminous. Also, CC (Cloud Computing) with its vast resources have contributed towards increase of network traffics. Thus, the internet is loaded with volumes of data which are transferred in terra bytes on a daily basis. CC data volumes from clouds is expected to increase at least 100 times by 2022 [1]. Thus, these voluminous data on networks presents many challenges of which security from malware attacks is the most important challenge. Malware can be defined as any malicious program that creates havoc in computer systems. Malwares keep changing and evolving consistently as network environments evolve. In spite of anti-malware measures, attackers have been consistent in their efforts to cripple networks and computer systems. As new technologies evolve, new forms of attacks originate sidelining current security mechanisms like firewalls or anti-viruses [2]. Cyber attacks target any new technological innovation like focusing more towards discrete infections through IoTs (Internet of Things). Damages caused by attacks is may cross 3 trillion by the end of 2021 [3]. Figure 1 depicts the attacks on computer ports.

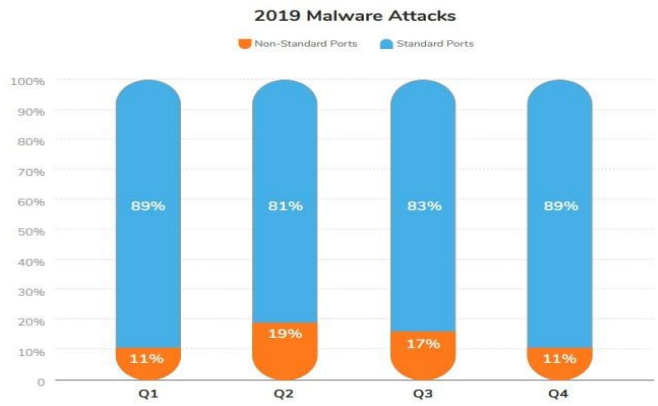


Fig. 1 – Malware Attacks on Ports [https://www.comparitech.com/antivirus/malware-statistics-facts/]

There is an increasing demand for proficient security systems. IDSs (Intrusion Detection Systems) have been playing an important role in cyber security IDSs have also been implemented using DMTs (Data Mining Techniques) including DLTs (Deep Learning Techniques). DLTs are a part of AIs (Artificial Intelligence) where they have the capability to learn from input data and classify them. When applied on dynamic data like network traffic flows, AIs can be very useful in identifying and classifying abnormal or malicious or anomalous data. Hence, intelligent and self-learning IDSs have been implemented along with existing security software as their combined capability helps in guarding networks. IDSs detect unwelcome behaviours in networks based on signatures or anomalies. Table 1 lists comparisons between these types [4].

Table 1 - Comparison of IDSs

Signature-based	Anomaly-based
Uses contextual references to detect previously known attacks	Identifies known and new or unnamed attacks based on anomalous behavior/packets
Software is implemented on major operating systems which is then used to detect attacks	The dependency on operating systems is low while examining network patterns is more
The reference signature database needs to be updated about new patterns or signatures	New pattern profiles are built, observed and then used for detections
Protocols are not included in these systems	Protocols are analyzed for packet information

This paper contributes in terms of IDS related studies, Datasets used in Evaluations and pros and cons of IDSs. The next section is a review of studies related to IDSs followed by DLTs proposed for IDS. Datasets are detailed in section four. Section five is results and discussions and the paper concludes subsequently.

2. Studies on IDSs

Networks have always been guarded by strong firewalls and anti-malware software. Users need authentications, packets transmitted after encryptions and monitoring network flows have been regular affairs in cyber security. But, these security measures lose focus with evolving technologies as intruders keep finding innovative ways to invade networks using new technologies [5] making development of very strong procedures a must to guard networks against attacks. IDSs have managed to detect new kinds of attacks when implemented. The earliest implementation of IDSs for network security used MLTs, DTs (Decision Trees) using Bagged boosting [6] and Kernel Miner [7]. The study in detailed on MLTs which used multiple datasets for IDS implementations [8]. Figure 2 depicts a range of MLTs used for IDS implementations.

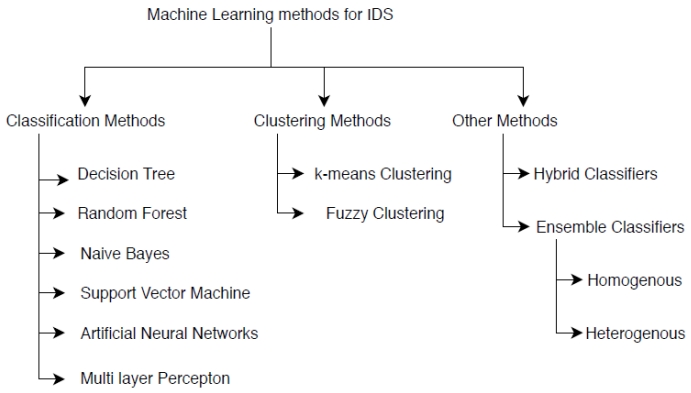


Fig. 2 – MLTs for IDSs

NB (Naive Bayes) classified attacks from previously selected features based on vitality using the NSL-KDD dataset in [9]. The proposed hybrid scheme showed above 97% accuracy in simulations. The same dataset was used in [10] for KMC (K-Means Clustering). Twenty percent of the samples were split into four groups for analysis and the detection results were satisfactory. A semi-supervised MLT scheme based on Fuzzy NNs (Neural Networks) was used in [11] for evaluating unlabeled instances from NSL-KDD dataset. The scheme trained using single-layer FFNN (Feed Forward NN) for generating membership vectors. The proposal showed unlabeled instances was classified better due to the use of fuzzy values. The study in [12] also used NSL-KDD dataset for its binary classification. The proposal used greedy random searches for building RF (Random Forest) trees which were then classified. The scheme used multiple techniques namely IG (Information Gain), SU (Symmetrical Uncertainty), and correlations for its feature selections. Their scheme outperformed other single MLTs including RF, NB and MLP (MultiLayer Perceptron) in terms of classification accuracy. Profiling was the main element in the study in [13] where Extreme MLTs detected intrusions by applying alpha profiles online while beta profile minimized training samples. Features were reduced using a combination filters and correlations. The scheme showed 98.6% accuracy on the NSL-KDD dataset while clocking 96.37% accuracy on the Kyoto University dataset.

3. IDSs using DLTs

IDSs are used to monitor networks. They raise alarms by sending alerts as soon as they sense unwanted or malicious activity on the network. IDSs are programmed using MLTs (Machine Learning Techniques) which follow distinct steps in their modelling namely Network Packet Captures, Analysis of captured Network Packets, Matching known attack patterns and Generating alerts. IDSs capture network packets using sniffing tools which are then filtered and examined where filtering is checking known signatures from database. Figure 3 depicts IDS operations.

Fig. 3 - IDS operations

MLTs do efficiently detect real network traffic intrusions and are tuned to identifying attacks like DoS, probes, U2R and R2L. Many MLTs work on classification based on feature sets without depth in contrast to DLTs which learn first before classifying. Moreover, accuracy of detecting intrusions that occur in real-time networks is based on finding the attack type which is a crucial task as some may be

missed while classifying attacks [14]. DLTs are used for their capability to learn like the human brain and classify. They use multiple layers to evaluate and combine these results of these layers for a final output. The study in [15] reviewed the use of DLTs in healthcare including DBNs (Deep Belief Networks), DBMs (Deep Boltzmann Machines), CNNs (Convolution Neural Networks) and RNNs (Recurrent Neural Networks). The study in [5] used DBNs where RBM (Restricted Boltzmann Machine) was used for the network's layers. AEs (Auto Encoders) used in [7] identified invariant features for monitoring faulty sensor signals. The scheme de-noised signals which were stacked as layers. The model also learnt global features thus proving its applicability to complex input data like multivariate time-series data. Short messages were audited using RNNs in [16]. The study classified prisoner sent messages as safe/non-safe as a part of security audits. Message features were extracted using word2vec and mapped as vectors which were then classified by RNNs. DNNs figured in the study [17] which was proposed for CC platforms. The proposal detected characters, localized information and segmented significant features. The model recognized licensing details in very challenging situations like congested traffic, multiple copies of licensed images, and distortions of multiple kinds in these images. RBM with one hidden layer was used by the study in [18]. The network was used to reduce dimensionality. The study also used LR (Logistic Regression) with soft-max for multi-class classifications. DLT was also used in [19] which proposed a flexible NIDS (Network IDS). The scheme used AEs and soft-max regression. The learner/classifier used was STL (Self-taught Learning) and tested with NSL-KDD for its ability to detect network intrusions. DNNs can also be used in parallel computing environments as demonstrated in [20]. The study's scheme used multi-core CPU/ GPU to evaluate DNN based IDS on voluminous network data. The results showed DLTs capability exploit parallel computing for desired results on network intrusions. Another DLT, Replicator Neural Networks , detected anomalies in networks encumbering wide range of attacks in [21]. The approach used unlabeled data and could detect network-wide anomalies without any presumptions on attack types.

4. IDS Datasets

The creation of an IDSs dataset includes network information collected from multiple sources like hosts, packets, destinations, connection, transmission duration, systems, system configurations etc [22]. Maximum network information is gathered to study patterns when networks are attacked or learn more about abnormal behaviours of networks. This set of information can be collected by recording and monitoring networks based on switches or routers data. On collecting switch/router information all outbound/inbound network flows are analyzed. This analysis termed Flow analysis examines Source/destination IP addresses, port numbers, network service types etc.[23]. Certain information can be collected only from hosts like for example, failed login attempts which can indicate that intrusions have been attempted. Thus, the datasets generated for evaluating IDSs have been generated from real network traffic. The preliminary dataset for IDS testing, DARPA, funded by DARPA, was generated in 1998 by MIT Lincoln Laboratory [24]. DARPA dataset's tcp dump files were refined to create the KDD CUP 99 d in 1999 by University of California researchers [25]. This dataset with duplicates and redundant data, was again refined to create new NSL-KDD dataset [26]. The dataset DEFCON was created for evaluating correlations in IDS alerts. Network packet's flag details were used to define port scanning and buffer overflow attacks [27]. Network packets flows were used in the creation of CAIDA by the Center of Applied Internet Data Analysis [28] and LBNL by Lawrence Berkeley National Laboratory [29]. CDX dataset was created for a network warfare competition by The US military academy which was subsequently used for IDS alert rule evaluations [30]. Honeypot activities at universities were monitored and analyzed by the creation of Kyoto dataset [31] and Twente dataset [32]. Trace files of network packets and wireless networks were used to create the UMASS dataset was wireless applications [33] where their alpha/beta profiles resulted in the ISCX IDS 2012 dataset [34]. System calls and attack pattern analysis led to the creation of the AFDA dataset [35]. Canadian Institute of Cyber Security introduced the latest datasets for analyzing techniques on intrusion detection and IDS evaluation called CIC-IDS-2017 and CSE-CIC-IDS-2018 [36]. Thus, datasets have been evolving over the years in an attempt to strengthen cyber security and helping

in evaluating proposed studies on IDSs. Table 2 lists the datasets and their details.

Table 2 – IDS/Intrusion Detection Datasets

Dataset Name	Developed By	Features	Attack types	Description
DARPA	MIT Lincoln Laboratory	41	Dos, Probe R2L,U2R,	It does not represent real network traffic, absence of false-positive instances, irregularities in attack data instances.
KDD CUP 99	University of California	41	Dos, Probe, R2L,U2R,	It consists of redundant and duplicate data samples-
NSL-KDD	University of California	41	Dos, Probe R2L,U2R,	Refined version of KDD CUP 99 dataset and con sist of a limited number of attack types.
DEFCON	Shmoo Group	Flag traces	Telnet Protocol Attacks	Features are captured through the "Capture the Flag" competition.
LBNL	Lawrence Berkeley National Laboratory	Internet traces	Malicious traces	It consist of 100 hours of activity specifying the traces of packet header for identifying malicious traffic.
CDX	United Military States Academy	5	Buffer Overflow	This dataset utilized network tools Nikto and Nes sus to capture the traffic and was used to evaluate the IDS alert rules
Kyoto	Kyoto University	24	Normal and Attack sessions	It was developed by deploying honeypots in the network but do not describe any details about the attack types.
Twente	Twente University	IP flows	Malicious Side effects Unknown traffic, and Uncorrelated alerts	The size of the dataset is small and scope of attack types is limited
ISCX2012	University of new Brunswick	IP flows	DoS, DDoS, Brute-force, Infiltration	This dataset consist of network scenarios with in-trusive activities and labeled data instances
AFDA	University Of New SOUTH Wales	System call traces	Zero-day attacks, Stealth attacks, C100 Webshell attack	This dataset consists of 10 attacks vectors a a limited range of attacks
CIC-IDS-2017	Canadian Institue Of Cyber	80	Brute force, Portscan, Botnet, Dos, DDoS, Web Infiltration	Network profiles are used to generate the dataset in a specific manner.

Even though the datasets are created from network data, application of viable techniques is also an important part of evaluations. Multitude of techniques that have been successfully applied in intrusion detections [37], [38], [39]. DMTs proposed for these datasets work on labelled data and classify attacks based on their learning where features help them classify attacks from normal traffic [40]. These generated datasets carry sufficient information as they are built from real-time data , thus paving the way for IDS implementations. DLTs split the datasets into two main parts name ly training and testing. The split may be 60/40 or 70/30 or 80/20. Certain techniques need larger number of training samples to learn and this learnt knowledge is then uses to test or classify information. Thus, many IDSs proposed have targeted variety of attacks as listed in the above table. Algorithmic performances also need to be evaluated using appropriate performance metrics where accuracy is the most common metric in evaluations [41]. Accuracy also depends on the method, test/train splits and selected features of the dataset taken for evaluations [42], [43]. Hence, most proposals depict multiple performance metrics including accuracy to project the validity of proposed schemes.

5. Results and discussions

This section displays results of studies as figures or tables which depict their performances. Multitude of algorithms have been used or proposed for intrusion detections. These algorithms or techniques work on certain types of information from datasets as detailed below

- Basic Information: TCP/IP protocol's connection parameters when communications occur.
- Host Information: The server or computer through which or to which connections are made and its log has details on logins including failed attempts or network failures or services running in the system.

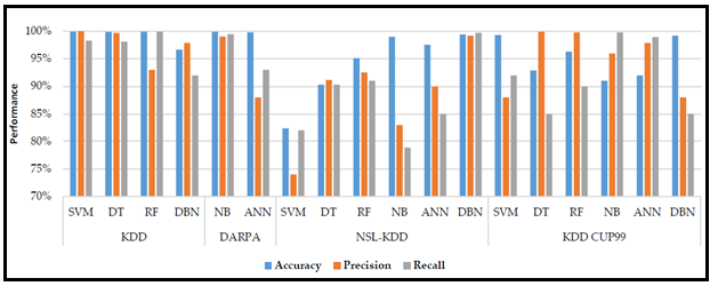
- Traffic Information: Logs or information on packets flows including hosts and destinations.

Researches post their results on several performance metrics like Precision, classification of true occurrences, Recall, the ratio between correct identification and total instances, Accuracy, exact classification of samples. Table 3 lists comparative performances of classifiers [44].

Table 3 – Comparison of MLT performances on IDS

Model	Dataset NO	Precision	Recall	Building Time
NB	1	0.653	0.653	34.46 s
	2	0.769	0.701	90.32 s
	3	0.627	0.672	32.82 s
MLP	1	0.671	0.702	470.84 s
	2	0.622	0.684	797.43 s
	3	0.965	0.972	477.18 s
J48	1	0.987	0.987	155.54 s
	2	0.821	0.791	347.82s
	3	0.539	0.384	168.56s
NB Tree	1	0.778	0.731	1607.98s
	2	0.813	0.777	4411.04 s
	3	0.657	0.76	1213.67 s
RF	1	0.782	0.726	433.25 s
	2	0.795	0.727	598.41 s
	3	0.979	0.979	327.46 s

Intrusions can be detected by examining network packet information. Figure 3 depicts comparative performances of IDSs basedon MLTs and DLTs.



. Fig. 3 - Comparative performances of IDSs based on MLTs and DLTs

Network intrusions often steal network resources or data jeopardizing its security thus cyber security can explained in two terms detection and prevention. IPSs (Intrusion Prevention System) are prevention

tools against attacks on networks. These tools drop malicious packets, jam offending IPs and alert about possible attacks. IPSs and IDSs may be the same at the outset, but are actually very different. IDSs work passively examining information in network packets while IPSs are proactive with direct actions and are extensions of IDSs. What is more important is the fact that networks can be guarded with certain safety measures as listed below

- **Password policies:** Maintaining complex/unpredictable passwords is a preliminary and important step in safeguarding networks. They need to be changes regularly as strong passwords are one of the best measures for preventing attacks.
- **OS (Operating System) Updates:** Oss have regular updates from their manufacturers informing users on new patches or updates for their software. Regular OS updates are important for guarding networks.
- Guarding the Router: Routers function automatically. They do not discriminate users while connecting or getting connected during transmissions. They open to misuse and hence network can transmit information using encryptions for data safety.
- **Backups:** Data is an invaluable asset and should be backup on a regular basis for restorations after attacks.
- **Employee Vulnerability:** The weakest point in the networks are employees who allow compromise of information due to their lack of knowledge or priorities or carelessness or laziness . They have to be educated about cyber security.
- **Response Time:** Administrators receiving IDS alerts should act immediately and verify even if the warnings are pseudo in nature. They need to develop breach response plan in advance using IDSs or IPSs.
- **Centralized firewalls:** These are the frontline soldiers in the battle. Configuring a firewall as guarding wall with multiple levels of trust is a vital part of network guards.
- **Proactive Auditing:** Regular audits of networks can project intrusions, locations, attack types and intervals. Thus, regular audits can help in safeguarding networks.

CONCLUSION

Networks have been targeted by cyber criminals for a long time. These intruders use sophisticated techniques for their tasks. History has shown that several organizations have lost billions of dollars by way of ransom attacks and network intrusions. Researches have also been evolving in network intrusions. This paper has detailed on several studies and by categorizations of studies. The study has also explained about datasets used in IDS evaluation, their creation reasons, style and usage. Several MLTs and DLTs that were proposed for network safety have been explained. Thus, thi paper concludes that IDSs can identify attacks in advance if implemented properly. The study has also proposed few safeguarding steps for preventing intrusions in networks.

References:

[1] Miller NJ, Aliasgari M. Benchmarks for evaluating anomaly-based intrusion detection solutions. California State University, Long Beach; 2018.

[2] Scaife N, Carter H, Traynor P, Butler KR. Cryptolock (and drop it): stopping ransomware attacks on user data. In: 2016 IEEE 36th International Conference on Distributed Computing Systems (ICDCS). IEEE; 2016. p. 303–312.

[3] Stevens T. Cyber security and the politics of time. Cambridge University Press; 2016.

[4] B, Agrawal DP, Yamaguchi S. Handbook of research on modern cryptographic solutions for computer and cyber security. IGI global; 2016.

[5] B. Dong and X. Wang, “Comparison deep learning method to traditional methods using for network intrusion detection,” in Proc. 8th IEEE Int.Conf. Commun. Softw. Netw, Beijing, China, Jun. 2016, pp. 581–585.

[6] R. Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, “Deep learning and its applications

to machine health monitoring: A survey," Submitted to IEEE Trans. Neural Netw. Learn. Syst., 2016.

[7] H. Lee, Y. Kim, and C. O. Kim, "A deep learning model for robust wafer fault monitoring with sensor measurement noise," IEEE Trans. Semicond. Manuf., vol. 30, no. 1, pp. 23–31, Feb. 2017.

[8] Buczak AL, Guven E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials. 2016;18(2):1153–1176.

[9] Mukherjee S, Sharma N. Intrusion detection using naive Bayes classifier with feature reduction. Procedia Technology. 2012;4:119–128.

[10] Kumar V, Chauhan H, Panwar D. K-means clustering approach to analyze NSL-KDD intrusion detection dataset. International Journal of Soft Computing and Engineering (IJSCE). 2013;.

[11] Ashfaq RAR, Wang XZ, Huang JZ, Abbas H, He YL. Fuzziness based semi-supervised learning approach for intrusion detection system. Information Sciences. 2017;378:484–497.

[12] Kanakarajan NK, Muniasamy K. Improving the accuracy of intrusion detection using GAR-Forest with feature selection. In: Proceedings of the 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA) 2015. Springer; 2016. p. 539–547.

[13] Singh R, Kumar H, Singla R. An intrusion detection system using network traffic profiling and online sequential extreme learning machine. Expert Systems with Applications. 2015;42(22):8609–8624.

[14] Farid DM, Harbi N, Rahman MZ. Combining naive bayes and decision tree for adaptive intrusion detection. arXiv preprint arXiv:10054496. 2010;.

[15] R . Zhao, R. Yan, Z. Chen, K. Mao, P. Wang, and R. X. Gao, "Deep learning and its applications to machine health monitoring: A survey," Submitted to IEEE Trans. Neural Netw. Learn. Syst., 2016.

[16] L. You, Y. Li, Y. Wang, J. Zhang, and Y. Yang, "A deep learning based RNNs model for automatic security audit of short messages," in Proc. 16th Int. Symp. Commun. Inf. Technol., Qingdao, China, Sep. 2016, pp. 225–229.

[17] R. Polishetty, M. Roopaei, and P. Rad, "A next-generation secure cloud based deep learning license plate recognition for smart cities," in Proc. 15th IEEE Int.

[18] K. Alrawashdeh and C. Purdy, "Toward an online anomaly intrusion detection system based on deep learning," in Proc. 15th IEEE Int. Conf. Mach. Learn. Appl., Anaheim, CA, USA, Dec. 2016, pp. 195– 200.

[19] A. Javaid, Q. Niyaz, W. Sun, and M. Alam, "A deep learning approach for network intrusion detection system," in Proc. 9th EAI Int.Conf. Bio-Inspired Inf.

[20] Commun. Technol., 2016, pp. 21–26. [Online]. Available: http://dx.doi.org/10.4108/eai.3-12-2015.2262516.

[21] S. Potluri and C. Diedrich, "Accelerated deep neural networks for enhanced intrusion detection system," in Proc. IEEE 21st Int. Conf. Emerg. Technol. Factory Autom., Berlin, Germany, Sep. 2016, pp. 1–8.

[22] Koch R. Towards next-generation intrusion detection. In: 2011 3rd International Conference on Cyber Conflict. IEEE; 2011. p. 1–18.

[23] Rajahalme J, Conta A, Carpenter B, Deering S. RFC 3697: IPv6 Flow Label Specification. In: The Internet Society; 2004.

[24] Cunningham RK, Lippmann RP, Fried DJ, Garfinkel SL, Graf I, Kendall KR, et al. Evaluating intrusion detection systems without attacking your friends: The 1998 DARPA intrusion detection evaluation. Massachusetts Institute of Technology Lexington Lincoln Lab; 1999.

[25] Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. In: 2009 IEEE Symposium on Computational Intelligence for Security and Defense Applications. IEEE; 2009. p. 1–6.

[26] Dhanabal L, Shantharajah S. A study on NSL-KDD dataset for intrusion detection system

based on classification algorithms. International Journal of Advanced Research in Computer and Communication Engineering. 2015;4(6):446–452.

[27] Nehinbe JO. A simple method for improving intrusion detections in corporate networks. In: International Conference on Information Security and Digital Forensics. Springer; 2009. p. 111–122.

[28] Shannon C, Moore D. The caida dataset on the witty worm. Support for the Witty Worm Dataset and the UCSD Network Telescope are provided by Cisco Systems, Limelight Networks, the US Department of Homeland Security, the National Science Foundation. 2004.

[29] Nechaev B, Allman M, Paxson V, Gurtov A. Lawrence berkeley national laboratory (lbnl)/icsi enterprise tracing project. Berkeley, CA: LBNL/ICSI. 2004.

[30] Sangster B, O'Connor T, Cook T, Fanelli R, Dean E, Morrell C, et al. Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets. In: CSET; 2009.

[31] Song J, Takakura H, Okabe Y, Eto M, Inoue D, Nakao K. Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for NIDS evaluation. In: Proceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security. ACM; 2011. p. 29–36.

[32] Barbosa RRR, Sadre R, Pras A, van de Meent R. Simpleweb/university of twente traffic traces data repository. Centre for Telematics and Information Technology University of Twente, Enschede, Technical Report. 2010.

[33] Liberatore M, Shenoy P. Umass trace repository. Accessed: May; 2017.

[34] Shiravi A, Shiravi H, Tavallaee M, Ghorbani AA. Toward developing a systematic approach to generate benchmark datasets for intrusion detection. computers & security. 2012;31(3):357–374.

[35] Creech G, Hu J. Generation of a new IDS test dataset: Time to retire the KDD collection. In: 2013 IEEE Wireless Communications and Networking Conference (WCNC). IEEE; 2013. p. 4487–4492.

[36] Sharafaldin I, Lashkari AH, Ghorbani AA. Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization. In: ICISSP; 2018. p. 108–116.

[37] Agrawal S, Agrawal J. Survey on anomaly detection using data mining techniques. Procedia Computer Science. 2015;60:708–713.

[38] Belavagi MC, Muniyal B. Performance evaluation of supervised machine learning algorithms for intrusion detection. Procedia Computer Science. 2016;89:117–123.

[39] Ektefa M, Memar S, Sidi F, Affendey LS. Intrusion detection using data mining techniques. In: 2010 International Conference on Information Retrieval & Knowledge Management (CAMP). IEEE; 2010. p. 200–203.

[40] Garcia-Teodoro P, Diaz-Verdejo J, Macia´-Fernandez´ G, Vazquez´ E. Anomaly-based network intrusion detection: Techniques, systems and challenges. computers & security. 2009;28(1-2):18–28.

[41] Tavallaee M, Stakhanova N, Ghorbani AA. Toward credible evaluation of anomaly-based intrusion-detection methods. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). 2010;40(5):516–524.

[42] Deshmukh DH, Ghorpade T, Padiya P. Intrusion detection system by improved preprocessing methods and Na¨ıve Bayes classifier using NSL-KDD 99 Dataset. In: 2014 International Conference on Electronics and Communication Systems (ICECS). IEEE; 2014. p. 1–7.

[43] Pervez MS, Farid DM. Feature selection and intrusion classification in NSL-KDD cup 99 dataset employing SVMs. In: The 8th International Conference on Software, Knowledge, Information Management and Applications (SKIMA 2014). IEEE; 2014. p. 1–6.

[44] Md. Zainal Abedin; Kazy Noor-e-Alam Siddiquee; M. S. Bhuyan; Razuan Karim; Mohammad Shahadat Hossein; Karl Andersson, "Performance Analysis of Anomaly Based Network Intrusion Detection Systems" 2018 IEEE 43rd Conference on Local Computer Networks

Workshops (LCN Workshops), INSPEC Accession Number: 18452166, DOI: 10.1109/LCNW.2018.8628599