

DoS and DDoS Attack Detection Using Deep Learning and IDS

Mohammad Shurman¹, Rami Khrais², and Abdulrahman Yateem¹

¹Jordan University of Science and Technology, Network Engineering and Security Department, Jordan

²Jordan University of Science and Technology, Computer Engineering Department, Jordan

Abstract: *In the recent years, Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS) attack has spread greatly and attackers make online systems unavailable to legitimate users by sending huge number of packets to the target system. In this paper, we proposed two methodologies to detect Distributed Reflection Denial of Service (DrDoS) attacks in IoT. The first methodology uses hybrid Intrusion Detection System (IDS) to detect IoT-DoS attack. The second methodology uses deep learning models, based on Long Short-Term Memory (LSTM) trained with latest dataset for such kinds of DrDoS. Our experimental results demonstrate that using the proposed methodologies can detect bad behaviour making the IoT network safe of Dos and DDoS attacks.*

Keywords: *Deep learning, DoS, DrDoS, IDS, IoT, LSTM.*

Received February 29, 2020; accepted June 9, 2020

<https://doi.org/10.34028/iajit/17/4A/10>

1. Introduction

Living in an era where IoT covers many modern human life aspects. IoT is made of multiple devices (things) from different technology backgrounds surrounded by many security challenges [16]. Security fundamentals and properties of each thing are different from each other, making it hard to find a common ground to operate them all together securely. Weak security measures enable attackers to target IoT devices [8]. In addition, multiple verticals, scalability, big data, availability, resource limitation, remote locations, mobility and delay sensitive services are other security issues in IoT that make traditional internet security mechanisms not always feasible to adopt. IoT networks and systems remain very vulnerable and require stronger protection mechanisms.

Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks can easily affect the client-side of any system [11]. Many attacks are based on personal goals or on behalf of other malicious entities who aim to disrupt the services of specific companies or people in return for an amount of money by performing a DoS or DDoS attack. As an amplified type of DoS attacks, DDoS attacks where attackers direct Hundreds or even thousands of compromised hosts called zombies to one destination [21]. There are many types of DDoS attacks where attacker's identity remains hidden by using legitimate third-party components. In reflection-based DDoS, attackers set the victim's IP address as a desirable target IP source and transfer packets to reflector servers to overpower the victim with response packets. Reflection-based DDoS are challenging and very tricky to detect because they are done via

application layer protocols, using transport layer protocols TCP, UDP, or both. Various attacks descend from TCP or UDP, for example, MSSQL attack depends on TCP to perform attacks, on the other hand, NTP and TFTP attack strategies depends on UDP.

Many cyber-attacks (include DoS and DDoS attacks) are mostly carried out by humanly instructed systems (*Bots or Botnets*) that consist of several devices with internet access. Bots may exist when a computer is infected with malware via specific software. These bots can perform various types of attacks such as DDoS, data stealing, or ransomware.

An Intrusion Detection System (IDS) is a security network aspect that detects networks and systems from malicious activities or policy breaches [3]. Recently, IDSs are gaining a lot of popularity and attention from security specialists to protect IoT devices along with hybrid approaches that combines two or more IDS methods. In this paper, we propose a hybrid IDS method based on detecting a potential DoS attack by traffic behaviour classification, while combining the advantages and overcoming the disadvantages of both the signature and anomaly based IDSs. Therefore, we propose another methodology to detect novel types of DDoS attacks using Deep learning based on LSTM Long Short-Term Memory that can successfully detect DDoS malicious packets regardless of their types.

The paper introduces some of the related work on hybrid methods and IoT-DoS in last years, also compares the differences between both (signature and anomaly) methodologies, discussing the data flow of the logic behind our approach along with the results obtained from the designed framework simulation of

this hybrid combination. In addition, we describe how to train data with deep learning model from some used datasets and how data pre-processing is done.

2. Related Work

A lot of researchers proposed designs tackling IoT-DoS in recent years, seeking hybrid methods IDS to increase network defences, such as using a hybrid system [26] of misuse and anomaly detection for training friendly and unfriendly (attack) packets respectively in 2009 by Bahrololum *et al.* [4]. Another hybrid method of IDS based on K-means, naive Bayes and back propagation neural network (KBB) was proposed [13]. A different method was introduced to make a decision about abnormal behaviour using a mechanism based on voting [7]. Their approach presents a real time hybrid IDS framework to detect hostile behaviours of sinkhole and selective forwarding attacks in 6LoWPAN. Another signature-based IDS design was introduced that involves both centralized and distributed IDS modules, using a simulator COOJA tool. Executing an IoT-DoS scheme then apply to IoT devices [15]. Razak and Salim [20] proposed a design using IDS to detect DoS attacks based on network traffic. In this approach, patterns are taken from network traffic that is not supposed to be normal behaviour and compared with normal traffic. If the outliers are more than the thresholds, the system will generate an alarm.

The earlier DDoS attacks are detected, the less catastrophic consequences can be dealt with, especially when it comes to IoT devices, making the Internet vulnerable to a variety of threats and hidden malicious patterns within carried data that are not noticeable, with underlining the challenges in distinguishing between legitimate and malicious flows. There are accredited efforts to overcome these issues by the implementation of various machine learning methods [10].

Bindra and Sood [6] employ and analyse several Machine Learning models to detect DDoS attacks to seek the best ML model with real-life attack datasets and obtained 96% accuracy by training the Random Forest classifier. Another study by Doshi and Apthorpe [12] focus on how IoT devices are dragged to use the specifications of IoT network behaviours for characteristic determination can succeed in high DDoS detection accuracy with the use of several machine-learning algorithms. Also, with the application of remarkable consumer IoT devices for generating traffic, home routers could automatically discover bounded IoT devices that are sources for DDoS attacks, employing low-cost machine learning algorithms. Their classifiers can remarkably identify malicious traffic with an accuracy rate higher than 0.999, showing that random forest, K-nearest neighbours, as well as declaring that neural net classifiers are the best for such detection. Other researchers went to evaluate their approach by the use of well-known datasets that attract Botnet

DDoS attack detection. Tuan *et al.* [25] conduct a performance analysis of the most typical machine-learning methods used in Botnet DDoS attack detection on different datasets and shows that KDD99 dataset is much better than the UNBS-NB 15 dataset in terms of performance. Furthermore, the approach shows that unsupervised machine learning is the most qualified method in its class in distinguishing between Botnet and regular network traffic in several terms that have a significant impact on network security.

In [1], the DDoS attack mitigation had been improved through a strategic machine learning approach. The most difficult type of DDoS in terms of mitigation is application-layer attacks that relies on HTTP to mimic flash crowd that appears to be realistic. Machine learning and Feature engineering is the two main components in this work and every one of them is applied on a certain DDoS dataset to manifest we can depend on Feature engineering and Machine learning in an extensive way to detect DDoS attacks with no chance of overfitting or collinearity. Initially, fifteen features have been eliminated under domain knowledge and flow-level features are prioritized over packet-level features. Due its zero impertinency, the resulting dataset contains 22 features and called 'DS00_Full', from this dataset three datasets have been obtained by applying feature selection method 'DS01_PVal, with 16 features' 'DS02_Chi2, with 7 features' and 'DS03_IG, with 7 features'. However, KNN, NB, SVM, RF, and ANN are the most common supervised machine learning algorithms, they were applied to the four datasets in order to mitigate DDoS attacks.

The classification metrics are error, accuracy, true positives, false positives, true negatives, and false negatives. Furthermore, to evaluate optimized accuracies analysis is done by determining the Area Under Curve (AUC) of the Receiver Operating Characteristic curve (ROC). 'DS00_Full' dataset shows the highest accuracy scores for 4 out of 5 machine learning algorithms, the scores of hits 'DS00_Full' 93.53% accuracy. On the other hand, 'DS03_IG' is the most promising dataset, as its AUC scores remain competitive in all machine learning experiments with other datasets. A small set of features of this dataset makes it a good choice for significant reduction in overhead processing.

3. IoT DoS Attack

When a DoS attack is launched towards an IoT network and floods the network with large traffic [2], the services are not available, network defences are absolute, and the availability factor will be jeopardized [5]. The existence of an Intrusion Detection and Preventing System (IDPS) has little chance to stand a DoS attack [22], although most of IDPS use one or more detection methodologies

classified into two categories, signature-based or anomaly-based [14]. Each category has its advantages and weak points, A DoS force its attack by exploiting the weaknesses of these methodologies.

With the employment of signature-based method or detection, also known as rule-based or misuse-based IDS, attack is detected by comparing well-known attack signatures, patterns, or malicious instruction sequences used by malware such as byte sequences with the monitored network traffic. A match generates an alarm for a potential attack. This type has fast detection time, detects most known attacks, and generally has low false positive rate, it does not signal an alarm for legitimate traffic. Signature detection is based on well-known DoS attacks patterns that are mostly malformed packets and protocol attacks. On the other hand, anomaly-based IDS, also known as behaviour-based detection, operates by comparing the network traffic behaviour against previous normal traffic behaviour, any deviation in the comparison is a sign of an attack. The system acquires a normal traffic profile, usually through training, and monitors the traffic for any differences from the normal profile. Anomaly detection can detect unknown attacks; however, it generally produces higher false positive rates than signature-based systems. We detail both methods advantages and weaknesses in Table1.

Table 1. Comparison of signature and anomaly based IDS.

	Signature-based	Anomaly-based
Advantages	<ul style="list-style-type: none"> • Low alarm measure, low false positive rate. • Signature based NID are very precise. • Fast detection period. • Based on well-known DoS attacks patterns. 	<ul style="list-style-type: none"> • Monitors unknown behaviors. • Detects unknown attacks. • Decrease limitations problem.
Weaknesses	<ul style="list-style-type: none"> • Weak protections against new attacks. • Updated on regular bases before securing network. • No alarm is set for authorized traffic. 	<ul style="list-style-type: none"> • Produces high false positive rates (captures a lot because behaviour based NIDs monitor a system based on their behaviour patterns). • Time-consuming in means of doing an exhaustive monitoring due to the amount of resources used.

4. Hybrid IDPS

We intend to combine the signature-based method and anomaly-based method to produce an integration of both methods, this integration can solve most of problems mentioned in Table1. Eventually, to provide a more broad and accurate detection technique, combination of both signature and anomaly-based techniques is our aim to overcome some attacks that may trigger DoS towards network connecting IoT services. To translate the initial idea by explaining how this hybrid method will look like, we demonstrate a visual representation of data flow that supports our proposed approach to spell out the logic behind this combination.

From the flowchart (Figure 1), if an attack passed the IDS network sensors without detection (in case it is a new IP), and reached the signature-based detector without detection, then it does not match any of the signature based attacks stored in (KAS-DB), the behaviour of the attack is already traced and carefully monitored by the anomaly-based detector. Because of collaborative efforts of previous actions, regardless whether they detected the attack or not, it will monitor the attacks behaviour of byte patterns along the outcome processes of each of the IDSs and the signature-based detect or output.

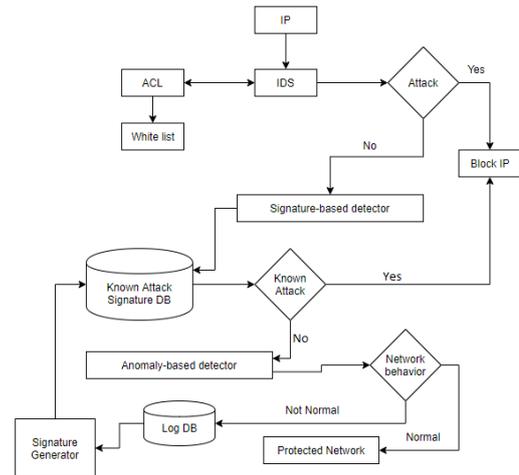


Figure 1. Flowchart representing the proposed model.

Based on our assumptions, if the network behaviour is normal during IP request time, it will be announced as a legitimate IP and approved to get into the secure network. On the other hand, if an abnormal behaviour is detected in any stage, the IP will be blocked.

First, let us assume the scenario when the IDS goes into action, the IDS sensor will detect an attack if the incoming IP request is a known attack or part of an attack segment based on a stored signature attack. it will generate an alarm to the router and blocks the IP address source, then updates dynamically the Access Control List (ACL) on the router to add this IP to the black listed IPs, while if not detected as a threat, it proceeds to the next detection border. Secondly, the signature-based detector will compare the signature of the incoming traffic with well-known attacks signature in its DB, if a match is found it will alarm for a potential attack and block the IP source from accessing the network. If no match is found, packet proceeds to our next detection stage. Thirdly, the anomaly-based detector is already operating by observing the byte sequence of the incoming network traffic behaviour, analysing the previous and the new byte sequences for a defined time interval and compare this analysis against normal behaviour. If any deviation in the comparison is detected, it is flagged as an attack. Therefore, it will update (Log DB) to store the newly detected attack record and generate a signature of this attack and updates the (KAS-DB).

Hereafter, the attack will be known, resulting in blocking IP address source using signature-based detection quickly.

4.1. Simulating the Hybrid Approach

To simulate the proposed approach. Java programming language was used to build our framework to verify the proposed system, using two testing datasets each containing various number of IPs on a network as shown in Table 2. In the beginning, the framework will check each IP if listed in the white list, therefore, grant it network access. In both cases, either listed or not listed, the IP address will be verified with Signature-based data, to detect and block the IP if selected as a known attack. However, if the same IP classified as an unknown attack, it will go through the Anomaly-based stage to check the IP in the sense of any unnormal behaviour and patterns. If so, the IP is blocked, and the known attack database is updated with the new malicious IP. Otherwise, network access is granted in case of normal IP behaviour.

Table 2. Data captured in a defined period of time.

Dataset	Number of IPs In our network	Number of Packets come from users	Dataset Numbers of IPs Classified as known attack (used by signature-based)
No.1	249	244,001	999
No.2	24	15,939	999

We also show how many IPs accessed the network by white-list checking, blocked from signature-based IDs and from anomaly-based IDS in Table 3.

Table 3. Results of data and number of blocked IPs.

Dataset	No.1	No.2
Passed White list checking	1	2
Number of probable IPs blocked from signature-based IDs	1	1
Number of probable IPs blocked from anomaly-based IDs	2	2

We observe from our experimental results that signature based uses DB with fast detection time but does not have the ability for new attacks detection. On the other hand, anomaly based does not use any kind of DB to recall attacks history but has high capability to detect new attacks and has variable detection time. In addition, both have reliable outcomes, but the hybrid method depends on data from a DB and has reliable outcome, it can detect suspicious attacks with vary detection time as shown in Table 4.

Table 4. IDS methods comparison.

Method	Using DB	Reliability	Detection Time	Detect New Attack
Signature-based	Yes	Yes	Fast	No
Anomaly-Based	No	Yes	Vary	Yes
Hybrid	Yes	Yes	Vary	Yes

5. Datasets

There are many DDoS attack datasets available to be used in deep learning training processes; the latest published dataset is CICDDoS2019 [23], which contains two kinds of DDoS attacks, reflection-based and exploitation-based. Reflection-based attacks are based on either TCP, UDP, or both. For instance, MMSQL attacks depend on TCP to affect the Microsoft SQL server by making sure that both the availability and connectivity of the TCP destination port, and then initializing the attack by sending NULL bytes packets. Another type of TCP based attack is the Simple Service Discovery Protocol (SSDP); this attack concentrates on sending massive traffic to a targeted victim, overloading the targeted network, and taking the web resource off-line. Furthermore, reflection-based consists of UDP based attacks, such as CharGen, Network Time Protocol (NTP), and Transfer Protocol (TFTP). The Character Generator Protocol (CharGen) is another attack based on providing an accessible service through port 19, and when the connection is complete, the attack will start by sending a random number of random characters. Also, the NTP attack relates to the monlist size, as opposed to the original packet size. Trivial File TFTP makes a default request for a file, and as a result of this request, the victim TFTP server returns data to the requesting target host regardless of the file name mismatch, it consumes time undertaking a futile task. In addition to TCP and UDP, reflection-based contains attacks based on both TCP/UDP, such as Domain Name System (DNS), Lightweight Directory Access Protocol (LDAP), NetBIOS, SNMP Protocol, and PORTMAP attack.

Exploitation-based attacks are based on TCP and UDP. The TCP attacks consist of SYN flood attacks that work by tapping a TCP connection's handshake mechanism. On the other hand, UDP attacks or UDP flood mainly works by exploiting the steps a server takes when reacting to a UDP packet sent to one of its open ports. Another attack is UDP-Lag; this kind of attack usually used by attackers to interrupt a connection in online games when the attacker (player) aims to influence the performance for other players.

The previous datasets contain favourable DDoS traffic with significant numbers of features, such as timestamp, source, and destination IPs, source and destination ports, generated using CICFlowMeter-V3 and saved as a CSV file.

5.1. Data Pre-Processing

Firstly, using the Reflection-based (DrDoS) dataset with deep learning is a significant consideration dedicated to ensuring the value of each data record not to be equal to NULL, so that each NULL record is to be filled with arithmetic means of its column. The next step was searching sets of records in numeric

type, the findings where we string type records, therefore, replacing them with arithmetic means in its column. The following step intends to replace data labels from string type (“benign” and “DDoS”) to integer type (1 and 0) due to the impossibility to train deep learning models with string data before any process, such as One hot encoder [19]. To achieve proper fitting with deep learning, selecting the essential feature is required from the dataset. The Random forest comes in handy, to comprehend the importance of each feature [19] and done under Gini impurity measuring the likelihood of incorrect classification of new instances of random variables given by Equation (1) where $P(i)$ is the probability of specific classification i , and j is the number of classes.

$$G(k) = \sum_{i=1}^j P(i) * (1 - P(i)) \quad (1)$$

Finally, by dropping non-useful data columns (features) and holding the essential features after the previous process, the dataset is ready to be used in deep learning models.

6. Deep Learning Models

In this work, a deep learning network is proposed in the detection process, based on using the most famous deep learning models LSTM and Recurrent Neural Network (RNN). The LSTM neural network aims to detect DrDoS, because LSTM networks are capable of solving the vanishing gradients problem (gradients become smaller and smaller; consequently, the parameter updates become very small; therefore, the learning process will take more time without no beneficial learning effectiveness) in RNN. Our deep learning model is built using the Keras framework [9] LSTM consists of three gates (Forget gates, Input and Output gates) and cell state. The forget gate ($f(t)$) is given by Equation (2) that controls which parts of the long-term state should be erased, the input gate ($i(t)$) is given by Equation (3) which controls what parts should be added to the long-term state, and the output gate ($o(t)$) given by Equation (4) controls which parts of the long-term state should be read and output at the current time step. Each gate has its weight given by W_f , W_i , and W_o . In all previous gates, the data from the previous hidden state and data from the current input is going over the sigmoid function (σ) given by Equation (5). In addition to the input gate, the past and current state will go over the (\tanh) function given by Equation (6) to help the network coordinate itself. The functions (σ) and (\tanh) are two sides of the same coin, but the sigmoid function gives results between 0 and 1, i.e., if the output gate is closer to 0, data will neglect while the output is closer to 1 data is stored, where (\tanh) output between -1 and 1. The architecture of LSTM is shown in Figure 2.

$$F(t) = \sigma(W_f[ht - 1, xt] + bf) \quad (2)$$

$$i(t) = \sigma(W_i[ht - 1, xt] + bi) \quad (3)$$

$$o(t) = \sigma(W_o[ht - 1, xt] + bo) \quad (4)$$

$$f(xt) = 1/(1 - e^{\alpha xt}) \quad (5)$$

$$\tanh(x) = \left(\frac{2}{1 + e^{-2x}} \right) - 1 \quad (6)$$

Where ($ht-1$) represents previous state, (α) learning rate, (xt) current input and (bf , bi , bo) bias for each gate.

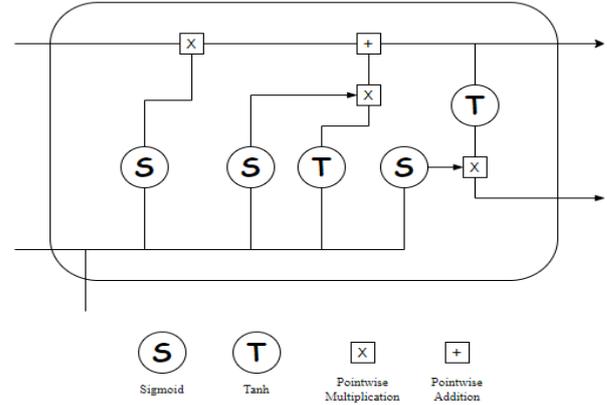


Figure 2. LSTM architecture.

6.1. Training Models

In this paper, a reflection-based dataset is used and split into (80% train dataset and 20% as the test dataset) to evaluate the models and to avoid overfitting problems.

The first used model consists of one LSTM layer with 64 unit and sigmoid as activation function, one dropout layer (a technique to avoid overfitting), and a dense layer with tanh. A second model consisted of two LSTM layers with 128 unit and sigmoid as the activation function with two dropout layers and dense layer and tanh function. The last model consists of three LSTM layers with 128 unit and sigmoid as activation function, three dropout layers, and a dense layer with tanh function. All models compiled with *categorical_crossentropy* as loss function and Root Mean Square Propagation (rmsprop) as an optimizer, we detail the difference between models in Table 5.

The result from the first model on the training set shows almost 92.05% accuracy and 91.54% on the test set. The second model reaches an average of 97.27% accuracy on the training set and 96.74% on the test set. In the last model, the results show 99.85% accuracy on the training set and 99.19% accuracy on the test set. All our accuracy results calculated according to Equation (7) the representation of our model's accuracy is shown in Figure 3. There are many related works on different datasets based on deep learning models such as ours; by reviewing some of them, we found that our model performs better with high test accuracy. In Table 6, we discuss and compare the results with the latest related works.

Table 5. Comparison of LSTM models.

	First Model	Second Model	Third Model
Train accuracy	92.05 %	97.27 %	99.85 %
Test accuracy	91.54 %	96.74 %	99.19 %
Activation function	Sigmoid, Tanh	Sigmoid, Tanh	Sigmoid, Tanh
Loss function	categorical_crossentropy	categorical_crossentropy	Categorical_crossentropy
Optimizer	Rmsprop	Rmsprop	Rmsprop

$$accuracy = \left(\frac{TP + TN}{TP + TN + FP + FN} \right) \quad (7)$$

Where:

- True Positive (TP): Attack record classified correctly as attack.
- True Negative (TN): Benign record classified correctly as benign.
- False Positive (FP): Benign record classified incorrectly as attack.
- False Negative (FN): Attack record classified incorrectly as benign.

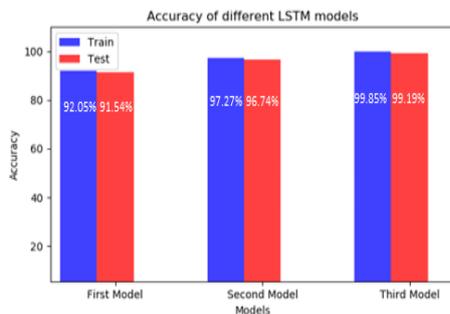


Figure 3. LSTM models accuracy.

Table 6. Comparison between our deep learning model and other models.

Models	Test accuracy	Dataset
Random Forest [18]	99.0 %	CICDDoS2019
Random Forest [14]	73.9 %	CICDDoS2019
Our model (Third model)	99.19 %	CICDDoS2019

7. Conclusions

In this paper, we propose two methodologies. The first method is a hybrid-based IDS for IoT networks, introducing an IDS framework scheme defined as an application, able to detect suspicious network traffic from any network nodes [23], with running datasets of IPs against it. It was capable of identifying unusual packets on the network moreover blocking unwelcomed IPs before escalating to be potential DoS threats. The second method was a deep learning model based on LSTM, able to detect DrDoS attacks and trained on CICDDoS2019 dataset with various kinds of DrDoS attacks. We plan to design a new deep learning model to detect the second type of DDoS attack in CICDDoS2019 dataset (Exploitation-based attacks) for

future work and to test the performance of these methodologies in a realistic system.

References

- [1] Aamir M. and Zaidi S., “DDoS Attack Detection with Feature Engineering and Machine Learning: The Framework and Performance Evaluation,” *International Journal of Information Security*, vol. 18, no. 3, pp. 761-785, 2019.
- [2] Alenezi M. and Reed M., “Denial of Service Detection through TCP Congestion Window Analysis,” in *Proceedings of World Congress on Internet Security*, London, pp. 145-150, 2013.
- [3] Babatope L., Babatunde L., and Ayobami I., “Strategic Sensor Placement for Intrusion Detection in Network-Based IDS,” *International Journal of Intelligent Systems and Applications*, vol. 6, no. 2, pp. 61-68, 2014.
- [4] Bahrololum M., Salah E., and Khaleghi M., “Anomaly Intrusion Detection Design Using Hybrid of Unsupervised and Supervised Neural Network,” *International Journal of Computer Networks and Communications*, vol. 1, no. 2, pp. 26-33, 2009.
- [5] Bhardwaj K., Miranda J., and Gavrilovska A., “Towards Iot-Ddos Prevention Using Edge Computing,” in *Proceedings of USENIX Workshop on Hot Topics in Edge Computing*, Boston, 2018.
- [6] Bindra N. and Sood M., “Detecting DDoS Attacks Using Machine Learning Techniques and Contemporary Intrusion Detection Dataset,” *Automatic Control and Computer Sciences*, vol. 53, no. 5, pp. 419-428, 2019.
- [7] Bostani H. and Sheikhan M., “Hybrid of Anomaly-Based and Specification-Based Ids for Internet of Things Using Unsupervised Opf Based on Mapreduce Approach,” *Computer Communications*, vol. 98, pp. 52-71, 2017.
- [8] Cartlidge E., “The Internet of Things: From Hype to Reality,” *Optics and Photonics News*, vol. 28, no. 9, pp. 26-33, 2017.
- [9] Chollet F., “Keras: Python Deep Learning Library,” <https://keras.io>, Last Visited, 2015.
- [10] Dabbagh M. and Rayes A., “Internet of Things Security and Privacy,” in *Internet of Things from Hype to Reality*, 2017.
- [11] Dalati I., “Towards More Enterprise Security for IoT,” <http://www.infosecourcemagazine.com/opinions/enterprise-security-iot/>, Last Visited, 2017.
- [12] Doshi R., Apthorpe N., and Feamster N., “Machine Learning DDoS Detection for Consumer Internet of Things Devices,” in *Proceedings of IEEE Security and Privacy Workshops*, San Francisco, pp. 29-35, 2018.

- [13] Dubey S. and Dubey J., "KBB: A Hybrid Method for Intrusion Detection," in *Proceedings of International Conference on Computer, Communication and Control*, Indore, pp. 1-6, 2015.
- [14] Gangwar A. and Sahu S., "A Survey on Anomaly and Signature-Based Intrusion Detection System," *International Journal of Engineering Research and Applications*, vol. 4, no. 4, pp. 67-72, 2014.
- [15] Ioulianou P., Vasilakis G., Moscholios I., and Logothetis M., "A Signature-based Intrusion Detection System for the Internet of Things," in *Proceedings of Information and Communication Technology Forum*, Austria, pp. 1-6, 2018.
- [16] Joshi S. and Kulkarni K., "Internet of Things: An Overview," *ISOR Journal of Computer Engineering*, vol. 18, no. 4, pp. 117-121, 2016.
- [17] Junhong L., "Detection of DDoS Attack Based on Dense Neural Networks, Autoencoders and Pearson Correlation Coefficient," Master Thesis, Dalhousie University, 2020.
- [18] Kiourkoulis S., "DDoS Datasets: Use of Machine Learning to Analyse Intrusion Detection Performance," Master Thesis, Luleå University of Technology, Space Engineering, 2020.
- [19] Pedregosa F., Varoquaux G., Gramfort A., Michel V., Thirion B., Grisel O., Blondel M., Prettenhofer P., Weiss R., Dubourg V., Vanderplas J., Passos A., Cournapeau D., Brucher M., Perrot M., and Duchesnay E., "Scikit-learn: Machine Learning in Python," *Journal of Machine Learning Research*, vol. 12, no. 85, pp. 2825-2830, 2011.
- [20] Razak T. and Salim I., "A Study on IDS for Preventing Denial of Service Attack Using Outliers' Techniques," in *Proceedings of IEEE International Conference on Engineering and Technology*, India, pp. 768-775, 2016.
- [21] Sachdeva M, Singh G., Kumar K., and Singh K., "DDoS Incidents and Their Impact: A Review," *The International Arab Journal of Information Technology*, vol. 7, no. 1, pp. 14-20, 2010.
- [22] Scarfone K. and Mell P., "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST. No. Special Publication (NIST SP)*, 2007.
- [23] Sharafaldin I., Lashkari A., Hakak S., and Ghorbani A., "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy," in *Proceedings of IEEE 53rd International Carnahan Conference on Security Technology*, Chennai, pp. 1-8, 2019.
- [24] Shurman M., Khrais R., and Yateem A., "IoT Denial-of-Service Attack Detection and Prevention Using Hybrid IDS," in *Proceedings of International Arab Conference on Information Technology*, Alain, pp. 252-254, 2019.
- [25] Tuan T., Long H., Son L., Kumar R., Priyadarshini I., and Son N., "Performance Evaluation of Botnet Ddos Attack Detection Using Machine Learning," *Evolutionary Intelligence*, vol. 13, no. 2, pp. 283-294, 2020.
- [26] Zekrifa D., "Hybrid Intrusion Detection System," Master Thesis, University of South Australia, 2014.



Mohammad Shurman received the B.Sc. degree in Electrical and Computer Engineering from Jordan University of Science and Technology, Irbid, Jordan, M.Sc. and Ph.D. degrees in Computer Engineering-Wireless Networks

from University of Alabama-Huntsville (UAH) in 2000, 2003, and 2006, respectively. Presently he is with the Network Engineering and Security Department, Jordan University of Science and Technology, Irbid, Jordan. His research interests include wireless Ad hoc networks, security and key management of wireless networks, wireless sensor networks, network coding, wireless communication and mobile networks, software defined networks (SDN), cognitive radio, WiMAX, 4G and 5G technology and Blockchains.



Rami Khrais received his B.Sc degree in computer science from Al-Balqa' Applied University, Jordan, in 2018. He is currently a graduate student in computer engineering at Jordan University of Science and Technology, Jordan. His research

interests are in deep learning, machine learning and information security.

Abdulrahman Yateem received his B.Sc degree in Information Technology from Ahlia University, Bahrain, in 2008. He is currently a graduate student in Network Engineering and Security at Jordan University of Science and Technology, Jordan. His research interests are in information warfare, network and information security.