Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 182 (2021) 13–20

Procedia Computer Science

www.elsevier.com/locate/procedia

17th International Learning & Technology Conference 2020 (17th L&T Conference)

A DDoS Attack Mitigation Framework for IoT Networks using Fog Computing

Muhammad Aminu Lawal [1], Riaz Ahmed Shaikh, Syed Raheel Hassan

Department of Computer Science, Faculty of Computing and Information Technology, King Abdulaziz University Jeddah, 21589, Saudi Arabia.

Abstract

The advent of 5G which strives to connect more devices with high speed and low latencies has aided the growth IoT network. Despite the benefits of IoT, its applications in several facets of our lives such as smart health, smart homes, smart cities, etc. have raised several security concerns such as Distributed Denial of Service (DDoS) attacks. In this paper, we propose a DDoS mitigation framework for IoT using fog computing to ensure fast and accurate attack detection. The fog provides resources for effective deployment of the mitigation framework, this solves the deficits in resources of the resource-constrained IoT devices. The mitigation framework uses an anomaly-based intrusion detection method and a database. The database stores signatures of previously detected attacks while the anomaly-based detection scheme utilizes k-NN classification algorithm for detecting the DDoS attacks. By using a database containing the attack signatures, attacks can be detected faster when the same type of attack is executed again. The evaluations using a DDoS based dataset show that the k-NN classification algorithm proposed for our framework achieves a satisfactory accuracy in detecting DDoS attacks.

Keywords: Internet of Things (IoT); Anomaly mitigation; DDoS, Fog computing; Classification Algorithm

1.Introduction

In recent times, the advancement of communication technologies such 5G, low cost and compactness of sensing devices have aided the growth of the Internet of Things (IoT) with applications across several fields such as smart health, smart homes, smart cities, smart agriculture, etc., where these devices are connected to the internet. The 5G seeks to connect more devices with high speed and low latencies which will enhance the efficiency of delay-sensitive IoT applications [1]. Although, these developments in IoT and 5G have affected our lives tremendously in positive ways. The IoT devices have a major challenge in terms of security, which is further complicated by the exponential growth of the devices aided by the 5G. The expected number of these devices will reach around 75 billion by 2025 [2]. In addition, the lack of sufficient resources on these devices has made deploying security solutions such as anomaly mitigation schemes an obstacle in ensuring safe IoT networks.

One of the major security challenges in the IoT networks is the Distributed Denial of Service (DDoS) attack, it dilapidates resources in order to make it unavailable for legitimate users. The DDoS attacks have different patterns and each has its unique behaviour in overwhelming or wasting the resources to accomplish its objective [3]. This threat necessitates the deployment of network anomaly mitigation schemes as an integral part of the defense mechanisms of IoT networks, which further protect the devices due to their positive impact and benefits in our daily activities. However, successful deployment of network anomaly mitigation usually performed by Intrusion Detection

* Corresponding author. Tel.: +966557639752
E-mail address: mlawal@stu.kau.sa

1877-0509 © 2021 The Authors. Published by Elsevier B.V.

10.1016/j.procs.2021.02.003

Systems (IDS) on the IoT networks is hindered by the lack of sufficient resources on the devices to be utilized by the mitigation schemes.

Intrusion Detection Systems (IDS) are used to detect an illegal access to a system or a network by malicious users. It is deployed in two ways, which are the network or host level. The host-level deployment observes the events of a device such as a computer system or a node in IoT. The network-level deployments monitor the network traffic flow to detect attacks or abnormal activities. The network-level IDS are usually hosted on dedicated devices or the gateways [4]. The network-level IDS (NIDS) can largely be classified into three classes based on its detection methodology. These classes are signature-based, anomaly-based or a hybrid based [5]. The signature-based IDS relies on attack signatures or rules stored in its database for detecting attacks, it detects the attacks by comparing and matching the network traffic flow with the stored attack signatures or rules. The signature-based IDS achieves a 100% accuracy in detecting known attacks. However, it suffers from zero-day or unknown attacks and it is unsuitable for the resource-constrained IoT due to its operational needs. The anomaly-based IDS relies on the profile of normal traffic flow created. It compares the network traffic flow with the normal profiles, any deviation from this profile is considered an attack. The anomaly based IDS is capable of detecting zero day or unknown attacks. It is widely developed using statistical or machine learning techniques. Even though its application is suitable for the IoT environment, it has its own challenges such as a high number of false-positives rate when network traffic flow is misclassified [6]. The hybrid IDS employs both signature-based and anomaly-based IDS detection methods in detecting attacks. It leverages the advantages of both while decreasing their disadvantages [7].

In efforts to solve the challenge of lack of resources on the IoT devices. The fog computing model can be utilized [8]. It brings resources such as storage, computation, and network services to the edge of the network in order to ensure improved services for the delay-sensitive applications [9]. This model will fit the deployment of the anomaly mitigation schemes in IoT networks, where the IoT devices can be released from the burden of computations and storage. This will ensure the efficient operation of the anomaly mitigation schemes.

In this paper, we proposed a DDoS attack mitigation framework that leverages the benefits of the fog to deploy an anomaly mitigation framework for the IoT network using machine learning. As compared with the existing schemes, our model provides fast attack detection with high accuracy and low false-positive rates as well as scalability. The framework classifies network traffic into legitimate and illegitimate before it passes it to the IoT gateway, the signature of the detected illegitimate traffic is stored in a database to ease computation and ensure faster response when the type of attack is performed again.

The rest of the paper is organized as follows. Section 2 presents related work. Section 3 describes the proposed DDoS mitigation framework. Section 4 contains the evaluation of the proposed framework. Finally, section 5 concludes the paper.

2. Related work

This section provides a review of some DoS and DDoS mitigation schemes in IoT. Several authors have proposed schemes using signature-based [10-11], anomaly-based [13-15] or hybrid based [16] approaches for attack detection, which ensures a secure and sustainable IoT network. Attacks such as DoS or DDOS should be detected before affecting the performance of the network. This can be achieved by designing robust anomaly mitigation schemes. Some of these proposed schemes are elaborated below.

A Denial-of-Service (DoS) detection scheme [10] is proposed for IPv6 over Low-power Wireless Personal Area Network protocol (6LoWPAN) based Internet of Things. The scheme is developed on the ebbits network framework, it uses probes that are placed in the area of interest and connected to an IDS in a wired mode. The probes operate in a promiscuous mode, it captures packets from network traffic for analysis using the adopted IDS system. The scheme employs Suricata that utilizes a packet threshold rule for detecting anomalies in the network traffic. The scheme was able to successfully detect a DoS attack (UDP flooding).

A real-time DDoS attack detection scheme [11] is proposed for IoT. The scheme employs on Complex Event Processing (CEP). The CEP scheme consists of three phases namely event filter, event processor (packet analyzer & attack detection) and action engine. The event filter observes and gathers the network traffic flow, the event processor analyses the packets' characteristics to decide which type of attack is occurring. The action engine is in charge of controlling events that trigger the CEP rules on presumed intrusion activity. It subsequently denies the events' access to important services. The scheme achieves better performance than Bro IDS.

A DDoS attack mitigation framework [12] is proposed for the Internet of Things. The framework is embedded in the border router and consists of two stages namely analysis and monitoring stages. The analysis stage monitors the inbound traffic and determine if it is suspicious or not. Firstly, by checking its blacklist saved on a dedicated server. Secondly, it analyses the packets by checking the bit rate and the payload size. It drops the packet with bit rates above a threshold and saves their source in a blacklist and forwards the packets with payload size above a threshold to a grey list on the dedicated server. The monitoring stage monitors packets on the grey list. It drops the packets if they keep coming from the same source, adds the source address in the blacklist and classifies them as DoS or DDoS attack packets. The framework fits the IoT environment and can adapt to different applications.

A lightweight intrusion detection scheme based on energy consumption analysis is proposed to detect DoS in IoT networks [13]. The scheme uses mesh-under and route-over routing energy prediction models to analyses energy consumption. Consumption of more than 30% of the previous consumption of any node is considered an attack. The scheme achieves efficient and accurate detection of DoS attacks with 100% detection rate.

A Multidimensional Trust-Based Anomaly Detection (MTBAD) scheme [14] is proposed for the IoT network. The MTBAD scheme evaluates trust based on reputation, Quality of Service (QoS), social relationship. The trust level of each node is evaluated using a fuzzy approach. The anomalies are detected when the trust value is above a threshold. In the event of an anomaly, the system is prompted to re-evaluate the trust of the whole system. The MTBAD scheme achieves a very low false alarm rate with a proper trust level threshold.

A DDoS detection and prevention scheme [15] is proposed for IoT networks. The scheme employs agent-based technology for attack detection. The scheme deploys the agent on the border router to stop attacks from outside the network. The scheme maintains a greylist and blacklist for monitoring and blocking access temporarily or permanently, respectively. The greylist is updated every 40s while the blacklist is updated every 300s. The scheme is suitable for small IoT networks.

A hybrid lightweight anomaly detection scheme for low-resource IoT devices using a game-theory approach is proposed [16]. The scheme employs a signature-based and anomaly-based detection (Back Propagation Network) schemes on the IoT devices. It utilizes a Nash Equilibrium to decide when to activate the anomaly-based detection technique in order to save energy of the constrained IoT devices. The scheme achieves a high detection rate and low false-positive rates with low energy consumption.

Although the above schemes proposed DDoS mitigation schemes in IoT, none of the schemes employ fog computing in deploying their solutions. This prompted the authors to propose a framework that utilizes the potentials of fog computing in DDoS attack mitigation.

3. Proposed framework

In this paper, we propose a DDoS mitigation framework using fog computing in order to ensure accurate and fast attack detection as well as scalability. The framework employs an anomaly-based mitigation methodology based on machine learning to detect a DDoS attack alongside a database. By employing fog computing in deploying the attack detection framework for IoT. The operational requirement challenges such as computation and storage of the anomaly mitigation schemes will be solved. The operational procedure of the framework is shown in figure 2. The network traffic flow is first scanned against attack signatures of previously detected attacks stored in a database. If an attack is detected, the flow is blocked/drop and an alarm is sent to the administrator. Otherwise, the traffic flow is passed through a classifier. The classifier distinguishes between the normal and abnormal network traffic flow by comparing the traffic flow with a model of a normal traffic flow created. Normal traffic flow is allowed to pass into the IoT network, on the other hand, an abnormal network traffic flow is considered as an attack. Hence, it is blocked or dropped, an alarm will send to the administrator. The signature of the abnormal traffic is updated in the database to ensure an up-to-date database. This will ensure a faster response when the same attack is performed in the future.

The DDoS mitigation framework utilizes a k-Nearest Neighbors (k-NN) classification algorithm [17] for the detection of DDoS attacks due to its simplicity, efficiency, and accuracy in classification [18]. Although, the k-NN algorithm has been utilized for DDoS detection in traditional networks [19], intrusion detection in Wireless Sensor Networks (WSN) [20] and detecting attacks such as User to Root (U2R) and Remote to Local (R2L) attacks in IoT networks [21][22]. We employ k-NN on the fog for DDoS attack detection in IoT networks. The k-NN classifies unknown data by observing the k data points in a training set that are near to it in the input space. Thus, it requires a distance measurement technique like Manhattan or Euclidean distance measuring technique. The Algorithm below shows the basic operation of the k-NN algorithm.

Algorithm: Basic k-NN algorithm [23]

```
Input: Training samples $D$, Test sample $d$, $K$
Output: Class label of the test sample
1: Compute the distance between d and every sample in $D$
2: Choose the $K$ samples in $D$ that are nearest to d; denote the set by $P$ ($2D$)
```

3: Assign d the class that is the most frequent class (or the majority class)

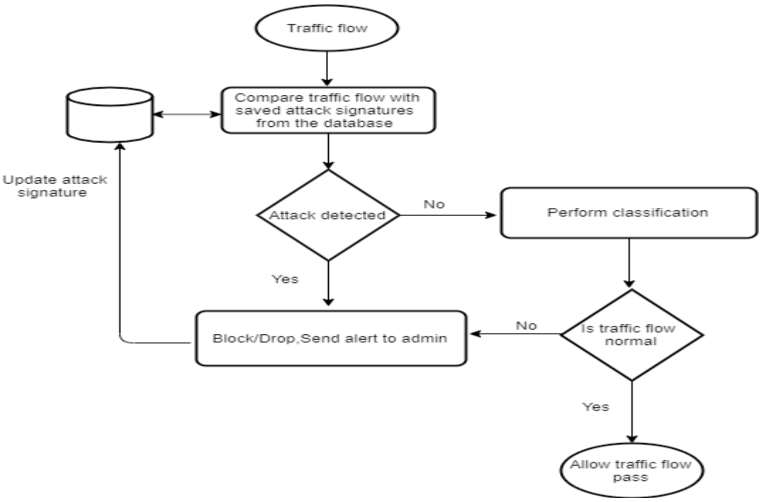

Fig. 1. Flowchart of the proposed framework.

4. Performance Evaluation

This section presents the performance evaluation of the k-NN classifier employed in the anomaly-based scheme of the framework. The description of the dataset utilized, evaluation methodology, and the results with discussions**.**

4.1 Description of Dataset

The DDoS attacks are one of the major security challenges in the IoT networks. To evaluate our DDoS mitigation framework. A dataset that provides a good representation of such attacks is required. We utilize the CICDDoS 2019 dataset [23] for the evaluations. The CICDDoS 2019 dataset is developed at the Canadian Institute for Cybersecurity (CIC), University of New Brunswick (UNB), Fredericton, NB, Canada. The dataset was generated on a testbed that consists of two networks, which are attack network and victim network. The victim network comprises of a web server, a firewall, two switches, and four computers. The normal traffic from the victim network is generated using the B-Profile approach [24]. The attacks are executed from a third party network. This network executes two types of DDoS attacks on TCP and UDP protocols namely reflective and exploitation DDoS attacks as shown in figure 3. The dataset comprises of 80 features extracted using CICFlowMeter [25].

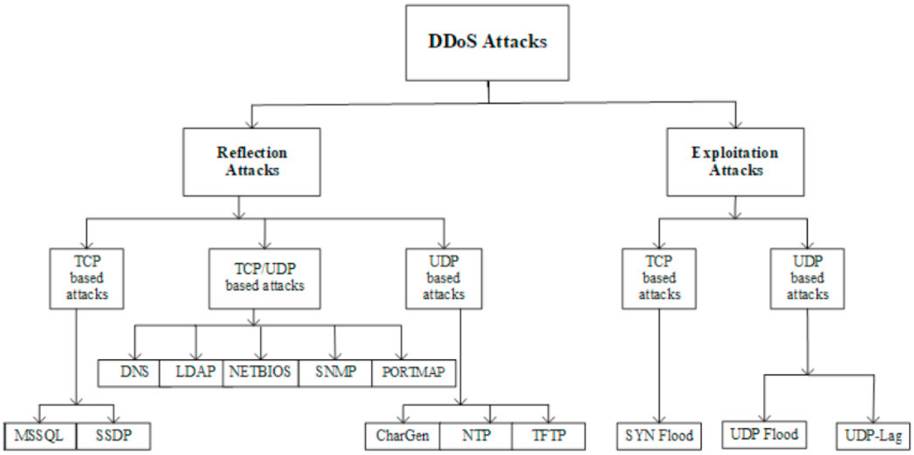

Fig. 2. Taxonomy of the DDoS attacks in CICDDoS 2019 dataset [23].

4.2 Evaluation methodology

In order to evaluate the k-NN classifier of our proposed framework. A total of 241173 instances were extracted randomly from the CICDDoS 2019 dataset. We selected 23 features using the feature selection by employing the ranker search method and information gain, which removes redundant and irrelevant features. These features selected represent the best features that will give good performance in terms of classification. The k-NN classifier is evaluated against Decision Tree (DT) and Naïve Bayes (NB) classifiers using the 10-fold cross-validation. The evaluations are in terms of accuracy, false-positive rate, precision, recall and F1 Score of binary classification (normal and attack). In addition, the effect of distance measurement techniques namely Euclidean, Manhattan, and Chebychev distance measurement techniques are investigated on the CICDDoS 2019 dataset in terms of accuracy. The performance metrics [26] evaluated are explained below

- **Accuracy** is a metric that estimates the overall percentages of detection and false alarms an IDS model produces, it reflects the overall success rate of any IDS, and is computed as,

$$\text{Accuracy} = (TN + TP)/(TP + FP + TN + FN) \qquad (1)$$

- The **Detection Rate (DR)**, also called the true positive rate (TPR) or recall, is the proportion of correctly classified malicious instances of the total number of malicious vectors and is computed as,

$$DR = TP/(FN + TP) \qquad (2)$$

- The **False Positive Rate (FPR)** also called false alarm rate is the percentage of normal vectors of the total number of normal vectors misclassified as attacks and is computed as,

$$FPR = FP/(FP + TN) \qquad (3)$$

- The **False Negative Rate (FNR)** also called precision is the percentage of misclassified attack vectors of the total number of attack instances, given as,

$$FNR = FN/(FN + TP) \qquad (4)$$

- The **F1 Score** is the weighted average of the recall and the precision and is computed as,

$$\text{F1 Score} = 2*(\text{Recall} * \text{Precision}) / (\text{Recall} + \text{Precision}) \qquad (5)$$

The F1 score is important and gives more insight into the performance of the IDS. It considers the false positives and false negatives. The F1 score is beneficial especially when the amount of the class labels is uneven or skewed.

Where,

- True Positive (TP): Total predicted classes as true that are actually true.
- False Positive (FP): Total predicted classes as true that are actually false.
- True Negative (TN): Total predicted classes as false that are actually false.
- False Negative (FN): Total predicted classes as false that are actually true.

The performance evaluation was performed using Waikato Environment for Knowledge Analysis (WEKA) [27] on a windows 10 operating system with 8GB RAM and i7 processor @ 2.70 GHz.

4.3 Results and Discussion

The evaluation results of the proposed k-NN classifier employed in our fog based framework in binary classification are discussed below.

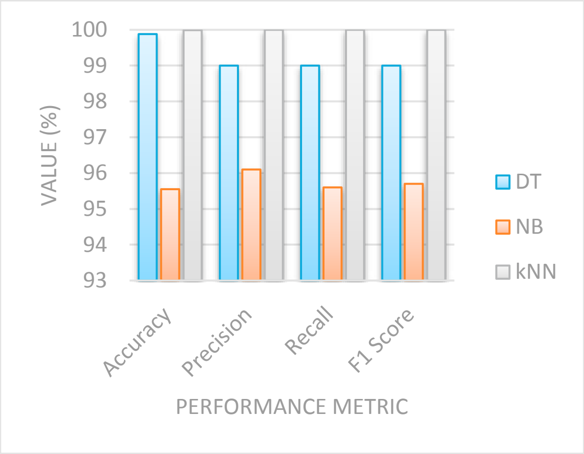

Fig. 3. Binary classification.

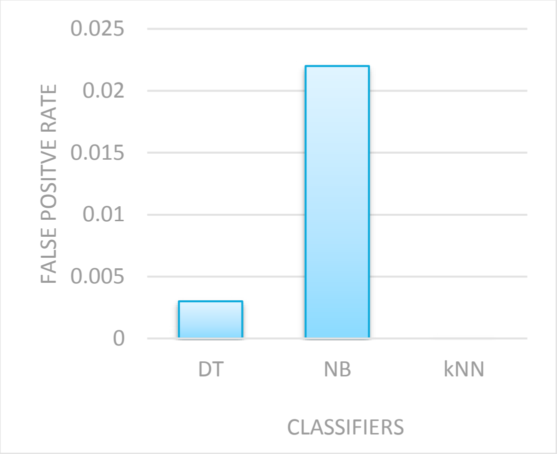

Fig. 4. false positives rates of the classifiers.

Figure 4 presents the binary classification results of k-NN, DT and NB classifiers. The k-NN achieved the best results in terms of accuracy with 99.99% while DT and NB recorded 99.88% and 95.55 %, respectively. The k-NN recorded 100% in terms of precision, recall and F1 score. The DT recorded 99% in terms of precision, recall and F1 score. While the NB recorded 96.10%, 95.60% and 95.70% in terms of precision, recall and F1 score, respectively. In addition, figure 5 shows the false positives rate of the classifiers with k-NN recording zero. The results show that the k-NN classifier has achieved superior results than DT and NB classifiers, which will translate to good performance in detecting DDoS attacks. Table 1 shows a summary of the binary classification results.

Table 1. Summary of binary classification results.

S/No	Classifiers	Accuracy (%)	False positive rate	Precision (%)	Recall (%)	F1 Score (%)
1	DT	99.88	0.0030	99	99	99
2	NB	95.55	0.022	96.10	95.60	95.70
3	k-NN	99.99	0	100	100	100

Table 2. Accuracy of k-NN classifier with different distance measurement techniques.

S/No	Distance Measurement Technique	Accuracy (%)
1	Euclidean	99.9954
2	Manhattan	99.9988
3	Chebychev	79.7577

Table 2 presents the accuracy results of the k-NN classifier employed in the proposed framework with different distance measurement techniques. The Euclidean and Manhattan distance measurement techniques recorded similar accuracy results with 99.99% while the Chebychev distance measurement techniques obtained a lower accuracy with 79.75%. Although, these distance measurement techniques belong to the same family, which is the power distance [28]. The Euclidean and Manhattan distance measurement techniques are suitable for distance calculation between two distances in any vector dimension provided the data is numerical. While the Chebychev distance measurement technique is suitable for the distance between two points if they are different in one dimension [18].

5. Conclusion

The combination of 5G and fog computing facilitates the efficient deployment of security solutions for IoT networks. The 5G enables connecting a large number of devices and provides communication with high speed and low latencies while the fog provides the resources (storage and computation) essential for security solutions such as anomaly mitigation. In this paper, a DDoS attack mitigation framework using fog computing is proposed to ensure fast and accurate detection. The framework employs an anomaly-based mitigation method that utilizes a k-NN classification algorithm alongside a database. The database stores signatures of previously detected attacks, which will offer a faster detection when the attack is executed again. We evaluated the proposed k-NN classifier for the framework using the CICDDoS 2019 dataset. The results demonstrate that the k-NN classifier will be able to detect DDoS attacks with high accuracy. In the future, we intend to implement the framework on available fog computing platforms to further evaluate our approach.

References

[1] Li S, Da L, Zhao S.(2018) "5G Internet of Things : A Survey." *Journal of Industrial Information Integration* :1–28.

[2] Statista. IoT: Number of connected devices worldwide 2015-2025, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed 2 December 2019).

[3] Hoang DH, Nguyen HD.(2018) "A PCA-based method for IoT network traffic anomaly detection." In: *International Conference on Advanced Communication Technology, ICACT*. Global IT Research Institute (GiRI): 381–386.

[4] Raza S, Wallgren L, Voigt T.(2013) "SVELTE: Real-time intrusion detection in the Internet of Things." *Ad Hoc Networks* **11**(**8**): 2661–2674.

[5] Shaikh RA, Jameel H, D'Auriol BJ, Lee, Heejo, Lee, Sungyoung, Song, Young Jae.(2009) "Intrusion-aware alert validation algorithm for cooperative distributed intrusion detection schemes of wireless sensor networks." *Sensors* **9(8)**: 5989–6007.

[6] AL-Hawawreh M, Moustafa N, Sitnikova E.(2018) "Identification of malicious activities in industrial internet of things based on deep learning models." *Journal of Information Security Applications* 41: 1–11.

[7] Zarpelão BB, Miani RS, Kawakani CT, Cláudio Toshio, De Sean Carlisto.(2017) "A survey of intrusion detection in Internet of Things." *Journal of Network and Computer Applications* 84: 25–37.

[8] Rauf A, Shaikh RA, Shah A. "Security and privacy for IoT and fog computing paradigm.(2018)" In: *15th Learning and Technology Conference (L&T).IEEE*. Jeddah, Saudi Arabia : 96–101.

[9] Yaseen Q, Albalas F, Jararwah Y, Al-Ayyoub M.(2018) "Leveraging fog computing and software defined systems for selective forwarding attacks detection in mobile wireless sensor networks." *Transactions on Emerging Telecommunication Technology* 2018 **29**(**4**): 1–13.

[10] Kasinathan P, Pastrone C, Spirito MA, Vinkovits M.(2013) "Denial-of-Service detection in 6LoWPAN based Internet of Things." In: *International Conference on Wireless and Mobile Computing, Networking and Communications*. IEEE: 600–607.

[11] Da Silva Cardoso AM, Lopes RF, Teles AS, Magalhaes Fernando B V .(2018) "Real-time DDoS detection based on complex event processing for IoT." In: *Proceedings - ACM/IEEE International Conference on Internet of Things Design and Implementation, IoTDI* : 273–274.

[12] Vipindev Adat, Gupta BB.(2017) "A DDoS attack mitigation framework for internet of things." *International Conference on Communication and Signal* Processing:2036–2041.

[13] Lee T-H, Wen C-H, Chang L-H, Chiang H S, Ming C H.(2014) "A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LowPAN." In: *Advanced Technologies, Embedded and Multimedia for Human-centric Computing* :1257–1268.

[14] Gai F, Zhang J, Zhu P, Xinwen Jiang B.(2017) "Multidimensional Trust-Based Anomaly Detection System in Internet of Things." In: *Wireless Algorithms, Systems, and Applications. WASA 2017. Lecture Notes in Computer Science*. Springer, Cham :302–313.

[15] Sonar K, Upadhyay H.(2016) "An Approach to Secure Internet of Things Against DDoS." In: *International Conference on ICT for Sustainable Development. Advances in Intelligent Systems and Computing*. Singapore: Springer.

[16] Sedjelmaci H, Senouci SM, Al-Bahri M.(2016) "A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology." In: *2016 IEEE International Conference on Communications, ICC 2016*. IEEE :1–6.

[17] Fix, E. and Hodges JL.(1951) "*Discriminatory analysis. Nonparametric discrimination; consistency properties". Technical Report 4, USAF School of Aviation Medicine Randolph Field, TX, USA*.

[18] Prasath VBS, Haneen Arafat Abu Alfeilat ABAH, Lasassmeh O, Lasassmeh O, Ahmad S. Tarawneh, Mahmoud B Alhasanat, Hamzeh S. Eyal Salman.(2017) "Distance and Similarity Measures Effect on the Performance of K-Nearest Neighbor Classifier -- A Review." arXiv preprints 1708.04321:1–39.

[19] Nguyen HV and Choi Y.(2009)"Proactive detection of DDoS attacks utilizing k-NN classifier in an anti-DDos framework." *International Journal of Computer, Electrical Automation, Control and Information Engineering* **39**(**3**): 640–645.

[20] Li W, Yi P, Wu Y, Pan L, Li J.(2014)"A new intrusion detection system based on KNN classification algorithm in wireless sensor network." *Journal of Electrical and Computer Engineering*.

[21] Aljawarneh SA and Vangipuram R.(2018) "GARUDA : Gaussian dissimilarity measure for feature things." *Journal of Supercomputing*.

[22] Pajouh HH, Javidan R, Khaymi R, Dehghantanha A,Choo Kim-Kwang R.(2016) "A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks." *IEEE Transactions in Emerging Topics in Computing* **7**(**2**):314-323

[23] Sharafaldin I, Lashkari AH, Hakak S, Ghorbani A A.(2019) "Developing Realistic Distributed Denial of Service (DDoS) Attack Dataset and Taxonomy". In: *International Carnahan Conference on Security Technology (ICCST)*. Chennai,India.

[24] Sharafaldin I, Gharib A, Lashkari AH,Ghorbani AA.(2018)"Towards a reliable intrusion detection benchmark dataset." *Software Networking* **1**: 177–200.

[25] Lashkari AH, Draper-Gil G, Mamun MS, Ghorbani AA.(2017) "Characterization of tor traffic using time based features." In: *International Conference on Information Systems Security and Privacy (ICISSP)* :253–262.

[26] Moustafa N, Hu J, Slay J. (2019)"A holistic review of Network Anomaly Detection Systems: A comprehensive survey." *Journal of Network and Computer Applications* **128**: 33–55.

[27] Frank E, Mark A. Hall, Witten IH. (2016)"*Data Mining: Practical machine learning tools and techniques."* Fourth edition. Morgan Kaufmann Publishers Inc.

[28] Weller-Fahy DJ, Borghetti BJ, Sodemann AA.(2015) "A Survey of Distance and Similarity Measures Used Within Network Intrusion Anomaly Detection." *IEEE Communications Surveys and Tutorials* **17**(**1**): 70–91.