IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 35, No. 1, February, 2021, pp. 11-21
Journal homepage: http://iieta.org/journals/ria

Attack and Anomaly Detection in IoT Networks Using Supervised Machine Learning Approaches

Himani Tyagi*, Rajendra Kumar

Department of Computer Science, Jamia Millia Islamia University, New Delhi 110025, India

Corresponding Author Email: him.tyagi30@gmail.com

https://doi.org/10.18280/ria.350102

Received: 7 December 2020
Accepted: 9 February 2021

Keywords:
IoT, intrusion detection system, attacks, BoT IoT dataset, detection, machine learning, SVM

ABSTRACT

IoT is characterized by communication between things (devices) that constantly share data, analyze, and make decisions while connected to the internet. This interconnected architecture is attracting cyber criminals to expose the IoT system to failure. Therefore, it becomes imperative to develop a system that can accurately and automatically detect anomalies and attacks occurring in IoT networks. Therefore, in this paper, an Intrsuion Detection System (IDS) based on extracted novel feature set synthesizing BoT-IoT dataset is developed that can swiftly, accurately and automatically differentiate benign and malicious traffic. Instead of using available feature reduction techniques like PCA that can change the core meaning of variables, a unique feature set consisting of only seven lightweight features is developed that is also IoT specific and attack traffic independent. Also, the results shown in the study demonstrates the effectiveness of fabricated seven features in detecting four wide variety of attacks namely DDoS, DoS, Reconnaissance, and Information Theft. Furthermore, this study also proves the applicability and efficiency of supervised machine learning algorithms (KNN, LR, SVM, MLP, DT, RF) in IoT security. The performance of the proposed system is validated using performance Metrics like accuracy, precision, recall, F-Score and ROC. Though the accuracy of Decision Tree (99.9%) and Randon Forest (99.9%) Classifiers are same but other metrics like training and testing time shows Random Forest comparatively better.

1. INTRODUCTION

Internet of Things (IoT) has evolved as an advancement in the technology field which integrates components from computer science (like networking, mobile computing, and software engineering) and electronics (sensors, actuators, embedded technology, communication protocols). The main goal of this technology is to ease human life by automating existing device infrastructure and thereby reaching every sphere of human life. The IoT infrastructure is identified by presence of millions of interconnected devices (things) sharing and analyzing data from anywhere and at any time with the help of the internet. The introduction of the internet in this technology has made communication fast and easy but at the same time open platforms for cybercriminals [1].

IoT architecture mainly consists of three layers namely Perception layer, Network layer, and Application layer [2]. Perception layer is responsible for everything extending from sensing (using sensors) to gathering information. The common attacks on perception layer are malicious physical attacks on sensor-equipped devices, unauthorized access to devices, etc. In Network layer, the devices equipped with sensors and actuators communicate with other IoT devices and gateway using wireless (WiFi, LAN, 3G, 4G) technology [3]. Therefore, most prominent attacks on this layer are DoS DDoS, information Theft, information gathering, gateway attacks, routing attacks, etc. To overcome these attacks, a detection and prevention system is required that can effectively monitor the traffic coming and leaving the network. The system is described as Intrusion Detection System (IDS). The goal of an IDS is to unmask all the malicious activities where even a traditional firewall fails [4]. IDS are responsible for continuously monitoring the network and searching suspicious behavior in the network [5]. IDS works on the network layer of protocol stack by quickly analyzing the packet traveling through a network. Intrusion detection systems are classified as SIDS (Signature based Intrusion Detection systems) and AIDS (Anomaly based Intrusion Detection System). Signature based IDSs relies on pre defined malicious activity by comparing current traffic pattern with database at regular interval of time and performs well on previously known attacks but fails on unknown or sudden attacks [6]. Hence, it would be impractical to rely on previously known patterns in a dynamic network like IoT. In contrast to this, Anomaly based IDSs are capable of tackling this situation by using network parameters learning approaches. These systems rely on deviation from normal behavior to detect intrusions [7, 8]. Hence, more fertile for a complex and diverse ecosystem like IoT. Therefore, an anomaly based Intrusion Detection systems (AIDS) responsible for monitoring the packets and raising alarms when there is any anomaly occurring in the network is proposed.

Machine Learning refers to giving machines the ability to make decisions using past experiences through learning [9]. Machine learning algorithms are classified into Supervised and Unsupervised algorithms. These algorithms are classified based on the task in hand. Supervised machine learning algorithms are used for classification, regression, and

predictions whereas unsupervised machine learning approaches are used for clustering applications, outlier detection, etc. Therefore, IDS is a classification task. Hence, in this paper, Supervised Machine Learning algorithms are employed that proved to be effective in detecting attacks in a complex environment like IoT.

Furthermore, most of the existing Intrusion Detection Systems are based on attack specific features like during DDoS speed of source IP address change [10] for detecting anomalies and attacks. These systems certainly Fail for detecting other types of attacks. Hence, in this Paper a novel feature set after comprehensively understanding the IoT environment characteristics is proposed. Since results show effective detection for Four types of attacks namely DoS DDoS, Reconnaissance or Information gathering, Information Theft synthesizing only seven derived features, the derived features set is IoT network characteristic dependent and attack independent. We expect that these features will also be effective in detecting other types of attacks in IoT networks.

Here, our goal is to develop a robust, secure, and deployable security system that provides effective and accurate detection against anomalies and attacks occurring in IoT networks. Therefore, in this paper, an intrusion detection system for securing IoT networks is proposed.

Our research contributions

- To propose a robust and deployable machine learning based attack and anomaly detection security system, by employing IoT specific characteristics instead of attack dependent characteristics.
- To illustrate the effectiveness and efficiency of supervised machine learning classifiers in providing accurate security systems for IoT networks.
- To compare the performance of supervised machine learning classifiers for binary (anomaly detection) and multi classification (attack detection).

2. RELATED WORK

In this section, Machine Learning based Intrusion detection system for securing IoT networks are discussed. Likewise, Thamilarasu and Chawla [1] developed an IDS to detect attacks namely blackhole, opportunistic, DDoS, sinkhole, and wormhole in IoT. Deep learning approach is employed for attack detection. The features selection in proposed system is based on information gain at each DNN layer. The performance of the proposed Deep Learning model showed 97% True Positive Rates and 95% average precision against all type of attacks. Five models are developed for each attack type detection. Whereas in our study a single model can predict a wide variety of attacks.

By applying dimensionality reduction technique [8] like PCA and LDA and two-tier classification using supervised machine learning classifiers for detecting DoS, U2L, R2L and probe attacks. From a feature count of 35 in NSL-KDD dataset is reduced to 2 features. The detection accuracy of the proposed system reaches to 84.82%. The feature reduction technique used changed the real meaning of the environment. Hence, results in low detection accuracy.

A scalable deep learning-based routing attack detection system in IoT is presented [11]. The dataset is produced by multiple simulation scenarios using real life equivalent COOJA simulator to ensure the fidelity of the models. The size of the generated data is 64×10^6 (64MB). They have focused on detecting three categories of network attack (decreased rank, hello-flood, and version number) using RPL based network parameters. The proposed IDS is a routing attack dependent security system. Yavuz et al. [12] proposed a framework to identify network probing and simple form of DoS (SYN flood, UDP flood) attacks using machine learning classifier. The proposed system shows low precision (high FP) and low recall (high FN) values for DoS attack detection. Hence, Not delivering promising results for attack detection.

Also, Hussain et al. [9] used synthetic dataset [13] containing total of 3,57,952 samples, 13 features (data type: nominal, continuous, discrete, nominal) and 8 classes. The feature set employed to assist machine learning classifier are static features. The proposed IDS is responsible for DOS, data type probing, malicious control, malicious operation, scan, spying, wrong setup attack detection occurring at various IoT sites in a smart home. Among all the supervised algorithms used Random Forest gave highest accuracy of 99.4% for all attack type detection.

Pahl and Aubet [14] designed an intrusion detection system using NSL-KDD dataset. Assuming that the dataset is modifiable, extensible, and reproducible. This data set contains four types of attacks (probe, R2L, U2R, DoS) but lacks IoT traces and modern attack types. In this work, binary and multiclass classification comparison for shallow and deep learning is shown. The authors claim reduction in FAR using deep learning to 0.85 in contrast to the value of 6.57 using shallow learning for binary classification. And FAR of 2.57 using DL and FAR of 4.97 employing SL for multiclass classification.

Machine learning detection process is evolving with great results and considerations in the security field of IoT. Consequently, Diro and Chilamkurti [15] proposed a method of securing IoT devices by using the difference between normal and attack traffic based on stateless and stateful features. This study illustrates the fact that the network traffic patterns from consumer IoT devices differ from non IoT device networks. Hence, the solution has applicability in IoT environment for providing detection and protection of consumable IoT devices. Doshi et al. [16] proposed a unique and novel anomaly based attack detection method named it as the Traffic log combined detection method. The proposed framework integrates log data and traffic data using fuzzy association rule for attack detection. The proposed strategy results in a significant decrement in False Positive and False Negative. This work also claims that the Network flow characteristics can help detect various types of attacks. Khraisat et al. [10] perform deep packet analysis for detecting DDoS attacks by using flow entries (like Source IP, Destination IP, Source Port, Destination Port, Number of packets) in a Software defined networks. The characteristic values extracted are attack dependent and Hence, fail for other types of attack besides DDoS attack. The False alarm rate of proposed IDS even reaches 0% which is practically not possible in a real life scenario. Lu et al. [17] derived classification rules using Decision tree technique to detect anomalies. Hence results in a Signature based Intrusion Detection System (SIDS). The proposed attack detection model works well for the known attacks but fails for zero-day attacks. Hence, not fruitful for IoT environment.

After analyzing all the views provided in the above research papers the importance of machine learning and deep learning approaches in IoT security is quite evident. The importance of features for performing classification also plays a vital role

before applying any machine learning classifier. Additionally, researchers tend to simulate IoT scenarios to develop an IoT specific IDS due to unavailability of datasets incorporating IoT scenarios.

3. DATASET AND PROCESS DESCRIPTION

The opensource dataset is collected from UNSW-Canberra-cyber data repository provided by Kumar et al. [18]. This dataset is designed at the Research Cyber Range Lab of UNSW Canberra. The environment includes both normal and botnet traffic. The Network platform consists of Virtual Machines managed through vSphere platform. The testbed configuration consists of 4 attacking nodes and 4 normal nodes and one server. The introduction of simulated (using Node Red tool) IoT services such as weather station for generating information about temperature, humidity and air pressure, a smart fridge, motion activated lights, garage door, a smart thermostat makes it different from other datasets like UNSW-NB15 [19], NSL-KDD, CIDDS-001, used in literature. This dataset is selected for the study because:

I. Most recent and advance dataset with simulated IoT services as compared to the abovementioned datasets [20].
II. The dataset contains modern wide variety of common IoT attack samples like DDoS (TCP Flooding, UDP Flooding, HTTP Flooding), DoS (TCP Flooding, UDP Flooding, HTTP Flooding, Reconnaissance (OS fingerprinting, service scan) and Information Theft (data exfiltration and keylogging).
III. The dataset contains modern networking (Wireless sensor Networks) features.

Table 1. Frequency distribution of considered attacks from dataset

Number of instances	Frequency	Tools used for generation
DdoS	28.4%	Golden-eye
DoS	33.8%	Hping3
Reconnaissance	28.4%	Nmap, xprobe2, metasploit
Information Theft	1.80%	Metasploit
Normal	7.32%	

3.1 Detection methodology

Dataset is a core ingredient in fabricating any intrusion detection system. Therefore, the first step towards developing proposed IDS contributes to dataset collection. The dataset collected for this study is provided by Kumar et al. [18], a recent modern dataset with the presence of IoT traces and BoT instances. The overall framework is illustrated in Figure 1.

The dataset is collected from 75 CSV files with almost 69.3 GB size. Inside these files, Datum has mixed values for four categories of traffic namely Denial of Service traffic (DoS, DDoS), Information gathering traffic (Service scan, OS fingerprinting), information theft traffic (data exfiltration, key logging) and Normal samples. Hereupon, the dataset is very large and complex. Therefore, out of 7,15,37,674 instances of DoS, random sampling is performed and 25,000 random samples are extracted, out of 18,21,639 instances of information gathering, 25000 instances are randomly extracted,1587 information theft instances are collected from 75 csv files. Similarly, out of 9543 normal instances distributed in 75 files 6430 instances are extracted. Resulted in a more balanced and maintainable dataset for analysis which is shown in Figure 2.

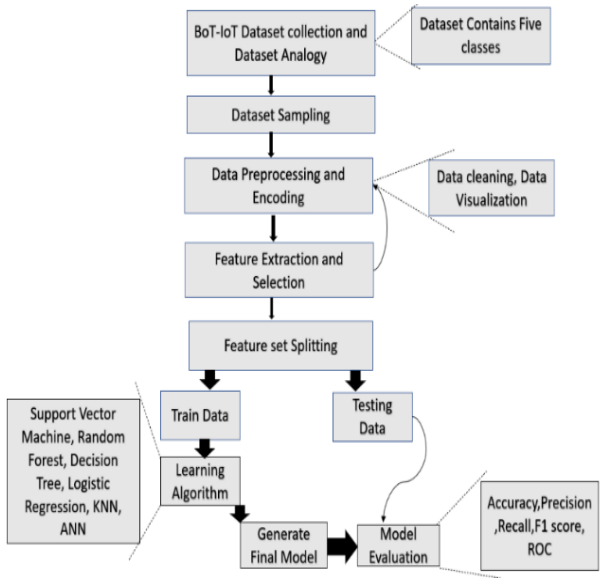


Figure 1. Overall attack and anomaly detection process

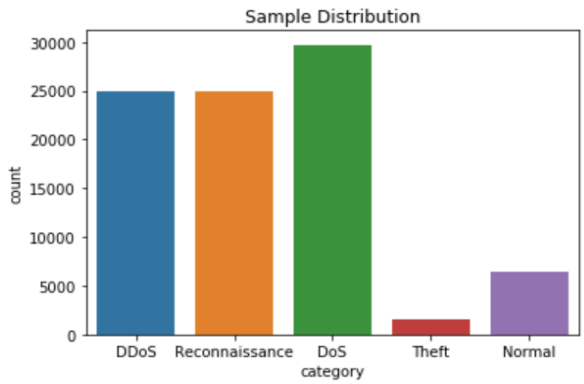


Figure 2. Dataset distribution after preprocessing

Now, the dataset contains instances belonging to majorly four categories of attack and normal data instances. These instances are comprehensively analyzed in pursuit of finding IoT specific feature set discussed later. Data cleaning is performed throughout the process. After the dataset collection, sampling, cleaning step, the next step is feature extraction and selection. The features are extracted and selected from the BoT-IoT dataset [21] after comprehensively understanding IoT network characteristics to derive IoT specific features from the dataset. Hence, results in a novel IoT specific flow based feature set. The extracted feature set represents how communication evolves in a smart environment such as a Smart Home. The derived features are Packet size, protocols used for communication, state of communication, packet ratio (PR), byte ratio (BR), number of requests at a given time (NR), and inter packet gap duration (IGP) shown in Table 2. These features are lightweight and can be easily derived from network recording systems like flow entries in SDN (software Defined Networks). The dataset contains some categorical features like protocol and state that are encoded using Label Encoder() to effectively analyze and visualize the traffic.

Table 2. Important features derived for fabricating IDS specifically for IoT networks

S.NO	FEATURES		DESCRIPTION	TYPE
1	Proto		Protocol used for communication	Categorical
2	BRV(Derived)	Sbytes Dbytes	Total byte count in transaction	Discrete
3	State		Transaction state	Categorical
4	NR(Derived)		Number of requests at a time	Discrete
5	PRV(Derived)	Spkts Dpkts	Total packet count in transaction	Discrete
6	Category		category of attack	Categorical
7	Packet size (Derived)		Size of each packet(bytes/packets)	Discrete
8	IPG (Derived)		Time between packets sent	Discrete

After feature extraction, the next step is again feature set cleaning. The feature Packet Ratio contains 867 rows as "NaN" values that are replaced with the mean of the column values. And byte ratio contains 1245 rows as "NaN" values that are also replaced with the mean of the column values. Now, the dataset with IoT specific features is ready to feed into a machine learning model.

These seven tuples represent input to the classifier. The classifier is trained on these features by splitting the dataset into training and testing set. The ratio of train and test set is taken as 70:30 respectively. Then the statistical performance of each classifier is evaluated using metrices like Accuracy, Precision, Recall, F-Score, and AUC. The performance difference is evaluated for both binary (anomaly detection) and multiclass classification (attack detection).

4. FEATURE SET EXTRACTION AND SELECTION PROCESS

The existing Intrusion Detection Systems discussed in background section lack in integrating IoT Traces. The inculcation of IoT traces is done by simulating IoT services like smart door, sensor services, smart door lock services, smart washing services, smart kitchen, thermostat, smart fridge, motion activated lights, garage door, etc. BoT-IoT dataset provides IoT traces specific to smart home by simulating five smart home services such as thermostat, smart door, smart fridge, motion activated lights, garage door. The effect of these services on network traffic logs is depicted by the following features.

On deploying the proposed system to gateway middleboxes like routers a strong security system to the network and devices connected to the network can be effectively implemented.

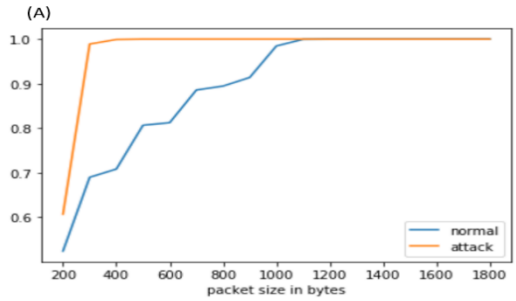
4.1 Extracted feature set

I. Packet size

The packet size represents size of command traveling in the network. And, IoT communication is characterized by regular ping commands like ON, OFF, START, STOP, connecting to the internet, or firmware updates [22] and Voice applications. Hence, Normal and attack traffic is separately visualized for finding out the size of packet traveling during communication. In this dataset, for each transmission, the size of a packet is derived using available features in the dataset i.e., Bytes and Packets. For each data sample S € {s1, s2,s3…..sn},

$$packet\ Size = \frac{Bytes}{Packets} \quad (1)$$

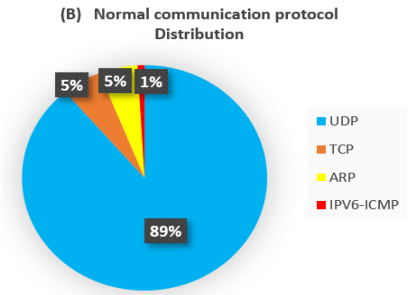
With reference to this, it has been observed that 90% of packet size values in attack traffic are under 200 bytes as an attacker wants to a send large number of small sized packets to overwhelm the target. Thus, causing Denial of legitimate services, downtime, network congestion, and packet dropping. In contrast to this, normal traffic corresponds to packet size range from 200 to 1200 bytes. The classifier can leverage this difference to classify benign and attack traffic.

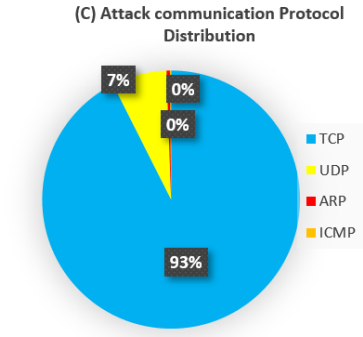


II. Protocol

The Protocol used for communication describes the way communication must take place in a wireless environment. IoT communication protocol significantly differ from traditional wireless network as they should have low latency, loss toleration connections, low power usage, and supports lightweight communication [23].

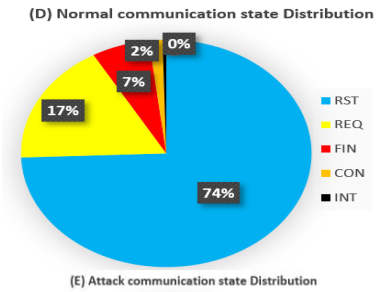
TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are two popular protocols for data transmission using the internet. But TCP follows strict rules of reliability and in order delivery of each and every byte which is inefficient practice for IoT communication. As an alternative to TCP an unreliable transmission protocol UDP is viewed as a better protocol in terms of energy efficiency, light weight communication, low latency and low powered applications like VoIP (Voice over IP) and streaming applications [24]. Also, In the dataset it has been observed that TCP and UDP communication protocols are used more frequently as compared to other protocols like ICMP, RARP, IGMP, IPv6-ICMP (Figure B). In normal traffic, UDP packets out number very small sized TCP packets due to frequent usage of streaming audios, video conferencing, voice over IP (VoIP), and video applications in smart home. In contrast to this, Attackers use TCP packets to target the victim.

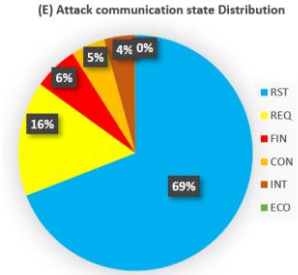




III. Connection state

UDP is a common protocol that allows data transfer between parties without establishing any agreement between the parties. Hence, UDP is suitable for light weight and low latency applications as discussed above. And, Connection state defines the state of communication using any data transfer protocol (UDP or TCP) with packets like FIN, ACC, CLO, CON, ECO, ECR, INT, NRS, URP, RST and REQ. These packets represent the real situation of communication parties.INT and CON packets represent connection establishment and initializing communication. Similarly, FIN is used for graceful communication termination. Whereas, When the network is in a congestion state, the packets are rejected by the server and in return, RST packets without any payload are sent by the server to the client informing about rejected SYN packet. Hence, a communication state with a large number of RST packets is an indication of anomalous activity in the network. In BoT-IoT dataset, a large number of RST packets are observed during attack traffic. In contrast to this, normal traffic contains a large number of INT and CON packets. These packets represent a normal communication state. This difference can be seen in the pie chart (Figure D and E).

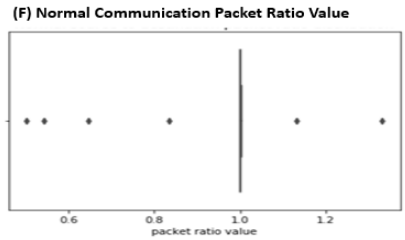


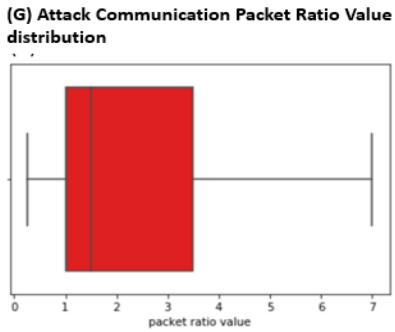


IV. Packet Ratio Value (PRV)

The packet is the basic unit of information traveling in the network. It consists of information like header information, sender and receiver address, and payload. The packets count traveling from source to destination must be equal to the packets count traveling from destination to host in reply. This value count increases or decreases but not equal in an event of attack [23]. Therefore, this feature is scanned closely in the dataset during this study. The packet drop count must be less or near to zero during the communication cycle. It has been found that 90% of Normal packets have the ratio value near to 1 Whereas, the values for packet ratio in attack data are greater than 1, Which clearly defines the difference between attack and normal scenario.

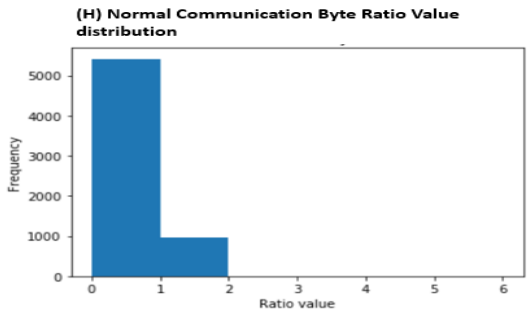
$$PRV = \frac{number\ of\ packets\ transmitted\ from\ source\ to\ destination}{number\ of\ packets\ received\ from\ destination\ to\ source} \quad (2)$$

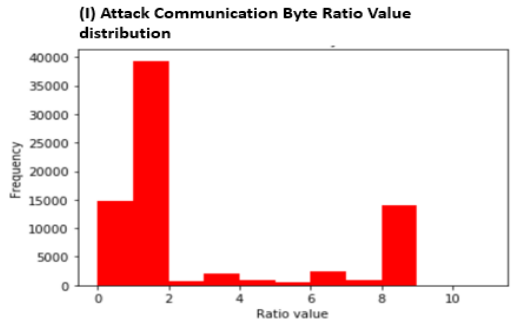




VI. Byte Ratio Value (BRV)

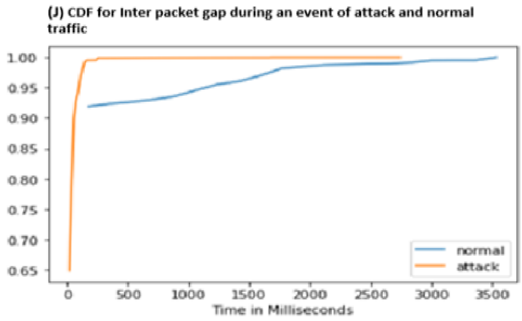
In circular communication between a sender and receiver, the number of bytes transferred from the sender to receiver and from receiver to sender should also be equal. During this study, this value is precisely observed for attack and normal traffic independently. This value ranges from 0 to 9. Out of 6430 normal samples, 5500 approximately 85% values represent ratio value between 0 to 1(approximately equal values). Whereas, out of 81293 attack samples, only about 18% values lie between this range. Rest 82% values are distributed among (2 to 9) value range. Hence, this feature can differentiate attack traffic from normal traffic.





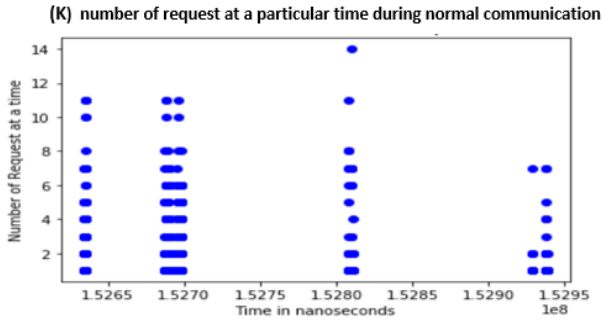
VII. InterPacketGap (IPG)

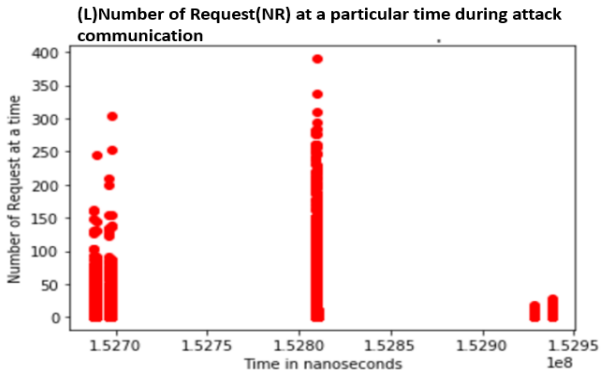
DDoS attack leads to other threatening events like data theft, data leakage, OS fingerprinting and data exfiltration attack. Hence, DDoS attack is a cascading attack. When this attack starts penetrating in the network, some unusual events with respect to time can also be observed. The interpacketgap is the time between sender starts sending packet and last time receiving a response. The time between request and response follows a regular pattern in normal IoT traffic due to regular services [14]. But, during an attack this time has 0 difference, means no gap between sending one to another packet, overwhelming the receiver with packets without waiting for the response. The difference using CDF (Cumulative distribution function) is shown that clearly shows the distribution in BoT-IoT dataset for attack and normal traffic. So, the classifier can leverage this difference to differentiate normal traffic from abnormal traffic.



VIII. Number of Requests (NR)

NR represents the number of requests at one particular time instance. The attacker tries to send as many requests as possible to overwhelm the target. In an attack scenario, it has been observed that the number of requests at a particular time is very large reaching 400 requests at a time. In a smart home a large number of requests do not usually occur. In the dataset Normal traffic represents a maximum of 14 requests at a particular time instance. A true scenario of a smart home environment. This difference can be leveraged by a classifier to differentiate between anomaly and normal traffic.





5. IMPLEMENTATION AND PERFORMANCE

5.1 Experimental setup

The work is carried out using DELL (inspiron13 5000) Laptop, with Windows 10 Enterprise 64-bit operating system installed, Intel(R)Core(TM)i5-8250U CPU @ 1.60GHz,1.80 GHz.8.00 GB RAM. Pandas, Numpy, Matplotlib, seaborn, scikit-learn, Keras Framework were used for all data related tasks.

5.2 Machine learning classifier algorithms

I. KNN

K Nearest Neighbor classifier is also known as Lazy classifier. In this, Distance is used as classification criteria. The distance between predicted values from all the values is calculated and based on the minimum value of distance the class of instance is decided. For this classification task, Euclidian distance is used with 5 neighbor voting (K=5). And, the distance between two points (X1,Y1), (X2,Y2) is calculated using,

$$\sum\sqrt{(X2-X1)^2+(Y2-Y1)^2} \qquad (3)$$

ROC curve shows good separability between TP and TN. Subsequently, KNN confusion matrix shows a clear distinction between DoS and DDoS samples, which indicates good classification accuracy of this classifier. But This algorithm is non-parametric and calculation intensive. In IoT environment, due to power and memory limitations more calculation intensive algorithm is not preferred.

II. Random Forest (RF)

Random forest is a supervised machine learning algorithm that creates a collection of decision trees. This classifier is fast and less complex. It has high accuracy than a single decision tree. In this study, ROC for RF shows promising results.

III. Support Vector Machine (SVM)

Support vector machine is another classification tool. In literature, SVM is widely used for intrusion detection in networks. But it is mostly used for anomaly detection (binary classification) where 99% accuracy is reached [15]. In this work, when SVM is employed for multi class classification. The soft margin SVM is trained by optimizing the following Lagrange Objective function.

$$argmax\ ai = \sum_{i=1}^{k} ai - \frac{1}{2}\sum_{i=1}^{k}\sum_{j=1}^{k} aiajyiyj\ \phi(xixj) \qquad (4)$$

The kernel function represented by $\phi(x_i x_j)$ will try to transform the non linearly separable data to a high dimensional space where data is linearly separable. The optimal C is 0.2 with RBF kernel, 0.001 tolerance is considered. The confusion matrix for SVM shows the confusion of classifier on almost all the classes. This classifier takes longest time as compared to other classifier on training and ROC curve generation.

Table 3. Evaluation metrics of our study

Classifier	Recall (multi)	(Binary)	Precision (multi)	(Binary)	Accuracy (Multi)	Accuracy (Binary)	F1-Score	AUROC
SVM	14.68%	67	92.6%	97.5	Testing =0.822 Training =0.85	Testing=0.952 Training=0.98	0.65	NA
RF	99.9%	99.9	99.9%	99.9	Testing= 0.99 Training=0.999	Testing=0.99 Training=0.99	0.99	1 for all classes
DT	99.8%	99.4	99.8%	98.6	Testing =0. 99 Training =0.99	Testing= 0.99 Training=0.998	0.99	1 for all classes
ANN	99.9%	96.4	99%	98	Testing=0.994 Training=0.992	Testing=0.93 Training=0.97	0.99	1for all except one class
LR	34%	46%	11%	50%	Training=33.8 Testing=33.87	Testing= 0.925 Training=0.927	17%	0.45
KNN	98.8%	96%	97.8%	98%	Testing=99 Training=99.2	Testing=0.991 Training= 0.994	0.99	1

IV. Logistic Regression (LR)

Linear Regression differs from Logistic regression in terms of bringing results of classification between 0 and 1. This is a powerful classifier for large dataset. This performs well for binary classification but on providing multiclass task, the classifier shows confusion and for some classes AUC reaches 0. That shows the incompatibility of this classifier for multiclassification. For binary classification also, it shows 92.2% accuracy but other parameters show inability for anomaly detection. The classifier is trained on 'lbfgs' solver with C=1 and 0.0001 tolerance.

V. Multilayer Perceptron (MLP)

MLP is complex as compared to the above mentioned classifiers. It is similar to a single layer perceptron with one more hidden layer added. ANN shows 1 ROC for all the classes with just class 4 that is Normal class as ROC value 0.99. Class 0 represents DDoS, Class 1 DoS, Class2 represents Reconnaissance Class 3 Theft and Class 4 represents Normal class in all the ROC curve. ANN with 7 input feature,10 first hidden layers with RELU activation function, output layer with Softmax activation function.

VI. Decision Tree (DT)

Decision tree is a powerful classification tool. The tree is represented by nodes and edges. Each node represents a test on an attribute and branch(edge) represents the outcome after testing. The path from top to bottom show classification rules applied across the tree. The split at each node is calculated on the basis of gini impurity values. The ROC for DT shows promising results as compared to Artificial Neural Network, SVM and Logistic Regression.

5.3 Performance metrics

Confusion matrix is the visualization of correct and incorrect predictions by the classifier. Therefore, the metrics (accuracy, precision, recall, F-Score and ROC) are calculated for all the classifiers independently using confusion matrix. The results are shown in (Figure 3).

a) Accuracy or degree of closeness

Accuracy represents the number of samples accurately classified by a classifier over total count of samples given to it, From the confusion matrix TP (True Positive), TN (True Negative), FP (False Positive), FN (False Negative) values are extracted to indicate correct and incorrect classifications. Here, two classes namely Anomaly are treated as Positive and Normal as Negative. The accuracy is calculated by Summation of TP (the count of actual anomaly and predicted as anomaly) with TN (the count of actually normal and predicted as normal) divided by TP, TN, FP (count of actually normal and predicted as anomaly), FN (count of actually normal and predicted as anomaly).

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (5)$$

		Predicted	
Actual		Positive (Anomaly)	Negative (Normal)
	Positive (Anomaly)	TP	FN
	Negative (Normal)	FP	TN

b) Precision

Precision tells the exactness of a classifier. FP rate of a classifier should be less thereby, precision value should be more. If this value is low means there are more False alarms.

$$Precision = \frac{TP}{TP + FP} \quad (6)$$

c) Recall (Sensitivity)

This is a measure of True positive rates. This value is high when the value of FN (False Negative) is low. This implies that predicted is normal but it is an anomaly. The classifier should have high sensitivity.

$$TPR = \frac{TP}{TP + FN} \quad (7)$$

d) F-score

$$F - score = \frac{2 * Precision * Recall}{Precision + Recall} \quad (8)$$

e) ROC

Area Under Receiver Operating curve is a measure of

separability between TN and TP. The classifier should be able to separate the classes with high accuracy.

(a)

	DDoS	DoS	Reconnaissance	Theft	Normal
DDoS	7558	0	0	0	1
DoS	0	8912	2	0	1
Reconnaissance	0	0	7429	0	0
Theft	0	0	0	457	3
Normal	0	0	1	3	1950

(b)

	DDoS	DoS	Reconnaissance	Theft	Normal
DDoS	7558	0	0	0	1
DoS	0	8915	0	0	0
Reconnaissance	0	0	7429	0	0
Theft	0	0	0	456	4
Normal	0	1	4	2	1947

(c)

	DDoS	DoS	Reconnaissance	Theft	Normal
DDoS	7558	0	0	0	1
DoS	0	8912	2	0	1
Reconnaissance	0	0	7429	0	0
Theft	0	0	0	457	3
Normal	0	0	1	3	1950

(d)

	DDoS	DoS	Reconnaissance	Theft	Normal
DDoS	5127	2432	0	0	0
DoS	0	8915	0	0	0
Reconnaissance	0	1028	6396	0	5
Theft	0	406	0	33	21
Normal	0	1091	0	0	863

(e)

	DDoS	DoS	Reconnaissance	Theft	Normal
DDoS	7559	0	0	0	0
DoS	0	8914	0	0	1
Reconnaissance	0	0	7300	0	129
Theft	0	0	0	455	5
Normal	8	0	66	12	1868

(f)

	DDoS	DoS	Reconnaissance	Theft	Normal
DDoS	0	7559	0	0	0
DoS	0	8915	0	0	0
Reconnaissance	0	7429	0	0	0
Theft	0	460	0	0	0
Normal	0	1954	0	0	0

Figure 3. Confusion Matrix for (a) random Forest (b) Decision Tree (c) Artificial Neural Network (d) Support Vector Machine (e) KNN (f) Logistic Regression

6. RESULTS AND DISCUSSION

As compared to available machine learning based security solution for IoT networks, our work provides more in depth information about IoT networks and attack characteristics. Additionally, available intrusion detection systems for IoT networks are fabricated using prior and old datasets like KDD99, NSLKDD, KDDCUP99, ISCX and UNSW-NB15 [7]. These datasets lack IoT traces, modern attack types and hardly contain features related to IoT. Therefore, in this paper, an IDS particularly for IoT networks is proposed.

Also, instead of using available feature reduction techniques like PCA (Principal Component Analysis) that can change the meaning of variables and affect accuracy of the system, this paper focus on extracting IoT specific feature set. The feature set extracted is unique and can differentiate attack and normal traffic in IoT environment. The comparison of proposed and existing IDS is provided in Table 4.

Additionally, With the help of the IoT specific feature set, a wide variety of attacks are detected with high accuracy. The classifier is trained on only Seven unique flow based feature set as compared to [14] where all 41 features without considering the importance of features is employed.

In this study, the importance of features is evaluated using Gini Importance matric to evaluate the effectiveness of extracted features in attack and anomaly detection. And, NR (number of requests at a particular time) feature showed highest importance among all the extracted features whereas interpacket gap as the least important feature for predicting the target (Figure 4). Furthermore, the efficacy of these features to detect other types of attacks like routing attacks and malicious node detection is treated as future work.

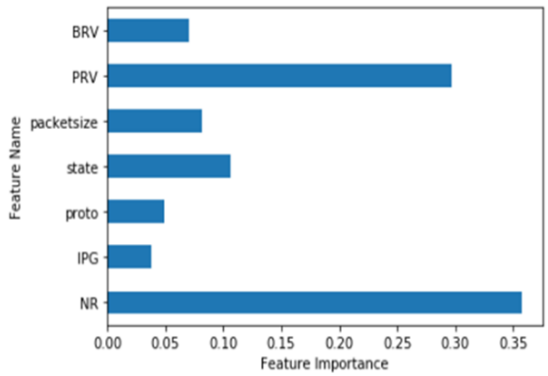


Figure 4. Gini importance value of each feature

Furthermore, this work also focuses on attack type detection in IoT environment as compared to only anomaly detection [7, 11]. The proposed single system is responsible for accurately detecting four type of attacks. The results of proposed system are validated by performing a comparison of supervised classifiers on multiclassification and binary classification task on the extracted feature set. Results show different performance of classifiers for binary and multi classification (Table 3).

Additionally, in previous studies best classifier is selected on the basis of Accuracy, precision and Recall. But accuracy alone cannot be treated as the only criteria for classifier performance. For instance, LR on binary classification shows 92% accuracy but while evaluating confusion matrix, a random guessing pattern has been observed. Confusion matrix

shows the real performance of the classifier that is hardly mentioned in studies. Additionally, most of the work avoids considering Area Under Receiver Operating Curve (AUC), time for training and testing as an important measure for benchmarking the classifier. AUC is a separability measure between TN and TP. The curve represents the relationship between TPR and FPR. TPR is the measure of correct classification (0-0,1-1) whereas FPR represents wrong classifications (0-1,1-0). In the proposed work RF classifier indicate AUC value of 1 for almost all the classes shown in (Figure 5).

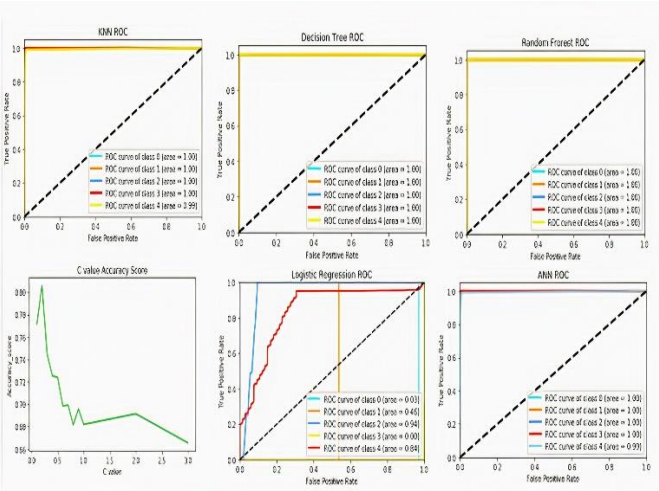


Figure 5. ROC curve of (a) KNN (b) Decision Tree (c) Random Forest (d) Accuracy and C value for SVM (e) Logistic Regression (f) ANN or MLP

Additionally, from confusion matrix it can be inferred that SVM cannot differentiate between most of the attack types. Hence, classify all classes wrongly. TPR (true positive rate) for this classifier is very low that represents more FN rate. Similarly, precision value shows high FP rate. ROC for SVM took 3 days and even after 3 days no output has been observed for attack detection using SVM. But for anomaly detection SVM shows satisfactory results with 95.2% accuracy, 67% precision and only misclassifying 98 attack samples as normal and 2 as normal when attack. Therefore, SVM cannot handle attack type detection (multiclassification) but can be easily used for anomaly detection. Similarly, Logistic Regression shows promising results on anomaly detection (binary classification) in terms of accuracy but other measures like precision and recall shown in (Table 3) provide high False alarms. And similarly, for attack type (multiclassification) detection LR performed even worse. The confusion matrix shows random guess of all the samples by LR. Therefore, LR is also not suitable for attack type detection in IoT environment (Figure 6).

Random Forest shows correct classification for almost all the classes with very little misclassifications. Only 3 misclassifications for DoS as normal and Reconnaissance, 3 theft and 4 normal misclassifications. This can be seen from confusion matrix that RF can differentiate between DDoS and DoS attack samples. TPR is high which shows low FN rate (means low False Alarms). Precision is also high which in turn shows low FP rates. The ROC curve for RF also shows clear distinction between all TPositive (attack) and TNegative (Normal) class. Hence, can be used for attack as well as anomaly detection in IoT specific environment.

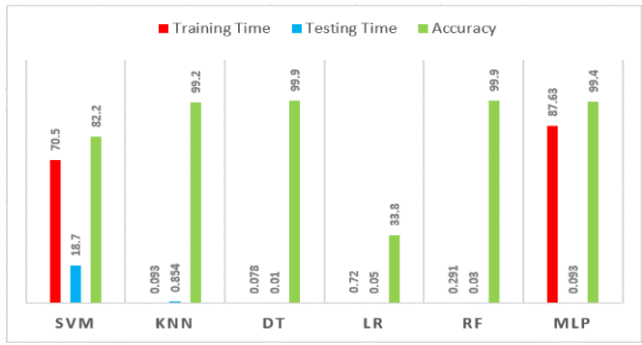


Figure 6. Performance of each classifier with respect to training time (in seconds), testing time (in seconds) and Accuracy

Table 4. Comparative presentation of proposed Intrusion Detection System with state-of-the-art

Attacks identified	Number of features considered	Techniques applied	IoT Traces	Metrics used and performance	Dataset used	Type	Classification Type
Sinkhole,DDoS, Blackhole,Opportunistic Service Attack, Wormhole Attack [1]	8	Deep Learning	Present	Avg Precision=96.88% Avg Recall,=98.02% F1 Score=0.974	Own simulated dataset	NIDS	Multi classification
DoS,Probe,U2L,R2L Attack [7]	2	Machine learning (Naïve Bayes)	Absent	Detection Rate(precision) (84.86) and False Alarm Rate(4.86)	NSL-KDD	NIDS	Binary classification
DR, HF, VN [11]	18	Deep Learning	Present	Accuracy=96.5% Precision=95%, Recall=96% F1=94	IRAD (simulated dataset using Contiki)	NIDS	Binary classification
DDoS Attack [15]	11	Machine Learning	Present	Accuracy=99%	Simulated dataset	NIDS	Binary classification
DoS,Exploit,Probe, Generic [17]	22	Rule based machine learning approach	Absent	Accuracy=88.92%	UNSW-NB15	SIDS	Binary classification

DoS, data type probing, malicious control, malicious operation, scan, spying, wrong setup [25]	13	Machine Learning	Present	Accuracy=99.4% Precision=98.6% Recall=98.6%	Open source dataset	NIDS	Multiclass classification
DoS attack [26]	All the features of these datasets	Ensemble Learning	Absent	Best reached by comparing classifier FAR=0.1326 Accuracy =96.74% Recall=97.3%	CIDDS-001,UNSWNB-15,NSL-KDD	NIDS	Binary classification
DoS, DDoS, Theft, Reconnaissance [proposed]	**7**	**Machine learning**	**Present**	**AUC=1, Accuracy=99.9% Recall=99.9% Precision=99.9%**	**BoT-IoT dataset [21]**	**NIDS**	**Multiclass classification**

7. CONCLUSION

In this study, a novel IoT specific feature set is extracted from BoT IoT dataset using which a wide variety of attacks are detected. The extracted feature set is attack characteristics independent and IoT network dependent. Hence, these features can assist machine learning model in detecting any suspicious activity in the IoT network. Using these features classifier can clearly distinguish between even Dos and DDoS attack. This study also addresses the comparison of various supervised machine learning classifiers for anomaly and attack detection in IoT networks. Hence, it proves the applicability and effectiveness of Machine Learning for IoT security. The performance of proposed system is evaluated using Accuracy, Precision, Recall, F-score, ROC, training time, and testing time. The obtained results have shown high detection accuracy and low False Alarms using these extracted features to detect a wide variety of attacks, which was the main goal of this study. Furthermore, Random Forest Classifier shows 99.9% accuracy and 0.03 seconds for both anomaly and attack type detection. Hence, RF technique should be used for IoT security systems. Future work includes detection of other types of attacks prevailing in IoT networks by employing the extracted feature set. At last, IoT communication can be stated as "A communication characterized by packets with size ranging from 200 to 1200 bytes, using a light weight UDP protocol with INT communication state along with a small number of packets sent at regular time intervals with equal number of packets received and sent".

FUNDINGS

This work is funded by SERB-DST (Science and Engineering Research Board- Department of Science & Technology), Government of India, grant number EEQ/2018/000118" and "The APC was funded by Project Grant".

REFERENCES

[1] Thamilarasu, G., Chawla, S. (2019). Towards deep-learning-driven intrusion detection for the Internet of Things. Sensors, 19(9): 1-19. https://doi.org/10.3390/s19091977

[2] Tama, B.A., Rhee, K.H. (2017). Attack classification analysis of IoT network via deep learning approach. Research Briefs on Information & Communication Technology Evolution (ReBICTE), 3: 1-9. https://doi.org/10.22667/ReBiCTE.2017.11.15.015

[3] Sethi, P., Sarangi, S.R. (2017). Internet of Things: Architectures, protocols, and applications. Journal of Electrical and Computer Engineering, 2017: 1-25. https://doi.org/10.1155/2017/9324035

[4] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. (2019). Survey of intrusion detection systems: Techniques, datasets and challenges. Cybersecurity, 2: 1-22. https://doi.org/10.1186/s42400-019-0038-7

[5] Timcenko, V.V., Gajin, S. (2018). Machine learning based network anomaly detection for IoT environments. Conference: ICIST 2018, at Kopaonik, Serbia.

[6] Alaidaros, H., Mahmuddin, M., Al mazari, A. (2011). An overview of flow-based and packet-based intrusion detection performance in high-speed networks. The International Arab Conference on Information Technology (ACIT'2011), Riyadh, pp. 323-331.

[7] Pajouh, H.H., Javidan, R., Khayami, R., Dehghantanha, A., Choo, K.R. (2019). A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks. IEEE Transactions on Emerging Topics in Computing, 7(2): 314-323. https://doi.org/10.1109/TETC.2016.2633228

[8] Anthi, E., Williams, L., Słowińska, M., Theodorakopoulos, G., Burnap, P. (2019). A supervised intrusion detection system for smart home IoT devices. IEEE Internet of Things Journal, 6(5): 9042-9053. https://doi.org/10.1109/JIOT.2019.2926365

[9] Hussain, F., Hussain, R., Hassan, S.A., Hossain, E. (2019). Machine learning in IoT security: Current solutions and future challenges. IEEE Communications Surveys & Tutorials, 22(3): 1686-1721. https://doi.org/10.1109/COMST.2020.2986444

[10] Ye, J., Cheng, X., Zhu, J., Feng, L., Song, L. (2018). A DDoS attack detection method based on SVM in software defined network. Security and Communication Networks, 2018: 1-8. https://doi.org/10.1155/2018/9804061

[11] Yavuz, F.Y., Ünal, D., Gül, E. (2018). Deep learning for detection of routing attacks in the internet of things. International Journal of Computational Intelligence Systems, 12(1): 39-58. https://doi.org/10.2991/ijcis.2018.25905181

[12] Anthi, E., Williams, L., Burnap, P. (2018). Pulse: An adaptive intrusion detection for the Internet of Things. Proceedings of Living in the Internet of Things:

Cybersecurity of the IoT Conference, London, UK, pp. 1-4.
[13] Pahl, M., Aubet, F. (2018). All eyes on you: Distributed multi-dimensional IoT microservice anomaly detection. 2018 14th International Conference on Network and Service Management (CNSM), Rome, Italy, pp. 72-80.
[14] Diro, A.A., Chilamkurti, N.K. (2017). Distributed attack detection scheme using deep learning approach for Internet of Things. Future Generation Computer Systems, 82: 761-768. https://doi.org/10.1016/j.future.2017.08.043
[15] Doshi, R., Apthorpe, N., Feamster, N. (2018). Machine learning DDoS detection for consumer internet of things devices. 2018 IEEE Security and Privacy Workshops (SPW), San Francisco, CA, pp. 29-35. https://doi.org/10.1109/SPW.2018.00013
[16] Lu, J., Lv, F., Zhuo, Z., Zhang, X., Liu, X., Hu, T., Deng, W. (2019). Integrating traffics with network device logs for anomaly detection. Security and Communication Networks, 2019: 1-10. https://doi.org/10.1155/2019/5695021
[17] Kumar, V., Das, A.K., Sinha, D. (2019). UIDS: A unified intrusion detection system for IoT environment. Journal Evolutionary Intelligence, 14: 47-59. http://doi.org/10.1007/s12065-019-00291-w
[18] Koroniotis, N., Moustafa, N., Sitnikova, E., Turnbull, B. (2019). Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems, 100: 779-796. https://doi.org/10.1016/j.future.2019.05.041
[19] Datasets[online], https://www.unsw.adfa.edu.au/unsw-canberra cyber/cybersecurity/ADFA-NB15-Datasets/, accessed on 8 August 2019.
[20] Moustafa, N., Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. Information Security Journal A Global Perspective, 25(1-3): 1-14. https://doi.org/10.1080/19393555.2015.1125974
[21] UNSWdataset.[online], https://www.unsw.adfa.edu.au/unsw-canberra-cyber/cybersecurity/ADFA-NB15-Datasets/bot_iot.php, accessed on 8 August 2019.
[22] Trimananda, R., Varmarken, J., Markopoulou, A., Demsky, B. (2019). PingPong: Packet-level signatures for smart home device events. arXiv:1907.11797.
[23] Dhanda, S.S., Singh, B., Jindal, P. (2020). Lightweight cryptography: A solution to secure IoT. Wireless Pers Communication, 112: 1947-1980. https://doi.org/10.1007/s11277-020-07134-3
[24] Chai, L., Reine, R. (2018). Performance of UDP-Lite for IoT network. IOP Conference Series: Materials Science and Engineering, 11th Curtin University Technology, Science and Engineering (CUTSE) International Conference 26-28 November 2018, Sarawak, Malaysia, 495: 012038. https://doi.org/10.1088/1757-899X/495/1/012038
[25] Hasan, M., Islam, M.M., Zarif, M.I., Hashem, M.M. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet Things, 7: 1-14. https://doi.org/10.1016/j.iot.2019.100059
[26] Verma, A., Ranga, V. (2019). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111:2287-2310. https://doi.org/10.1007/s11277-019-06986-8