International Journal of Control and Automation
Vol. 11, No. 5 (2018), pp.11-24
http//dx.doi.org/10.14257/ijca.2018.11.5.02

Performance Evaluation of Machine Learning Classifiers on Internet of Things Security Dataset

Ravi Singh[1] and Virender Ranga[2]

[1,2]*Department of Computer Engineering, National Institute of Technology Kurukshetra, Kurukshetra, Haryana 136119*
[1]*ravibhankhar5@gmail.com*, [2]*virender.ranga@nitkkr.ac.in*

Abstract

In the recent years a huge growth has been observed in the area of Internet of Things (IoT). IoT is used as a term where things can communicate with each other without human intervention. Security is one of the key concerns when devices are communicating through Internet. There are many systems that have been made to counter these security issues. In this paper, we have evaluated Machine Learning algorithms on newly created synthetic dataset to counter the IoT security issues. This dataset contains the traces of different types of attacks in IoT. The different classification algorithms are evaluated based on different parameters i.e. accuracy, precision, recall and f-measure. After evaluation we have observed that support vector machine shows better performance on this dataset and also shows 94% accuracy, 0.95 precision, 0.94 recall and 0.94 F-measure.

Keyword: *Internet of Things, Machine Learning, RPL, SVM, KNN, and Intrusion Detection System*

1. Introduction

IoT has gained lots of attention from the researchers and industries throughout the past decade. This is due to the number of capabilities that it could offer. IoT means a world where everything is connected to every other thing and can communicate with each other through Internet without any or little human intervention [1]. It simply means to create a smart world where every object is smart and its main aim to create a world where every object knows everything about us such as which types of things we like, what things we want and what is required for us and it acts accordingly without any human involvement. IoT has many types of applications like smart homes, smart health facilities, building smart cities, making environment smart etc. As the technology is emerging widely numbers of IoT devices connected to each other is also increasing. As per the estimation of various researchers number of IoT devices connected through Internet would be around some billions by 2020. IoT devices are resource constraint having low power, low memory, and low bandwidth. They use the different types of protocols than the traditional networking protocol due to these constraints for communication. These devices use RPL (Routing Protocol for Low Power and Lossy Network) protocol and 6LoWPAN (IPv6 over Low Power Personal Area Network) protocols for communication [2]. Since the number of IoT application is increasing number of issues related to it is also increasing. Security is one of the crucial issues if we want to realize all IoT applications in diverse fields. There is various numbers of attacks that could take place in IoT over RPL and 6LoWPAN.Following are the different types of attack that could take place in RPL and 6LoWPAN in IoT:

Received (December 15, 2017), Review Result (March 22, 2018), Accepted (March 29, 2018)

ISSN: 2005-4297 IJCA

- *Selective Forwarding Attack:* In this attack, attacker only forwards the selective packets and drops the rest of the traffic. This attack in RPL takes place by just forwarding the control packets and dropping the rest of the traffic [2].
- *Clone Id Attack:* In this type of attack, an attacker clones the identity of a legitimate node and behaves as a legitimate node. Therefore, when the packets are transmitted through this node then all the packets dropped by this clone attacker node [2].
- *Hello Flooding Attack:* At the beginning of the network every node starts with the HELLO message to join the network. In this attack, an attacker sends HELLO messages containing strong routing and other metrics to join the network. In RPL DIO (DODAG Information Object) message is used instead of HELLO message to join the network. In this way, attacker joins the network by using this message [2].
- *Local Repair Attack:* In this attack, an attacker sends the local repair messages periodically without any problem in the network. This triggers to all the nodes to hear the local repair massages. Therefore, without any link problem in the network all the nodes hear this message. It takes a lot of time for communicating with these messages. This creates more number of control packets and it causes the delay in the end-to-end delivery of packets. It also consumes a lot of bandwidth of the network. Therefore, due to all these messages a number of legitimate packets are dropped [2].
- *Sinkhole Attack:* In this, attacker nodes falsely showing a beneficiary routing path to its neighbors. Therefore, when a legitimate node sends packets through this node it starts dropping all the packets. It could become a very powerful attack when combines with other types of attacks [2].
- *Blackhole Attack:* In this, attacker node acted as a hole node so whatever the packets come through it silently drops them. Therefore, all the nodes whoever traffic goes through this node does not reach to the destination and lost in the midway by the malicious hole node. [2].
- *Sybil Attack:* In this, a malicious node replicates the identities of many other nodes in the network without deploying them physically. Since a node replicates many numbers of identities on a particular node so it impacts is also on the large part of the network. Therefore, a huge part of the network comes under attack when this attack takes place [2].

All these attacks could become major threats to human life, as IoT is having diversity in various fields like smart home, smart hospital, smart traffic system *etc*. If some critical majors are not taken then it could become a serious problem since IoT has a great impact on our daily life needs. Thus, these threats must be addressed efficiently to ensure that IoT applications perform in a secure and better way. There are some security issues that must be addressed for any networking devices that are communicating through Internet. These issues are:

- *Confidentiality:* An attacker can capture the information when a message is passing from a sender to receiver, with the help of this data breaching attacker can easily leak the private information and it can also modify the content of the message. Therefore, security must be needed when the message is sent from source to destination [3].
- *Availability:* It means whenever a legitimate user request for data it must be available. There must not be any denying of data for a legitimate user. Resources are made unavailable by attackers by flooding the bandwidth of the available resources. This can be done by flooding attack, blackhole attack etc. by attackers [3].

- *Integrity:* Data received by the receiver is must be same as it is sent by the sender. The attacker or any malicious node must not alter it. Integrity gives guaranty to the users that any malicious node does not alter its data [3].
- *Non-repudiation:* It means both the sender and the receiver cannot deny any data related information when they are communicating. Sender cannot deny that it does not send the data and receiver cannot refuse the receiving of data [3].
- *Data Freshness:* There is some procedure of refreshing of data periodically. It must not show the old messages when the data is needed by the user [3].
- *Authenticity:* It Authenticate the identity proof for both sender and receiver. User must authenticate each other while they are communicating. Users can authenticate themselves by authentication process so that any malicious node must not take part in the communication [3].

1.1. Intrusion Detection System

Intrusion Detection System (IDS) is a tool that is used to monitor the harmful traffic in a specific node or in the entire network [3]. It could work as a defense mechanism tool for a network to protect it from the attackers. IDS can be used as hardware as well as a software tools. Intrusion is something malicious that is harmful to our node or network and it hinder the conventional working of a network. The IDS is very helpful in detecting these types of malicious or harmful nodes. The IDS contain mainly three components: Observing, Analysis and Detection, and Alarm. The Observing component observes the traffic of the network, resources and different patterns. Analysis and Detection is the main component because it detects the malicious traffic according to a stated algorithm. Alarm component elevate an alarm when an intruder or attacker is detected.

1.1.1. Categories of IDS

- *Signature based IDS:* In this, IDS detects the attacks based on stored signature in the database. So, whenever there is an attack occurs in the network then it matches attack with the stored signature in the database if both the signature matches then it raises an alarm. It stores the entire signatures in the database hence it requires large memory for storing more number of attacks signatures. It is very useful in detecting the known attacks only. So whenever there is a new attack strikes and signature of it is not store in its database then it is not able to detect these new attacks [4].
- *Anomaly based IDS:* Firstly it captures and then defines the normal behavior of the network and a threshold is used for changes in normal behavior. So, whenever any malicious activity happens then it compares the normal behavior with the malicious behavior and if the changes are beyond the threshold then it treat it as an intruder and IDS raises an alarm. Therefore, it is much more efficient than signature based in detecting new unknown attacks. It gives very less false positive rate [4].
- *Specification based IDS:* This is similar technique to anomaly based IDS. But in this rules are defined manually and based on these rules intruders are identified. Since the rules are defined manually it has less incorrect positive rates. It is lies between signature based and anomaly based IDS. Since all the rules are defines manually it takes lots of time to define rules for IDS [4].

In this paper, we build an Intrusion Detection System (IDS) based on machine learning classification algorithms that is able to detect different types of attacks. It is a type of anomaly based IDS. The IDS we are building is based on machine learning. In this IDS, we are using different machine learning algorithms for classification like Logistic Regression (LR), Linear Discriminant Analysis (LDA), K-Nearest Neighbors (KNN),

Classification and Regression Trees (CART), Gaussian Naïve Bayes (NB), Support Vector Machine (SVM) [5, 6]. After creating the classification models for all the above algorithms we are comparing their results and finds out which is the best suitable model for intrusion detection [7]. For this we have considered a newly created dataset for IoT security for evaluation of training and testing of these models for RPL attacks in IoT.

Dataset: The dataset is taken for this research work is from Verma *et* al. [20]. It is a synthetic dataset, which is built by using Netsim Simulation Platform for Network R&D. Netsim is capable of simulating numerous environments such as IoT, Cellular Networks, and Cognitive Radio Networks etc. This dataset contains 20 features and 2 labeling attributes. The dataset is present in the csv format. Dataset contains the following types of attacks based on Routing protocol for low power and lossy networks (RPL) in it:

i) Clone ID

ii) Hello Flooding

iii) Local Repair

iv) Sinkhole

v) Selective Forwarding

vi) Sybil

vii) Blackhole

It is also having the following types of features:

i) Flow Features
This set contains features that are identifiers between source and destination.

ii) Time Features
This set contains different features of time in IoT stack layer. It contains information about the packet arrival and packet transmission.

iii) Basic Features
This category contains the protocol connections related attributes.

2. Related Work

Researchers are currently working on IoT and wireless sensor networks but still there is a lot of works needs to be done in case of their security related areas. In this section, we explained some of the works done by the researchers in recent years in IDS in IoT. Raza *et al.*, [8] proposed system is called SVELTE that is based on real time IDS implemented on Contiki Operating System. Their proposed approach contains three main components. These components are placed on the 6LoWPAN Border router. The first component is 6LoWPAN mapper that gathers all information about the RPL protocol and reconstructs the network. The second component is Intrusion detection analyzes the mapped data and detects the intrusion. The third component filters the malicious traffic is a mini firewall. The authors of [9] have proposed a system that is based on finite state machine. Finite state machine is employed on every monitor node that captures the flow of objects. Attack is detected when there is a change in rule otherwise if there is no change then it checks the behavior of doubted node and detects the intruder. A threshold is used for Local Repair attack if attacker surpasses the threshold then alarm is raised. It can detect the local repair and rank attack. Kashinathan *et al.*, [10] proposed a system on ebbit network framework. It is used to detect DoS attack. In this, they used IDS probe messages for monitoring 6LoWPAN traffic. IDS is placed using hybrid methodology. An alarm is raised by the DOS protection manager whenever there is an attack occurs. It uses the information presented in Network manager component. In [11] a statistical study of CIDDS-001 dataset is carried out. Authors used two distance based Machine Learning techniques for

analyzing the complexity of the dataset. Pongle *et al.*, [12] proposed IDS using COOJA simulator and is implemented on Contiki operating system. It identifies wormhole attack and attacker by using location information and neighbor information respectively. The IDS is placed using centralized and distributed methodology.

3. Proposed Work

3.1. Research Methodology

Following steps have been proposed in our research methodology:

a.) The newly created dataset of Verma *et al.*, [20] is considered in this research work.

b.) In this step summarization of data is done. In the first part of summarization dimension of the dataset is calculated. After that statistical summary of the dataset is done. In the last part of summarization we found out a particular class contain how many attributes.

c.) After that visualization of data is done. In this univariate and multivariate visualization of data is done for better understanding of the dataset.

d.) Evaluation of classification algorithms on dataset is done in this stage. In this step, firstly we separate out the training dataset and testing dataset. 70% dataset is used for training and 30% is used for testing. After that different classification algorithms are used on training dataset.

e.) After that Comparison of their result on the training dataset is done and find out which algorithm gives the best result.

f.) In this step, applying all classification algorithms mentioned above the testing dataset is performed and then computes the different evaluation metrics for the performance evaluation.

g.) In the final step selection of best classification algorithm and then prediction of output is done.

3.2. Classification Algorithms

3.2.1. Logistic Regression (LR)

It is a special case of Linear Regression model [14]. It is used to predict the outcome of an independent variable in discrete terms which is between 0 and 1.In simple terms; it is used to calculate the probability of the happening of an event by using some logit function. That's why it is called as logistic regression. Suppose you are given a problem there are two possibilities either you can solve the problem or not. So, LR is used to predict the probability of solving the problem or not. Mathematical representation of the LR is given below:

$$t = \textit{probability of the occurrence of an event}$$

$$1 - t = \textit{probability of not occurrence}$$

Then, the formula for LR using legit function is

$$Logit\ (\mathrm{t}) = \ln\left(\frac{t}{1-t}\right) = a_0 + a_1 * 1 + a_2 * 2 + a_3 * 3 + \cdots + a_k * k \quad (1)$$

3.2.2. Linear Discriminant Analysis (LDA)

LDA is one of the classification techniques that use the concept of combination of linear variables that separates two classes [15]. We have to select best combination of linear variables for classification from a given set of inputs. The main objective of LDA is to preserve the discriminatory information of the class as much as possible while

performing the dimensionality reduction to it. For this, we have to define a measure of split-up between the two classes. Fisher provides a solution for this by maximizing a function, which represents the means difference, and inside class scattering is normalized by a measure.

3.2.3. K-Nearest Neighbors (KNN)

In KNN, firstly it stores the values of all available cases and then classify into a new class by voting [16]. The type of cases that is having the highest numbers of neighbors of a class is turn into that type of class. A distance function is used to assign the most k nearest neighbors of a particular case. The distance functions used for this are Manhattan, Minkowski, and Euclidean and Hamming distance. The first three functions are continuous and fourth one is a discrete function. For special case we assigned class to its most nearest neighbor when value of k=1.

3.2.4. Decision Tree Classifier (CART)

It is a type of supervised machine learning algorithm [17]. In this data splitting happens at a particular node. In this, data is splitting continuously according to a given parameter until certain condition is satisfied. After every split, a child node is created. At each split there is need to check whether the subset is pure or not. If the subset is pure then algorithm stop otherwise it split recursively. A decision tree contains three types of nodes that are branch nodes, leaf nodes and a root node. At branch nodes data splitting takes place and at the leaves nodes algorithm stops and gives the final outcome of an input. Following Conditions needs to be satisfied for the end of partitioning of a node:

i) When all nodes belong to the same class.

ii) When there is no further attributes remaining for partitioning and then voting is used for classification and selection of leaf nodes.

iii) No further data is available.

3.2.5. Naïve Bayes (NB)

It is based on the Bayes algorithm and it is a supervised classification technique [18]. It assumes that all attributes are independent of one another. In simple way, a specific feature of a class is dissimilar to the existence of any other feature. It uses the Bayes probability distribution for classification. Bayes formula for probability distribution is given as:

$P\left(\frac{c}{x}\right)$ = *Posterior Probability of class(c, target) given predictor (x, attributes)*

$P(c)$ =*Prior probability*

$P\left(\frac{x}{c}\right)$ = *Likelihood which is the probability of a given class*

$P(x)$ = *Prior probability of predictor*

$$P\left(\frac{c}{x}\right) = \frac{P\left(\frac{x}{c}\right) * P(c)}{P(x)} \quad (2)$$

3.2.6. Support Vector Machines (SVM)

It is a supervised machine-learning algorithm, which is based on decision plane for separation of classes [19]. A Decision plane is a plane that classifies two classes by taking

the maximum margin condition. In SVM, it defines each data item as a point in an n-dimensional space and value of coordinates as its feature. After that there is a need to find a hyper plane that correctly separates the data items of classes. There could be many numbers of hyper planes in this but we have to find out the hyper plane, which is having the maximum margin between the data items.

4. Evaluation Metrics

Accuracy is not only the parameter to calculate the performance of a classification-based algorithm. There are also many evaluation metrics need to calculate the performance of an IDS that is built using classification algorithms. The other parameters are Precision, Recall, F-measure, and Loss Function to find out the performance of these types of algorithms. To find out whether a packet is an attack packet or not in the network is a type of binary classification problem. There are four possible outcomes in any binary classification algorithm. They are True Positive (TP), True Negative (TN), False Positive (FP), and False Negative (FN). True Positive defines the rightly projected value of a true when the actual class value is also true and TN is rightly predicted true negative when the actual class is also negative. Similarly, FN is predicted negative class when the actual class is positive and FP is predicted positive but in actual class it is negative. Accuracy is the ratio of rightly predicted observations to the total number of observations. Precision is the ratio of correctly predicted observation to the total positive observations. Recall is the ratio of positive observation to the total observation in the actual class. Loss function defines the how much loss occurs while calculating the accuracy. It must be minimum for a good classification algorithm. F-measure is the weighted average of precision and recall. Confusion metrics is used to show the relationship between predicted class and actual class in the classification algorithms. The confusion metrics is evaluated as follows:

Classifier		**Actual Class**	
		Attack	**Normal**
Predicted Class	Attack	TN	FN
	Normal	FP	TP

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \tag{3}$$

$$Recall = \frac{TP}{TP + FN} \tag{4}$$

$$Precision = \frac{TP}{TP + FP} \tag{5}$$

$$F - measure = \frac{2TP}{2TP + FP + FN} \tag{6}$$

5. Experimental Result and Discussion

In this section, an experiment has been conducted which shows the comparison of different classification algorithms on the same dataset as mentioned in the paper. The classification algorithms used in this paper are Logistic Regression (LR), Linear Discriminant Analysis (LDA), K-Nearest Neighbors (KNN), Decision Tree (CART), Naïve Bayes (NB) and Support Vector Machines (SVM). Results show that KNN and SVM have better accuracy than other algorithms on training sets. After that we apply these algorithms on testing dataset then it observes that KNN and SVM also outperform in testing set. The dataset taken for this is in csv format containing the different types of

attacks that are present in the IoT scenario. The dataset is partitioned in two parts training and testing set which contains 70% and 30% of the total dataset respectively.

5.1. Analysis using Classifiers

The Algorithms analysis is done by comparing their accuracy, precision, recall, f-measure and loss function. Then we select the best algorithm which suites best according to our system specifications. Classification techniques give the output whether a particular input is attack or normal. Accuracy and loss values of the different classification model on the training set and the testing set is given as:

Table 1. Performance of Classifiers

Name of the Classifier	Training Set Accuracy (in%)	Testing Set Accuracy (in %)	Loss value
Logistic Regression	79.78	80.02	0.44
Linear Discriminant Analysis	79.50	79.72	0.37
K-Nearest Neighbors	92.99	92.73	0.22
Decision Tree	92.30	92.12	0.23
Naïve Bayes	60.86	61.21	0.80
Support Vector Machine	94.07	94.26	0.21

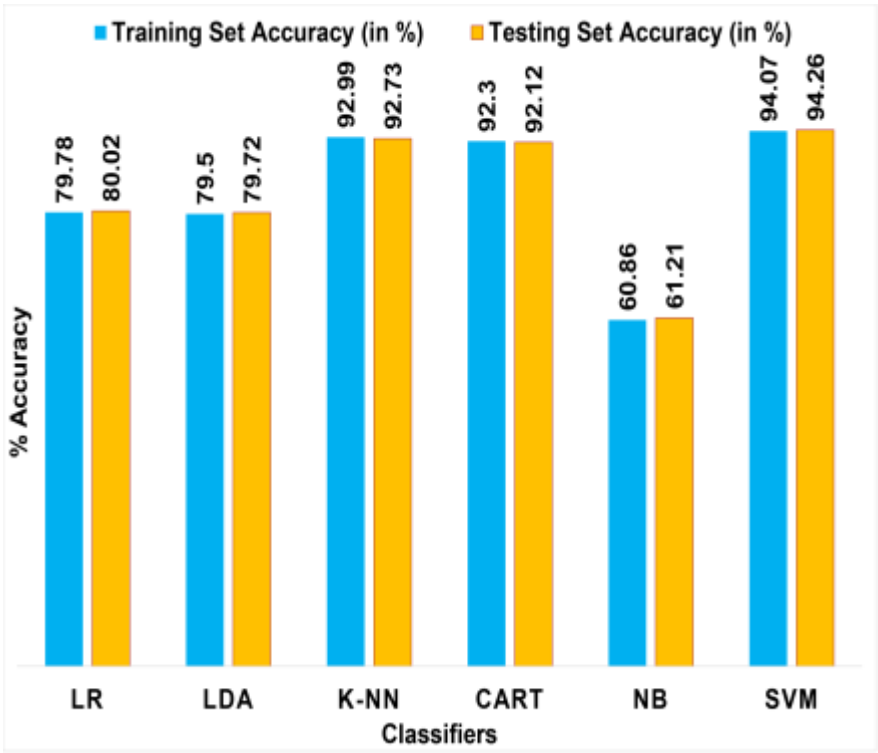

Figure 1. Comparison of Algorithms in Training and Testing Set

Table 2. Confusion Metrics of Various Classifiers

LR Classifier		Actual Class	
		Attack	Normal
Predicted Class	Attack	3763	2995
	Normal	2997	20249
Decision tree		Actual Class	
		Attack	Normal
Predicted Class	Attack	6083	1687
	Normal	677	21557
LDA Classifier		Actual Class	
		Attack	Normal
Predicted Class	Attack	5857	5181
	Normal	903	18063
SVM Classifier		Actual Class	
		Attack	Normal
Predicted Class	Attack	6534	1494
	Normal	226	21750
NB Classifier		Actual Class	
		Attack	Normal
Predicted Class	Attack	6760	11637
	Normal	0	11607
KNN Classifier		Actual Class	
		Attack	Normal
Predicted Class	Attack	6147	1566
	Normal	613	21678

Table 3. Performance Evaluation of Metrics Precision

Name of classifier	**Precision**		
	Type of Packet		
	Normal Packet	**Attack Packet**	**Avg/Total**
Logistic Regression	0.87	0.56	0.80
Linear Discriminant Analysis	0.95	0.53	0.86
K-Nearest Neighbors	0.97	0.80	0.93
Decision Tree	0.97	0.78	0.93
Naïve Bayes	1.00	0.37	0.86
Support Vector Machine	0.99	0.81	0.95

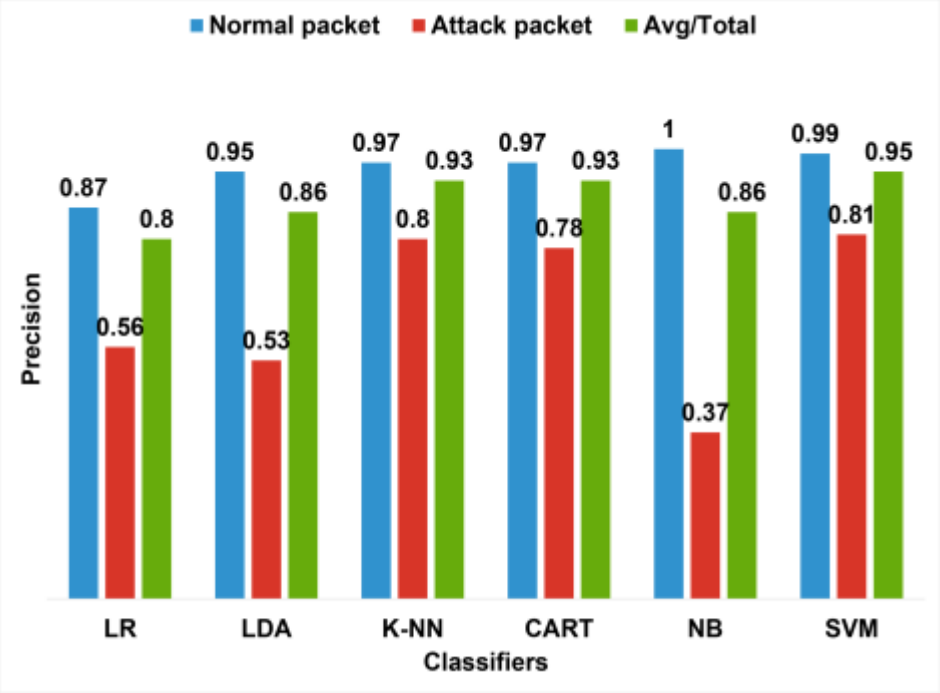

Figure 2. Comparison of Precision of Various Techniques on Testing Dataset

Table 4. Performance Evaluation of Metrics Recall

Name of classifier	Recall		
	Type of Packet		
	Normal Packet	Attack Packet	Avg/Total
Logistic Regression	0.87	0.56	0.80
Linear Discriminant Analysis	0.78	0.87	0.80
K-Nearest Neighbors	0.93	0.91	0.93
Decision Tree	0.93	0.90	0.92
Naïve Bayes	0.50	1.00	0.61
Support Vector Machine	0.94	0.97	0.94

After applying all these classification models to the given dataset which contains both normal and attack packet and average number of packets that is containing both the attack and normal packets, we find that KNN, CART and SVM have very good accuracy in both training and testing set. LR and LDA also show good accuracy but NB shows the worst accuracy among all. Loss function of NB is also very high but other models have very acceptable loss function. We have also shown the accuracy of both the training and testing dataset in Figure 1 and there values are given the Table 1. After that the confusion metrics of each model is given in Table 2. In the confusion metrics, two types of packets are shown one is normal packet and the other is attack packet. We have calculated the precision, recall and f-measure of each model by using the formulas given in the equations 4, 5 and 6. To be an efficient classification models these parameters needs to be high. A model is good as the value of these observed parameters is high. The results of precision, recall and f-measure are shown in the Tables 3, 4 and 5 respectively and the graphical representation is also shown in Figures 2, 3 and 4. From the above results we observed that SVM is the best classification algorithms for intrusion detection in an IoT network. This classification technique successfully classify weather a packet is normal

packet or a malicious packet than the others techniques with a high accuracy and is having higher values of other evaluation parameters.

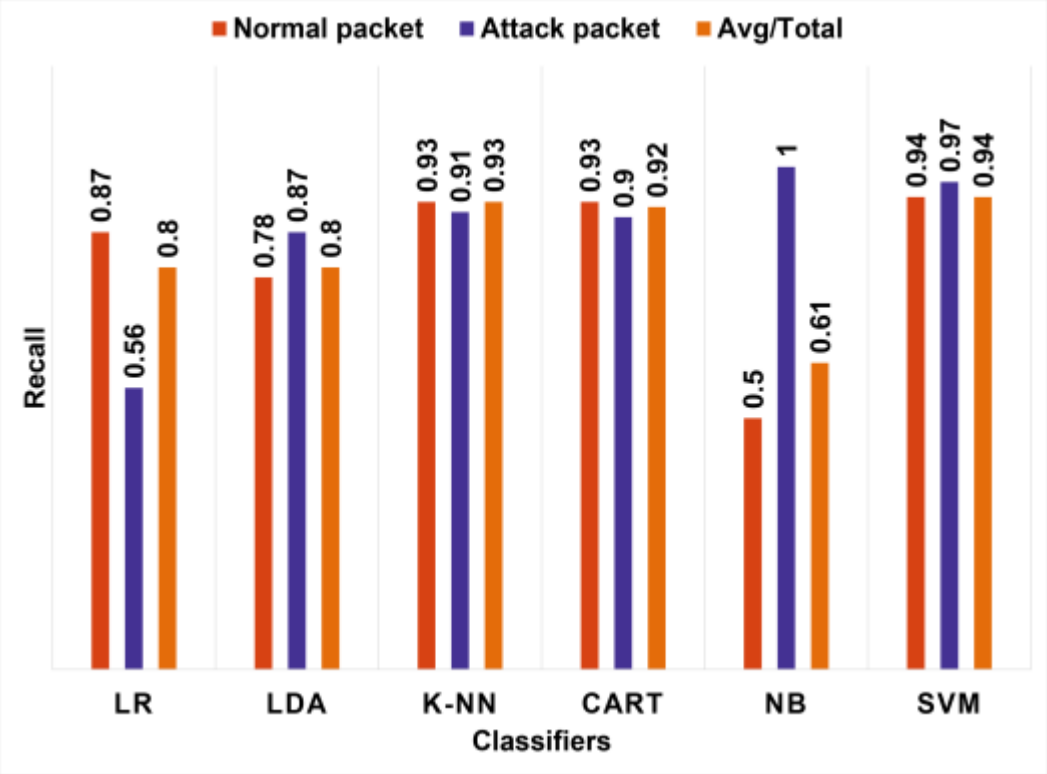

Figure 3. Comparison of Recall of Various Techniques on Testing Dataset

Table 5. Performance Evaluation Metrics F-Measure

Name of classifier	F-Measure		
	Type of Packet		
	Normal Packet	Attack Packet	Avg/Total
Logistic Regression	0.87	0.56	0.80
Linear Discriminant Analysis	0.86	0.66	0.81
K-Nearest Neighbors	0.95	0.85	0.93
Decision Tree	0.95	0.84	0.92
Naïve Bayes	0.67	0.54	0.64
Support Vector Machine	0.96	0.88	0.94

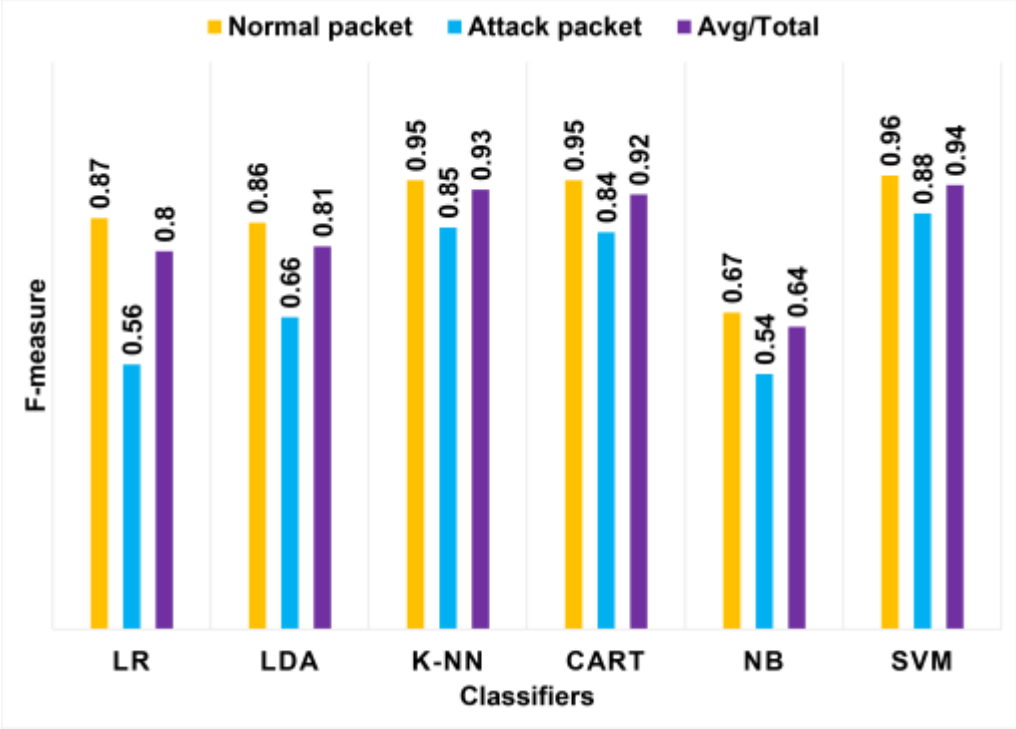

Figure 4. Comparison of F-Measure of Various Techniques on Testing Dataset

6. Conclusions and Future Scope

In this research work, evaluation of machine learning algorithms in RPL and 6LoWPAN in IoT is done by using various classification techniques as discussed above. These classifications algorithms can classify the packet into two types i.e. attack packet or normal packet on the basis of their behavior, which is available in the used dataset. We divide the dataset in two parts training dataset and testing dataset 70% and 30% respectively. Firstly, the entire dataset is trained using different classification algorithms as mentioned in the paper. Then, we apply all those algorithms on testing dataset. Their performance is measured by calculating various evaluation metrics namely accuracy, precision, recall, f-measure and loss function. After that we observed that the most of the algorithms used in this paper have a good accuracy in terms of classifying between attack packet and normal packet and could be very useful in detecting an intrusion. But SVM is showing much better performance than all other techniques. SVM could be very helpful in the detection of malicious activities in the network in an efficient way when we use classification algorithms for discovering attacks. Therefore, this model could be used as an Intrusion Detection System for IoT technology. For the future work we will be looking some better classification techniques for IoT security which will show the better results than current and will find out which is the appropriate model that is best suitable for IoT based IDS.

Acknowledgement

The authors of this research paper heartily thank to Abhishek Verma for providing the newly created dataset for evaluation of Internet of things security systems.

References

[1] C. Perera, A. Zaslavsky, P. Christen and D. Georgakopoulos, "Context aware computing for the Internet of things: A survey", IEEE communications surveys & tutorials, vol. 16, no. 1, **(2014)**, pp. 414-454.
[2] P. Pongle and G. Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT", In Pervasive Computing (ICPC), International Conference on IEEE, **(2015)**, pp. 1-6.
[3] T. Sherasiya and H. Upadhyay, "Intrusion detection system for internet of things", International Journal of Adv. Res. Innov. Ideas Educ. (IJARIIE), vol. 2, no. 3, **(2016)**, pp. 2244-2249.
[4] B. B. Zarpelão, R. S. Miani, C. T. Kawakani and S. C. de Alvarenga, "A survey of intrusion detection in Internet of Things", Journal of Network and Computer Applications, vol. 84, **(2017)**, pp. 25-37.
[5] N. Pise and P. Kulkarni, "Algorithm selection for classification problems", SAI Computing Conference (SAI), IEEE, **(2016)**, pp, 203-211.
[6] J. Han and M. Kamber, "Data Mining Concepts and Techniques", Morgan Kaufmann Publishers, Elsevier, **(2006)**.
[7] B. Subba, S. Biswas and S. Karmakar, "A Neural Network based system for Intrusion Detection and attack classification", Communication (NCC), Twenty Second National Conference, IEEE, **(2016)**, pp. 1-6.
[8] S. Raza, L. Wallgren and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", Ad hoc networks, vol. 11, no. 8, **(2013)**, pp. 2661-2674.
[9] A. Le, J. Loo, Y. Luo and A. Lasebae, "Specification-based IDS for securing RPL from topology attacks", Wireless Days (WD), IFIP, **(2011)**, pp. 1-3.
[10] P. Kasinathan, C. Pastrone, M. A. Spirito and M. Vinkovits, "Denial-of-Service detection in 6LoWPAN based Internet of Things", Wireless and Mobile Computing, Networking and Communications (WiMob), IEEE 9th International Conference, IEEE, **(2013)**, pp. 600-607.
[11] A. Verma and V. Ranga, "Statistical analysis of CIDDS-001 dataset for Network Intrusion Detection system using Distance-based Machine Learning", Procedia Computer Science, vol. 125, **(2018)**, pp. 709-716.
[12] M. H. Bhuyan, D. K. Bhattacharyya and J. K. Kalita, "Network anomaly detection: methods, systems and tools", IEEE communications surveys & tutorials, vol. 16, no. 1, **(2014)**, pp. 303-336.
[13] M. Ahmad, A. N. Mahmood and J. Hu, "A Survey of Network Intrusion Detection Techniques", Journal of Network and Computer Applications, vol. 60, **(2016)**, pp. 19-31.
[14] S. Menard, "Applied logistic regression analysis", SAGE publications, vol. 106, **(2018)**.
[15] J. Matas and J. Kostliva, "Linear Discriminant Analysis", **(2014)**.
[16] P. Le, "K-nearest neighbor algorithm", Scholarpedia, vol. 4, no. 2**, (2009)**.
[17] G. Stein, B. Chen, A. S. Wu and K. A. Hua, "Decision tree classifier for network intrusion detection with GA-based feature selection", Proceedings of the 43rd annual Southeast regional conference, ACM, vol. 2, **(2005)**, pp. 136-141.
[18] N. B. Amor, S. Benferhat and Z. Elouedi, "Naive bayes vs decision trees in intrusion detection systems", Proceedings of the 2004 ACM symposium on Applied computing, ACM, **(2004)**, pp. 420-424.
[19] A. J. Suykens and J. Vandewalle, "Least squares support vector machine classifiers", Neural processing letters, vol. 9, no. 3, **(1999)**, pp. 293-300.
[20] IoT security dataset, https://data.world/abhishek-verma, accessed on **(2018)** February 20.

