HYBRID ANOMALY DETECTION MECHANISM FOR IOT NETWORKS

Harish Kumar Saini, Monika Poriye

Department of Computer Science and Applications, Kurukshetra University, India

ABSTRACT

The Internet of Things (IoT) is the fastest-growing collection of physical entities embedded with technologies to sense and exchange information with other connected devices over the Internet.Since IoT systems are resource-constrained and ad hoc, they are an obvious target for cyberattacks. IoT system security thus requires continual observation and analysis. The application of machine learning (ML) to IoT security holds particular promise for identifying any anomalies in the system's typical operation. In this paper, we propose to design a Random Forest-Support Vector Machine (RF-SVM) based Anomaly detection framework for IoT. The RF classifier is applied for selecting the optimal features from the extracted traffic data. It includes removing the outliers, redundant data, and choosing the best features with high weight values. Then, SVM is applied for classifying the extracted features and detecting the anomalies. The fitness function is derived in terms of true positives, false positives, and false negatives. From the detected anomalies, the attack type is then determined, and a corresponding warning is sent to the monitoring nodes.In the experimental results, it is shown that the proposed RF-SVM classifier attains increased detection accuracy with reduced detection overhead and packet drops.

KEYWORDS

IoT, Machine Learning, Ensemble, Anomaly detection

1. INTRODUCTION

The Internet of Things (IoT) is the network of physical devices, such as smartphones, and other smart objects that exchange information and provide useful services online. The Internet of Things is a global revolution. It provides the potential for use in a wide range of application areas. It has been widely used in retail, agriculture, smart cities, smart homes, smart industries, and environmentmonitoring, among other areas. Connecting devices is the aim of the Internet of Things. Wireless Sensor Network (WSN) upgrades are very common. WSNs connect IoT devices to gather environmental data. Due to its limited energy, memory, and processing capabilities, IoT is resource-constrained [1].

Due to IoT systems' ad hoc and limited resources, they are an obvious target for cyber-attacks. As a result, protecting IoT systems requires constant monitoring and analysis. Prior to an attack, it's critical to know what to do in the event of an unforeseen situation, take precautions, protect important data, and assure continuity [2]. During the routing of data packets, data packets are quite likely to be exposed. The data packets would be lost if the rogue node invaded the nodes.As a result, the security of data packets in IoT-constrained devices has a significant impact because it is linked to the users [3]. For resource-constrained environments, standard security measures are prohibitively expensive. [4]

In IoT based sensor network, a Distributed Denial of Service (DDoS) attack is feasible whose main purpose is to interrupt the data transfer between end users. This exploit generates malicious

traffic flooding, causing other valid nodes to receive unnecessary packets. Actions of these attackers contribute to the deterioration of the network in terms of greater bandwidth usage, memory utilization, energy consumption, etc. [5]. Malicious Control, Malicious Operation, and Wrong Setup are just some of the additional assaults and abnormalities that might cause an IoT device to malfunction [6].

An intrusion-detection system (IDS) is a must for any IoT traffic environment that is particularly sensitive. A majority of current research on IDS for the Internet of Things is based on rule-based detection. Anomaly-based detection methods are crucial in IoT environments [7] for efficient threat detection.

Any anomalies in the system's behaviour can be detected by using machine learning (ML) for IoT security. An aberrant situation can be detected and protected by a variety of machine learning algorithms. [6][7].

Among the ML algorithms,SVM and RF have been widely used in recent years to suggest feasible solutions to the IDS problem. SVM can provide good decision surfaces by maximizing margins using soft-margin approaches. Though SVM is slightly more accurate,it consumes more time. RF produces similar accuracy in a much faster manner if given modelling parameters. Hence,by combining these two classifiers and creating a hybrid RF-SVM classifier will result in increased accuracy in less time [11].

In this paper, RF-SVM classifier is designed to detect the IoT network traffic anomalies. In contrast to the existing RF-SVM classifiers, here RF classifier is applied for extracting the optimal features from the network traffic data and theSVM is applied for classifying the extracted features and detecting the anomalies.

This paper is organized as follows. Section 2 presents the related works on anomaly detection using ML classifiers and RF-SVM classifiers. Section 3 presents the detailed methodology of the proposed RF-SVM classifier. Section 4 presents the experimental results and Section 5 presents the conclusion.

2. RELATED WORKS

2.1. Anomaly Detection using Machine learning (ML) classifiers

IoT attacks and anomalies can be detected using a group of ML classifiers [6]. Decision Tree (DT), Logistic Regression (LR), Support Vector Machine (SVM), Neural Network (ANN). Final models were created using an optimization method based on the training datasets.

This system uses a Deep Learning [7] algorithm to identify fraudulent traffic in IoT networks. Network traffic is organised into sessions and anomalous activity is examined. During the training phase, the work is done offline and spans a long period of time. When the data is pre-processed, tuples of features are generated and used to train the model. The perceptual learning model utilises information gained at each perceptual layer to filter out the preferred traits before feeding it to the next perceptual layer.

To combat DDoS attacks, a machine-learning framework [8] was developed. The IoT device traffic capture mechanism is capable of capturing a wide range of data. Categorizing and retrieving features based on IoT activity has been done and as a final step, a variety of binary

classification techniques were used to correctly distinguish between normal communication and DoS communications.

For low-resource IoT devices, a game theory-based lightweight anomaly detection approach has been proposed [9]. IoT security has been shown as a game between IDS agents and the attackers in this approach. There are new attack patterns that need to be tracked down by the IDS agent. The training, classification, and rule-making phases of the anomaly detection process are all included.

Using deep migrating learning, a new IoT data feature extraction and IDS has been developed [10]. This document outlines the migration learning model and data feature extraction. Migrating from one subject or activity to another is a process of acquiring new knowledge. Research shows that an IDS model can effectively shorten clustering times while retaining the accuracy required to identify intrusions. However, the accuracy of categorisation can suffer throughout the compression process.

2.2. RF-SVM Classifiers for Anomaly Detection

Shanmuga sundari et al [12] have shown that fraud detection using RF and SVM techniques may be compared in terms of accuracy. Using data mining algorithms, they are able to identify both normal and fraudulent transactions based on the past information, including exchanges that have been misrepresented.

Prithi et al [13] have proposed a two-stage hybrid classification technique for intrusion detection. Anomaly detection is done using SVM, while abuse detection is done using (RF)/Decision Tree (DT). In the beginning, the abnormalities are spotted. Second-stage investigation recognises the most common types of DoS and Probe, as well as recognised R2L assaults and User to Root (U2R) assaults.

Two categorization models have been developed by Md. Al MehediHasan et al [14]. The SVM and RF model are used for each. Experiments have shown that any classifier works here. SVM is a little more accurate, but it takes a lot longer to run. RF provides the same level of precision in a considerably faster manner if the model parameters are provided. These classifiers can help improve the accuracy of an IDS system. The KDD'99 Dataset is employed in this study in order to determine which intrusion detector is more effective on this dataset.

In [15], RF-SVM classifier has been applied to classify the gene expression data in Chronic Kidney Disease (CKD). Here, RF is highly accurate and is interpretable and SVM effectively predicts the gene expression data with very high dimensions.

2.2.1. Challenges

Developing an effective and efficient anomaly detection model using machine learning algorithms is a challenging process because of the following reasons[16]:

- The classical machine learning algorithms are weak in extracting the best features to represent the given data.
- It’s difficult to deploy a machine learning model over resource-constrained IoT devices.
- A huge amount of data is required to train machine learning models to reduce false positives and false negatives.

- The processing overhead due to data dimensionality is also an issue in selecting any anomaly detection mechanism.

3. Proposed Solution

3.1. Overview

In this paper, we propose to design RF-SVM-basedAnomaly detection mechanism for IoT. Here RF-SVM classifier module is applied to detect the IoT network traffic anomalies. Although there are hybrid RF–SVM pipelines, our work is different in three significant ways: A fitness-driven SVM objective that explicitly optimizes TP, FP, and FN to prioritize anomalous-event recall under IoT IDS constraints, a gateway-centric RF feature selection with an empirically tuned stability threshold that filters redundant/noisy traffic fields before classification, and a deployment-oriented evaluation in NS-2 with TwoRayGround propagation and workload sweeps (monitoring interval and attack-rate) that reports accuracy as well as detection delay and packet drop as first-class metrics pertinent to IoT networks. Together, these components represent a novel experimental and methodological contribution that goes beyond the simple statement, "RF for features, SVM for classification. The RF classifier is applied for selecting the optimal features from the extracted traffic data. It includes removing the outliers, redundant dataand choosing the best features with high weight values. Then, SVM is applied for classifying the extracted features and detecting the anomalies. The fitness function is derived in terms of true positives, false positives and false negatives. From the detected anomalies, the attack type is then determined, and a corresponding warning will be sent to the monitoring nodes.

3.2. Decision Trees

The decision tree is a type of supervised learning algorithm that is mostly used in classification problems. The simplicity and efficiency are considered the major attributes in the decision trees which are very useful in applications where the computational power resources are scarce.

The decision trees adopt a top-down approach in splitting the data samples in smaller subsets based on different decision criteria, which will be discussed. The root node is considered the best predictor. The decision node is the attribute where the highest splitting criterion (information gain ,for example) is achieved. At a terminal node or leaf node, the splitting process halts; it represents a decision. In this case, a splitting criterion such as the information gain is equal to zero.

A major type of decision tree is an ensemble-based decision tree or Random Forest (RF).

3.2.1. Random Forest (RF) Algorithm

RF algorithm is a set of trees and a supervised classification algorithm that generates each tree using a basic sample of the exclusive training data. In order to classify a new item from an input trace, the trace will be positioned beneath each tree in the forest. There is a direct correlation between the number of trees in a forest and the potential fallout; that is, the more trees there are, the more accurate the result. Each and every tree offers a vote to indicate the tree's preference regarding the item's category. The group that generates the most votes out of all the trees is chosen by the forest. [14][17].

There are two stages in the RF algorithm: (i) RF creation, (ii) creating a calculation from the arbitrary forest classifier made in the preliminary phase [17].

The whole process is shown below:

(i) Arbitrary forest formation

1. Select "K" aspects at random from the aggregate "M" aspects where K < M.
2. Use the finest divided point to assess the node "D" among the "K" aspects.
3. Use the best split to split the node into daughter nodes.
4. Repeat steps 1 through 3 until "L" nodes are reached.
5. Create a forest by repeating steps 1 through 4 "N" times to create "N" trees.

(ii) Arbitrary forest estimation

1. Uses the test features and each decision tree's rubrics to compute the outcome and store the anticipated outcome (objective).
2. Calculate the number of votes for each anticipated goal.
3. Use the highly voted anticipated objective as the arbitrary forest procedure's closing expectation.

3.2.2. RF-based Feature Selection

RF uses a technique called bootstrap aggregation (Bagging), which samples the data set used in the classification task, randomly with replacement. The bootstrap method is a resampling technique to generate slightly different data sets from the original training data set, and bagging combines many classifiers trained with slightly.

Let m represent how many instances there are in the real training set. Create a bootstrap model of dimension m using the real training data. Let m represent the total number of input structures found in the real training set. For each tree where k<m, only k features are randomly chosen from the bootstrap model data. At each node of the tree, the traits from this group form the best possible fragment. The value of m should remain constant throughout the forest's ascent [18].

The original Packet Capturing Files (PCAP),which have the network packages were primarily changed and characterized in a Packet Description Markup Language (PDML) format.

The features that reflect the device characteristics and behaviour related to various attacks are only considered. Each feature has been assigned a weight value. The best subset of features with higher weight values is selected by RF algorithm.

Table 1 :Extracted features and assigned weights

S.No	Features	Weight value
1	Protocol type	1
2	src (bytes)	2
3	sest (bytes)	2
4	Duration	1
5	Flag	1
6	Service	3
7	dst_host_count	3
8	serv_count	2
9	serv_error_rate	4
10	same_serv_rate	3
11	diff_serv_rate	3

S.No	Features	Weight value
12	dst_host_same_serv_rate	2
13	dst_host_diff_serv_rate	2
14	dst_host_same_src_port	3
15	dst_host_diff_src_port	3
16	Dst_host_serror_rate	5
17	No_failed_attempts	5
18	No_file_creations	4
19	No_access_files	4
20	No_compromized	5

Let S be the source node and {F} be the set of selected features. Let DS(A) be the actual data set, $BS_m(A)$ represents the bootstrap model of m features, and DS(C) represent the collected dataset by each gateway . The overall weight value (W) is the number of most repeated features divided by the total number of features. Let MinWbe the minimum threshold or lower bound of W. In our work, the value of MinW is kept as 3 based on sensitivity analysis by testing the MinW value (1-5) and observing that MinW = 3 provided the best detection accuracy without an increase in false positives.The features which are having weight values greater than MinW are included for classification. The features that were given the highest weight values, as shown in Table 1, were rated the highest due to being accountable, through the Random Forest feature selection and importance ranking, for the greatest strength in distinguishing normal traffic from compromised traffic or exhibiting the most discriminative power. These features (e.g., repeated failed attempts or session errors) are clearly related to attack behavior and are therefore useful signals for the SVM classifier. The selection of these parameters, along with their high weighting, is corroborated by previous research and domain knowledge, confirming that anomalies found in these domains are significant indicators of malicious activity or intrusion attempts in IoT environments.

The proposed RF-based feature selection algorithm is presented below:

Algorithm: RF-based feature selection

---

1. For each IoT gateway
2. Read DS(A)
3. construct $BS_m(A)$ using RF
4. Divide $BS_m(A)$ into training and trial
5. DS is provided for training in RF
6. Train (BSm(A)
7. Estimate DR
8. End For
9. For each gatewayG_j
10. At time interval t_i,
11. Collects data from its devices
12. Constructs DS(C)
13. Estimates W using the RF classifier
14. Transmit all W to SCH
15. G_j transmits W towards S
16. S computes the variance (W)
17. For each feature f_i
18. If $W(f_i)$ >MinW, then
19. S adds f_i into {F}
20. End For

21. Move to the next interval $T_{(i+1)}$
22. End For
23. Stop

According to this algorithm, the optimum features selected by the RF classifier algorithm are: serv_error_rate, Dst_host_serror_rate, No_failed_attempts, No_file_creations, No_access_files, and No_compromized**.**

3.3. SVM Classifier

The basic principle of SVM is finding the optimal linear hyperplane in the feature space that maximally separates the two target classes [16]. Geometrically, the SVM modelling algorithm finds an optimal hyperplane with the maximal margin to separate two classes,

In SVM, the training set is provided as

$(x_1,y_1),(x_2,y_2),\ldots.(x_n,y_n)$, $x_j \in R^n$, $y_j \in \{+1,-1\}$.

Here, x_j is the input characteristic vector of thej^{th}model, and y_j is the output catalogue = +1 or -1. SVM splits the +ve and -ve instances by means of a hyperplane as

$$w..x + b = 0, w \in R^n, b \in R \qquad (1)$$

Here, w.x signifies the dot product of w & x.

SVM calculates the finest hyperplane by exploiting the border.

The choice function f(x) = sgn(g(x)) for an event is provided as

$$g(x) = \left(\sum_{i=1}^{l} \lambda_i y_i x_i..x + b \right) \qquad (2)$$

where i is the numerical limit for imminent vector x_i

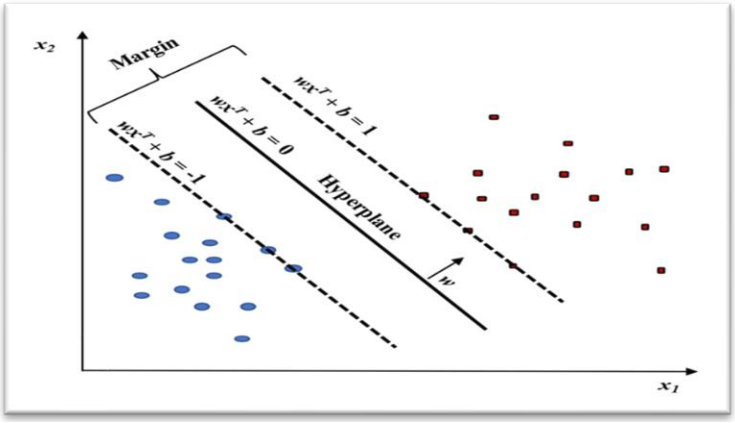

Figure 3 Concept of SVM

3.4. Detection Algorithm using SVM

For classifying the extracted features and detecting the anomalies, we use SVM. The fitness function (F) is derived in terms of True positives (TP), False positives (FP) and False negatives (FN) as follows:

$$F = 2.\ TP / (TP+FP+FN) \quad (3)$$

Since the algorithm focuses on anomalous event prioritization and minimization of missed detections True negatives are excluded, as recommended in IoT IDS literature.

By means of the training vector in two sets and the label vector y, the provision vector method needs the resolution of the succeeding issue

$$\min_{w,b,v} \frac{1}{2} w^T w + C\sum_{i=1}^{l} v_i \quad (4)$$

subject to $y_y(w^T \varsigma(x_i) + b) \geq 1 - v_i, v_i \geq 0, i = 1,...l$

where $w \in R_d$ is the mass vector

$C \in R_+$ is the regularization constant

ς is the mapping function that projects the training data into a suitable feature space so as to allow non-linear decision surfaces.

The following algorithm shows the process of the SVM classifier to classify the malicious traffic flows.

Procedure: SVM Classification

---

1. Remove deal data equivalent to 10 aspects
2. Build the feature vector X_{ij}, i=1..10,j=1….n
3. Construct the training set (x_{ij}, y_{ij})
4. Utilise the labelled data to train the sample
5. For every input user U_j of aspect F_i
6. Do
7. Remove the data from U_j
8. For every classifier j
9. Do
10. Regulate the symbol by means of $g^j(x)$ via (2)
11. While (i<10)
12. End For
13. Evaluate the utmost output (select the maximum output)
14. Regulate the ideal brim.
15. Return the equivalent operator U_j such that F_i=max(Fi)
16. End For

The features of legitimate devices will have unique fitness values, whereas the features of compromised devices will deviate from others. Hence, the fitness function is applied to the

extracted features and the, features having the least fitness values are considered as anomalies. The corresponding device or user is fetched from the PCAP history and blocked from further operations.

4. EXPERIMENTAL RESULTS

4.1. Dataset and PDML

The training and testing were performed on the DARPA 2009 IDS dataset. Though the DARPA 2009 dataset is old and not specific to IoT, it is still used in some research for baseline benchmarking and method validation purposes. The dataset is well-structured and the labeled traffic is publicly available, allowing researchers to compare their results with a large number of previous studies that were conducted using the same dataset and its labeled traffic. In doing so, the DARPA 2009 dataset allows researchers to have a common dataset to refer to when evaluating a new algorithm against the established results from a long-standing body of intrusion detection research. Additionally, the DARPA 2009 dataset can also serve as a useful avenue for testing the general detection capacity of models as they are deployed and applied to more complex and heterogeneous datasets after testing them first under a controlled and well-established environment.

The dataset comprises about 7000 PCAP files. The dataset comprises a variety of security events and attack types. PCAP files are data files generated using tools such as Libpcap of Linux. These files contain packet data of a network and are used to analyze the network characteristics. They alsocontribute to controlling the network traffic and determining network status.

Wireshark can save network packet dissections in a PDML file. PDML conforms to the XML standard and contains details about the packet analysis**.**

4.2. Comparison with Existing Techniques

The proposed RF-SVM based anomaly detection framework is simulated in NS2 and compared with the existing Lightweight Anomaly Detection (LAD) [10] and Deep Migration Learning (DML) based IDS [11]. The performance is evaluated in terms of detection delay, detection accuracy, and packet drop. Table 3 shows the experimental parameters used in the simulation.

Table 3: Experimental parameters

Number of Nodes	22
Simulation area	500 X 500m
MAC Protocol	IEEE 802.11
Traffic type	CBR and Exponential
Number of Wired Nodes	2
Number of wireless nodes	20
Propagation	TwoRayGround
Antenna	OmniAntenna
Simulation Time	20,40,60,80 and 100 sec
Rate	25,50,75,100 and 125Kb

A. Varying the Monitoring interval

In this first experiment we vary the simulation time as 20,40,60,80 and 100sec.

Table 4 Results of detection delay for various intervals

Monitoring Interval(sec)	RF-SVM (ms)	DML (ms)	LAD (ms)
20	4.50	4.73	4.98
40	7.63	10.05	10.17
60	10.78	15.31	15.76
80	13.91	20.61	21.45
100	17.23	25.93	27.06

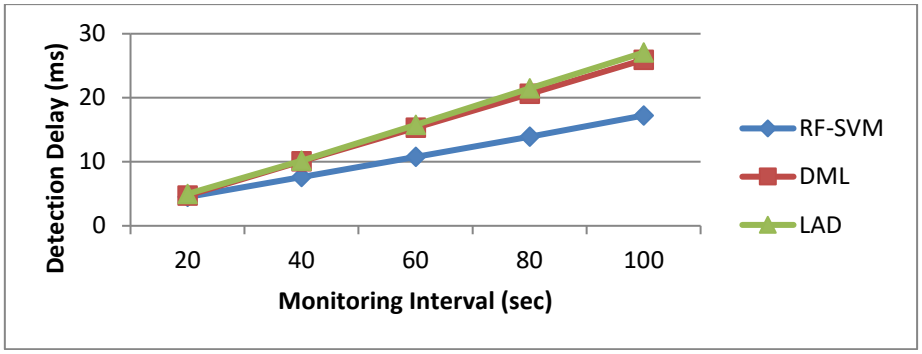

Figure 7 Detection Delay for various intervals

Table 4 and Figure 7 show the detection delay measured for RF-SVM, LAD and DML when the monitoring intervals flows are varied. As we can see from the figure, the delay of RF-SVM is 25% of lesser than DML and 27% lesser than LAD.

Table 5 Results of detection accuracy for various intervals

Monitoring Interval (sec)	RF-SVM	DML	LAD
20	0.8244	0.5598	0.4018
40	0.8422	0.584	0.4959
60	0.8481	0.6112	0.5413
80	0.8531	0.6428	0.5915
100	0.8539	0.6816	0.6626

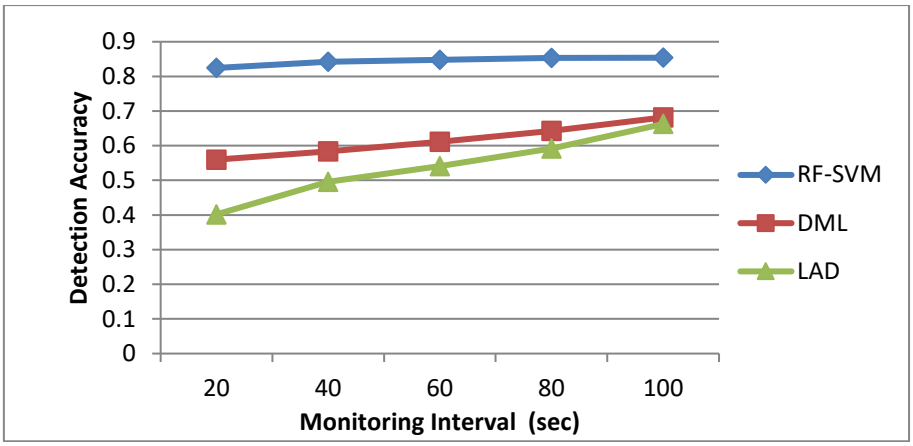

Figure 8 Detection accuracy for various intervals

Table 5 and Figure 8 show the detection accuracy measured for RF-SVM, LAD and DML when the monitoring intervals are varied. As we can see from the figure, the detection accuracy of RF-SVM is 28% higher when compared to DML and 65% higher than LAD.

Table 6 Results of packet drop for various intervals

Monitoring Interval(sec)	RF-SVM	DML	LAD
20	523	1447	3209
40	963	2033	4797
60	1623	3784	5519
80	2823	4287	6187
100	4453	8098	9639

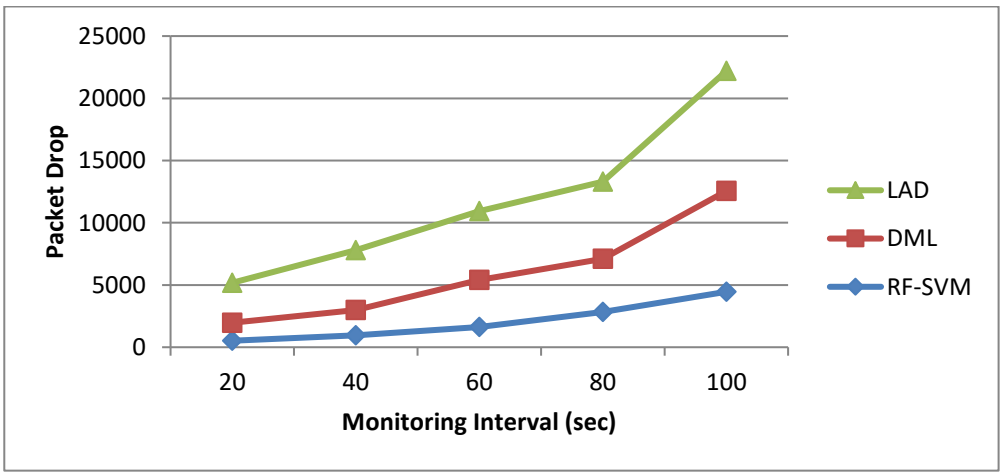

Figure 9 Packet drop for various intervals

Table 6 and Figure 9 show the packet drop measured for RF-SVM, LAD and DML when the monitoring intervals are varied. As we can see from the figure, the packet drop of RF-SVM is 50% less when compared to DML and 93% lesser than LAD.

B. Based on Attack Frequency

In our second experiment we vary the frequency of attacks from 25Kb/s to 125Kb/s

Table 7 Results of detection delay for various attack frequency

AttackFrequency (Kb/s)	RF-SVM (ms)	DML (ms)	LAD (ms)
25	4.254	6.628	11.30
50	6.916	8.692	12.57
75	7.542	10.334	13.26
100	8.030	11.424	13.28
125	9.255	12.209	13.27

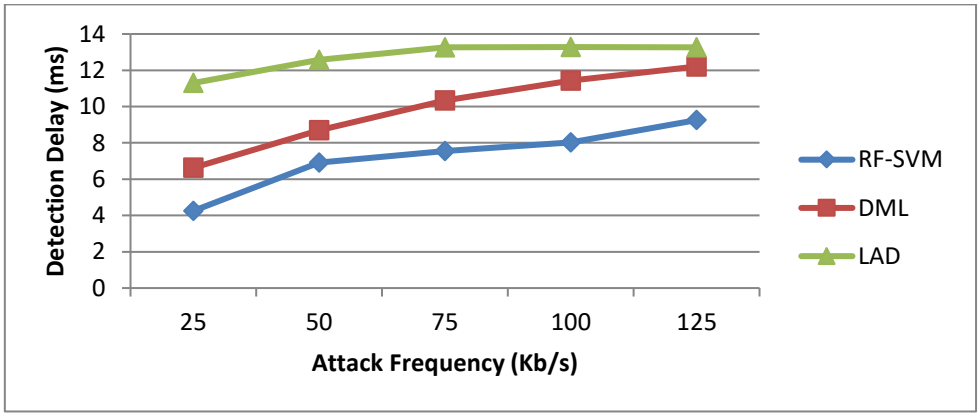

Figure 10 Detection delay for various attack frequency

Table 7 and Figure 10 show the detection delay measured for RF-SVM,LAD and DML when the attack frequencies are varied. As we can see from figure, the detection delay of RF-SVM is 27% lesser then DML and 44% lesser than LAD.

Table 8 Results of detection accuracy for various attack frequency

Attack Frequency	RF-SVM	DML	LAD
25	0.7791	0.7431	0.6549
50	0.7003	0.6254	0.5824
75	0.6734	0.5436	0.5141
100	0.6598	0.4858	0.4681
125	0.6479	0.4231	0.3969

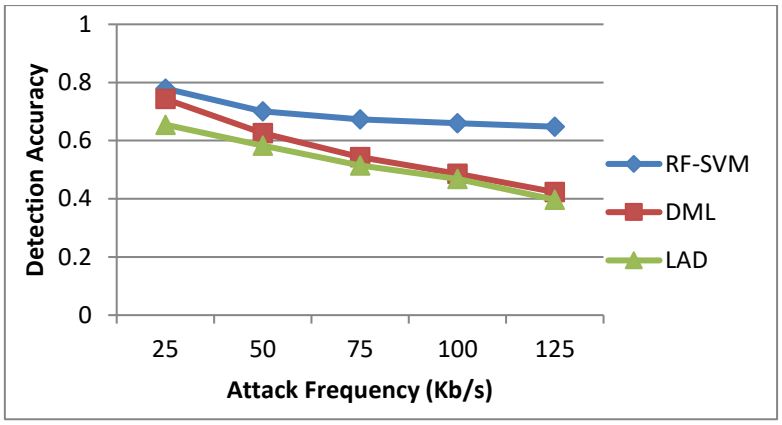

Figure11 Detection accuracy for various attack frequency

Table 8 and Figure 11 shows the detection accuracy measured for RF-SVM, LAD and DML when the attack frequencies are varied. As we can see from figure, the detection accuracy of RF-SVM is 19% high when compared to DML and 42% higher than LAD.

Table 9 Results of packet drop for various attack frequency

Attack Frequency	RF-SVM	DML	LAD
25	18	2141	2750
50	186	3443	4647
75	263	4842	5574
100	337	5845	6434
125	523	7722	8960

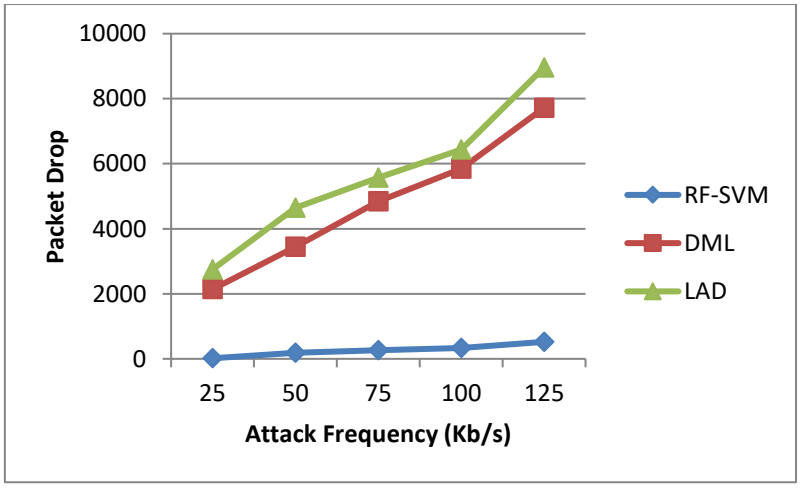

Figure12 Packet drop for various attack frequency

Table 9 and Figure 12 show the packet drop measured for RF-SVM, LAD and DML when the flows attack frequencies are varied. We can see that, the packet drop of RF-SVM is 69% less when compared to DML and 92% lessthan LAD.

5. CONCLUSION

In this paper, we propose to develop a Random Forest-Support Vector Machine (RF-SVM) based Anomaly detection mechanism for IoT. The RF classifier is applied for selecting the optimal features from the extracted traffic data. It includes removing the outliers, redundant data, and choosing the best features with high weight values. Then, SVM is applied for classifying the extracted features and detecting the anomalies. The fitness function is derived in terms of true positives, false positives, and false negatives. From the detected anomalies, the attack type is then determined, and a corresponding warning is sent to the monitoring nodes.

The proposed RF-SVM attains the highest accuracy, precision, recall, and the F1-score when compared to these algorithms. The proposed RF-SVM-based anomaly detection framework is simulated in NS2 and compared with the existing LAD and DML-based IDS techniques. The performance is evaluated in terms of detection delay, detection accuracy, and packet drop. In the experimental results, it is shown that the proposed RF-SVM classifier attains increased detection accuracy with reduced packet drops.

CONFLICTS OF INTEREST

The authors have no competing interests to declare that are relevant to thecontent of this article. There is no conflict of interest.

REFERENCES

[1] R. Stephen and L. Arockiam, "RIAIDRPL: Rank Increased Attack (RIA) Identification Algorithm for Avoiding Loop in the RPL DODAG," *Int. J. Pure Appl. Math.*, vol. 119, no. 16, 2018.

[2] F. Y. Yavuz, D. Ünal, and E. Gül, "Deep learning for detection of routing attacks in the Internet of Things," *Int. J. Comput. Intell. Syst.*, vol. 12, pp. 39–58, 2018.

[3] Z. A. Almusaylim, N. Z. Jhanjhi, and A. Alhumam, "Detection and mitigation of RPL rank and version number attacks in the Internet of Things: SRPL-RP," *Sensors*, vol. 20, 2020.

[4] A. Aris, S. F. Oktug, and B. O. Yalcin, "RPL version number attacks: In-depth study," in *Proc. IEEE Conf.*, 2016.

[5] B. A. Alabsi, M. Anbar, S. Manickam, and O. E. Elejla, "DDoS attack aware environment with secure clustering and routing based on RPL protocol operation," *IET Circuits Devices Syst.*,2019.

[6] M. Hasan, M. M. Islam, M. I. Islam Zarif, and M. M. A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches," *Internet Things*, vol. 7, 2019.

[7] G. Thamilarasu and S. Chawla, "Towards deep-learning-driven intrusion detection for the Internet of Things," *Sensors*, 2019.

[8] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning DDoS detection for consumer Internet of Things devices," arXiv:1804.04159v1 [cs.CR], 2018.

[9] H. Sedjelmaci, S. M. Senouci, and M. Al-Bahri, "A lightweight anomaly detection technique for low-resource IoT devices: a game-theoretic methodology," in *IEEE Int. Conf. Commun. (ICC), Mobile and Wireless Networking Symp.*,2016.

[10] D. Lia, L. Deng, M. Lee, and H. Wang, "IoT data feature extraction and intrusion detection system for smart cities based on deep migration learning," *Int. J. Inf. Manag.*, vol. 49, pp. 533–545, 2019.

[11] F. Huang, J. Shen, Q. Guo, and Y. Shi, "eRFSVM: A hybrid classifier to predict enhancers—integrating random forests with support vector machines," *Hereditas*, 2016.

[12] M. Shanmugasundari and R. K. Nayak, "Master card anomaly detection using random forest and support vector machine algorithms," *J. Crit. Rev.*, vol. 7, no. 9, 2020.

[13] S. Prithi and S. Sumathi, "Intrusion detection system using hybrid SVM-RF and SVM-DT in wireless sensor networks," *Int. J. Recent Technol. Eng.*, vol. 8, no. 2S8, 2019.

[14] M. A. M. Hasan, M. Nasser, B. Pal, and S. Ahmad, "Support vector machine and random forest modelling for intrusion detection system (IDS)," *J. Intell. Learn. Syst. Appl.*, vol. 6, no. 1, Feb. 2014.

[15] Z. Rustam, E. Sudarsono, and D. Sarwinda, "Random-Forest (RF) and support vector machine (SVM) implementation for analysis of gene expression data in chronic kidney disease (CKD)," in *Proc. 9th Annu. Basic Sci. Int. Conf.*, 2019.

[16] A. Diro et al., "A comprehensive study of anomaly detection schemes in IoT networks using machine learning algorithms," *Sensors*, vol. 21, no. 24, Art. no. 8320, 2021.

[17] Pughazendi N, Valarmathi K, Rajaraman PV, Balaji S. RETRACTED: Reliable cluster based data collection framework for IoT-big data healthcare applications. Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology. 2023;0(0). doi:10.3233/JIFS-233505.

[18] B. Duraisamy, S. Gopalakrishnan, S.-Y. Hsieh, and S.-L. Peng, Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2021. Springer, 2021.