I.J. Wireless and Microwave Technologies, **2021, 6, 46-54**
Published Online December 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijwmt.2021.06.05

Feature Engineering for Cyber-attack detection in Internet of Things

Maheshi B. Dissanayake
Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Peradeniya, Sri Lanka.
E-mail: maheshid@eng.pdn.ac.lk

Received: 22 September 2021; Accepted: 28 October 2021; Published: 08 December 2021

Abstract: Internet of Things (IoT) consists of group of devices which communicates information over private networks. One of the key challenges faced by IoT networks is the security breaches. With the objective of automating the detection of possible security breaches in five categories, IoT traffic created with Message Queue Telemetry Transport (MQTT) protocol is analyzed. The five categories of cyber-attacks considered are brute force, denial of service (DoS), flooding, malformed data, and SlowITe attacks along with legitimate traffic. The popular five machine learning (ML) models, LightGBM, Random Forest, MLP, AdaBoost, and Decision Tree Classifiers are trained to predict cyber-attacks. In traditional traffic analysis all the available features of MQTT traffic were utilized for the ML modeling and in this work, we challenge the practice by showing that automated feature selection improves the performance of the overall ML models. The average accuracy, precision, recall and the F1 score are used as performance evaluation metrics. It is observed that all models in average are able to achieve 90% of accuracy in classification, while MLP model is trained 10 times faster than the other models. Further the optimal number of features for correct classification is identified as 10 features through Monte Carlo analysis. With the reduced features, it is possible to detect DoS, flooding, and SlowITe attacks with more than 90% accuracy and precision. Yet, it is difficult to tell apart brute force and malformed data attacks.

Index Terms: IoT Traffic, Machine learning, cyber attacks, Feature importance, DoS, Brute Force attack

1. Introduction

Advancements in the digital technologies have immensely impacted the life style of the mankind. Since the past decade man has highly relied on new technologies and devices. This has given rise to smart home systems, when household devices with communication agents create networks to communicate and mange information in order to provide better service to their users. This has given rise to the concept of Internet of Things (IoT). In IoT networks, connected devices communicate sensitive information. The venerability in the network can be exploited by unauthorised person, with the intension of accessing this sensitive information and damaging the network. Hence, it is obligatory to implement security measures and continuously monitor the traffic for cyber attacks.

To protect data traversing in IoT networks, service providers adopt detect and mitigate systems to identify possible security breaches. With the advancement of Artificial Intelligence and Machine Learning (AI/ML), these algorithms can be employed to predict an incoming cyber attack.

With this objective, this work investigates the feasibility of employing Message Queue Telemetry Transport (MQTT) protocol [1] with popular state of the art ML models to detect and classify common cyber-threats in IoT networks. Decision tree, neural network and Ensemble based five classifiers are designed, trained, validated and tested with MQTT traffic dataset pre-recorded from a smart home IoT network [2].

To train a ML model for detecting and identifying, the legitimate behavior clearly apart from malicious behaviors, a large dataset is required. By nature, IoT appliances generate huge volume of data on daily basis. Yet, the bulkiness of the dataset, cause a considerable challenge for resource management. One of the simplest solutions for reducing the bulkiness of the dataset is the feature selection and storage of only the necessary and sufficient features for AI/ML model training and tuning. The traditional practice for feature selection of MQTT traffic, has been manually-crafted task specific feature selection approach. In this manuscript this practice is challenged as it is unclear whether the typical all 33 features in MQTT traffic in [1], contributes equally and significantly for the cyber attack detection. With this view, this work further investigates the key feature of MQTT traffic which helps the identification of malicious behavior, through automatic feature selection [3].

The rest of the paper is structured as follows. Section 2 reports a summary of the background work, related to the research presented. Section 3 presents the methodology adopted, while section 4 presents and discusses the results. Finally, section 5 concludes the paper by summarising the findings and future directions.

2. Background Work

Prediction of malicious behaviors in networks is a popular research which dates back to 1990s. With the advancement of ML, many research has immerged which investigates the possibility of using ML models to predict cyber threats [4]. Most research in this domain favors the KDDCUP99 dataset [5], which was developed using Transmission Control Protocol/Internet Protocol (TCP/IP) traffic for IP network. Yet, this dataset fails to provide a realistic scenario for malicious traffic behavior in IoT network.

In general, most IoT networks are private networks, where an agent controls and detects the behavior of devices connected to form the network. IoT networks found in smart home automation systems, favour MQTT protocol which runs over TCP as the communication protocol, due to its simplicity and low resource requirement [1]. The MQTT defines 3 components, namely MQTT Broker, who acts as the server, MQTT Publisher, who communicates with clients and MQTT Subscriber, who act as a client. These three entities create IoT network, where information is exchanged using MQTT protocol.

Although MQTT is popular choice for IoT, there is very little research which analyzes the behavior of MQTT traffic to predict cyber-attacks [6]. Most of the research which uses MQTT traffic analysis does not have a publicly available dataset, nor do they consider a smart home IoT network [7-12]. Hence, it is challenging to reproduce the results in literature for comparative analysis. Furthermore, they focus on detecting the most popular cyber-attacks, denial of service (DoS) and intrusion.

A novel attacks that can be present in IoT network is Slow DoS against Internet of Things Environments (SlowITe) [13]. It is a denial of service type attack which can target MQTT server which is running on TCP environment. Moreover, Brute force attack, Flooding, traditional DoS, and attacks by means of Malformed data are common security breaches in IoT.

In supervised ML based classifiers, a model is trained using labeled data to predict the labeled outcome. Naïve Bayes, Linear Discriminant analysis, Stochastic gradient decent, Support vector machines, Neural network, decision tree and ensemble models are popular state of the art supervised learning classifiers [14,15]. Each of these models has its own weakness and strengths [14], while requiring different levels of processing and computational capacity. Hence, any popular ML model would not suit all application scenarios, and selection must be made with care. Table 1 summaries the strengths and weaknesses of selected models for the research presented in this manuscript.

Modern IoT networks consist of miniature sensing devices with limited computational power, and limited data storage capabilities. Hence, when designing ML models for tracking and detecting cyber-attacks, it is essential to consider the limitation of resources as well as the capability of implementing these models on the IoT network itself. The models presented in Table 1 are selected considering the above limitations of the IoT network.

Table 1. The strengths and weaknesses of selected ML models.

Machine learning techniques	Specific model used	Strength	Weakness
Artificial neural network:	MLP Classifier [15]	Higher flexibility to learn highly complex non-linear relationships between features.	User specific network structure. Difficult to optimize and interpret the outcome.
Decision Tree	Decision Tree Classifier [15]	Good Interpretability and visualization. Little Computational time. Feature scaling is not required	Sensitive to slight changes in the data and can converge in correctly. Overfitting can easily happen.
Ensemble Method: bagging methods	Random forest [16]	Exhibits consistent performance with faster and robust training. Capable of identifying most sensitive, independent as well as important feature for the task.	Output is sensitive to the user selection of hyperparameters, such as number of branches and trees. Overfitting is possible
Ensemble Method: boosting methods	AdaBoost Classifier [17]	Has the ability to decrease bias. Less susceptible for overfitting.	High sensitivity to outliers
Ensemble Method boosting methods	LightGBM [18]	Highest performing boosting method. Faster to train and predict	Significant number of hyperparameter selection is present. To avoid overfitting, it is essential to tune these parameters with care.

Overall, literature shows that with the expansion of IoT networks, security breaches are a major threat for the network [19,20]. The research presented in this paper, predicts the most common five types of cyber-attacks in IoT networks, using MQTT traffic dataset in [1]. Popular machine learning models in literature, such as Random forest, MLPClassifier, AdaBoostClassifier, DecisionTreeClassifier are compared against the newly proposed LightGBM Classifier for the task of classifying cyber-attacks. Furthermore, we analyze the feature importance in detecting an attack. By doing so, we aim to identify key features which could be used in real time data processing in resource limited IoT environments to predict a cyber threat.

3. Methodology

3.1. Dataset

IoT networks, find many applications in modern digital world such as in smart homes [21], health care sector [22] insdustrial application [23], etc. The dataset used in this study is generated using MQTT protocol in a simulated IoT smart home network and the data is freely available in public domain at [1]. The IoT network used for data generation consist of IoT smart home sensors such as temperature sensors, humidity sensors, Gas monitors, motion sensors and light sensors connected to a MQTT broker. When a compromised sensor generates malicious traffic, it is categorised as a security attack. In this study 5 types of attacks are predicted, based on the behaviour of the malicious traffic. Each incoming traffic consists of 33 parameters, i.e features, as shown in Table 2 [1]. Lastly the dataset carries labelling information related to the type of attack or the legitimacy of the traffic generated. Hence, there are 5 types of attack labels and one label as legitimate traffic.

Table 2. The list of TCP and MQTT features recorded.

Full Description	Abbreviation
TCP flags	tcp.flags
Time TCP stream	tcp.time_delta
TCP Segment Len	tcp.len
Acknowledge Flags	mqtt.conack.flags
Reserved	mqtt.conack.flags.reserved
Session Present	mqtt.conack.flags.sp
Return Code	mqtt.conack.val
Clean Session Flag	mqtt.conflag.cleansess
Password Flag	mqtt.conflag.passwd
QoS Level	mqtt.conflag.qos
(Reserved)	mqtt.conflag.reserved
Will Retain	mqtt.conflag.retain
User Name Flag	mqtt.conflag.uname
Will Flag	mqtt.conflag.willflag
Connect Flags	mqtt.conflags
DUP Flag	mqtt.dupflag
Header Flags	mqtt.hdrflags
Keep Alive	mqtt.kalive
Msg Len	mqtt.len
Message	mqtt.msg
Message Identifier	mqtt.msgid
Message Type	mqtt.msgtype
Protocol Name Length	mqtt.proto_len
Protocol Name	mqtt.protoname
QoS Level	mqtt.qos
Retain	mqtt.retain
Requested QoS	mqtt.sub.qos
Granted QoS	mqtt.suback.qos
Version	mqtt.ver
Will Message	mqtt.willmsg
Will Message Length	mqtt.willmsg_len
Will Topic	mqtt.willtopic
Will Topic Length	mqtt.willtopic_len

3.2. Data Refining and Model Training

The complete dataset consists of 99290 entries of traffic ranging from both legitimate to malicious with 33 features for each entry. Each entry belongs to one specific class out of the six listed above depending on the behaviour of the traffic. Hence, the classification models are trained for multi-class prediction problem.

The main task of the problem presented in this study is the identification of legitimate and malicious traffic in IoT network. With this objective the study presented has tested the performance of popular machine learning models, namely Random forest, MLPClassifier, AdaBoostClassifier, DecisionTreeClassifier and LightGBM Classifier for the task of cyber-attack detection in IoT network. For a fair comparison between models, hyper parameter optimization was carried out for each model using Grid-Search algorithm [24].

One of the key hypotheses tested in this work is whether all 33 features of MQTT traffic recorded, contribute equally or at all, to the task of cyber-attack detection and whether an automated feature selection process can further enhance the performance of the detection process. With this objective, we have performed feature analysis using RF Classifier to detect the most prominent feature in MQTT traffic which contributes to the correct classification outcome.

During the experiment we first derived the feature importance value for each of the 33 features of the input data using fine tuned RF classifier. Next random numbers of sub-sampled datasets are created using only the features with highest feature importance values. Thereafter, these new sub-sampled datasets are used to train the selected five state of the art ML models tabulted in Table 1. Each ML model is hyper parameter optimised for each sub-sampled dataset tested. The performance evaluation metrics; average accuracy, precision, recall and the F1 score are calculated for each ML model instance. Later this model performance was compared to evaluate cyber-attack detection performance as well as the minimum number of feature needed to make an accurate prediction.

4. Results

This section presents the results of applying machine learning models, Random forest, MLPClassifier, AdaBoostClassifier, DecisionTreeClassifier and LightGBM Classifier. All the experiments are repeated at least 3 times, and 3 fold cross-validated where applicable. The dataset considered is split 70:30 ratio for the training and testing sets at the data pre-processing stage of the experiment. The experiments are carried out in python environment and ML models were implemented using Sklearn, and lightgbm libraries.

4.1. Hyperparameter Tuning.

Each machine learning model carries different hyper-parameters. Yet, it is essential to fine tune the hyperparameters for performance and cost optimization as well as to obtain a common platform before the comparison of the classification process of all models. The optimized hyperparameters utilized for each model presented in this study are summarized in Table 3 and it will facilitate comparative verification of the implementation in future use.

Table 3. Optimized hyper parameters for each ML model

Model name	Values of optimized hyperparameter

LGBMClassifier	learning_rate= 0.05,
	max_depth= 10,
	n_estimators=100,
	num_leaves= 20,
	boosting_type= 'gbdt',
	colsample_bytree= 1.0,
	reg_lambda= 0.5,

DecisionTreeClassifier	criterion= 'gini',
	max_depth= 30,
	splitter='best',
	random_state=3, min_samples_leaf=4

MLPClassifier	max_iter=100,
	activation= 'relu',
	alpha= 0.0001,
	hidden_layer_sizes
	=(10, 30, 10),
	learning_rate= 'constant',
	solver= 'adam'

AdaBoostClassifier	DecisionTreeClassifier(max_depth=10),
	algorithm="SAMME",
	n_estimators=200

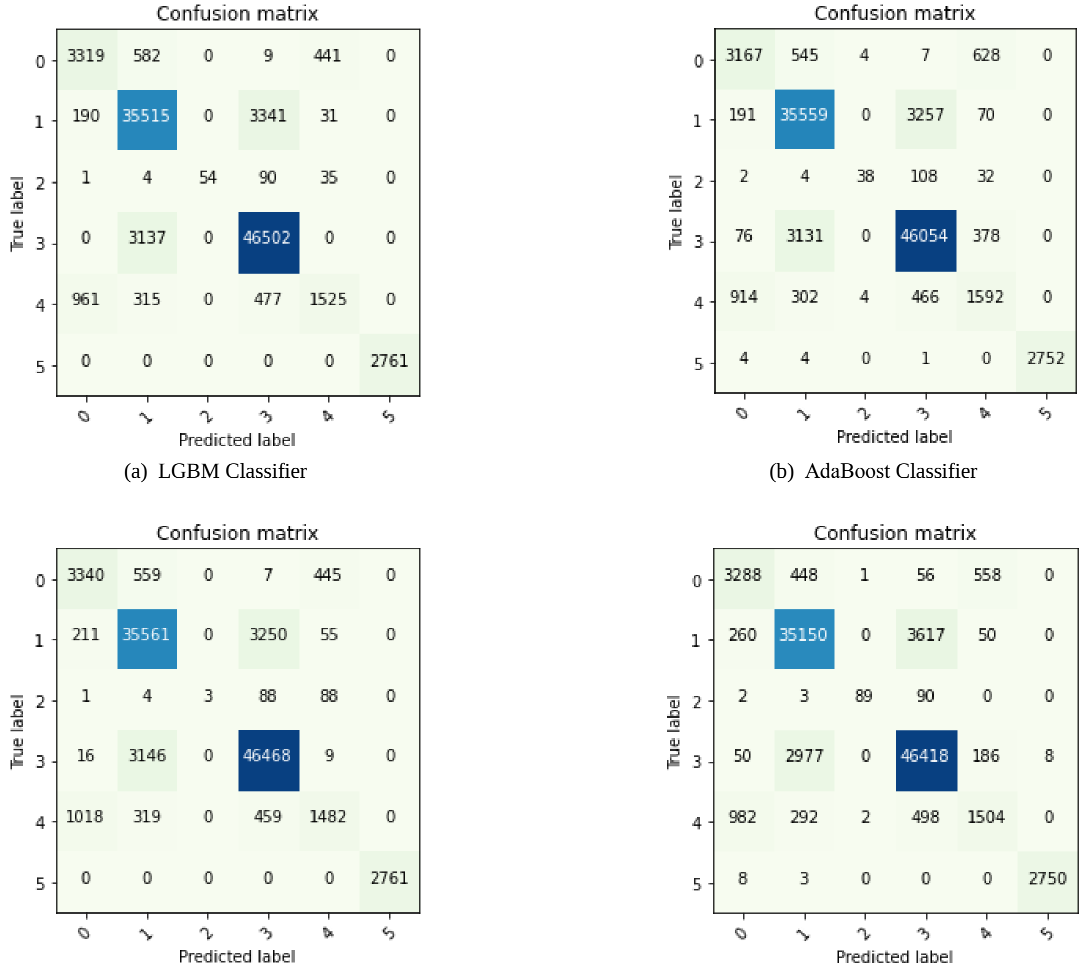
4.2 Performance Analysis of Classification Using All Features

Fig. 1, illustrates the accuracy of classification of each tuned model for the 6 classes, namely 0-'bruteforce', 1-'DoS', 2-'flooding', 3-'legitimate', 4-'malformed data', and 5- ‘SlowITe’. According to the results, almost all the models are successful in predicting, DoS, and legitimate cyber-attacks with more than 90% of accuracy, while all models detected SlowITe with more than 99% of accuracy although the sample set is relatively smaller than DoS, and legitimate classes. The flooding class carries the smallest amount of sample data, hence all the models significantly failed to identify flood type attacks. Moreover, it can be observed that most erroneous predictions are incorrectly predicted as legitimate traffic.

It is observed that the selection of the classification model does not impact the outcome foremost; nevertheless, the model training and testing time vary significantly between MLP classifier and other tested model as shown in Table 4. In fact, significant differences in the model performances could arise depending on the hyperparameter values selected.

Table 4. Comparison of training and testing time for each model

Model	Training time/s	Testing time/s
LGBM Classifier	6205	1.026
AdaBoost Classifier	1110.2	2.743
DecisionTree Classifier	1639.79	0.014
MLP Classifier	146.11	0.223



(a) LGBM Classifier

(b) AdaBoost Classifier

(c) Decision Tree Classifier

(d) MLP Classifier

Fig. 1. Classification accuracy for LGBM Classifier AdaBoost Classifier , Decision Tree Classifier and MLP Classifier,

4.3 Feature Importance Analysis

IoT networks have the potential to generate significant amount of traffic at short intervals by default. It causes a bottleneck at the computational efficiency in real time implementation. The feature selection method, determines the relevant features within the input data for efficient classification. In turn feature selection assists the researchers to significantly reduce the size of larger datasets for analysis. Moreover, feature selection itself can function as a filtering process and would assist the model to focus on important features at training phase.

In this research the feature importance analysis for the MQTT traffic is carried out using random forest model. According to the feature importance plot obtained using random forest model (Fig. 2.), the fifteen (15) key features that determine the type of cyber-attack in descending order of importance are 'tcp.time_delta', 'mqtt.msgid', 'mqtt.hdrflags', 'mqtt.msg', 'tcp.len', 'mqtt.len', 'tcp.flags', 'mqtt.msgtype', 'mqtt.qos', 'mqtt.conack.val', 'mqtt.dupflag', 'mqtt.conflags', 'mqtt.conack.flags', 'mqtt.kalive', and 'mqtt.ver'. Out of all the 33 features present in the dataset only 19 features contributed to the decision, the rest of the features have a feature importance score of zero can be seen in Fig. 2.

To test the accuracy of this observation, we have repeated, model training and prediction using only the top 5, 7, 10 and 15 features. As of Fig. 3, the reduction of features does not significantly affect the outcome of the overall performance of the model. In depth analysis shows that the reduction of features, affect the classification of the malformed data and brute force attacks significantly. This observation is statistically presented in Table 5.

A thorough analysis of results shows that using only the 10 features with the top feature importance values, it is possible to achieve a same level of performance as of the full feature set. Thus, it can be concluded that in resource limited scenarios, it is sufficient to concentrate only on 10 features; namely 'tcp.time_delta', 'mqtt.msgid', 'mqtt.hdrflags', 'mqtt.msg', 'tcp.len', 'mqtt.len', 'tcp.flags', 'mqtt.msgtype', 'mqtt.qos', and 'mqtt.conack.val' of MQTT traffic. Hence, when analyzing cyber-attacks on IoT network using MQTT traffic, it is sufficient to store and even process the top 10 features identified in Fig. 2. In general, this reduced feature set, detects all types of malicious traffics with sufficient average accuracy.

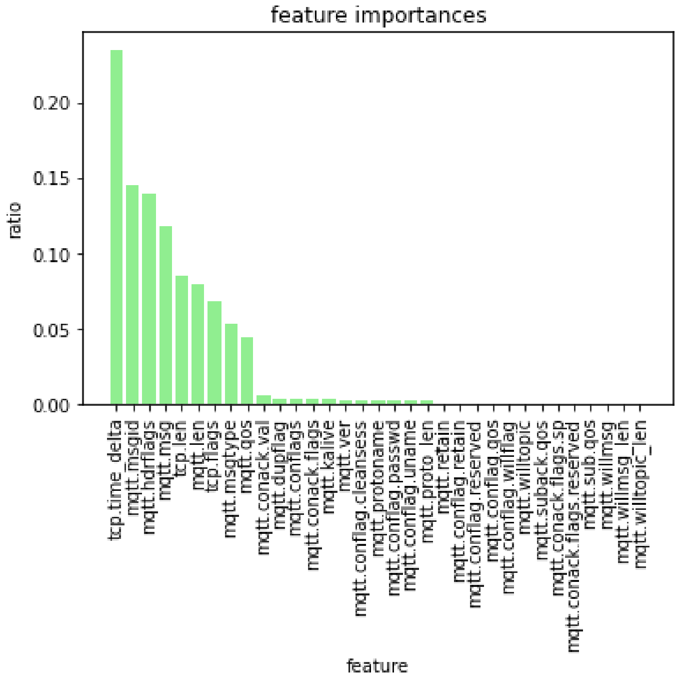
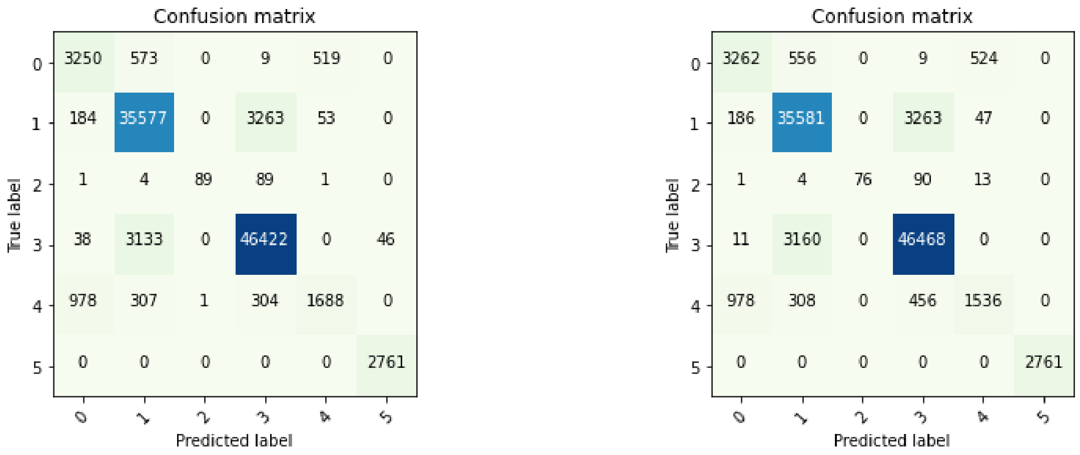
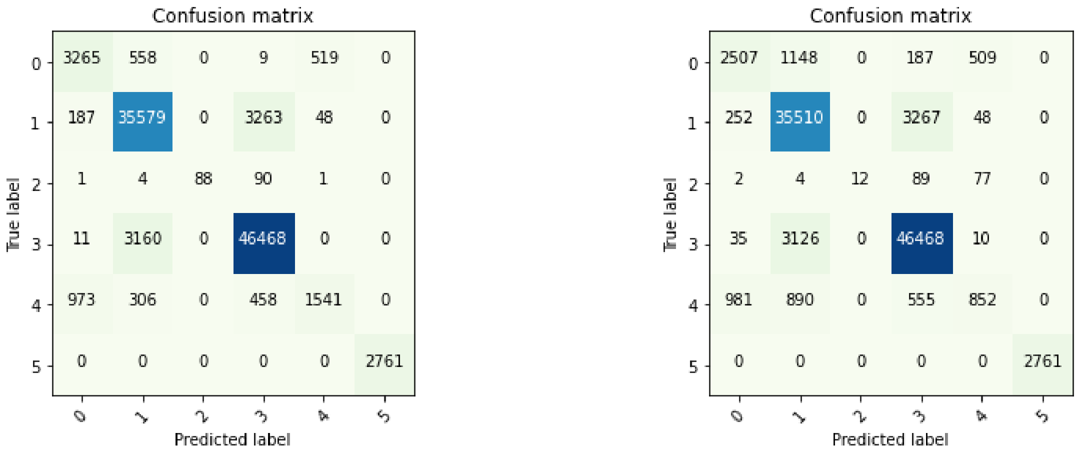


Fig. 2. Feature importance map for Random forest classifier



(a) Full (33) feature Set

(b) Reduced (10) feature set



(c) Reduced (15) feature set

(d) Reduced (5) feature set

Fig. 3. Classification accuracy for Random forest with full (33) and reduce feature sets

Table 5. Performance variation with feature set size

Performance measure	Number of features in an entry				
	33	15	10	7	5
Avg. Accuracy	0.90	0.90	0.90	0.90	0.90
Confidence interval for accuracy	0.86-0.92	0.88-0.92	0.89-0.90	0.88-0..93	0.85-0.94
Precision	0.88	0.88	0.88	0.88	0.84
recall	0.77	0.75	0.75	0.75	0.62
F1- score	0.80	0.79	0.79	0.79	0.65
Class specific observation of precision score					
Malformed	0.75	0.72	0.72	0.70	0.57
Brute force	0.73	0.73	0.74	0.70	0.66
DoS	0.9	0.90	0.90	0.90	0.87
Legitimate	0.92	0.92	0.93	0.92	0.92

5. Conclusion

IoT devices in smart home networks are growing in numbers in the resent years. Since these devices communicates sensitive information, the potential of cyber-attack remains highly viable. Hence, it is important to study the aspect of cyber-security for IoT networks. The analysis presented in this work is two folds. As the first step traditional ML models, namely MLP Classifier, AdaBoost Classifier, DecisionTree Classifier and LightGBM Classifier, are trained to predict the type of cyber-attack based on incoming MQTT traffic data. The findings show that it is possible to detect cyber-attacks with high accuracy using these models whereas the MLP classifier exhibits the lowest computational time with 90% of average accuracy. Hence, for a real time traffic analysis MLP classifier is highly suitable.

Furthermore, we explore the effect of automated feature engineering, i.e task dependent automated feature selection, on the cyber-attack classification. It is a known fact that although a larger dataset is desirable for training a ML model, it is challenging in terms of data storing and processing. Since, IoT networks are light weighted networks with low processing and storage capacity, we explore the possibility of reducing the number of features used for the model training, as high number of features in a larger dataset challenges the processing and training of these models.

The random forest algorithm is utilized to evaluate the feature importance score for the each 33 features of the original dataset. Monte Carlo approach was utlised to train different instances of ML models using random samples of feature sets, according to its feature importance values. After thorough analyzis of the results, we conclude that in resource limited scenarios, it is sufficient to concentrate only on 10 features, namely 'tcp.time_delta', 'mqtt.msgid', 'mqtt.hdrflags', 'mqtt.msg', 'tcp.len', 'mqtt.len', 'tcp.flags', 'mqtt.msgtype', 'mqtt.qos', and 'mqtt.conack.val'.

Although the dataset consists of staggering 99290 entries of traffic, it shows a significant class imbalance. Further, the study relies on a dataset collected at one specific environment. Hence as future directions, the analysis can be expanded using combined datasets from different environments with improved entries in low represented classes. This would indeed help to converge at a better outcome in malicious traffic detection, which is favorable to implement in practical settings.

References

[1] M. O. Al Enany, H. M. Harb, and G. Attiya, “A Comparative analysis of MQTT and IoT application protocols,” in Proceedings of the 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRISs2021 International Conference on Electronic Engineering (ICEEM), pp. 1–6, Menouf, Egypt, July 2021

[2] Vaccari, I.; Chiola, G.; Aiello, M.; Mongelli, M.; Cambiaso, E. MQTTset, a New Dataset for Machine Learning Techniques on MQTT. Sensors 2020, 20, 6578.

[3] Khurana, U., Samulowitz, H., and Turaga, D. Feature engineering for predictive modeling using reinforcement learning. In Thirty-Second AAAI Conference on Artificial Intelligence, April. 2018.

[4] I. Vaccari, S. Narteni, M. Aiello, M. Mongelli and E. Cambiaso, "Exploiting Internet of Things Protocols for Malicious Data Exfiltration Activities," in IEEE Access, vol. 9, pp. 104261-104280, 2021

[5] Komar, M.; Dorosh, V.; Hladiy, G.; Sachenko, A. Deep neural network for detection of cyber attacks. In Proceedings of the 2018 IEEE First International Conference on System Analysis & Intelligent Computing (SAIC), Kiev, Ukraine, 8–12 October 2018; pp. 1–4.

[6] Ferrag, M.A.; Maglaras, L.; Moschoyiannis, S.; Janicke, H. Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. J. Inf. Secur. Appl. 2020, 50, 102419.

[7] M.; Fu, X.; Syed, N.; Baig, Z.; Teo, G.; Robles-Kelly, A. Deep Learning-Based Intrusion Detection for IoT Networks. In Proceedings of the 2019 IEEE 24th Pacific Rim International Symposium on Dependable Computing (PRDC), Kyoto, Japan, 1–3 December 2019; pp. 256–25609.

[8] Khraisat, A.; Gondal, I.; Vamplew, P.; Kamruzzaman, J.; Alazab, A. A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks. Electronics 2019, 8, 1210.

[9] Ciklabakkal, E. et al. ARTEMIS: An Intrusion Detection System for MQTT Attacks in Internet of Things. In Proceedings of the 2019 38th Symposium on Reliable Distributed Systems (SRDS), Lyon, France, 1–4 October 2019; pp. 369–3692.

[10] Morales, L.V.V.; López-Vizcaíno, M.; Iglesias, D.F.; Díaz, V.M.C. Anomaly Detection in IoT: Methods, Techniques and Tools. Proceedings 2019, 21, 4.

[11] Alaiz-Moreton, H. et al. Multiclass classification procedure for detecting attacks on MQTT-IoT protocol. Complexity 2019, 2019, 6516253

[12] Saritas, M.M.; Yasar, A. Performance analysis of ANN and Naive Bayes classification algorithm for data classification. Int. J. Intell. Syst. Appl. Eng. 2019, 7, 88–91

[13] Vaccari, I., Aiello, M., & Cambiaso, E. SlowITe, a Novel Denial of Service Attack Affecting MQTT. Sensors 2020 (Basel, Switzerland), 20(10), 2932.

[14] Bonaccorso, Giuseppe. Machine learning algorithms. Packt Publishing Ltd, 2017.

[15] Ghori, K. M. et al., "Performance Analysis of Different Types of Machine Learning Classifiers for Non-Technical Loss Detection," in IEEE Access, vol. 8, pp. 16033-16048, 2020

[16] Ho, T.K., Random Decision Forest. Proceedings of the 3rd International Conference on Document Analysis and Recognition, Montreal, 14-16 August 1995, 278-282.

[17] Yoav Freund, Robert Schapire, and Naoki Abe. A short introduction to boosting. JournalJapanese Society For Artificial Intelligence, 14(771-780):1612, 1999.

[18] Guolin Ke, et al. LightGBM: a highly efficient gradient boosting decision tree. In Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS'17). Curran Associates Inc., Red Hook, NY, USA, 3149–3157, 2017

[19] Derek Johnson, Mohammed Ketel,"IoT: Application Protocols and Security", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.4, pp.1-8, 2019

[20] Asifa Nazir, Sahil Sholla, Adil Bashir, " An Ontology based Approach for Context-Aware Security in the Internet of Things (IoT)", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.1, pp. 28-46, 2021

[21] Syed Kashan Ali Shah, Waqas Mahmood, " Smart Home Automation Using IOT and its Low Cost Implementation ", International Journal of Engineering and Manufacturing (IJEM), Vol.10, No.5, pp.28-36, 2020.

[22] Samah Osama M. Kamel, Sanaa Abou Elhamayed, "Mitigating the Impact of IoT Routing Attacks on Power Consumption in IoT Healthcare Environment using Convolutional Neural Network", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.4, pp.11-29, 2020

[23] Ahmet Ali Süzen, "A Risk-Assessment of Cyber Attacks and Defense Strategies in Industry 4.0 Ecosystem", International Journal of Computer Network and Information Security(IJCNIS), Vol.12, No.1, pp.1-12, 2020

[24] Seunghyun Park, Jin-Young Choi, "Malware Detection in Self-Driving Vehicles Using Machine Learning Algorithms", Journal of Advanced Transportation, vol. 2020, Article ID 3035741, 9 pages, 2020.

Author’s Profile

Maheshi Buddhinee Dissanayake received the B.Sc. Engineering degree with First Class Honors in electrical and electronic engineering from the University of Peradeniya, Sri Lanka, in 2006, and the Ph.D. in electronic engineering from the University of Surrey, U.K., in 2010.

Since 2013, she has been a Senior Lecturer with the Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Peradeniya. She has been a visiting research fellow at King's College London from 2015-2017. Her research interests include error correction codes, robust video communication, molecular communication, machine learning, and biomedical image analysis. She has co-authored nearly 75 conference and journal articles and has a citation record of more than 200.

Dr. Dissanayake is a Senior Member of Institute of Electrical and Electronics Engineers (IEEE) and Associate member of Institution of Engineers, Sri Lanka (IESL). She has served as an organizing committee member and TPC Member of many IEEE conferences, and as a reviewer in IEEE journals in the area of Molecular communication and image processing. At present she is the Chairperson of IEEE Sri Lanka Section, and the founder as well as the immediate past Chair of IEEE Women in Engineering Sri Lanka section.

How to cite this paper: Maheshi B. Dissanayake, " Feature Engineering for Cyber-attack detection in Internet of Things", International Journal of Wireless and Microwave Technologies(IJWMT), Vol.11, No.6, pp. 46-54, 2021.DOI: 10.5815/ijwmt.2021.06.05