Predicting the Characteristics of Cyber Attacks on IoT Devices

Anthony McKinzie, Esha Singh, Taruna Sanjay Pakhare, Lewis Davis
Department of Information Systems, University of Maryland Baltimore county

Introduction

Many IoT devices are vulnerable to cyber attacks due to their lack of consideration towards security. With millions of IoT devices connected to the internet, It is inevitable that they will become prime attack targets. Methods to detect these cyber attacks currently need to be improved. We attempt to leverage machine learning to identify the common characteristics of cyber attacks by analyzing network traffic on IoT devices.

Our goal is find out which machine learning techniques will be the suitable for our task. Three algorithms are used to attempt this achieve goal: J48 decision tree, Apriori, and K-means clustering. Of the three algorithms J48 decision tree was the successful at providing meaning characteristics of IoT cyber attacks. However, all three algorithms had their flaws and require further improvements.

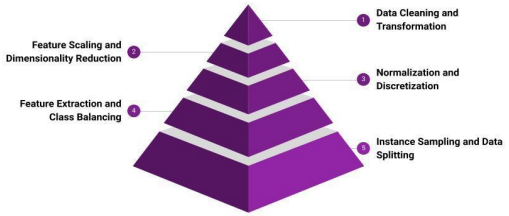
Research and Methodology

Aldhaheri et al. attempted similar work in their paper that suggests various deep learning models to detect cyber threats in IoT networks [1]. While the algorithms used by Aldhaheri et al. are much more advanced than the ones we present here, they do utilize the Edge-IIot dataset [2] that we are analyzing Aldhaheri et al. identify deep learning as the superior strategy for IDS systems that are running on Iot networks due to the volatile nature of IoT devices. [1].

We used a dataset of network traffic to IoT devices to conduct or research. The dataset has a mix of normal traffic as well as traffic from simulated cyber security attacks that the datacollects ran against the IoT device [2]. The data was reduced to 1,250 entries and balanced so that there were roughly 600 instances of normal traffic and 650 instances of attack traffic. Features with variance above 85% were removed. Attack-label was selected as the classify over Attack_type so that class labels were binary.

We deployed three strategies to create a model that could predict the characteristics of cyber attacks on IoT devices. First, we ran our data through a J48 decision tree and analyzed attributes the algorithm sorted the data on. Next we attempted association rule mining with Apriori. Our goal with apriori was to determine if we could gain any information through the association of certain attributes in the dataset. Finally, we implemented K-means clustering to see if certain sets of attributes could produce class clusters with outliers. If suitable class clusters are generated, it could indicated that the select group of attributes has a high correlation with one of our class labels.

Results

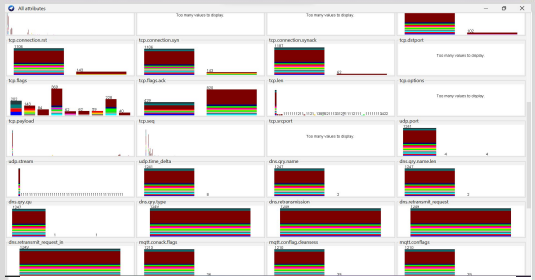


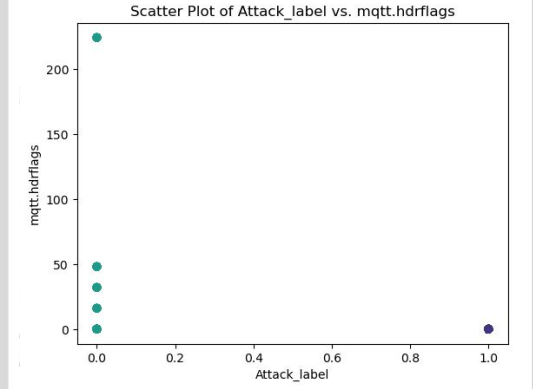
When using a J48 tree on the data, Weka was able to detect an attack with 83.11% accuracy. The model relied on the mqtt header field which is a standard communication protocol for IoT devices. Traffic lacking mqtt.hdr flags was classified as an attack. For traffic that that had mqtt.hdr flags, the algorithm then sorted based on the number of tcp.flags. If there were >20 or <4 flags the traffic was classified as an attack. The algorithm attempted a further sort on rows with a tcp.flag length of 16. This was not useful though as everything in this sort had already been correctly classified in a previous branch. By forcing binary splits on nominal values, the tree become vertical with more branches and leaves. This change also kept the same accuracy.

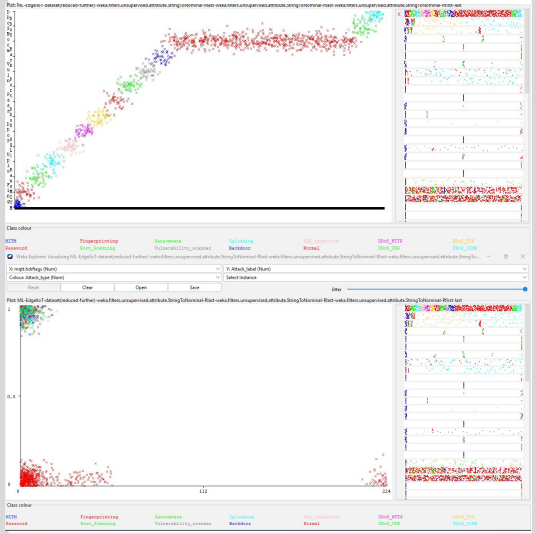
Using the Apriori algorithm was not useful for predicting characteristics of cyber attacks. The algorithm required a lot of processing power which forced use to filter out attributes with over 85% variance. Even with that complete, the association rules were stuck on associating DNS query names to DNS query name lengths. Even by filtering out the DNS attributes, Apriori still did not make meaningful associations. It simply would try to make associations than one attribute being 0 likely meant some other attribute was also 0.

Using K-means clustering for identifying outliers in predicting cyber attacks on IoT devices has several limitations. K-means assumes that clusters are spherical and equally sized, which may not be representative of the complex and diverse nature of cyber attacks. IoT networks often exhibit heterogeneous patterns, and attacks can vary significantly in terms of scale, type, and execution. K-means may struggle to capture irregularly shaped clusters or clusters with varying densities, leading to suboptimal outlier detection performance. Moreover, K-means is sensitive to the choice of the number of clusters (K), which is a critical parameter. Selecting an inappropriate value for K might result in the merging or splitting of clusters, leading to misidentification of outliers or overlooking genuine threats.Our K-means clustering has encountered problems related to the initial placement of cluster centers, as K-Means clustering identifies groups of devices with similar behavior. The results can vary depending on where the clusters start, making the algorithm unsuitable for our task.

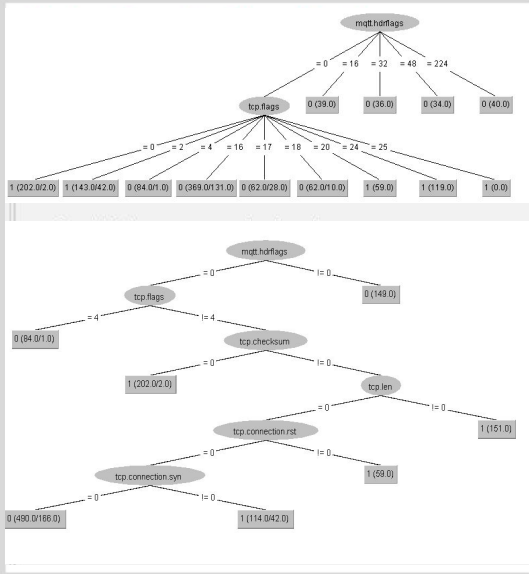
Clustering Results







Classification Results



Conclusion & Future Work

While we has some positive results with the J48 classification tree, our methods need a lot of improvement before they can be trusted to predict attacks on IoT devices. The J48 tree, one of our most accurate models, relied heavily on the presence of MQTT messages to determine attacks. If an attacker were to spoof these messages, they would completely fool our model. Apriori was not suitable for this task as the associations it generated provided no meaningful connections to the class labels to determine if they were related to an attack. K-means clustering was also determined to not be a suitable model for us due to several limitations. The complex nature of the traffic data led to irregular clusters that were difficult to capture and analyze for outliers. Additionally, K-means clustering is less effective as more attributes are introduced into the data.

Our future work includes finding a way to split our numeric attributes into nominal ranges rather than individual values. A greater focus decision trees and other classification algorithms, and revised feature selection methods.

References

1. Aldhaheri, A., Alwahedi, F., Ferrag, M. A., & Battah, A. (2024). Deep learning for cyber threat detection in IoT networks: A review. Internet of Things and Cyber-Physical Systems, 4, 110–128. doi:10.1016/j.iotcps.2023.09.003
2.Mohamed Amine Ferrag, Othmane Friha, Djallel Hamouda, Leandros Maglaras, Helge Janicke. (2022). Edge-IIoTset: A New Comprehensive Realistic Cyber Security Dataset of IoT and IIoT Applications: Centralized and Federated Learning. IEEE Dataport. https://dx.doi.org/10.21227/mbc1-1h68