TRUSTING MACHINE LEARNING ALGORITHMS IN PREDICTING MALICIOUS NODES ATTACKS

Basim Mahbooba, Mohan Timilsina and Martin Serrano

Insight Centre for Data Analytics, NUI Galway, Galway City, Ireland

ABSTRACT

Identifying network attacks is a very crucial task for Internet of things (IoT) security. The increasing amount of IoT devices is creating a massive amount of data and opening new security vulnerabilities that malicious users can exploit to gain access. Recently, the research community in IoT Security has been using a data- driven approach to detect anomaly, intrusion, and cyber-attacks. However, getting accurate IoT attack data is time-consuming and expensive. On the other hand, evaluating complex security systems requires costly and sophisticated modeling practices with expert security professionals. Thus, we have used simulated datasets to create different possible scenarios for IoT data labeled with malicious and non-malicious nodes. For each scenario, we tested off a shelf machine learning algorithm for malicious node detection. Experiments on the scenarios demonstrate the benefits of the simulated datasets to assess the performance of the ML algorithms.

KEYWORDS

IoT Simulation, Data Labels, Malicious Nodes, Attacks, Trust, Prediction.

1. INTRODUCTION

Network security has become one of the important agendas of most organizations due to the increasing risks brought by network attack threats. As a result, companies are spending a tremendous amount of money on information technology and cybersecurity solutions. For example, in 2019, one of the leading research and advisory companies known as Gartner[1] spent over 124 billion dollars on information security. Thus, network security is one of the serious and vulnerable issues worldwide.

A **network attack** is any derogatory action that targets information systems, infrastructures, Internet of Things (IoT) devices, computers using various methods to steal, alter or destroy data or information systems. There are different variants of these attacks known by other names, such as Denial of Service (DoS), Man in the Middle (MitM), Phishing, Password attack, SQL injection attack, Birthday, Malware attack, and many more. Understanding these variants of attacks requires extensive background knowledge of the mechanism of attacks. Unfortunately, it is tough to do this because each of the attacks is different.

[1] 1https://www.gartner.com/en/newsroom/pressreleases/2018-08-15-gartner-forecasts-worldwideinformation-security-spending-to-exceed-124-billionin-2019

David C. Wyld et al. (Eds): AIAP, IT, MoWiN, CCSEIT, CNSA, ICBB - 2022
pp. 93-103, 2022. CS & IT - CSCP 2022 DOI: 10.5121/csit.2022.120408

In Figure 1, demonstrates the example of IoT security attack. Alex's smart coffee machine is connected to the Internet via a special app. The hackers can target that app and steal Alex's bank card details. The smart coffee machine allows Alex to control it remotely by his phone. As coffee machines are not designed for security, the hackers can easily access Alex's bank information navigating via coffee machine apps. It is just one example. However, there are swarms of physical objects on the Internet at an unprecedented scale due to the Internet of Things (IoT) [7]. Recently, the boom of IoT devices has opened the fear of mass vulnerabilities [3]. There are billions of IoT devices in the world, which all collect loads of data in real-time. These physical objects include, but are not limited to, temperature sensors, smartphones, air conditioning, medical equipment, light bulbs, smart grid,

thermostats, and TVs [8]. These devices are connected to consumers, enterprises, and healthcare organizations. Their internal vulnerabilities have created a security blind spot where cybercriminals can launch various attacks to compromise devices like webcams, smart TV, routers, printers, and even a smart home.

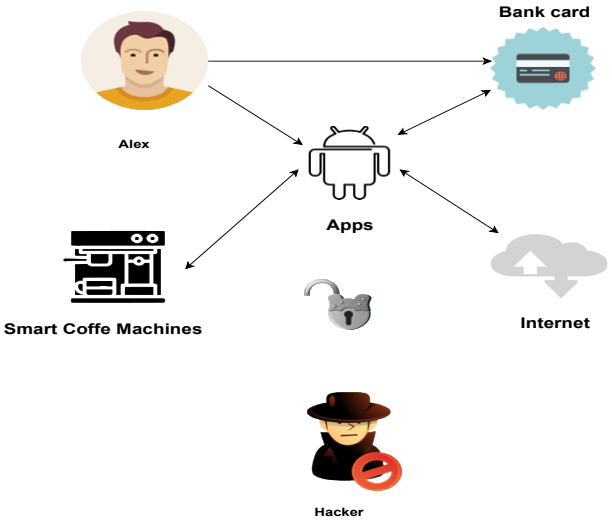


Figure 1. Example of IoT security Attack

There are many attacks due to the IoT devices when connected to the Internet. It is due to the limitations of these devices. Those limitations comprise small memory, minimal processing power, and shortbattery life. Nowadays, the attackers are focusing on IoT devices malicious intends [4]. The possible attack can be from hackers, hacktivists, and cybercriminals. The security in IoT is defined as the proper protection against acts such as data theft, unauthorized access, physical tampering, data manipulation, and network attacks [8]. Thus, cybersecurity is crucial for the proper operation of the IoT industry [22].

IoT raises many challenges, one of which is the massive amount of data generated by sensor devices. However, it was observed that, with the increase in sensor density, data generated by IoT devices tend to be highly redundant [23]. Thus, the redundant data consumes extra network re-sources and reduces network efficiency, making the IoT attacks easier for hackers. Also, another problemis inaccurate sensor data, which can mislead the net-work resources with erroneous information and lead to possible false reactions at the network center andmakes it vulnerable to attack. Thirdly, in the beginning, if the attack happens in a real-world scenario, there are few malicious nodes and large non-malicious nodes. Thus, early identifying such malicious nodes will reduce the massive loss of network resources.

In this paper, we address the problems as mentioned earlier using simple simulated data sets. As new technology is being accustomed to data- driven infrastructure, this leads the research more on to Machine Learning (ML) based applications along- side IoT. Thus, we are using an off-the-shelf machine learning suite to predict malicious nodes in a simulated setting. Such settings will allow us to test various ML algorithms to find which one works in what cases. The ML system provides high-performance indicators such as showing high accuracy score, which could enhance people's trust and acceptance of the system [30]. Thus, in this work, we explore different ML models to assess the prediction performance in a simulated environment. We believe that people trust an ML model if it can give high accuracy in unseen data.

Contributions: Our contributions are summarized as follows:

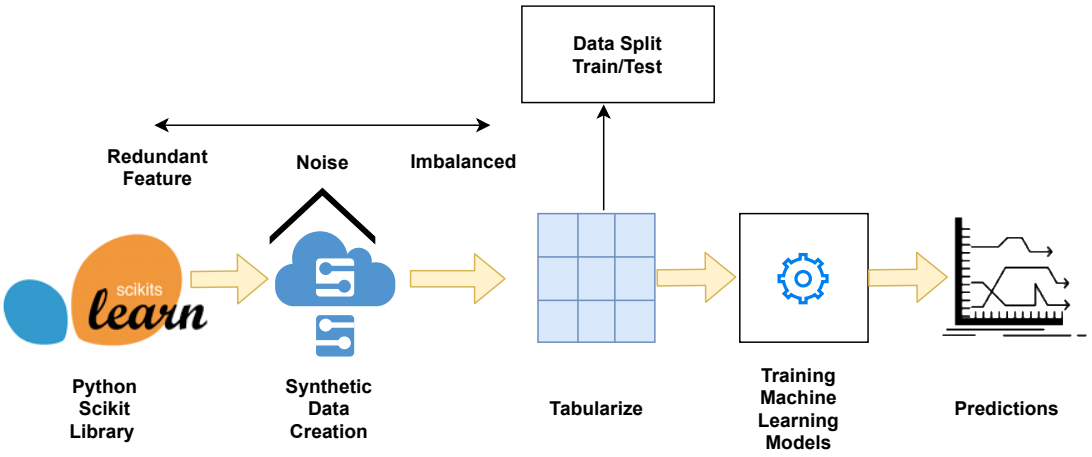
- Simulated data: We showed how we can take ad- vantage of generating simple simulated data creating different scenarios for malicious node detection.
- Evaluation: We applied off-the-shelf ML algorithms in the simulated datasets and evaluated the accuracy of those algorithms in those scenarios.

The rest of the paper is organized as standard: related work, method description, and experimental analysis, discussion and conclusion.

2. RELATED WORK

Trust is based on the evaluation of quantifying decision-making process [10]. For a sensor network, trust assessment based on malicious node detection can support to ensure the security of the network [32]. Similarly, in a social network, trust evaluation helps users build social relationships, reduce the risk of social activities and improve the quality of social networking [19][28]. Trust evaluation is also used to ensure secure interactions between automated agents and to promote the success of automation in a multi-agent system [26][15]. In Peer-to-Peer (P2P) networking, trust evaluation helps to identify interactive objects, ensuring resource sharing with friendly peers, and identifying malicious peers [14]. The majority of these trust algorithms determine trust by aggregating trust factors through weighting and other relevant calculations. Thus, to calculate such weight is not trivial and is hard to ensure evaluation accuracy. Therefore, many researchers in this field suggested using the ML approach for trust [29].

The problem of the identification of malicious nodes is regarded as a complex problem. It requires an in-depth analysis of nodes behaviors, and this motivates to use of ML-based models [1]. The study by Moore and Zuev [17] used the Na¨ıve Bayes estimator to classify internet traffic into security monitoring applications. They defined trust as how much the classification algorithms can be trusted based on their ac- curacy in unseen data. In this case, trust towards a dependable ML tool can be initiated as the accuracy with which the decision-maker follows the model's prediction [20][25]. One of the aspects of trust- worthy ML is based on the idea of maintaining high levels of performance and accuracy [27]. Every ML application requires a certain measure of overall trust in the model. It is assumed that the greater the accuracy values or the performance of the model, the higher the credibility of the ML models. The user forms a trust in ML algorithms based on the repeated interaction and accuracy of predictions produced by the machine learning models [13]. The study by [30] showed that how model accuracy can affect user trust. Similarly, findings from [31] demonstrated that the accuracy of the model did have a significant effect on the extent to which people trust the model.



To train the ML models for malicious node identification, a dataset of samples of intrusion signs that would reflect the abnormal behavior in the network under different scenarios is required. Thus, to create such real datasets is expensive, complicated, and time-consuming. The study by Belanko [5] showed the usefulness of synthetic data generation for intrusion detection in VANET (vehicular ad-hoc network). Many cybersecurity problems for malicious node detection are studied in simulated datasets [18][16]. IoT data is considered as noisy, heterogeneous, incomplete, high-dimensional, and nonlinear [9]. Thus, simulating such data and detecting threats using off-the-shelf ML algorithms is the main objective of this work. To the best of our knowledge, there is no such approach to demonstrate which ML algorithms work better in which scenario and which model is helpful to the user for identifying malicious nodes.

3. METHODS

This section presents the synthetic data preparation and ML models and evaluation criteria that we used in the study.

3.1. Datasets

Three different synthetic datasets are created using the Python Scikit-learn library[2] . Scikitlearn (sklearn) is an open-source machine learning library built on top of the Python programming language. This library contains a lot of efficient tools for machine learning and statistical modelling. The properties of the created datasets are shown in Table 1.

3.2. Evaluation Criteria

We evaluated the ML algorithms using 5-fold cross-validation. It is because cross-validation helps us to estimate the skill of a machine learning model on unseen data in different folds. For every fold, we receive the performance metrics of the ML algorithms, which enable us to draw important conclusions about the model.

3.3. Evaluation Metric

We have used the Area Under Precision-Recall Curve (AUPR) as the evaluation metric. One of the reasons for this is that we would like to know the skill of ML algorithms to predict positive

[2]https://scikit-learn.org/stable/

Table 1: Synthetic Datasets. ✓: Presence, ×: Absence, N: Number of data points

Question Addressed	N	Features	Label Percentage	Redundant Features	Noise
Q1	1000	10	50% malicious, 50% Non-Malicious	✓	×
Q2	1000	10	50% malicious, 50% Non-Malicious	×	✓
Q3	1000	10	1% malicious, 99% Non-Malicious 5% malicious, 95% Non-Malicious 10% malicious,90% Non-Malicious 20% malicious, 80 Non-Malicious	××	

class, which in our context is the identification of malicious nodes. On the other hand, AUPR provides an accurate prediction of future classification performance since they evaluate the fraction of true positives among positive predictions [24] and is considered robust performance metrics for imbalanced datasets. • Machine Learning Classification Models. We applied a set of six off-the-shelf classification models: Logistic Regression, Decision Tree Classifier, Support Vector Classification (SVC), Gradient Boosting Classifier, Multilayer perceptron (MLP) Classifier, Random Forests Classifier. In the next, we provide a short explanation of each of these models:

⋆ **Logistic Regression** is an appealing classification model because it is fast and straightforward to execute. The model is very applicable for linear data; however, it is not highly accurate for predicting complex non-linear data.
⋆ **Decision Tree Classifier** organizes rules in a tree to classify data. The rules produced by the decision tree are very intuitive and easy to understand. However, if a tree is designed to perfectly fit all training data set, it can easily be over-fitted and leads to a poor generalization in the test.
⋆ **SVC's** main advantage is that it can account for complex, non-linear relationships between features and survival. SVC finds a line that acts as a boundary to separate the data. This makes SVC extremely adaptable and applicable to a wide range of data.
⋆ **Gradient Boosting Classifier** is similar to a Random Forests Classifier because it depends on numerous base learners to produce an overall prediction, but varies in how those are aggregated. While a Random Forests Classifier fits a set of classification Trees separately and then averages their predictions, a Gradient Boosting Classifier is constructed back-to-back in a greedy stagewise manner.
⋆ **MLP classifiers** simulates a biological interconnected neuron. MLP is considered to have high accuracy and strong parallel distributed processing ability. The model works with a large number of parameters and provides quality prediction performance; however, the output results are difficult to explain and are termed, black-box models.
⋆ **Random Forests Classifier** is an ensemble of tree-based learners. It ensures that individual trees are de-correlated by 1) constructing each classification tree on a different bootstrap sample of the initial training data and 2) at each node, only estimate the split criterion for a randomly selected subset of features and thresholds. Predictions are formed by aggregating predictions of individual trees in the ensemble. • Model training pipeline. We trained the above-described ML models on the synthetic data using the procedure demonstrated in Figure 2. The ML models are trained using five-fold cross-validation. The model parameters are identified using grid search in the training sets.

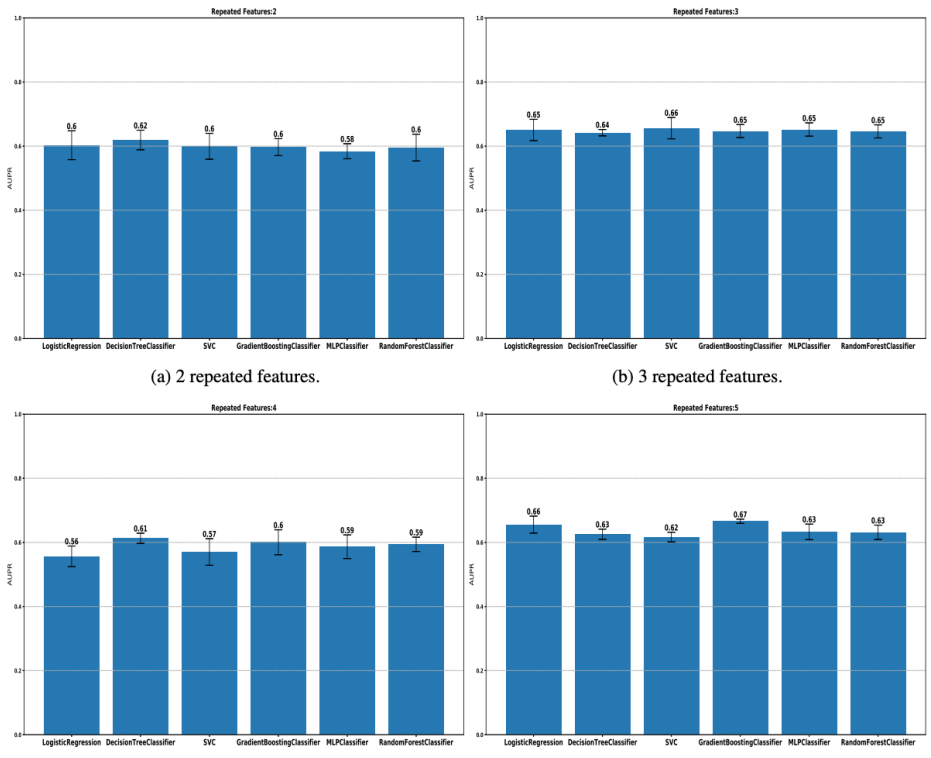
4. EXPERIMENTS

We investigated three questions. The questions are as follows:

- Q1-Redundant Features: Can we identify the malicious nodes in a setting where we have repeated features?
- Q2-Noise: How accurate are the ML models to predict malicious nodes in the noisy setting?
- Q3-Imbalanced: Are ML models still be able to learn and predict the malicious nodes in an imbalanced label distribution?

4.1. Q1- Redundant Features

IoT data can exhibit redundancy [21]. This behavior might impact degradation of the overall performance of the IoT sensor networks [12]. We varied the redundant features from 2,3,4, and 5 in our synthetic datasets. The performance of different algorithms in different redundant feature settings is shown in Figure 3. We ran all the ML algorithms in this setting. We found that in the highest number of repeated features, which is five, the Gradient Boosting classifier performed best compared to other algorithms. Similarly, the Gradient Boosting classifier has competitive performance with its competitors Decision Tree, Random Forest, and MLP Classifier for four repeated features. For two and three repeated features, we can see from the bar-plot (Figure 3) that all the algorithms have similar performance. It implies that in the setting where there are many repeated features, score. ensemble-based models like Gradient Boosting Classifier or Random Forest Classifier would be applicable.



(a) 2 repeated features. (b) 3 repeated features.

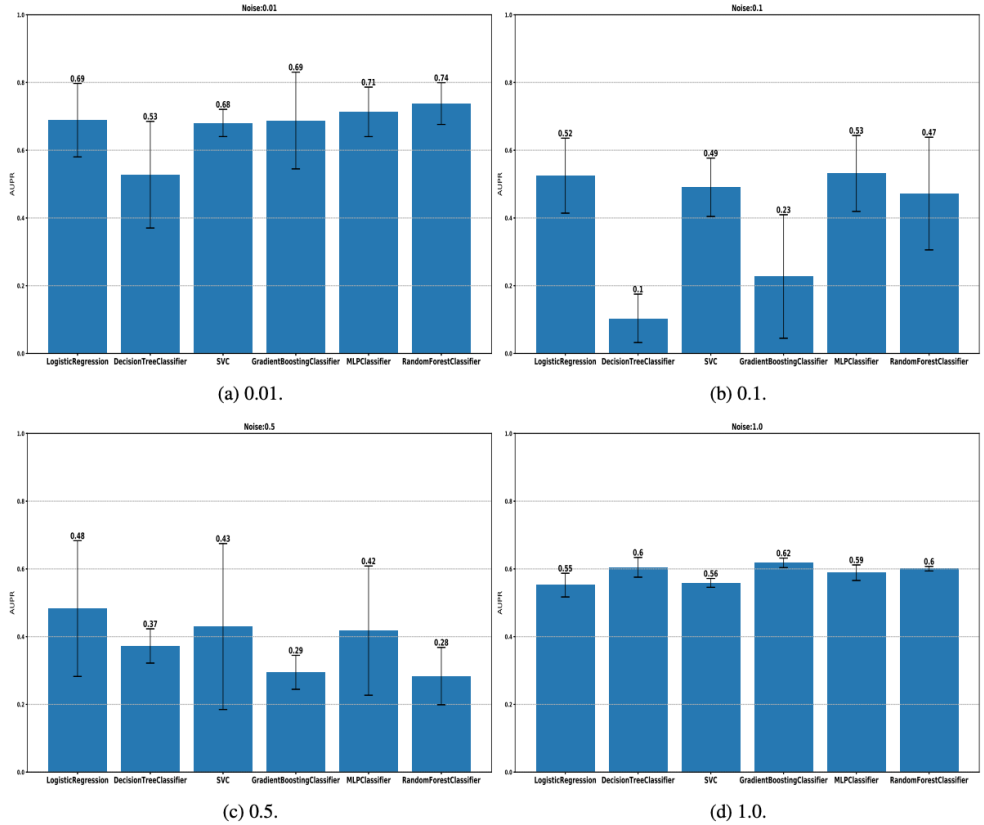
(c) 4 repeated features. (d) 5 repeated features.

Figure 3: The bar chart shows the Mean AUC-PR score of 5-Fold cross validation to predict malicious nodes. The error bar is the standard deviation obtained from the 5-Fold cross validation of AUC-PR score.

4.2. Q2- Noise

In IoT devices, it might suffer from irregularities in the correct readings of the sensor data, which might make them vulnerable for attack. Often data collected by IoT devices are noisy and corrupted [20]. To simulate that situation, we created synthetic datasets with different noise proportions from 0.01 to 1.0. 0.01 is a tiny noise distribution in the data, whereas 1.0 is high

noise in the data. We trained the ML models in this setting, and the result is presented in Figure 4. We observe that as the noise increases, the AUPR score of the model decreases. From Figure 4(b), we can see there is a huge drop in AUPR score when the noise is increased from 0.01 to 0.1. One of the reasons for that might be adding noise may under-fit the data, and a valuable signal is lost, so the ML model has performance degradation. However, in Figure 4(d), there is quite improved performance of the ML models with noise 1.0. For noise at 1.0, there is a positive influence in ML models that worked as regularizes to reduce over-fitting and has improved performance.



(a) 0.01. (b) 0.1.

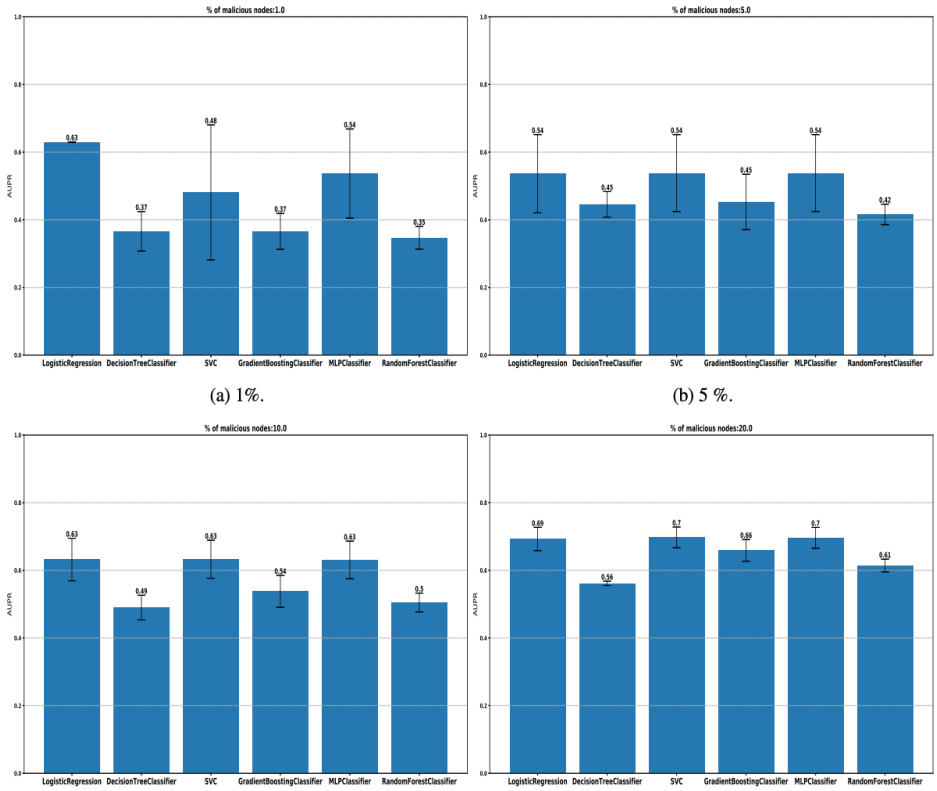
(c) 0.5. (d) 1.0.

Figure 4: The bar chart shows the Mean AUC-PR score of 5 Fold cross validation to predict malicious nodes. The error bar is the standard deviation obtained from the 5 Fold cross validation of AUC-PR score.

Q3- Imbalanced Data

When the attack happens, there is a chance that there are few malicious nodes and large non-malicious nodes at first. In such an event identifying the malicious node in advance will save the huge loss. Thus, we created a synthetic dataset with 1%, 5%, 10%, and 20% malicious nodes for this setting and applied the ML models. The result is shown in Figure 5.

For 1% malicious node, we observed that Logistic Regression had performed better than other models. It is because logistic regression performs better when the dataset is linearly separable and less prone to overfitting. However, when more malicious nodes are introduced, other models start to perform better. For example, in the case of 20% malicious nodes, SVC and MLP classifiers outperform all the other methods. Similarly, in 5% and 10%, Logistic regression, MLP, and SVC have similar performances.



(a) 1%. (b) 5 %.

(c) 10%. (d) 20%.

Figure 5: The bar chart shows the Mean AUC-PR score of 5-Fold cross validation to predict malicious nodes. The error bar is the standard deviation obtained from the 5-Fold cross validation of AUC-PR score.

5. DISCUSSION

From the experiment, we came up with the following summary shown in Table 2. We have demonstrated the summary for extreme cases, namely the maximum redundant features, noise, and imbalanced dataset with only 1% labeled malicious and 99% Non-malicious due to space limitation. We can see at the Gradient Boosting Classifier performs the best for a high repeated number of features and maximum noise. Gradient Boosting trains many models in a gradual, additive, and sequential manner to enhance the predictive performance and has better performance than others. Similarly, we observe that the Logistic Regression performed the best in predicting few malicious nodes and large non-malicious ones. If there is a linear association between features and the outcome variable, then logistic regression is able to capture that information and gives better performance in comparison to other methods. We tested off-the-shelf ML classification algorithms for our synthetic data to identify the best performing algorithm. However, picking up a suitable algorithm is always not enough. We must also choose the correct configuration of the algorithm for a dataset by tuning the parameters to get high predictions. These high predictions are evaluated by metric.

An ML algorithm's performance metric can represent effectiveness. For many years, machine learning researchers measured the trustworthiness of the models through evaluation metrics. The evaluation metric like AUPR which we used in our studies describe the number of correct predictions made by the model. It answers an important question: if a model is making a random guess or has learned to classify the data correctly. The higher the AUPR score, the better is the prediction and the more trust we can do in the machine learning algorithms. However,

transparency, explainability, computational complexity are also the primary step for enhancing trust in an ML system for malicious node detection and choosing suitable ML algorithms. We have not explored this scope, which is the limitation of this work, but we would like to explore this further in our future work.

The subjectivity is a basic characteristic of trust. In this work, we have not looked into the subjective aspect of the user for the trust in algorithms for predicting malicious nodes. The user studies in the trust is an important issue. As this is the initial stage of our work, we consider user studies part of our further research.

Table 2. Qualitative comparison of the performance of the ML classification models in a synthetic data.✓: higher performance, ×: poor performance

	Machine Learning Classification Models					
	Logistic Regression	Decision Tree Classifier	SVC	Gradient Boosting Classifier	MLP Classifier	Random Forest Classifier
Scenarios						
Maximum Redundant Features (5)	×	×	×	✓	×	×
Maximum Noise (1.0)	×	×	×	✓	×	×
Imbalance Dataset (1% Malicious, 99% Non Malicious)	✓	×	×	×	×	×

6. CONCLUSIONS

We presented the malicious node classification using off-the-shelf ML algorithms in a synthetic dataset. We showed the ability of ML algorithms in the scenarios mimicking for IoT devices: (a) redundant features, (b) noisy, and (c)imbalanced datasets and reported the AUPR score of the algorithms. Our work explores looking at the synthetic data and applying ML models to see which one performed the best in what setting.

We believe the evaluation metric provides the first step towards trusting the ML for developing malicious node detection. However, this idea will give a simple, cheap, and effective way to generate the data and perform ML experiments for secure systems.

ACKNOWLEDGEMENTS

We would like to acknowledge Science Foundation Ireland (SFI/12/RC/2289_P2) for funding this research.

REFERENCES

[1] Abdelghani, W., Zayani, C. A., Amous, I., and Se`des, F. (2018). Trust evaluation model for attack detection in social internet of things. In International Conference on Risks and Security of Internet and Systems, pages 48–64. Springer.

[2] Abdul-Ghani, H. A., Konstantas, D., and Mahyoub, M. (2018). A comprehensive iot attacks survey based on a building-blocked reference model. International Jour- nal of Advanced Computer Science and Applications, 9(3):355–373.

[3] Anand, P., Singh, Y., Selwal, A., Alazab, M., Tanwar, S., and Kumar, N. (2020). Iot vulnerability assess- ment for sustainable computing: threats, current solu- tions, and open challenges. IEEE Access, 8:168825– 168853.

[4] Arıs, A., Oktug, S. F., and Voigt, T. (2018). Security of internet of things for a reliable internet of services.

[5] Belenko, V., Krundyshev, V., and Kalinin, M. (2018). Syn- thetic datasets generation for intrusion detection in vanet. In Proceedings of the 11th international confer- ence on security of information and networks, pages 1–6.

[6] Cao, N., Nasir, S. B., Sen, S., and Raychowdhury, A. (2017). Self-optimizing iot wireless video sensor node with in-situ data analytics and context-driven energy- aware real-time adaptation. IEEE Transactions on Circuits and Systems I: Regular Papers, 64(9):2470– 2480.

[7] DaCosta, F. and Henderson, B. (2013). Rethinking the In- ternet of Things: a scalable approach to connecting everything. Springer Nature.

[8] Deogirikar, J. and Vidhate, A. (2017). Security attacks in iot: A survey. In 2017 International Conference on I- SMAC (IoT in Social, Mobile, Analytics and Cloud)(I- SMAC), pages 32–37. IEEE.

[9] El-Zeheiry, H., Elmogy, M., Elaraby, N., and Barakat, S.(2018). Fuzzy c-mean and density-based spatial clus- tering for internet of things data processing. In Med- ical Big Data and Internet of Medical Things, pages 161–187. CRC Press.

[10] Jiang, W., Wu, J., Li, F., Wang, G., and Zheng, H. (2016). Trust evaluation in online social networks using gen- eralized network flow. IEEE Transactions on Comput- ers, 65(3):952–963.

[11] Kang, M.-J. and Kang, J.-W. (2016). Intrusion detection system using deep neural network for in-vehicle net- work security. PloS one, 11(6):e0155781.

[12] Krishnamurthi, R., Kumar, A., Gopinathan, D., Nayyar, A., and Qureshi, B. (2020). An overview of iot sensor data processing, fusion, and analysis techniques. Sensors, 20(21):6076.

[13] Lee, E. (2021). How do we build trust in machine learning models? Available at SSRN 3822437.

[14] Li, X., Zhou, F., and Yang, X. (2011). A multi-dimensional trust evaluation model for large-scale p2p comput- ing. Journal of Parallel and Distributed Computing, 71(6):837–847.

[15] Mahbooba, B., Timilsina, M., Sahal, R., and Serrano, M. (2021). Explainable artificial intelligence (xai) to en- hance trust management in intrusion detection sys- tems using decision tree model. Complexity, 2021.

[16] Milenkovic, M. (2020). Internet of Things: Concepts and System Design. Springer.

[17] Moore, A. W. and Zuev, D. (2005). Internet traffic classi- fication using bayesian analysis techniques. In Pro- ceedings of the 2005 ACM SIGMETRICS interna- tional conference on Measurement and modeling of computer systems, pages 50–60.

[18] Navarro-Lara, J., Deruyver, A., and Parrend, P. (2016). Morwilog: an aco-based system for outlining multi- step attacks. In 2016 IEEE Symposium Series on Com- putational Intelligence (SSCI), pages 1–8.

[19] Niu, D., Rui, L., Huang, H., and Qiu, X. (2017). A service recovery method based on trust evaluation in mobile social network. Multimedia Tools and Applications, 76(3):3255–3277.

[20] Poursabzi-Sangdeh, F., Goldstein, D. G., Hofman, J. M., Wortman Vaughan, J. W., and Wallach, H. (2021). Manipulating and measuring model interpretability. In Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, pages 1–52.

[21] Qin, Y., Sheng, Q. Z., Falkner, N. J., Dustdar, S., Wang, H., and Vasilakos, A. V. (2016). When things matter: A survey on data-centric internet of things. Journal of Network and Computer Applications, 64:137–153.

[22] Rajendran, G., Nivash, R. R., Parthy, P. P.,and Balamurugan, S. (2019). Modern security threats in the internet of things (iot): Attacks and countermeasures. In 2019 International Carnahan Conference on Security Technology (ICCST), pages 1–6. IEEE.

[23] Razafimandimby, C., Loscri, V., Vegni, A. M., and Neri, A. (2017). A bayesian and smart gateway based communication for noisy iot scenario. In 2017 International Conference on Computing, Networking and Communications (ICNC), pages 481–485. IEEE.

[24] Saito, T. and Rehmsmeier, M. (2015). The precision-recall plot is more informative than the roc plot when evaluating binary classifiers on imbalanced datasets. PloS one, 10(3):e0118432.

[25] Schmidt, P. and Biessmann, F. (2019). Quantifying interpretability and trust in machine learning systems. arXiv preprint arXiv:1901.08558.

[26] Schmidt, S., Steele, R., Dillon, T. S., and Chang, E. (2007). Fuzzy trust evaluation and credibility development in multi-agent systems. Applied Soft Computing, 7(2):492–505.

[27] Thiebes, S., Lins, S., and Sunyaev, A. (2020). Trustworthy artificial intelligence. Electronic Markets, pages 1–18.

[28] Timilsina, M., Davis, B., Taylor, M., and Hayes, C. (2017). Predicting citations from mainstream news, weblogs and discussion forums. In Proceedings of the International Conference on Web Intelligence, pages 237– 244.
[29] Wang, J., Jing, X., Yan, Z., Fu, Y., Pedrycz, W., and Yang, L. T. (2020). A survey on trust evaluation based on machine learning. ACM Computing Surveys (CSUR), 53(5):1–36.
[30] Yin, M., Vaughan, J. W., and Wallach, H. (2018). Does stated accuracy affect trust in machine learning algorithms. In Proceedings of ICML2018 Workshop on Human Interpretability in. Machine Learning (WHI 2018), volume 7.
[31] Yin, M., Wortman Vaughan, J., and Wallach, H. (2019). Understanding the effect of accuracy on trust in machine learning models. In Proceedings of the 2019 chi conference on human factors in computing systems, pages 1–12.
[32] Zhang, T., Yan, L., and Yang, Y. (2018). Trust evaluation method for clustered wireless sensor networks based on cloud model. Wireless Networks, 24(3):777–797.

AUTHORS

Basim Mahbooba
I am a Ph.D. student in the Unit of Internet of Thing and Network security of INSIGHT at the National University of Ireland, Galway. Before joining Insight, I was a researcher at Kufa University, Iraq.

Mohan Timilsina
Working as a postdoc in the Unit of Information Mining and Retrieval of INSIGHT at the National University of Ireland, Galway.

Martin Serrano
Dr. Martin Serrano (PhD. MSc. Eng. B.Eng) Data Scientist IoT-M2M Semantic Interoperability Expert National University of Ireland Galway (NUI Galway)