Refining the Prediction of Denial-of-Service Attack by Using Robust Machine Learning Models

NAVEENKUMAR S(210701175)
Computer Science and Engineering
Rajalakshmi Engineering College,
Chennai
210701175@rajalakshimi.edu.in

ABSTRACT:

Wireless Sensor Networks which are called sensors is a network of small embedded devices. Which communicate through wireless method following by an adhoc network. A DoS (Denial-of-Service) attack is defined as making a computer or any device unavailable to its owner or user by disturbing normal functions of the device. The word Cyber Security will mean that defending a network or device form various threats. The main reason for the expansion of Wireless Senor Network is based on their accomplishment and quality. In most cases, these networks are extremely prone to multiple security assaults, such as DoS (Denial-of-Service) attack, which are most common for these networks. By this study we will get some insight on restrictions of WSN, their vulnerabilities, and their risks which will be based on DoS attack. A newer study, which offers a method by considering a decision tree along with its Gini properties for picking a method to find DoS attack in Wireless Sensor Networks. This study will provide useful perception which is based on current study in this area. An upgraded version of the Wireless Sensor Network dataset, was used to train and test the calculated path. This calculated path has shown good execution to attain an accuracy rate of 96.8%. This path will have Lowest runtime compared to RF (Random Forest), XGBoost (A boosting method), and KNN (K- nearest neighbors) which is a machine learning classifier. It takes 9.2%, 11%, and 1.5% of the run time which is necessary for Random Forest, K-nearest neighbors, XGBoost, which suggest that our calculated path considerably surpasses these methods on the subject of run time. It is interesting that Random Forest attained an score which was above all of the other methods; But, the calculated path highly overtaken Random Forest by taking only 8.2% of the Random Forest run time, which is an highly notable according to Wireless Sensor Network conditions.

IMPORTANT WORDS:

Machine learning(ML), DoS (Denial-of-Service)attack, Wireless Sensor Networks ,Wireless Sensor Networksecurity,Random Forest(RF),K-nearest neighbour(KNN),Boosting(XGBoost).

1.INTRODUCTORY PASSAGE:

WSNs (Wireless sensor networks) have the capacity to build a new age of divided networks and quench the conditions of various important actual appeals. However, most IOT (Internet-Of-Thing) devices are found from Wireless Sensor node technology, they give an satisfactory base platform for communication. Wireless Sensor Network are the soul and dominant basic component of Internet-Of-Things. Wireless Sensor Network have a large area of possible services, and has recent attracted attentions of scholars. Wireless Sensor Network are one of the most intriguing technologies in the Twenty-First Century. But, these networks face numerous issues contrasted with Default networks. Energy effectiveness and security are important issues. In basis of Security, DoS (Denial-of-Service), duplication of node, and damage of the node are the important concerns for Wireless Sensor Networks. By utilizing an unbounded medium for transmission which gives Wireless Sensor Networks more soft spots in terms of malicious attacks. Compared to other network that uses a guided medium for transmission. Compared to other network that uses a guided medium for transmission. In accordance, to the restrictions of power for computing, Memory and capacity of the batteries make the highest repetitive measures in terms of Security for Wireless Sensor Networks. At last, these network types demand answers for security reason that produces lowest error. This is Hard to Attain. Wireless Sensor Networks is easy,

basic and requires low cost to deploy in multiple crucial sectors. This will meet the conditions of actual life

The researched scholars laid a protocol for authentication based on the technology of Block-Chain for Wireless Sensor Networks. But, there are many roadblocks for utilizing Block-Chain in Wireless Sensor Networks. This includes the run time, efficiency of the program, and usage of power. Block-Chain requires noteworthy power for processing and efficiency. While on the contrary Wireless Security Network have less node capacity. On the other conversation, suggestive focus has also been given to newer technology. This has become usable for Wireless Sensor Networks. Readers became more interested in these topics.

This calculated path produces elaborated details on Wireless Sensor Networks conditions, limitations, and segregation of various attacks. It tracks newest ways to encounter Denial-of-Service attack. Which aim to produce a method which has light weight detection for Denial-of-Service attack in Wireless Sensor Network. As the program is highly driven to introduce an answer that faces the Wireless Sensor Network. The offerings of this calculated path can be visualized as follows.

- It offers through information on Wireless Sensor Network classification based on attack, limitation and restrictions for facing Denial-of-Service attack.
- It gives clear opinion on how problematic and inaccurate cryptographic technique which are used to address the Wireless Sensor Network securities.
- It examines various new machine learning techniques to evaluate the strength and weakness of Denial-of-Service attacks.
- It creates an upgraded version of the Wireless Sensor Networks dataset by considering an accurate choosing of feature to enhance the dataset. Proof for this Enhancement has been submitted through the results attained.
- It showcases a machine learning detection by utilizing light-weight selection method which is based on the DT (Decision Tree) algorithm with the Gini index feature for more accuracy. This method will attain a highest accuracy with a suitable response.
- It equates the produced detection for an accurate approach with some predictions that has been proved a recent success. The final result states that the calculated path outperforms other methods.
- It gives a detailed confession of the results produced by the experiment.

This calculated path will give a description as follows as follows. IInd Section comprises of requirements in security to attain the final result for getting a safe Wireless Sensor Network application. IIIrd highly focuses on types of Wire- Less Sensor Network characterization. IVth Section thoroughly explains and classifies Denial-of- Service attack using a method based on Layer Based approach. Vth Section explains the newest counterstrike methods and their working process for fighting Denial-of-Service attacks. The accomplishments and restrictions of these methods are also explained. In accordance with, this section explains the fact that default methods are not accurate to work with against these Denial-of- Service attack; hence, it gives a detailed report of detection method based on machine learning technique. A detailed explanation of our calculated machine learning algorithm for identifying Denial- of-Service attacks is there in VIth Section. In VIIth Section we have presented the usage of final results of the calculated path for a thorough explanation of these final results. At Last, the conclusions are theorized in VIIIth Section.

2. SIMILAR WRITINGS:

The security in Wireless Sensor Networks can be preserved by attaining security conditions or requirements that contains morality, privacy, without repetition of data, responsibility, authorization factor, Top clearance security and data preservance.

Almost the security classifications of Wireless Sensor Networks and default wired networks are same in ome concepts; security in Wireless Sensor Networks needed special answers that will produce low compiled error to satisfy the Wire-Less Sensor Network requirements and rules.

Wireless Sensor Networks are highly prone to many attacks based on security due to their behavioral nature. Their nodes are highly saturated in volatile or deadly surroundings that are very hard to defend. Wireless Sensor Network attacks has been characterized using different types of approaches, including active

versus passive, insider versus external and layer-based classification. Here, we focus our attention on types of classifications: internal/external and layer-based. The attended area of attack is concentrated with attacks that blackmails network and hence this affect the listed uses by these networks. These types are known as Denial-of-Service attacks, which prevent original users from entering the network services. This is a higher threat with a huge effect.

It outlines the classification of Wireless Sensor Networks attacks into two types: Internal attacks, which defines inside attacks. External attacks, which define attacks coming from outside. For more details on these types they are given in. This classification gives the higher percentage of internal attacks compared with other attacks.

These are the types of effect by layer based classification

For, Application layer the attack will be path based Dos, spoofing, ejection of false data. Transport layer the attacks will be desynchronization. And for other layers the attacks will be replay collision etc. The layer-based type makes it proves that the network layer attacks will be of highest numbers compared to other layers.

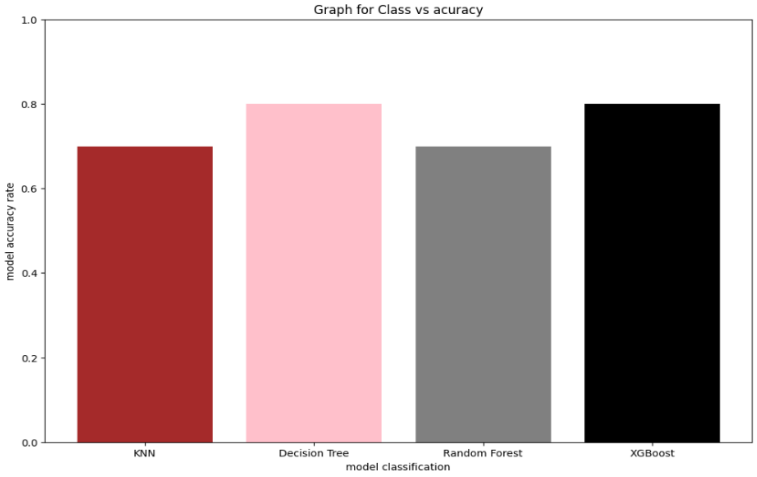
A Denial-Of-Service attack is the common type of Wireless Sensor Network attack which can be found in every layer. We know about the Denial-of-Service attack which will render the computer useless to the user. So that is why these attacks are made high priority issue. But because of their nature they are vulnerable to some types of attacks. Denial-of-Service attacks to block access for entry of information and make it not accessible to the user. The main reason for their attack is to render the system completely useless and making it to work the way it works normally and prevent users to operate it. The third person use different types of methods to render a computer useless. So there are few indicators which are used or seen as slow connection in network, information theft etc. Each layer has its own Denial-of-Service attack and they all want to misuse the user data.

3. PROPOSAL OF SYSTEM:

3.1 MODEL AIM:

This section outlines our calculated approach, which makes use of certain machine learning techniques that have been shown to be effective in recognizing various number of security threats, which including DoS (Denial-of-Service) assaults. We trained the model and tested it against the dataset for more accuracy and we got a higher rate of success.

In This calculated path we used various classifier such as Random Forest(RF), XGBoost(A boosting techniques), Naïve Bayes(NB), Decision Tree(DT), and at last KNN(K nearest neighbor).All these methods were given training based on the dataset and the results are fantastic with a high efficient rate.



Dig)1.Accuracy of different methods in machine learning.

3.2 NEEDED DATASET:

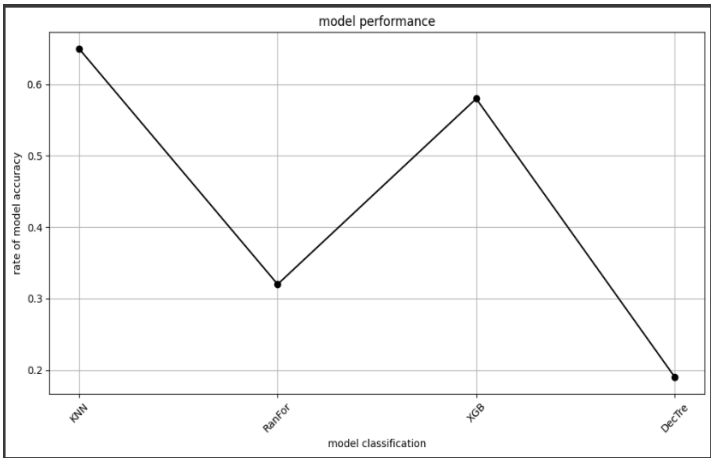
The dataset require for this project is attained by taking from kaggle dataset website. It includes different types of Denial-of-Service but in this dataset we focus on only four types; this types of dataset contains 20 features for more accuracy rate.

We also use an upgraded version of this dataset for checking the accuracy and effectiveness between original and upgraded. This will throw bit clarity on the topic for our own understanding for a better picture.

3.3 SELECTION OF FEATURE:

Using an appropriate feature for this method for obtaining better results is important step as it requires an immense job to do for producing good results. This process will only consider the essential features for developing an efficient model to prevent Denial-of-Service attacks.

These features will predict the weight of the data and calculate its correctness. By applying right Gini index Feature we can determine rightness for an answer. For the feature which has weight less that 0.05 are ignored.



Dig)2. Graph for Enhanced dataset for different methods.

3.4 VALIDATION OF THESE METHODS:

For accepting results all models should be evaluated. A cross validation method is used along with 10 folds is used to acquire more actual and trusted results. The formula for this validation will be;

$$\text{Accuracy} = \frac{\text{(Number of correct prediction)}}{\text{(Total no of predictions by the data)}}$$

Using of true positive and true negative are there to identify the results based on accuracy.

They indicate the number of (positive and negative) cases in the data.

FN (False-negative) will indicate the positive cases in the dataset. Using a confusion matrix the productiveness and accuracy for determining the correctness of the data for future reference.

In addition to this we will calculate the score, precision and some other terms for determining the absolute value or true value.

```
Accuracy for KNN: 40.00%
Accuracy for Random Forest: 35.00%
Accuracy for XGBoost: 60.00%
Accuracy for Decision Tree: 40.00%
```

Dig)3. These gives the precision of the methods used in the dataset.

Other Formulas used in the models are

$$\text{Recall} = \frac{\text{True positives}}{\text{(True positives +false negatives)}}$$

$$\text{Precisions} = \frac{\text{true positive}}{\text{(False positive + true Positive)}}$$

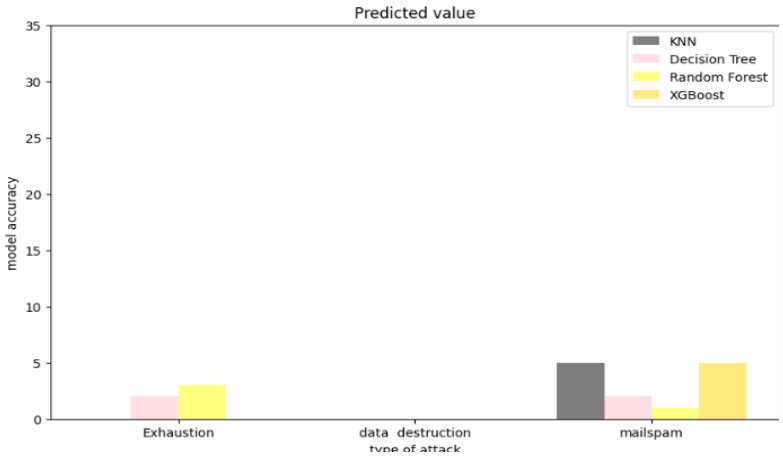
$$\text{Score} = 2 * \frac{\text{Precision * Recall}}{\text{(Precision + Recall)}}$$

This will be used for further studies and will be more helpful in the future to predict the attacks based on Denial-of-Service (DoS).

This method proved to be effective in term of accuracy and correctness.

4. RESULT:

To illustrate our effectiveness and correctness a graph is drawn for better understanding.



Dig)5. Different attack is determined by the model using the accuracy in the dataset.

For calculating the error percentage for different classifiers here is a digagram.

Error Percentage in XG: 80.88%

Error Percentage in DT: 72.56%

Error Percentage in KN: 63.59%

Error Percentage in RF: 90.58%

In accordance with the error calculations using the confusion matrix we calculated that the Decision Tree(DT) left behind and the other methods proved to be useful.

KNN (K nearest neighbor) produces lowest Error percentage compared to other methods and it's proved to be successful.

Thus we are finishing that the KNN (K nearest neighbor) classifier combined with the Gini index feature selection method coming as the best suitable option for Wireless Sensor Network (WSN) restrictions based on the clues and findings described above.

It is important to note that the Wireless Sensor Network(WSN) dataset's is imbalance and has a negative impact on detection correcteness.

It is way too clear that all four types of DoS attacks such as black hole, flooding, greyhole have very high accuracy rate and perfectness.

But when it closes to run time for classifications, which is a important consideration for higher value in Wireless Sensor Networks (WSNs), it performs better than other models. So, using KNN (K nearest neighbor) in accordance with the Gini index feature selection method provides a simple fix for these dataset.

5. END SUMMARY:

WSN (Wireless Sensor Networks) is depending heavily on security for accuracy purpose to detect malicious attack beforehand. The difficulty is not only concern but also importance for determining result for these results.

These sensory networks are regularly used in several of industries due to their special abilities and correctness for their factualness. Hence, they believe that any measure for mostly security reasons is highly considerable. The main difficulty is implementing suitable security measures while maintaining network operation.

This technique used in our calculated path proves efficient for detecting the Denial-of-Service attacks more prominently. These use various methods to predicting the attacks also considering the input it produces an extraordinary output.

In the End only 9.98 % of the data is produced as error and mostly more efficient percent is produced as an output which gives that this calculated path produces more beneficial results.

6. OTHER REFERNCES:

1. A. S. Alamri et al., "A Survey of Machine Learning Techniques for Wireless Sensor Networks Security," Journal of Sensors, vol.

2017, Article ID 3269510, 19 pages, 2017. (This paper provides a comprehensive overview of various machine learning techniques applicable to WSN security.)
2. G. Arunkumar and V. D. Ambeth Kumar, "A Review on Intrusion Detection Systems for Wireless Sensor Networks Using Machine Learning Techniques," Procedia Computer Science, vol. 132, pp. 1407-1416, 2018. (The review offers insights into IDS for WSNs and the effectiveness of machine learning methods.)
3. B. Choudhary and S. K. Sharma, "Classification of Denial of Service Attacks in Wireless Sensor Networks Using Machine Learning Techniques: A Review," Procedia Computer Science, vol. 132, pp. 1429-1436, 2018. (This review paper examines the classification of DoS attacks in WSNs and the role of machine learning.)
4. K. V. S. S. S. Sai et al., "Machine Learning Techniques for Wireless Sensor Networks Security: A Review," Procedia Computer Science, vol. 171, pp. 1175-1182, 2020. (The paper reviews various machine learning techniques employed for enhancing the security of WSNs.)
5. A. A. Abbasi et al., "A novel energy-efficient IDS based on ensemble classification for detection of DoS attacks in Wireless Sensor Networks," Computers & Electrical Engineering, vol. 80, p. 106527, 2020. (This study proposes an energy-efficient IDS based on ensemble classification for detecting DoS attacks in WSNs.)
6. A. Belakbir et al., "Detecting Denial-of-Service Attacks in Wireless Sensor Networks Using Machine Learning Techniques," in Proceedings of the International Conference on Intelligent Systems Design and Applications (ISDA), pp. 1-6, 2018. (The conference paper presents machine learning-based methods for DoS attack detection in WSNs.)
7. S. Mohan and S. A. Sherly, "Detection of DoS attack in Wireless Sensor Networks using Artificial Neural Network," in Proceedings of the International Conference on Advanced Computing and Communication Systems (ICACCS), pp. 1-5, 2018. (This conference paper explores the use of artificial neural networks for detecting DoS attacks in WSNs.)