Hybrid Intrusion Detection

Athava Bhanu Naga Pavan, Kalyan Reddy Atmakur, Gangireddy Nagarjunareddy, Muppuri Lakshmi Narayana, Chitturi Rakesh and Muskhan Kumari

March 31, 2024

HYBRID INTRUSION DETECTION

A Bhanu Naga Pavan*[1],A Kalyan Reddy*[2],G nagajuna Reddy*[3],M lakshmi Narayana*[4], CH Rakesh*[5],Muskhan Kumari*[6]

*[1,2,3,4,5.]Student, Department Of Computer Science And Engineering, PIET, Vadodara, Gujarat, India.

*[6,]Professor, Department Of Computer Science And Engineering, PIET, Vadodara, Gujarat, India.

Abstract

With the increasing population of Industry 4.0, industrial big data (IBD) has become a hotly discussed topic in digital and intelligent industry field. The security problem existing in the signal processing on large scale of data stream is still a challenge issue in industrial internet of things, especially when dealing with the high-dimensional DDoS attack detection for intelligent industrial application. DDoS attcak detection has been widely used to ensure network security, but classical detection means are usually signature-based or explicit-behavior-based and fail to detect unknown attacks intelligently, which are hard to satisfy the requirements of SD-IoT Networks.

In this process we propose a machine learning algorithm and to detect the DDoS attack from network. Firstly, we need apply the UNSW NB15 as input. Then find the target variable and split the data into training set and testing set Then it will applied into classification method. In this method the machine learning algorithm like Extra Tree classifier and Random Forest is applied to detect the DDoS attack. Finally predict the type of DoS attack and find the result based on accuracy, precision, recall, and f1-measure.

Keywords*:* *Intrusion Detection System, Finding of Vulnerabilities, Prevention of security breaches and threats ,Discovery of hidden performance opportunities*

1. INTRODUCTION.

General Introduction

The Internet of Things, or IoT, is seen as a rapidly growing paradigm in computing history. In recent years, IoT has made great strides in a number of technical areas. It has been brought together by the internet and hundreds of billions of devices from different systems (smart grid, smart automobiles, smart homes, smart health care, etc.). However, because IoT links the physical and digital realms, there have been a number of cyberattacks against IoT devices as a result of this convergence. IoT security has grown more challenging due to the global accessibility, heterogeneity, large scale, and constrained hardware resources of IoT systems. IoT technology has grown quickly as information technology has advanced and is now widely utilized in a variety of industries, including the military, agriculture, and industry. These days, a variety of devices are continuously integrated with the Internet of Things (IoT), either as IoT terminals or as one of the IoT branches, due to the IoT's widespread use and technological diversity. IoT, an open ecosystem built on the Internet, has a variety of complicated security threats in its gadgets since the outside world is always attacking and destroying them. As a result, improving the identification of security vulnerabilities in IoT is imperative. The most common security technologies currently in use include security gateways, firewalls, code signatures, encryption technologies, etc. However, each of these technologies is a passive *security defense strategy and is unable to perform active detection and response.IoT intrusion security detection determines whether an IoT is in a dangerous environment by analyzing attack activity and data properties.*

PROBLEM STATEMENT

Anomaly (DDoS) detection is the problem of finding patterns in data that differ from expected behavior. These non-conforming patterns go by a variety of names in different application domains, including anomalies, outliers, discordant discoveries, exceptions, aberrations, surprises, oddities, and contaminants.

2. METHODOLOGY

Mobile ad hoc networks (MANETs) function on the core tenet that every participating node fully cooperates in self-organizing activities. However, maintaining a network calls for more resources and energy. Consequently, certain nodes in the network may decide not to cooperate with one another. Providing these egocentric nodes—also referred to as problematic nodes-with an incentive to cooperate has been a hot study area lately. In this work, we provide two systems that may be readily implemented on any source routing protocol: TWOACK and S-TWOACK. These systems are based on network-layer acknowledgmentIn an effort to fix the problem, the TWOACK scheme detects one of these problematic nodes and alerts the routing protocol to avoid it on ensuing routes.

The two methods are described in full in this article, together with the outcomes of our simulation-based evaluation. With a reasonable additional routing expenditure, we find that the TWOACK approach increases packet delivery ratio by 20 percent in a network where up to 40 percent of the nodes may be misbehaving.

3.RESULT AND CLASIFICATION

Result:

The Final Result will be produced using the entire projection as the foundation. The efficacy of this proposed method is evaluated using metrics like F1-measure Specificity, Precision, Accuracy, and Recall.

Clasification:

ETA The Extra Trees Classifier, sometimes called the Extremely Randomized Trees Classifier, is a type of ensemble learning technique that generates a classification result by aggregating the output of several de-correlated decision trees collected in a "forest." The only conceptual difference between it and a Random Forest Classifier is in the construction of the forest's decision trees. REF.
Random forests, also called random decision forests, are ensemble learning techniques that work by building a large number of decision trees during training and producing a class that represents the mean/average prediction (regression) or the mode of the classes (classification) of the individual trees. These techniques are useful for a variety of tasks, including classification and regression.

4.CONCLUSION

We present a DDoS detection prediction in this study. The DDoS assault is predicted by applying machine learning algorithms. First, pre-processing is conducted to the UNSW-NB15 dataset as an input. Clean the dataset using this procedure. The dataset was separated into training and testing datasets for the model selection technique. In order to forecast DDoS attacks, the classification algorithm is further processed. The outcome is produced in terms of accuracy, classification report, confusion matrix, and specificity.

Summary of Objectives:

Give a quick overview of the IDS project’s primary goals to start. This reminds the reader of the project’s objectives and gives them some perspective.

Key Findings:

Highlight the most important findings or results obtained during the project. This could include statistics on detection accuracy, false positives, false negatives, and any noteworthy incidents or patterns identified.

Contributions:

Explain the contributions of the project to the field of intrusion detection. What new knowledge, techniques, or insights have been generated as a result of the project?

Practical Implications:

Discuss how the findings and outcomes of the project can be applied in practice. What are the real-world implications for network security and intrusion detection?

Acknowledge the limitations of the project. Every project has constraints, such as time, resources, or specific conditions. Discuss how these limitations may have affected the results.

5.REFERENCES

1. G. Karatas, O. Demir, and O. K. Sahingoz, “Increasing the performance of machine learningbased IDSs on an imbalanced and up-to-date dataset,’‘ IEEE Access, vol. 8, pp. 3215032162, 2020.

2. T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, “BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset,” IEEE Access, vol. 8, pp. 2957529585, 2020.

3. H. Jiang, Z. He, G. Ye, and H. Zhang, “Network intrusion detection based on PSO-xgboost model,” IEEE Access, vol. 8, pp. 5839258401, 2020

4. A. Nagaraja, U. Boregowda, K. Khatatneh, R. Vangipuram, R. Nuvvusetty, and V. S. Kiran, “Similarity based feature transformation for network anomaly detection,” IEEE Access, vol. 8, pp. 3918439196, 2020.

5. L. D’hooge, T. Wauters, B. Volckaert, and F. De Turck, “Classication hardness for supervised learners on 20 years of intrusion detection data,’‘ IEEE Access, vol. 7, pp. 167455167469, 2022