**International Journal in Management and Social Science**
Volume 09 Issue 11, November 2021 ISSN: 2321-1784 Impact Factor: 7.088
Journal Homepage: http://ijmr.net.in, Email: irjmss@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal

# EVALUATING SIGNIFINCANCE AND VARIOUS TECHNIQUES USED FOR DDOS DETECTION

**J RAMESH**
Research Scholar, Radha Govind University, Ramgarh, Jharkhand

## ABSTRACT

*Intrusion detection system is an imperative role in increasing security and decreasing the harm of the computer security system and information system when using of network. It observes different events in a network or system to decide occurring an intrusion or not and it is used to make strategic decision, security purposes and analyzing directions. This paper describes host based intrusion detection system architecture for DDoS attack, which intelligently detects the intrusion periodically and dynamically by evaluating the intruder group respective to the present node with its neighbors. We analyze a dependable dataset named CICIDS 2017 that contains benign and DDoS attack network flows, which meets certifiable criteria and is openly accessible. It evaluates the performance of a complete arrangement of machine learning algorithms and network traffic features to indicate the best features for detecting the assured attack classes. Our goal is storing the address of destination IP that is utilized to detect an intruder by method of misuse detection.*

**Keywords: -** DDoS, Network, Functions, Security, Services.

## I. INTRODUCTION

## DDOS ATTACKS

The relevance of DDoS attacks are increasing day by day, where the targeted host or network is flooded with network packets until the authentic users are unable to access the network resources. It affects the availability of network services or devices by overwhelming networks through consuming a large amount of bandwidth. Inaccessibility of network devices, unavailability of services, and the performance degradation of resources cost the business both time and money. Since the role of network technology and rapid internet usage are so important in many major areas, DDoS assaults not only create enormous monetary losses, time loss, and server failures by blocking network resources, but they also harm reputation and lives of people.

Furthermore, DDoS attacks affected 83% of businesses in 2020, owing to the COVID-19 pandemic's considerable shift in internet usage. Multiple record-breaking incidents occurred in the year 2020, with DDoS attacks exceeding the threshold for a single month (929K) and a single year (>10 million). The COVID-19 pandemic was the apparent catalyst for this year's

extraordinary DDoS assault activity, according to research of Net scout's ATLAS Security Engineering & Response Team (ASERT) and the 16th annual Worldwide Infrastructure Security Report (WISR) survey. The survey reported that DDoS assaults were named the top concern in 2020 by 71% of service providers, and 75% of enterprises, wherein the five vertical targets for the DDoS attacks are financial services, government, education, cloud services, and e-commerce. This shows the significance in the demand for DDoS detection and mitigation services grows in tandem with the size, frequency, and complexity of DDoS attacks.

### Category of DDoS attacks

DDoS attack is one of the most widespread common attacks that is growing stronger, which blocks the legitimate users from accessing the network resources or services by overloading the network with an unwanted flood of requests. Thus, the network is parallelized due to the attacks on resource consumption and bandwidth consumption resulting in uniform degradation of resources or networks. It brings down the entire system or network and causes a serious availability problem. So, the DDoS attacks are categorized broadly as two, namely, bandwidth depletion attack and the resource depletion attack. The different variants of DDoS attacks result in zero-day attacks too.

### Significance of DDoS attack detection

The causes of difficulty in DDoS detection are as follows:

- Since DDoS attacks are difficult to identify using packet header identification, malicious packets can masquerade as normal packets.
- In a dynamic real-world network scenario, creating simple policies based on the packet headers is not enough for the identification of DDoS attacks. So, a proper detection mechanism needs to be addressed.
- Since DDoS attacks overwhelm and cripple the entire network, it has to be detected as fast as possible through an efficient IDS framework.

## II. TECHNOLOGIES USED FOR DDOS DETECTION

### Middle box technologies

Traditionally, the DDoS attack has been detected by using middle box technologies involving monitoring tools, NAT, Firewall, IDS, and load balancer. The detection performance of middle box services is superior but they are inflexible with network progression, as it is incompatible

with new protocols and network architecture. Furthermore, it is highly complex, vendor-specific, and hampers a holistic view of network status, which increases hurdles for fast DDoS detection.

**Overview of network virtualization**

The recent effort in the network evolution is to shift the pace of hardware to software. Network virtualization enables network architects to design, build, manage, and automate network services or functions efficiently and effortlessly. It decouples the infrastructure service from the physical appliances on which it functions.

Network functions are the software-implemented functional behaviour of network Infrastructure components such as routing, IPS, and IDS. It contributes to the development of an agile network with significant CAPEX and OPEX savings. As a result, recent efforts have been focused on providing middle box functions as network virtualized services [28]. But in a traditional network, the network functions are physical resources that are manually installed in the network that leads to operational rigidity and preventing the rapid development of new network functions.

## III. INTRUSION DETECTION SYSTEM

An IDS is a sensor or software application that monitors the vulnerability which exploits the integrity, confidentiality, and availability of the network. It monitors the entire activity of the network including policy violation and all malicious activities which are reported to the administrator or Security Information and Event Management (SIEM) system.

Threats from the outside network to the internal network are blocked by the firewall, whereas the IDS analyses the traffic patterns inside the network, detect network vulnerabilities, and alerts the administrator. IDS is the second line of defense in addition to firewall. Moreover, internal attacks are stronger and more hazardous than external attacks. Here comes the importance of an efficient IDS in the network.

**The characteristics used for the comparison of anomaly and signature based detection techniques are:**

**Alarm rate:**An ideal intrusion detection system detects 100% of attacks with 0% false alarms. In anomaly based IDS, the chances of false alarms are high since it identifies outliers from the normal behavior to trigger alerts. So, previously unknown, but legitimate, behavior can be accidentally flagged as well. In signature based IDS, the false alarm rate is low because of the threat identification based on existing attack signatures.

**Speed:**The data processing speed of signature based IDS is faster than anomaly detection, since it used preprogrammed list of known attacks to identify the attacks than allowing acceptable behavior of normal traffic by ML algorithms. The extensive monitoring of anomaly detection causes slow and exhaustion of resources.

**Flexibility:**The ability of the system to adjust to uncertainty in order to maintain system performance. Signature based IDS has limited flexibility due to the inability to detect new or previously unknown attacks.

**Reliability:**Reliability is the likelihood that a system will function successfully over a certain period. The known attack signature reduces the false alarm, which makes the signature based IDS more reliable. Even though, anomaly based IDS identifies new exploits, the false alarm rate is substantial. This causes exhaustion of resources and time to rule out the high volume of alerts generated.

**Scalability:**The ability of a system to manage increasing workloads by adding resources. Signature based IDS is only good as how up to date its database is at a given moment. The larger the database of attack signature, the higher the processing load for the system to analyze each connection and compare it to the attack signatures. The system's performance suffers as a result of insufficient scalability.

**Robustness:**The degree at which a system can function correctly during an exception occurs. Since attackers can get around signature based IDS by frequently changing small things about how the attack is carried out, the database cannot keep pace. So, the robustness of the signature based IDS is low since it unable to stand when a packet has no existing attack signature in the database. Since anomaly detection is based on pattern identification, it is effective at detecting malicious network activity. On other hand, IDS may have difficulty determining which traffic to flag if network is configured differently. As a result, robustness of anomaly based IDS rated as moderate.

**Attack detection:**Attack detection in signature based IDS depends on the preprogrammed list of known threats and their attack signatures, whereas anomaly IDS is designed to automatically understand attacks that are unknown and unpredictable for signatures using ML algorithms.

**Monitoring:**Rather than inspecting attack signature in the database of signature based IDS, anomaly based IDS requires significant effort in continuously monitoring the traffic patterns of a large volume of data.

## IDS CHARACTERISTICS AND CONFUSION MATRIX

The IDS characteristics used for determining the presence of the attacks are depicted in Table 1. It includes:

- True positive (TP): When IDS detects an actual attack.
- True Negative (TN): When IDS does not detect normal traffic as attack.
- False Positive (FP): When IDS falsely detect normal traffic as attack.
- False Negative (FN): When IDS falsely misses to detect an attack.

**Table 1. Characteristics of IDS**

| Types | Attacks | Alarms |
|---|---|---|
| TP | Y | Y |
| TN | N | N |
| FP | N | Y |
| FN | Y | N |

From the characteristics of the IDS, the FN (α-error) is the serious attack case where no attacks are detected when attacks are going on, which has to be eliminated.

## IV. CONCLUSION

A dependable "publicly available IDS evaluation datasets is one of the essential concerns of researchers and producers in this domain. In this paper," we have described the latest intrusion detection dataset and we presented the evaluation of its using common machine learning algorithms performance. The complexity of classification algorithms depends on the number of features and the number of training data samples. If the number of features increases, then the amounts of training data which are required are increasing.

## REFERENCES:-

1. Madni H., Javed M. and M.J. Arshad, "An Overview of Intrusion Detection System (IDS) along with its Commonly Used Techniques and Classifications", International Journal of Computer Science and Telecommunications Vol. 5, Issue 2, 2014.

2. AdrienBonguet and Martine Bellaiche (2017), A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing.

3. Santra A. K. and Christy C. J.," Genetic Algorithm and Confusion Matrix for Document Clustering ", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.

4. Tesfahun, A., and Bhaskari, D. L. (2013, November). Intrusion detection using random forests classifier with SMOTE and feature reduction. InCloud and Ubiquitous Computing and Emerging Technologies (CUBE), 2013 International Conference on (pp. 127 −132). IEEE

5. Jaina Patel J. and Mr. Panchal K., "Effective Intrusion Detection System using Data Mining Technique", Journal of Emerging Technologies andInnovative Research (JETIR) Vol. 2, Issue 6, 2015.

6. Y. Yu, L. Guo, Y. Liu, J. Zheng, and Y. Zong, “An efficient sdn-based ddos attack detection and rapid response platform in vehicular networks,” IEEE access, vol. 6, pp. 44570–44579, 2018.