Available Online at www.ijcsmc.com/journal

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 7.056

IJCSMC, Vol. 11, Issue. 6, June 2022, pg.78 – 86

Comparative Analysis of Several Anomaly Detection Algorithm with its Impact Towards the Security and its Performance

[1]Niranjan Singh Patel; [2]Dr. Tryambak Hiwarkar

[1]Ph.D Research Scholar; [2] Professor CSE

[1,2]School of Engineering and Technology

[1,2]Sardar Patel University Balaghat

DOI: https://doi.org/10.47760/ijcsmc.2022.v11i06.006

Abstract: Anomaly detection in network traffic is a promising and effective technique to enhance network security. In addition to traditional statistical analysis and rule-based detection techniques, machine learning models are introduced for intelligent detection of abnormal traffic data.
A Denial of Service (DoS) attack is a malicious effort to keep endorsed users of a website or web service from accessing it, or limiting their ability to do so. A Distributed Denial of Service (DDoS) attack is a type of DoS attack in which many computers are used to cripple a web page, website or web based service. Fault either in users' implementation of a network or in the standard specification of protocols has resulted in gaps that allow various kinds of network attack to be launched of the type of network attacks, denial-of-service flood attacks have reason the most severe impact. This analysis study on flood attacks and Flash Crowd their improvement, classifying such attacks as either high-rate flood or low-rate flood. Finally, the attacks are appraised against principle related to their characteristics, technique and collision. This paper discusses a statistical approach to analysis the distribution of network traffic to recognize the normal network traffic behavior. This paper also discusses a various method to recognize anomalies in network traffic.

Keywords: statistical-based, anomaly detection, DDos attack

I. Introduction:

Anomaly detection requires constant monitoring and analysis of selected network metrics. Anomaly detection system covers a scenario, when something unexpected is detected and the analysis evaluates this as an anomaly, it can be reported to the network administrator. There are two main categories of network monitoring that allow detecting anomalies:

Passive network monitoring

The computer network includes probes that receive data from the network and evaluate it. This data can be either intended directly for the probes (for example, events sent via the SNMP protocol) or it can be a copy of the production traffic, which occurs in the network whether the probe is connected or not.

Active network monitoring

Networks may also contain probes as in passive monitoring, but these probes generate additional traffic, which they send through the network. With the help of this traffic, it is possible to regularly determine the availability or general parameters of the tested services, network lines, and devices.

Differences between active and passive network monitoring in network anomaly detection

It may seem that active monitoring adds to the capabilities of passive monitoring, making it automatically the better option. Yet, the problem with active monitoring is that it generates additional data in the network. Therefore, in active monitoring, the monitoring devices become part of the production network (which brings with it, for example, security risks) and the monitoring is consequently not fully transparent. Another potential problem is that the monitoring data itself can affect the functionality of the network and thus be a source of problems and anomalies (for instance, it can increase the load on an already busy server). Given these disadvantages, this article focuses only on the passive monitoring of network anomalies.

In general, anomaly detection can be divided into several basic components; see Figure 1 (diagram on the right side). They have the following functionalities:

- **Parameterization** - The monitored data is separated from the input data in a form suitable for further processing.

- **Training** - When this mode is selected, the network model (trained status) is updated. This update can be done automatically as well as manually.

- **Detection** - The created (trained) model is then used for comparing data from the monitored network. If it meets certain criteria, an anomaly detection report is generated.

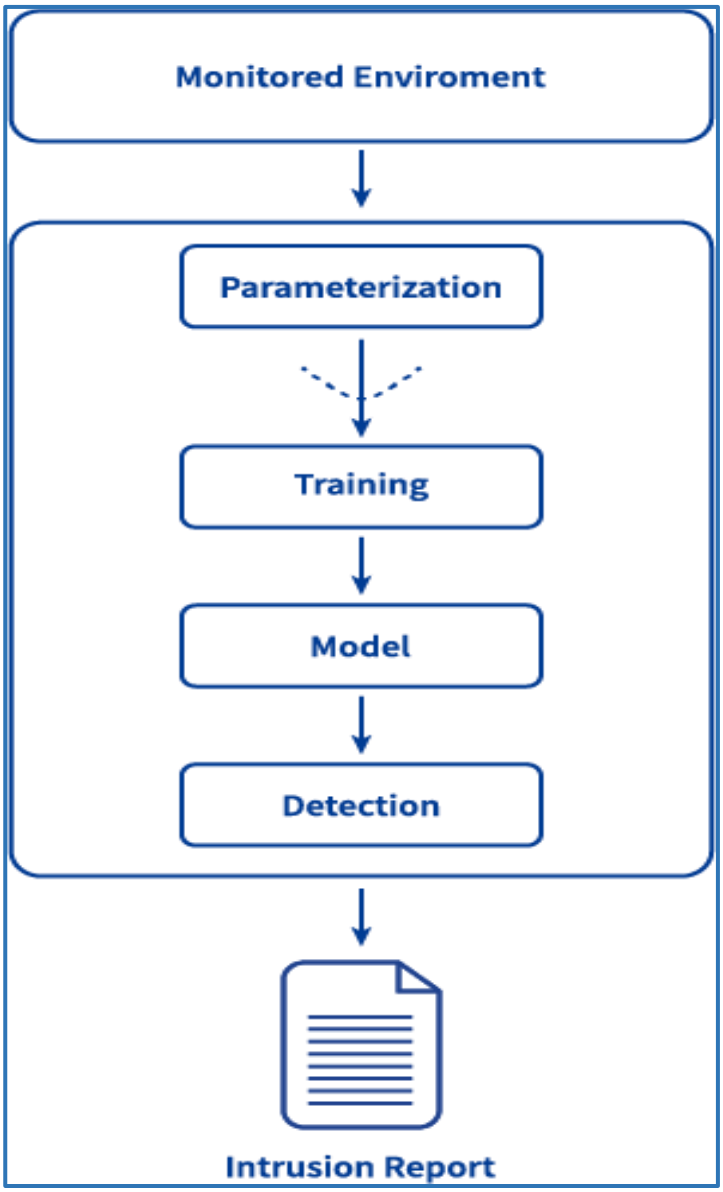

Fig: 1 Generalize anomaly Detection model

II. What is anomaly detection used for?

- **Ransomware detection** - detection is done via looking for a signature of the executable file
- **DDoS attack detection** - by comparing the amount of the current traffic with the expected amount, the attack can be detected

- **Botnet activity tracking** - with a list of known botnet command and control servers, it is possible to detect connections with those servers
- **Dictionary attack detection** - by counting the number of login tries and comparing the number with threshold values, it is possible to detect attempts to hack an account
- **Link failure detection** - this can be identified by detecting the increased amount of connections on the backup link
- **Incorrect application configuration detection** - this can be detected by an increased amount of error codes within application connections
- **Server overload detection** - by detecting a decrease in quality of experience, it is possible to detect overload services or servers
- **Suspicious device behavior detection** - by creating behavior profiles and checking if some device behaves outside of created profiles, it is possible to detect suspicious activity

III. Anomaly detection via methods:

Signatures or knowledge-based

A signature accurately describes what type of data the system looks for. An example of a signature can be searching for a packet that has the same source IP address as the destination IP address, or when searching for a specific content in the packet.

Baseline or statistical-based

A baseline describes an amount of data transferred that share certain common features. For example, it can be the number of detected TCP connections per every 5 minutes. An anomaly occurs when the current value (the number of queries over the last 5 minutes) digresses from the learned baseline in a significant way; see Figure 2. Another example is seeking a change in packet distribution according to the ports they are headed to. Figure 3 shows a case where an anomaly manifests itself as an increase in the amount of packets sent to one destination port.

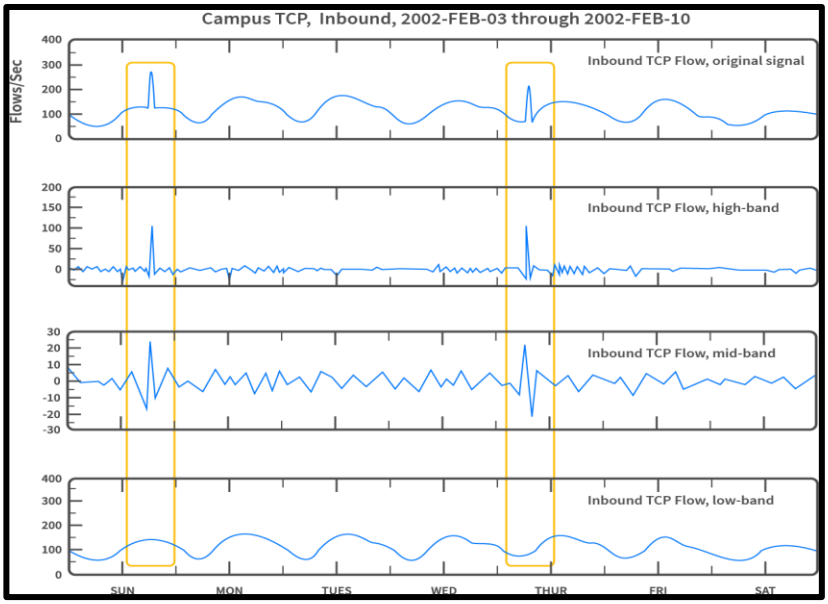

Figure 2: Anomaly detection according to a change in the amount of TCP connections detected [A Signal Analysis of Network Traffic Anomalies]

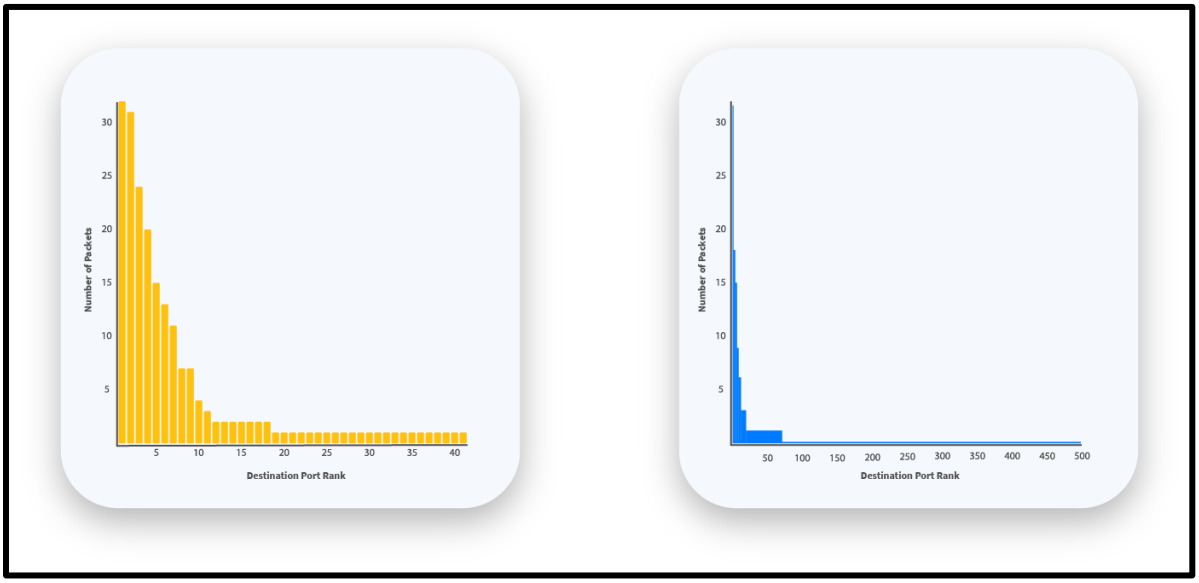

Figure 3: A change of the distribution of packets by destination port. When transferring large amounts of data to a single port, the resulting distribution changes significantly.

Differences between network anomaly detection using signatures and baselines

Attribute	Signature	Baseline
Ability to detect known errors or attacks	High - if the signature exists	Low - deviation from the baseline is not tied to a specific situation
Ability to detect unknown errors or attacks	Low - if no signature exists for the error or attack, it cannot be detected	High - deviation from the baseline is not tied to a specific situation
Difficulty of knowledge base maintenance	High - existing signatures require updates and new ones must be created	Low - the baseline can be recalculated automatically over time
Detection speed	Fast - the moment some data meets the detection criteria, the anomaly is found	Fast - the moment some data meets the detection criteria, the anomaly is found
Deployment speed	Fast - anomalies can be detected immediately after deployment	Slow - the baseline needs to be trained before it can start detecting
Number of false-positive detections	Smaller - if the signatures are well-defined, ordinary packets will not meet their criteria	Larger - any fluctuation can cause an anomaly

IV. Statistical Approach for Network Anomaly Detection:

In statistical-based approach include a normal network act and then all traffic that deviates from the normal is noticeable as anomalous. This method is used to study network traffic prototype on an exacting network. By examine network traffic and processing the information with complex statistical algorithms, this systems look for anomalies in the known normal network traffic patterns. All packets are given an anomaly score and if the anomaly score is higher than a certain threshold, the intrusion detection system will generate an alert.

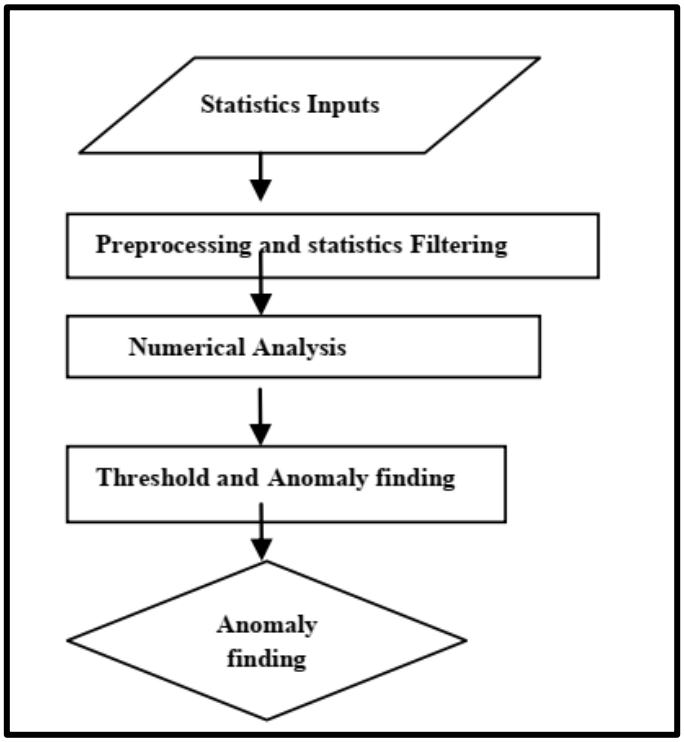

Fig.4 Statistical Approach for Network Anomaly finding

V. CATEGORIZATION of DDoS FLOOD ATTACK:

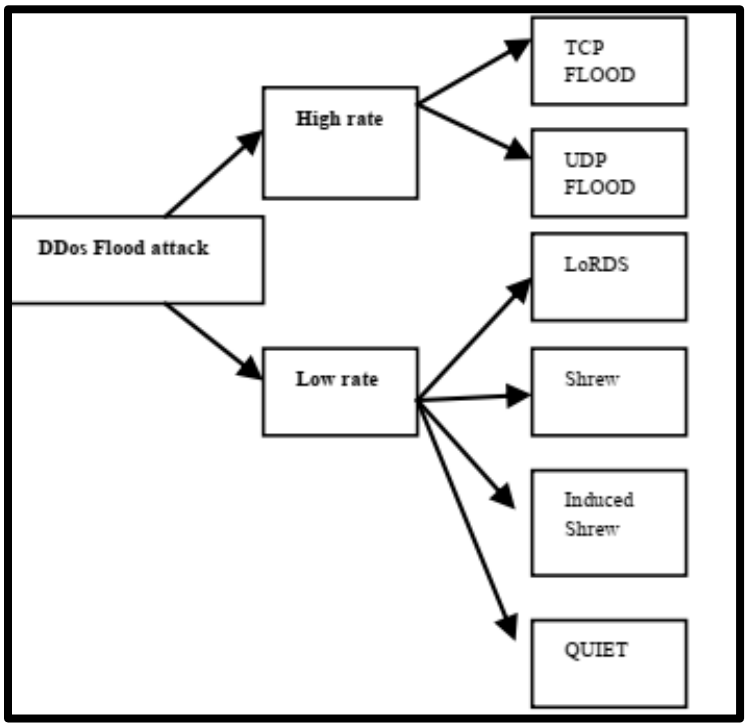

Fig.5 categorization of DDoS Attack

High rate flood attacks**:** at first, flood attacks are high rate flood. This is gifted by generating traffics from many machines, which may number thousands, distributed all over the world. Attack of the flood packets from the attackers will destroy the target hence degrading its routine to the extent of depiction it impractical. The high rate flood attacks examination in this study is the UDP attacks and TCP attacks.

They are classify as high rate flood attacks because the attacks are launched by flooding a massive amount of TCP or UDP datagram's to overpower the victim. Li *et al*. (2008), quantitative behaviors of flood attacks under diverse protocols. Quantitative performance of the attacks become the center in (Li *et al*., 2008) in order to explain the attacks randomly due to the shortage of traffic data of the real attack events. The reason is that in a lot of events of attacks, they will only be statement after the goal machines are already besieged and traffic data is lost.

Low rate flood attacks: opposing to the high rate flood, low rate flood uses carefully skill attack packets. The attack traffic rate is attuned in order to make them hidden by the traditional flood detector which regards high rate of incoming traffic as attack.

VI. Conclusion

In this paper, we study various anomaly Detection algorithms. Specifically, discuss anomaly detection using signatures and baselines. This paper also gives idea about the DDoS Attacks and their impact on network traffic. Here paper studied a DDoS attack to analysis the distribution of network traffic to recognize the normal network traffic behavior.

References

[1]. Anup Bhange "DDoS Attacks Impact on Network Traffic and its Detection Approach" International Journal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012

[2]. Anup Bhange "Anomaly detection in network traffic: A statistical approach" International Journal of IT, Engineering and Applied Sciences Research (IJIEASR) Volume 1Issue3Pages16-20

[3]. Anup Bhange "Comparative analysis of several cryptography algorithm with its effectiveness towards the security and its performance" Journal of the Gujarat Research SocietyVolume21Issue6Pages42-46

[4]. https://www.flowmon.com/en/blog/science-of-network-anomalies

[5]. Anup Bhange "Design and Evaluation to Calculate the Performance of Hybrid Cryptography to make Secure Transaction over Network" Turkish Journal of Computer and Mathematics Education Vol.11 No.3 (2020), 1208-1218

[6]. M. Li. An approach to reliably identifying signs of DDOS flood attacks based on LRD traffic pattern Recognition. Computers & Security, 23(7): 549-558, 2004.

[7]. C.S. Sastry, S. Rawat and A.K. Pujari. Network traffic analysis using singular value decomposition and multiscale transforms. Information Sciences, 177(23): 5275-5291, 2007.

[8]. H. Hajji. Statistical analysis of network traffic for adaptive faults detection. IEEE Transactions on Neural Networks, 16(5):1053–1063, September 2005

[9]. O. Salem, S. Vaton, and A. Gravey. An efficient online anomalies detection mechanism for high-speed networks. In IEEE Workshop on Monitoring, Attack Detection and Migitation (MonAM 2007), November 2007.

