System for Denial-of-Service Attack Detection Based On Triangle Area Generation

[1,] Heena Salim Shaikh, [2]N Pratik Pramod Shinde, [3]Prathamesh Ravindra Patil, [4] Parag Ramesh Kadam
[1, 2, 3, 4]Student
[1, 2, 3, 4] Alard College of Engineering and Management

***Abstract* -Denial of service attack is attempt to make service or network resource unavailable to intended users .the service may be interrupted for few seconds, minute, for hour or for days also and the major impact of this is mainly on computing systems such as business and financial systems. it can cause huge losses of corrors and millions. So in this paper we are presenting a dos attack detection system which uses multivariate correlation analysis in which we will find the relation between multiple features of network packet .Our mca based system using principle of anomaly based detection system for attack reorganization. Therefore we can detect the known as well as unknown dos attack by observing the network traffic. We are using triangle area map generation technique which increases a speed of our proposed system .also we used kdd cup-99 dataset which speed up the process of detection, at server side.**

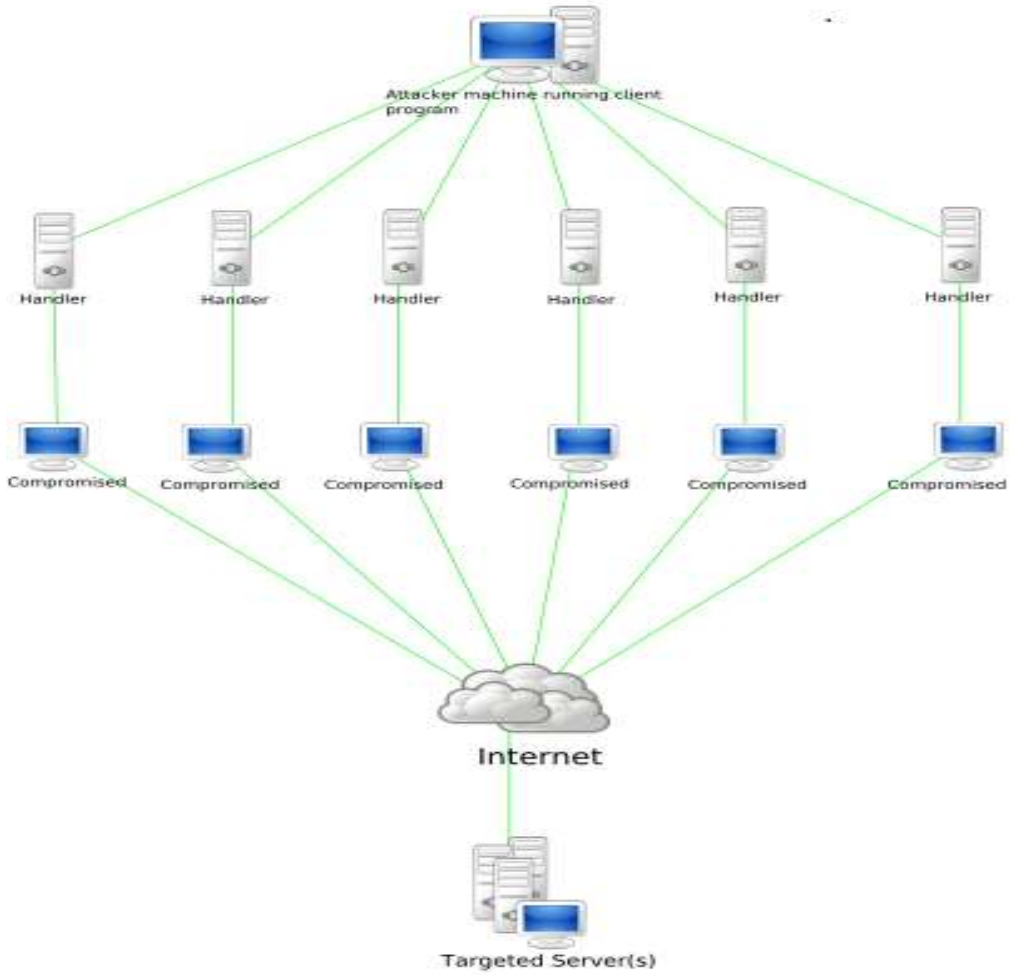
Keywords- **Multivariate, Correlation, and Anomaly Based, Kdd Cup -99 Dataset**.

1. INTRODUCTION-

Dos attack is very hugely occurring attack nowadays to networking systems.dos attack is preventing the users to use a particular services .it make network resources unavailable to the user by sending too much packets at a same time to break network capacity. A **denial-of-service attack** (**dos**) is when someone tries to stop someone else from viewing parts of the internet.dos attack is unauthorized attempt to 1. Access unauthorized information 2. Manipulate information and harm its integrity or 3. Render a system to unavailable or unreachable to the user .[1]h. Peoples are now under threats of impact of this attack on interconnected system such as web servers, database servers and cloud computing servers etc. Generally, network-based detection systems can be classified into two main categories, namely misuse based detection systems [1] and anomaly-based detection systems [2]. Misuse-based detection systems detect the attacks by monitoring network activities and looking matches with the existing attack signature. In spite of having high detection rates to known attacks and low false positive rates, misuse-based detection systems are easily evaded by any new attacks and even different types of the existing attacks. Furthermore, drawbacks of this system are 1. It is a complicated and 2.labor intensive task to keep signature database updated because signature generation is a manual process and heavily involves network security expertise. Therefore we are showing a anomaly based detection system. In this system we will used a correlation of network traffic features based on multivariate correlation analysis. we divided our system into the three steps 1.first we will generate basic profile for each participants in the network ie client ,router ,ports etc .2. In second step we will implement our mca here we will normalized the profile ie we will eliminate any bias in the features(duplicate features) then the triangle area map generation{{ [high 2320-088x]} module can be applied , to find out the correlation between distinct features , 3 thw third step further divided into two steps 3.1 test phase and 3.2 training phase. In training phase te normalize profile will be generated using {{ kdd-cup 99 dataset[975-9646]}}.and in test phase we will generate test profile for each participants in the network. then we will compare the profiles from both the phases and detect the subsequent attack. We can remove a detected node temporary to prevent it by disabling access to network for that node.

2. SYSTEM IMPLEMENTATION-

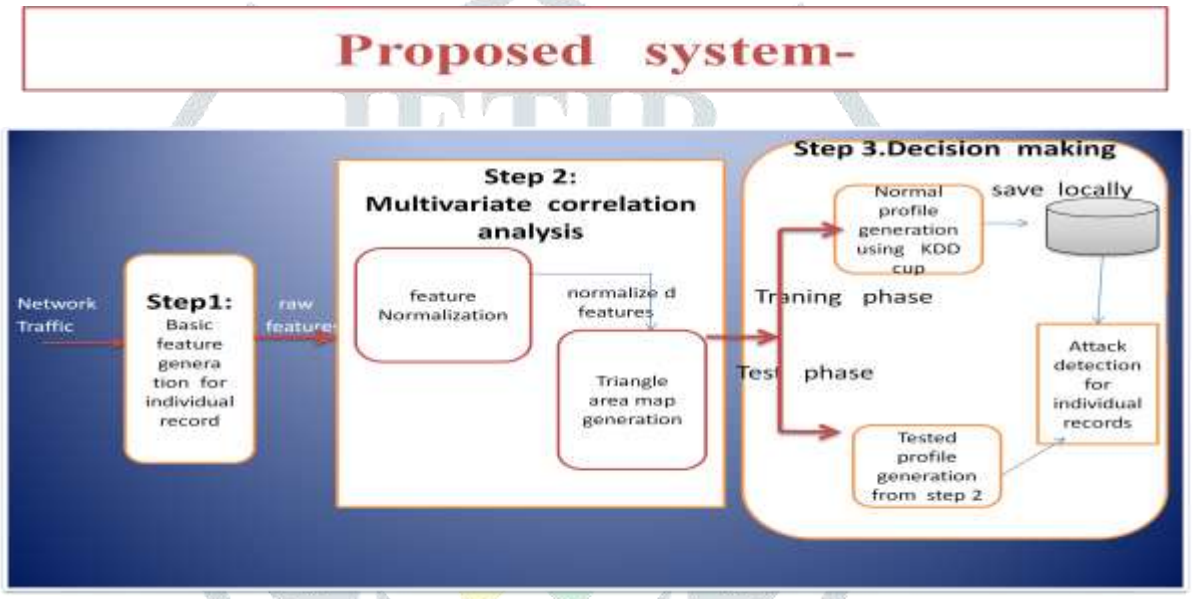
Anomaly-based detection system is a system for detecting intrusions in the computer and misuse by monitoring system activity and classifying it as either normal or anomalous and the traffic attack, the system must be taught to recognize normal system activity; these cause more effect in the communication system. A covariance Matrix based approach was designed to mine the multivariate correlation for sequential samples in this triangle area map generation technique is introduced to speed up the process and a statistical normalization technique is used to eliminate the bias from the raw data and anomalies can be detected. The dos attack detection system presented here; it employs the principles of mca and anomaly-based detection. They provide our detection system with capabilities of accurate characterization for traffic behaviors and anomaly detection respectively. A triangle area map generation technique is developed to speed up the process of multivariate correlation analysis .a technique called statistical normalization is used to eliminate the error from the raw data. Our proposed dos detection system and the traffic data is evaluated using kdd cup 99 dataset. Multivariate correlation analysis, in which the "triangle area map generation" module is applied to extract the correlations between two distinct features in the traffic record and high who have slower internet connections, such as dial-up, are affected more by attacks [5].



3. SYSTEM FRAMEWORK AND MODULES-

The overview of our proposed dos attack detection system architecture is given in this section, where the System framework and the sample-by-sample detection mechanism are discussed. Our proposes system consists of the three steps

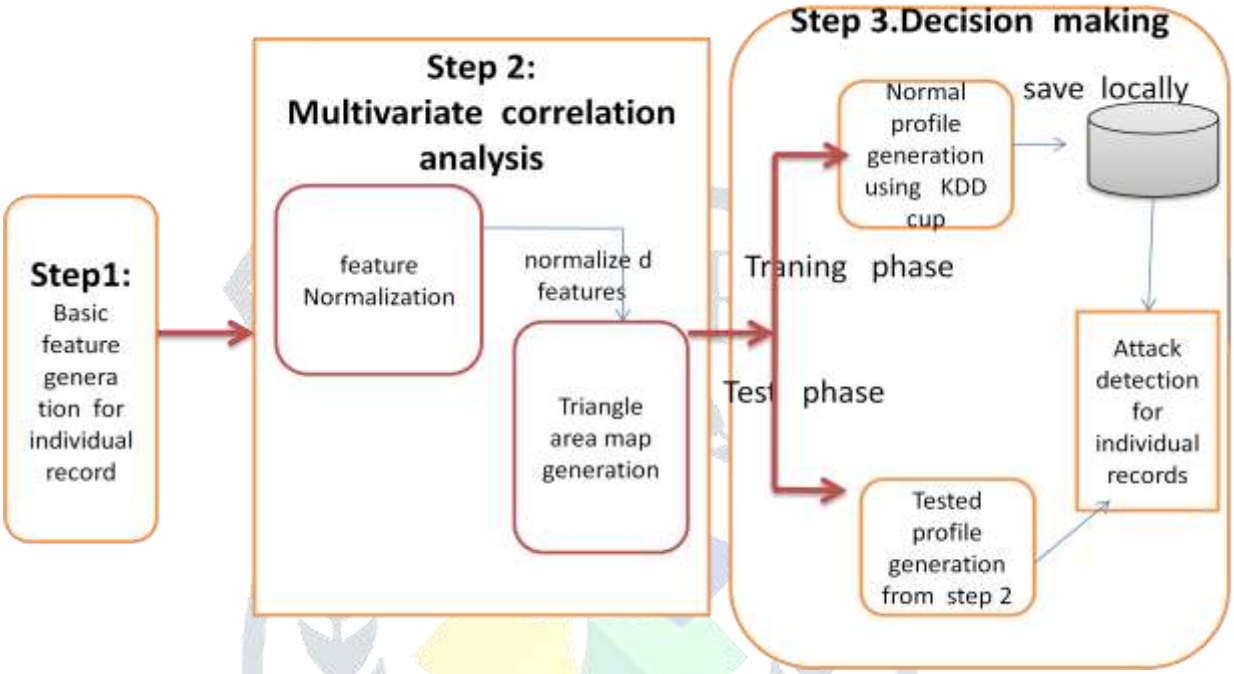
1. Basic feature generation-
   The first step is basic feature generation. The input the first step is our network traffic that mean various clients, routers, ports, intermediate nodes in the network. for this network traffic we will generate the basic network features such as source id, destination id ,delay ,bandwidth, jitter and port number etc for each participant in the network. now this raw features are submitted to the second step[1]-[5].



2. Multivariate correlation analysis-
   In the second step the basic features generated in the first step are taken as input .
   Again there are two steps in this 1. Normalization of the features- here all the basic features are examined and normalization of the features are done , if any bias or duplicate features can be eliminated 2. Then this normalized features are given to the triangle area map generation phase. Where the all normalized features of corresponding specific node are mapped to the triangles or triangular areas. Then all such triangular areas for each node are gathered to store in the triangle area map(tam).it uses the correlation matrix which is used to find out the correlation between features[6]. The matrix is used to find out the correlation of every feature i with jth feature. Then when we will compare different tam, we can imagine the map into two images symmetric along their main diagonals[3].if we see all the attributes along the diagonals are same therefore we don't need to compare it[7]. So value at diagonal will be zero. And attributes at upper triangle is similar to the lower triangle. So we can compare the attributes in either triangle [4].

3. The third step is of decision making using anomaly based detection mechanism , it is divided into the two steps 3.1 training phase- in this phase normal profile is generated for the various type of the traffic records and then it is saved in database 3.2 test phase - in this phase for the observed traffic records profiles are builded individually. after that the normal

profiles from the training phase is compared with the new generated tested profile(individually builded profiles) in the test phase[2] . And if it is not match it can be mark as attack .otherwise it will be treat as normal legitimate traffic record if the difference between both the profiles is greater than specific threshold for normal distribution the threshold value is ranged from 1 to 3.. It improves performance because it can detect any type of the dos attack without using any information about that attack also gives robustness to our system[4].



Detection System for Denial of Service Attack-(feature generation step, multivariate correlation analysis, decision making)

5. CALCULATION

We can calculate the distance based on following theorem-

Mahalanobis distance is given by
Require: Observed traffic
Record Toobserved, normal profileParameters: (N(μ, σ2), TAMnormal lower ,Cov) and parameter α
1: Generate TAMobserved lower for the observed trafficrecordTobserved
2: MDobserved← MD(TAMobservedlower ,TAMnormallower)
3: if $(\mu - \sigma * \alpha) \leq MDobserved \leq (\mu + \sigma * \alpha)$ then
4: return Normal
5: else
6: return Attack
7: end

6. CONCLUSION-

Hence we studied to detect dos attack and prevent it. Dos attack which can deny service the whole service and user cant able to log to the service such as network, power etc. Here we used triangle area map generation technique .this technique generates the geometrical relations in individual features bandwidth and network frequency etc.

7. REFERENCES

[1] P. Garca-Teodoro, J. Daz-Verdejo, G. Maci-Fernndez, and E. Vzquez, "Anomaly-based Network Intrusion Detection: Techniques, Systems and Challenges," *Computers & Security*, vol. 28, pp. 18-28, 2009.

[2] A. A. Cardenas, J. S. Baras, and V. Ramezani, "Distributed change detection for worms, DDoS and other network attacks," The American Control Conference, Vol.2, pp. 1008-1013, 2004.

[3] S. J. Stolfo, W. Fan, W. Lee, A. Prodromidis, and P. K. Chan, "Costbased modeling for fraud and intrusion detection: results from the JAM project," The DARPA Information Survivability Conference and Exposition 2000 (DISCEX '00), Vol.2, pp. 130-144, 2000.

[4] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Triangle- Area-Based Multivariate Correlation Analysis for Effective Denialof- Service Attack Detection," The 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, United Kingdom, 2012, pp. 33-40.

[5] Z. Tan, A. Jamdagni, X. He, P. Nanda, and R. P. Liu, "Denialof- Service Attack Detection Based on Multivariate Correlation Analysis," Neural Information Processing, 2011, pp. 756-765.

[6] A. Jamdagni, Z. Tan, X. He, P. Nanda, and R. P. Liu, "RePIDS: A multi tier Real-time Payload-based Intrusion Detection System," Computer networks, vol. 57, pp. 811-824, 2013.

[7] G. Thatte, U. Mitra, and J. Heidemann, "Parametric Methods for Anomaly Detection in Aggregate Traffic," Networking, IEEE/ACM Transactions on, vol. 19, no. 2, pp. 512-525, 2011.