International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 1, January 2024 ||

Improvising DoS Attack Detection Using Multivariate Correlation Analysis

Archana K. Salaskar, Bharti Kale

Dhole Patil College of Engineering, Pune, India

Dhole Patil College of Engineering, Pune, India

ABSTRACT: Denial of service (DoS) attack is potential damaging attack which degrades the performance of online servers within seconds. This attack imposes intensive computation on the target server by flooding it with large useless packets. The target server can be forced out of service from a few minutes to even several days. This causes work down of crucial business services running on the target victim. To cope with such damaging attacks becomes challenge for the researchers. Solution for this attack mainly focuses on the development of network-based detection mechanisms. Detection systems based on these mechanisms monitor traffic transmitting over the protected networks. The proposed system monitors the network traffic to extract the features which are directly associated with DoS attacks. Based on these features, the multivariate correlation model generates geometrical triangular area measurements for normal profiles. These models are used as reference to detect any unknown DoS attack in the network. But alone MCA based system may not be accurate for attack detection. The innovative work imposes behavioral model integrated with MCA to enhance the accuracy of DoS attack detection.

KEYWORDS: energy efficient algorithm; Manets; total transmission energy; maximum number of hops; network lifetime

I. INTRODUCTION

The explosive growth of internet based business services induced need of lot of research in the area of network security. Apart from various security attacks, denial of service DoS is one of the potential harmful attacks, which degrades the performance of the target server within few seconds by imposing intensive computation by flooding it with large number of useless packets. This causes work down of crucial business services running on the target victim. To cope such DoS attacks various researches have been conducted which results in implementation of various security systems and protocols. These systems include signature based, anomaly based and various other network intrusion systems. The major drawback this system possesses is the accuracy of detection.

Another approach in this field is multivariate correlation analysis, which extracts the geometrical features of known normal profiles and uses them as reference for further detection of unknown profiles by mapping them with reference profiles. This approach has been approved and can be used for the DoS detection. But alone this approach is not sufficient to achieve maximum accuracy which is crucial part of the research in this field. To deal with this issue, the proposed architecture imposes behavioural based attack detection integrated with existing multivariate correlation analysis (MCA) based attack detection system.

The behaviour based system extract all the behaviours which consist of set of patterns of attributes including source IP, source port, checksum, window size, payload length etc. To store such behaviours the system maintains database structure. These behaviours are used after MCA detection to increase the accuracy of the system.

II. RELATED WORK

To detect different kinds of DoS attacks effectively, various techniques have evolved. These techniques have shown some constraint such as they are applicable for certain network traffic. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He, Priyadarsi Nanda1, and Ren Ping Liu proposed technique which runs analysis on original feature space (first-order statistics) and extracts the multivariate correlations between the first-order statistics [1]. The extracted multivariate correlations, namely second-order statistics, preserve significant discriminative information for accurate characterizations of network traffic records, and these multivariate correlations can be the high-quality potential features for DoS attack detection. The effectiveness of the proposed technique is evaluated using KDD CUP 99 dataset and experimental analysis shows encouraging results.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 1, January 2024 ||

Shuyuan Jin, Daniel S. Yeung proposed technique which discusses the effects of multivariate correlation analysis on the DDoS detection and proposes a covariance analysis model for detecting SYN flooding attacks [2]. The simulation results show that this method is highly accurate in detecting malicious network traffic in DDoS attacks of different intensities. This method can effectively differentiate between normal and attack traffic. Indeed, this method can detect even very subtle attacks only slightly different from normal behaviors. The linear complexity of the method makes its real time detection practical.

Mihui Kim, Hyunjung Na, Kijoon Chae, Hyochan Bang, and Jungchan Na proposed a technique which presents a combined data mining approach for modeling the traffic pattern of normal and diverse attacks [3]. This approach uses the automatic feature selection mechanism for selecting the important attributes. And the classifier is built with the theoretically selected attribute through the neural network. And then, our experimental results show that our approach can provide the best performance on the real network, in comparison with that by heuristic feature selection and any other single data mining approaches.

Aikaterini Mitrokotsa, Christos Douligeris proposed a technique which presents an approach that detects Denial of Service attacks using Emergent Self-Organizing Maps [4]. The approach is based on classifying “normal” traffic against “abnormal” traffic in the sense of Denial of Service attacks. The approach permits the automatic classification of events that are contained in logs and visualization of network traffic. Extensive simulations show the effectiveness of this approach compared to previously proposed approaches regarding false alarms and detection probabilities.

Haining Wang Danlu Zhang Kang G. Shin proposed a technique which presents a simple and robust mechanism, called Change-Point Monitoring (CPM), to detect denial of service (DoS) attacks [5]. The core of CPM is based on the inherent network protocol behaviours, and is an instance of the Sequential Change Point Detection. To make the detection mechanism insensitive to sites and traffic patterns, a non-parametric Cumulative Sum (CUSUM) method is applied, thus making the detection mechanism robust, more generally applicable and its deployment much easier. CPM does not require per-flow state information and only introduces a few variables to record the protocol behaviours. The statelessness and low computation overhead of CPM make it immune to any flooding attacks. As a case study, the efficacy of CPM is evaluated by detecting a SYN flooding attack. The most common DoS attack. The evaluation results show that CPM has short detection latency and high detection accuracy.

III. PROPOSED ALGORITHM

Require: Observed traffic record $x^{observed}$, normal profile $pro : (N(\mu, \sigma^2), \overline{TAM_{lower}^{Normal}}, Cov$ and α

1: Generate $TAM_{lower}^{observed}$ $for\ the\ observed\ traffic\ record\ x^{observed}$

2: $MD^{observed} \leftarrow MD\left(TAM_{lower}^{observed}, \overline{TAM_{lower}^{Normal}}\right)$

3: if $(\mu - \sigma * \alpha) \leq MD^{observed} \leq (\mu + \sigma * \alpha) then$

MCA Based Attack =False

Else

MCA Based Attack= True

End If

4: If (MCA Based Attack == True)

Return Attack

Else

Generate beh^{attack} containing behaviors of the attack profile features. Generate $beh^{observed}$ contaning behaviors the observed profile features

If $beh^{attack} \approx beh^{observed}$

Return Attack

Else

Return Normal

End If

End If

IV. PROPOSED WORK

The proposed work consist of implementation of innovative intrusion detection system for denial of service attack detection with maximum accuracy using multivariate correlation analysis integrated with behavioural based systems.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 1, January 2024 ||

This approach monitors the network traffic and extracts the features. These features are mapped with the reference normal features taken from KDD Cup 99. The extracted normal features are further applied to triangular area map generation where geometrical areas of all the normal features are computed. Along with the triangular map areas, another model known as behavioural based model extracts the behavioural patterns of normal profiles and stores them into database. This phase is training phase, which mainly consists of computation and storage of geometrical TAM (Triangular Area Map) as well as normal behavioural patterns. These entities are further used to classify any unknown profile with high accuracy in testing phase.

V. PROPOSED ARCHITECTURE

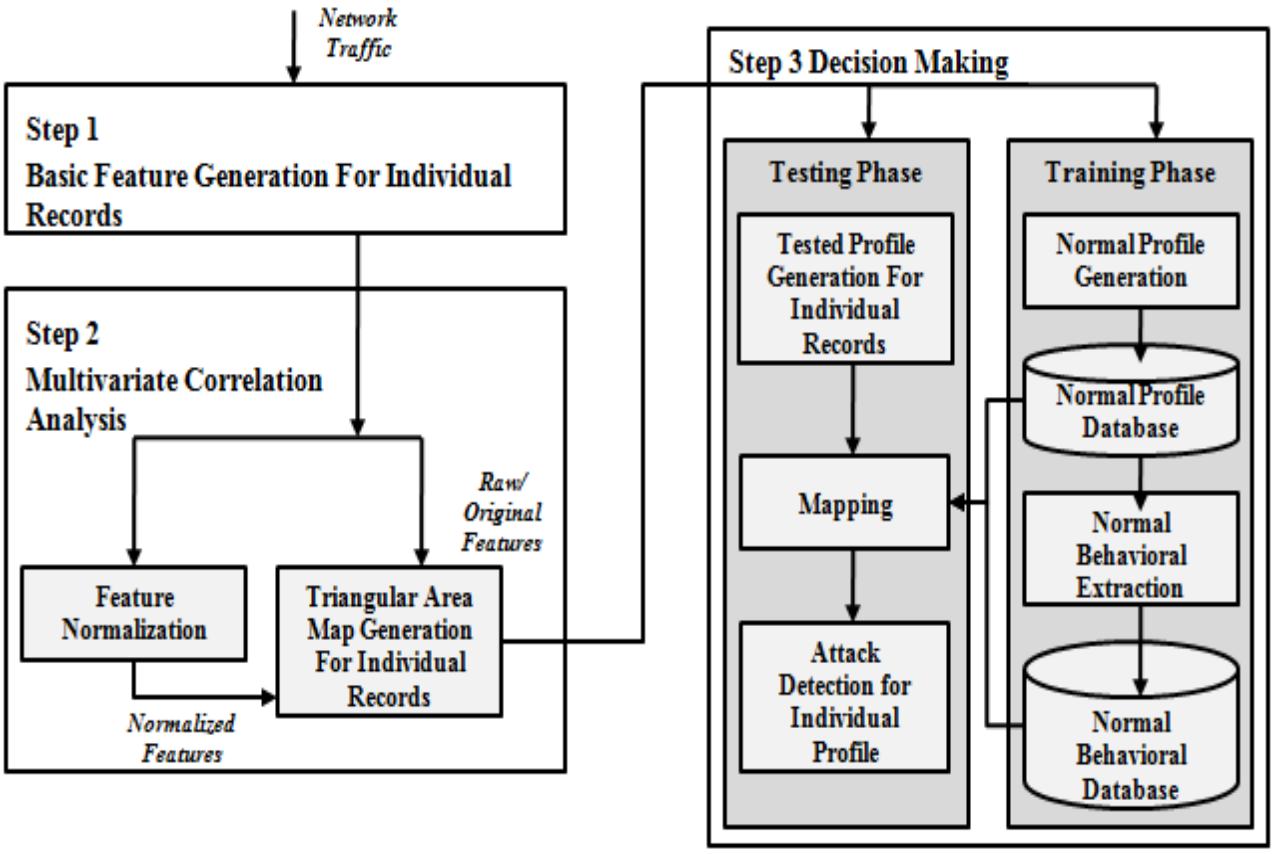


Fig.1. Proposed system

The proposed architecture consists of three steps. In step 1, basic features are generated from ingress network traffic to the internal network where protected servers reside in and are used to form traffic records for a well-defined time interval. Monitoring and analysing at the destination network reduce the overhead of detecting malicious activities by concentrating only on relevant inbound traffic. This also enables our detector to provide protection which is the best fit for the targeted internal network because legitimate traffic profiles used by the detectors are developed for a smaller number of network services.

Step 2 is multivariate correlation analysis, in which the “triangle area map generation” technique is applied to extract the correlations between two distinct features within each traffic record coming from the first step or the traffic record normalized by the “feature normalization” module in this step (Step 2). The occurrence of network intrusions cause changes to these correlations so that the changes can use as indicators to identify the intrusive activities. All the extracted correlations, namely, triangle areas stored in triangle area maps (TAMs), are then used to replace the original basic features or the normalized features to represent the traffic records. This provides higher discriminative information to differentiate between legitimate and illegitimate traffic records.

In Step 3, the behavioural based detection mechanism is adopted in decision making. The behavioural model extracts important behaviours of normal profiles and stores in normal behaviour database. These normal behaviour profiles are then mapped with tested profiles. This technique further increases the accuracy of attack detection.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 1, January 2024 ||

VI. SIMULATION RESULTS

The simulation studies involve finding multivariance among different features of packets as well as computing Pearson correlation among various features. The simulation results are computed in R and using standard dataset KDD Cup99. The features shown in following plots are associated with known normal profiles of standard dataset.

Figure 2 shows multivariance plot between length of IP payload and source port. Figure 3 shows multivariance plot between source port and window size. Figure 4 shows multivarince plot between length of IP payload and TCP header length. Figure 5 shows Pearson correlation among IP payload length, source port, destination port, TCP header and TCP window size. The Pearson correlation matrix is further used to compute TAM profiles.

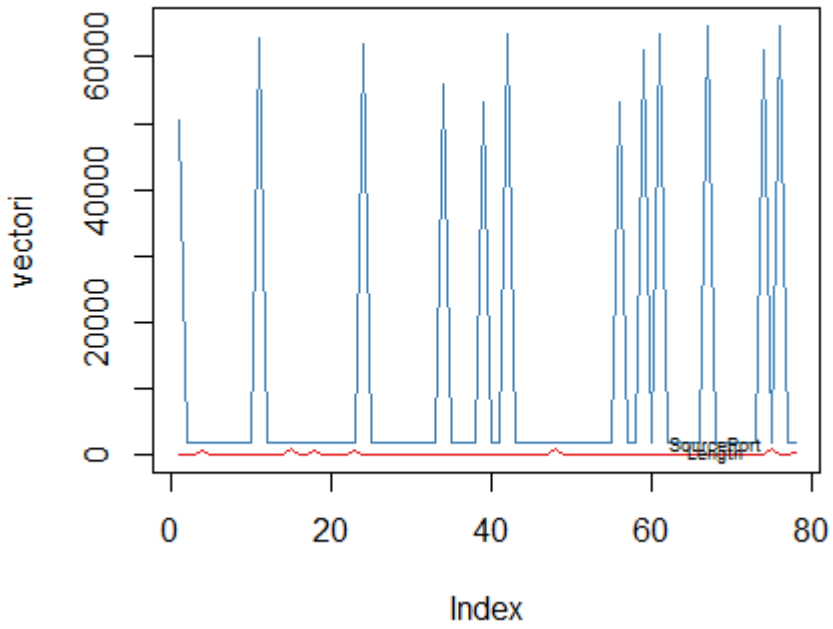


Fig 2. Multivariance between IP payload length and Source Port

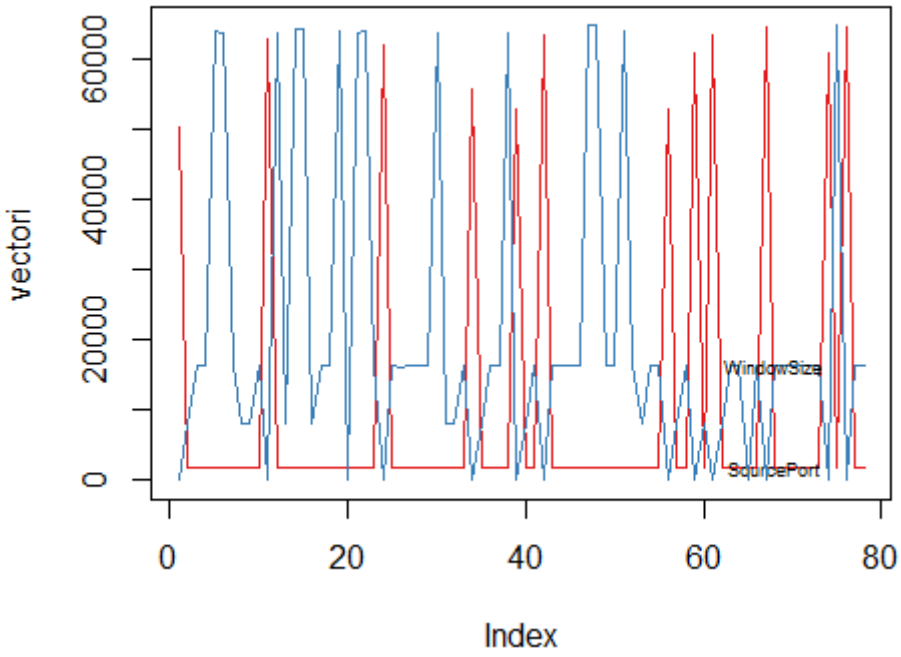


Fig 3. Multivariance between Source Port and Window Size

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 1, January 2024 ||

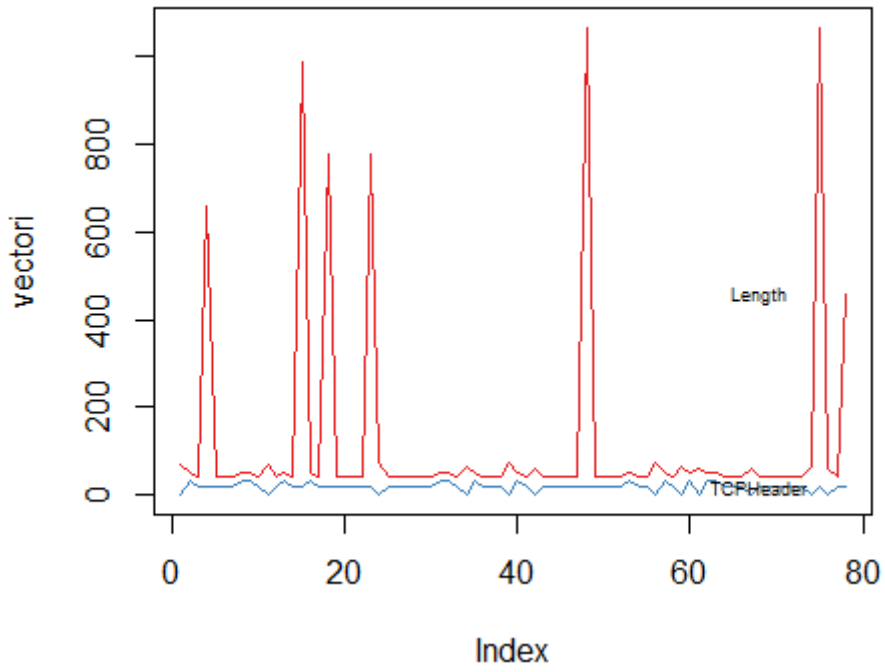
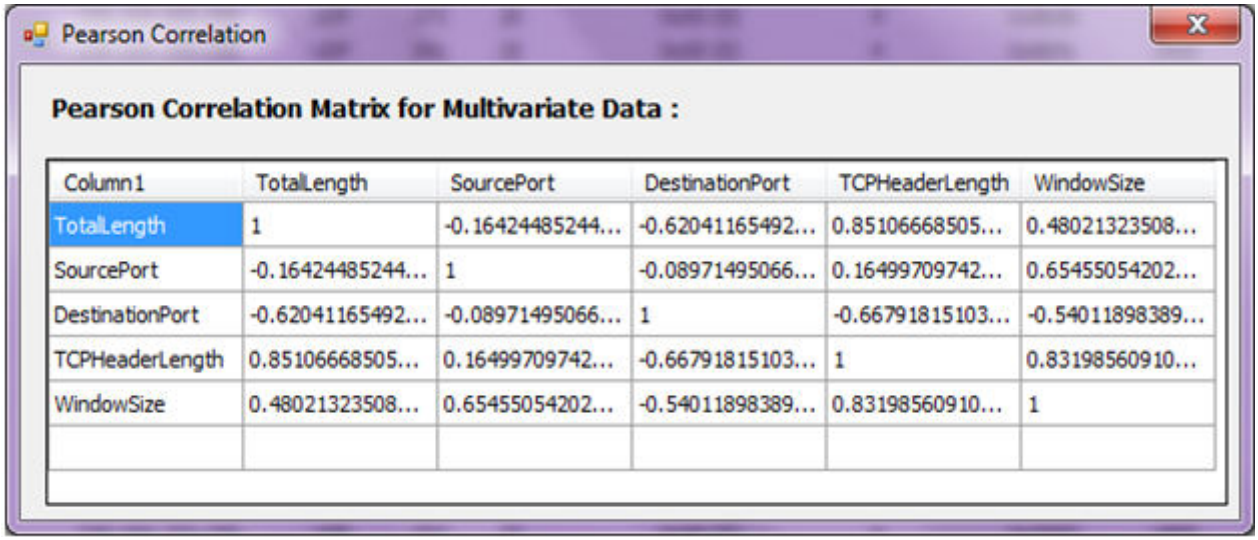


Fig 4. Multivariance between IP payload length and TCP Header Length



Column1	TotalLength	SourcePort	DestinationPort	TCPHeaderLength	WindowSize
TotalLength	1	-0.16424485244...	-0.62041165492...	0.85106668505...	0.48021323508...
SourcePort	-0.16424485244...	1	-0.08971495066...	0.16499709742...	0.65455054202...
DestinationPort	-0.62041165492...	-0.08971495066...	1	-0.66791815103...	-0.54011898389...
TCPHeaderLength	0.85106668505...	0.16499709742...	-0.66791815103...	1	0.83198560910...
WindowSize	0.48021323508...	0.65455054202...	-0.54011898389...	0.83198560910...	1

Fig 5. Pearson Correlation among different features

VII. CONCLUSION AND FUTURE WORK

The multivariate correlation analysis is effective for attack detection as it computes the geometrical triangular area's from correlation among different features. This approach focuses on all possible combinations of correlations and hence proved as effective measures not only in the network security but also image processing and machine learning. But probability of attack detection is always low in spite of any innovative system because attacker always alters the way of attacks. To deal with this alteration, behavioral based model proposed in this work is best suited. It pinpoints the major symptoms of attacks by monitoring its behaviors. This includes all patterns of various features of attack profiles. Like other systems this system requires much learning about the network profiles in training phase but it may give maximum accuracy after sufficient observations. The future work in this context includes mining of behavioral patterns so that there is no need to store all patterns in database but only classified data need to be store. This would increase the speed of detection and minimizes the size of the database.

| ISSN: 2349-6037 | www.ijmserh.com ||Impact Factor: 9.274||Quarterly, Peer Reviewed & Refereed Journal|

|| Volume 12, Issue 1, January 2024 ||

REFERENCES

1. Zhiyuan Tan, Aruna Jamdagni, Xiangjian He,Priyadarsi Nanda, Ren Ping Liu , 'A System for Denial-of-Service Attack Detection Based on Multivariate Correlation Analysis', IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2, February 2014
2. Shuyuan Jin,Daniel S. Yeung, 'A Covariance Analysis Model for DDoS Attack Detection'. IEEE Communications Society 0-7803-8533-0/04/$20.00 (c) 2004 IEEE Hong Kong RGC project research grant number B-Q571
3. Mihui Kim, Hyunjung Na, Kijoon Chae, Hyochan Bang, and Jungchan Na, 'A Combined Data Mining Approach for DDoS Attack Detection'. ICOIN 2004, LNCS 3090, pp. 943–950, 2004 Springer-Verlag Berlin Heidelberg 2004
4. Aikaterini Mitrokotsa, Christos Douligeris, 'Detecting Denial of Service Attacks Using Emergent Self-Organizing Maps'. 2005 IEEE International Symposium on Signal Processing and Information Technology
5. Zhiyuan Tan1; Aruna Jamdagni1; Xiangjian He1, Priyadarsi Nanda1, and Ren Ping Liu, 'Multivariate Correlation Analysis Technique Based on Euclidean Distance Map for Network Trac Characterization'.
6. Lata1, Indu Kashyap , 'Study and Analysis of Network based Intrusion Detection System',International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 5, May 2013
7. Ajoy Kumar, Eduardo B. Fernandez,' Security Patterns for Intrusion Detection Systems', 1 st LACCEI International Symposium on Software Architecture and Patterns (LACCEI-ISAP-MiniPLoP'2012), July 23-27, 2012, Panama City, Panama
8. Punit Gupta , 'Behavior Based IDS for Cloud IaaS' , International Journal of Software and Web Sciences (IJSWS)