Time Variant Predicate Based Traffic Approximation Algorithm for Efficient low Rate DDoS Attack Detection

M. Baskar[1], T. Gnanasekaran[2,] J. Frank Vijay[3]

[1] KCG College of Technology
Karapakkam,Chennai,Tamilnadu - India
[E-mail: baashkarcse@gmail.com]

[2] RMK. Engineering College
R S M Nagar, Kavaraipettai, Gummidipoondi Taluk
Tiruvallur District, Chennai, Tamil Nadu, India
[E-mail:t.gnanasekaran@gmail.com]

[3]KCG College of Technology
Karapakkam,Chennai,Tamilnadu - India
[E-mail: jeirus.jeff@gmail.com]

***Corresponding Author: M.Baskar**

Abstract:

The low rate Distribute Denial of Service (DDoS) attack issue has been approached with different methods in the literature. Still, the performance of attack detection has not been achieved up to noticeable rate. With the intension to improve the performance of low rate DDoS attack detection, an efficient time variant predicate based traffic approximation algorithm is presented in this paper. The method maintains set of predicates about the low rate attacks in each time window. The predicates are generated using the access trace available. It is necessary to identify the changing attacking behavior of malicious nodes. The proposed algorithm generates the predicates from the malicious access trace and how well they can be performed in low level. Using the predicates generated, the method classifies the current request as genuine or malicious. To classify the request, the method computes the predicate closure weight, which is computed based on the frequency of the service being accessed in related to the predicate and their state of finish. The proposed method generates higher efficient result in the mitigation of low rate DDoS attacks and improves the network performance.

Keywords:

Predicates, DDoS attack Mitigation, Time variant Approach. Traffic Approximation, Predicate Closure.

1. Introduction:

The modern internet technology has opened the gate for the users to access the service through number of devices either with mobile phones or PDA and etc. However, the services provided by the network service provider faces number of challenges in maintaining their throughput. The malicious users could be able to generate number of threats towards the services available. The major issue considered here is the denial of service attack. Further, the DDos attacks are generated in low level which has been identified as negligible but has higher impact in the service performance.

In general, the denials of service attacks are performed in a distributed manner by many numbers of users. They generate malicious packets or request to the service point in the intension to degrade the service performance. There are number of approaches available for the prediction of such attacks. The host based approaches are used to identify the malicious user but has the problem of genuine user access from the particular host and also it cannot be defined that the entire request from the host are malicious. Similarly, the traffic based approaches are available which uses the traffic or flow of packets to classify the request. The behavior based approaches are defined with the help of behavior in accessing the service. Further, there exist different approaches to detect the low rate DDoS attacks, where each uses different methods and measures.

The low rate DDoS attacks are hard to notice due to their lower frequency which has been missed or ignored by the general DDoS detection mechanisms. But they introduce higher impact in the throughput performance of the network. The low rate attacks are generated in a low numbers but not in a continuous fashion. They would appear in once or twice in a time window but in cumulative they would have higher impact in the network throughput. So it is necessary to monitor such threats towards the improvement network performance.

The time variant approaches are using the traces of service access from different time window. By monitoring the service access in different time window, how the service has been accessed and how the malicious threats are appeared can be identified. Using the access trace, you can generate set of predicates as what type of request at what time and their features. Such predicates would help to identify the malicious threats in more accurate manner. Even the low rate attacks are generated in a low frequency in any time window; it can be identified and mitigated.

This paper presents such a mitigation approach towards the development of network performance. The method uses the predicates of service access in monitoring the low rated denial of service attacks. However the method estimates the predicate closure weight which represents the closeness of the access type in classifying the request. The detailed methods will be discussed in the next section.

2. Related Works:

The detection of low rate DDoS attack has been approached with various methods among them each uses different measures and features. This section explores a subset of methods towards the problem.

The measures of low rate attack detection have been evaluated for their performance in attack detection in [1]. The author considered different entropy measures like generalized, Rany’s, Hartley, Shannon with generalized information distance measures. Each measure has been applied and their performance has been evaluated. Their performance in low rate and high rate attack detection has been evaluated.

The data analysis of multiple traffic has been used to perform low rate attack detection in [2]. The method reads the traffic data and computes a feature score to differ it from normal traffic. Based on the feature score the malicious traffic has been identified. The methods analyze the behavior of the nodes and computes entropy measures to perform low rate detection.

The information regarding the traffic has been used for low rate attack detection in [3]. The method combines distance metric and entropy measure to perform low rate attacks. Both measures are estimated for normal and attack traffic. Based on the measures estimated, the low rate attack has been detected.

In most situations, the payload feature would help the detection of low rate attacks. The malicious user would send huge amount of data in less number of packets. Such frequency would be low but still there is an intension in low rate DDoS attacks. Such threat has been handled in [4], which monitors the packet size and differentiate with different attacks and their traffic patterns.

The entropy measure computed on the network traffic and by clustering the traffic for the improvement of low rate attack detection has been presented in [5]. The method has been evaluated on DETER testbed which is explicitly available for the cyber defense technology experimental research laboratory. Various simulation scenarios has been deployed on DETER bed which is the mixture of genuine and malicious traffic with different packet sizes. For each of the simulation the entropy measure has been estimated and evaluated for their performance.

The web traffic has been taken as the key in identifying application layer denial of service attacks in [6]. The method considers heavy traffic which takes care of flash crowd traffic. The method uses the Real time Frequency Vector (RFV) which characterizes the real time traffic.

The problem of low rate attack detection has been handled with a mathematical model in [7]. The method reads the behaviors of TCP traffic and its congestion window. Using them, the method generates a attack pattern and computes the impact matrix. Using them the method performs DDoS attack detection.

The correlation measure has noticeable impact in the detection of low rate DDoS attacks. Such correlation measure has been used in a combined nature to perform the DDoS attack detection. In [8], the spearmen and partial rank correlation measures has been adapted in a combined nature to perform low rate attack detection. The real life data set has been used for the evaluation purpose. They have produced good results in the detection rate.

The entropy measures have great impact in identifying the Low-rate DDOS Attacks. In [9], the author introduces an Optimal Objective Entropy (OOE) measure for the detection of low-rate DDOS attacks. The method improves the performance than traditional entropy measures. The similar entropy measure has been used in a light weight mode for the detection of flooding attacks in [10]. The author presents a trace back algorithm to monitor the flooding attack using E-LDAT which is an extended entropy measure. The method is capable of distinguish the legitimate and malicious traffic.

The generalized entropy measure has been used in different stage of low rate attack detection. But its trustworthy is questionable in different results. Such investigation on generalized entropy has been performed in [11]. The artificial neural network has been adapted for the problem of unknown attack detection in [12]. The method uses the patterns for the representation of features received from different users and adapts the artificial neural network for detection purpose.

Various features have been used to correlate the genuine and malicious traffic. In [13], the author presented a correlation measure for the detection of low rate attacks which uses the flow feature. The method uses the coefficient to measure the similarity between legitimate and malicious traffic.

The data rend fluctuation has been used in the Low-Rate DoS Attacks Detection [14]. The method analyzes the changing features of network traffic and performs data rend fluctuation in multiple fractions. The wavelet analysis is performed for the detection of low rate attack.

The flow rate based low rate attack detection is presented in [15]. The flow traffic pattern has been used in this and they monitor the flow rate and how long the flow is continued in this approach. The FlowTrApp (Flow Traffic Application) approach is deployed in data centers for efficient detection of low rate attack.

The correlation measures have good records in detecting low rate attacks. Such measures have been adapted with k-nearest neighbor technique in [16]. The method reads the neighbor traffic and correlates with its own. The grid based approach has been used to calculate the correlation measure and the real time internet traffic has been used for evaluation.

The correlation measure has noticeable impact in the detection of low rate DDoS attacks. Such correlation measure has been used in a combined nature to perform the DDoS attack detection. In [17], the spearmen and partial rank correlation measures has been adapted in a combined nature to perform low rate attack detection. The real life data set has been used for the evaluation purpose. They have produced good results in the detection rate.

The orthogonal matching and matching algorithms of greedy method has been presented in [18]. The method maintains the features of malicious traffic in form of tree to improve the classification performance and to reduce the time complexity.

The self similarity based low rate attack detection is presented in [19], which differentiate the similarity on the regular flow and the new flow in different times. Based on the similarity measure, the low rate attack detection is performed. In [20], the flow feature has been used to perform low rate attack detection. The ant colony algorithm has been used to measure the flow feature and sum of the flows has been considered for the detection of low rate attacks.

All the methods discussed suffer to achieve the required performance in low rate attack detection.

3. Time Variant Predicate Based Traffic Approximation:

The network trace has been read and split into different subset according to the time window they have been generated. For each subset of time window log, the method collects the malicious access trace and has been used to generate the predicates. Generates predicates has been used to estimate the predicate closure weight for low rate attack detection. Based on the predicate closure weight the method performs denial of service attack detection. The detailed approach is presented in this section.

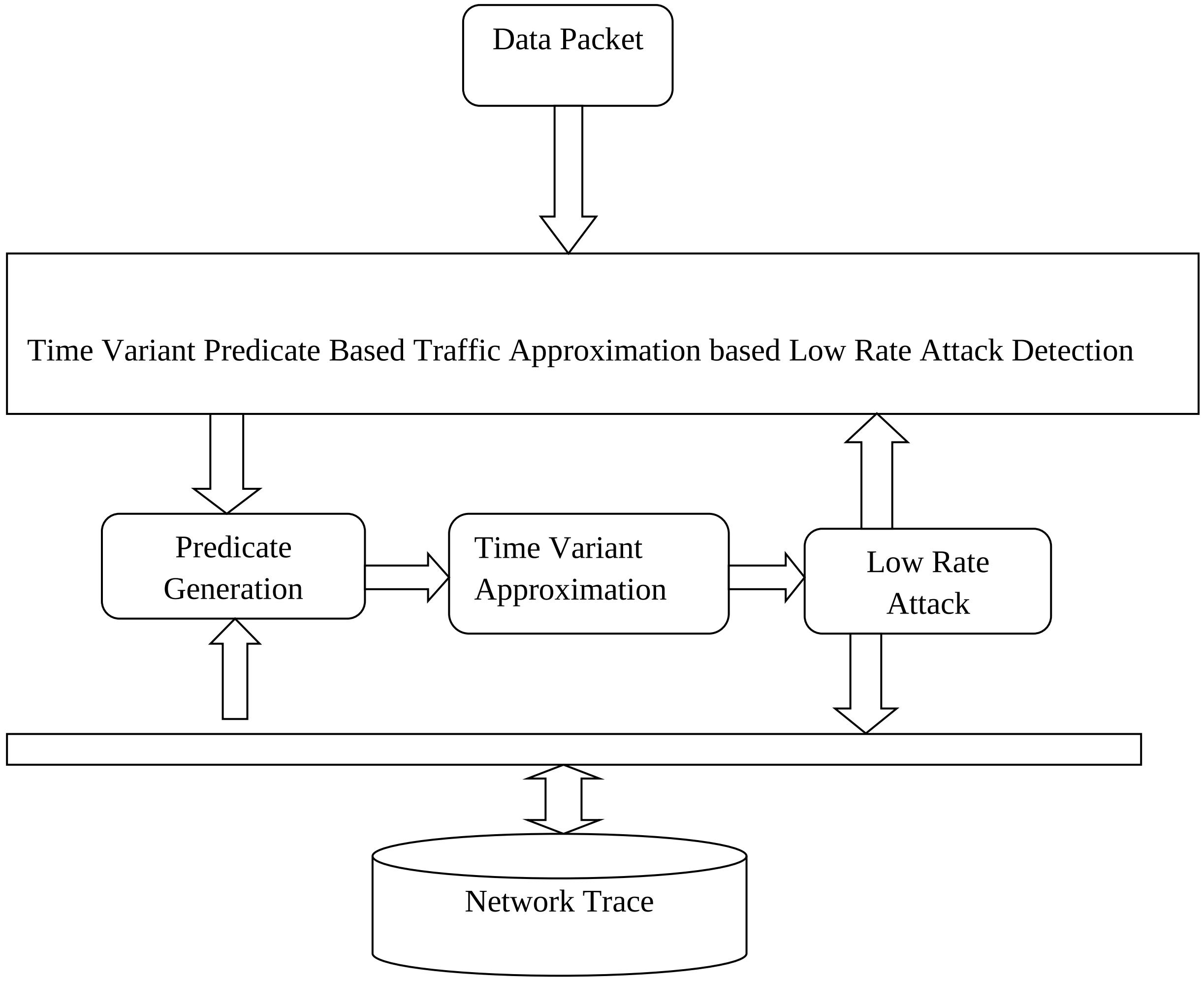

Data Packet
Time Variant Predicate Based Traffic Approximation based Low Rate Attack Detection
Predicate Generation
Time Variant Approximation
Low Rate Attack
Network Trace

Figure 1: Architecture of proposed algorithm.

The Figure 1 shows the architecture of predicate based time variant approximation algorithm for low rate attack detection.

3.1 Predicate Generation:

The predicate is the features which represent the pattern of service access being performed for the malicious attack. It has been generated for each time window considered and based on the malicious access, the method generates the predicates for the service access. To generate the predicate for the service Si, first the access logs has to be split into different time window Tw.

Consider the entire time window is represented as Ø which consist of number of time window Ti. For each time window T_i{ Ø}, the access log and malicious logs has to be splited. So that the time window log of Ti, must be identified as follows:

Generate time window log A-Ti{ Ø} = $f(Ti) = \sum_{n=1}^{size(Al)} \text{Al(n). Time} \leftrightarrow \text{Ti}$ –(1)

Generate Time window log MA-Ti(Ø) = $f(Ti) = \sum_{n=1}^{size(MAl)} \text{MAl(n). Time} \leftrightarrow \text{Ti}$ -- (2)

Here Al-represent the access log where MAL is the malicious access log.

Once the logs has been split based on the time window, then it can be used to generate the predicates. The predicate of any service has following features. The service being access for the number of times NSA, the successful access NSS, Number of malicious access NMA, Average payload Apl, Average Hop count Ahc, Average latency Alt. All these features have to be extracted from the access log and malicious access log to generate the predicates.

First the number of times the service being accessed is estimated as follows:

NSA = $f(A - Ti) = \sum_{n=1}^{size(ATi)} \text{ATi(n). Service == SR}$ --(3)

SR- is the service being requested.

NSC = $f(A - Ti) = \sum_{n=1}^{size(ATi)} \text{ATi(n). Service == SR \&\&}\ ATi\text{(n). Status = Completed}$ --(4)

Now compute the average payload Apl as follows:

Apl = $\frac{\sum_{i=1}^{size(ATi)} ATi(i).payload}{size(ATi)}$ --(5)

Compute average hop count Ahc.

Ahc = $\frac{\sum_{i=1}^{size(ATi)} ATi(i).hopcount}{size(ATi)}$ -- (6)

Compute average latency Alt = $\frac{\sum_{i=1}^{size(ATi)} ATi(i).latency}{size(ATi)}$ -- (7)

.

Now compute the number of malicious access NMA.

NMA = $(MA - Ti) = \sum_{n=1}^{size(MATi)} \mathrm{MATi(n).Service} == \mathrm{SR}$ --(8)

Now compute the average malicious payload Ampl as follows:

Ampl = $\frac{\sum_{i=1}^{size(MATi)} MATi(i).payload}{size(MATi)}$ --(9)

Compute average malicious hop count Amhc.

AMhc = $\frac{\sum_{i=1}^{size(AMTi)} MATi(i).hopcount}{size(MATi)}$ --(10)

Compute average malicious latency AMlt = $\frac{\sum_{i=1}^{size(AMTi)} AMTi(i).latency}{size(AMTi)}$ --(11)

Now the predicate for the service S can be generated as follows:

Predicate of service SP = {NSA, NSC, NMA,NSC, APl, Ampl, Ahc, Amhc, Alt, AMlt}

The generated predicate will be used for the traffic approximation in the next stage.

3.2 Time Variant Traffic Approximation:

The traffic being produced by the users has been approximated based on the predicate generated in the previous stage. First the method reads the user request and identifies the service being claimed. Then the method extracts the features like payload, hop count, latency from the request packet. Then the exact service predicate being identified. Using the features of the predicate and the feature extracted, the method computes the predicate closure weight. The closure weight is estimated based on the features of the predicated and features of the packet being received. Estimated predicate closure weight will be used to perform denial of service mitigation.

To estimate the predicate closure weight, it is necessary to extract the following features from the packet received.

Identify the service Sreq = P.Service.

```
    Extract the payload Pl = $Payload \in P$
    Extract the hop count Hc = $\sum Hops \in p$
    Compute latency lat = P.received – P.sent.
    Now compute the predicate closure weight as follows:
```

$$\text{Pcw} = \frac{NSC}{NSA} \times \frac{NMA}{NSA} \times \frac{Dist(Apl,Ampl)}{Apl} \times \frac{Dist(Ahc,Amhc)}{Ahc} \times \frac{Dist(Alt,Amlt)}{Alt} \quad \text{-- (12)}$$

The computed PCW value will be used to perform distributed denial of service attack detection.

3.3 Low Rate Attack Detection:

The presence of malicious DDoS low rate attack has been identified and mitigated using the time variant traffic approximation with the predicates. The method first receives the user request, and identifies the service being requested. Then for the service identified, the method generates the predicates. Using the predicate, and the features of the service packet received, the method estimates the predicate closure weight. Using the PCW value estimated, the method performs the decision making.

Algorithm:

```
Input: Network Trace NT, Packet P
Output: Boolean
Start
    Read network trace NT.
    Read the access trace AT, Malicious Trace MT.
    Read the packet P.
    Identify the service requested Sreq from the packet P.
    Generate Predicates.
```

```
        PCW = Estimate Predicate Closure weight.
        If PCW > Th then
                Allow
        Else
                Deny service
                Generate malicious trace.
        End
Stop.
```

The above discussed algorithm receives the user packet and identifies and extracts the features. Using the features extracted and generated predicates, the method performs denial of service attack detection in a lower rate.

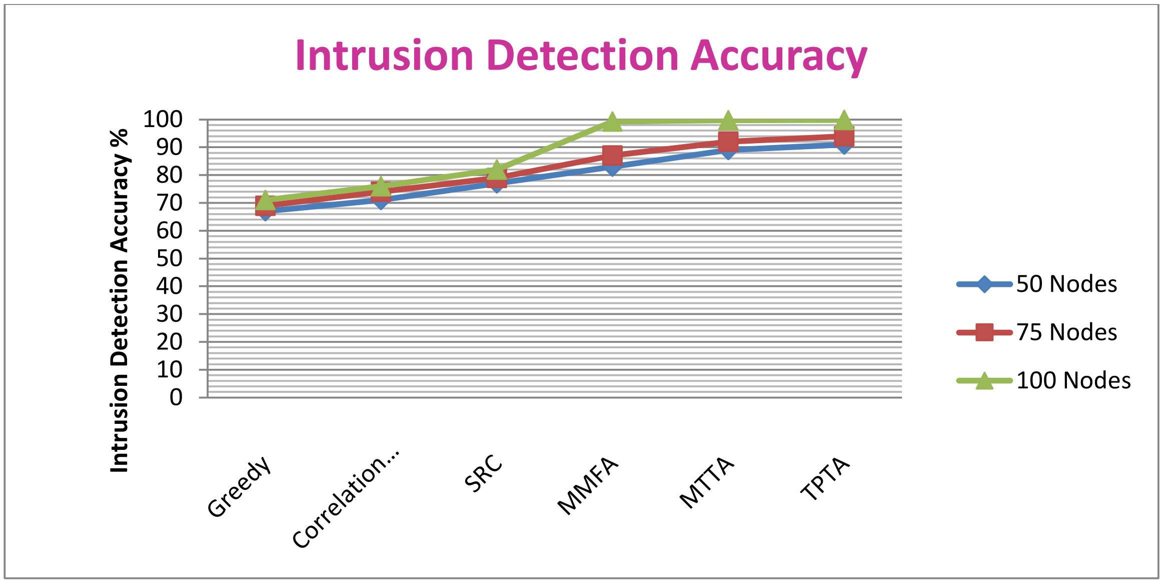
4. Result and Discussion:

The proposed TPTA algorithm has been implemented on advanced java. The performance on low rate attack detection has been measured and compared with different other methods. For evaluation, various simulation scenarios have been considered and its performance has been measured on various parameters

Table 1: Simulation Information

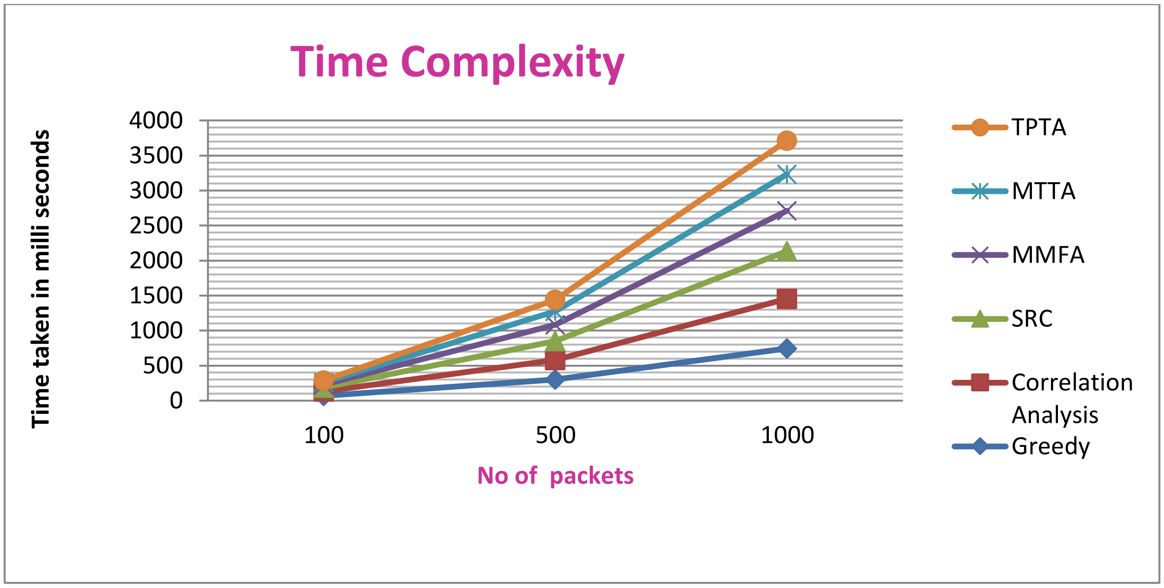
Property	**Value**
Name	TPTA
Nodes for Testing	200
Time for Evaluation	600 Seconds
Implemented Tool	Advanced Java

The details of simulation have been presented on Table 1. Based on the information, the performance of the TPTA algorithm in low rate attack detection has been measured.



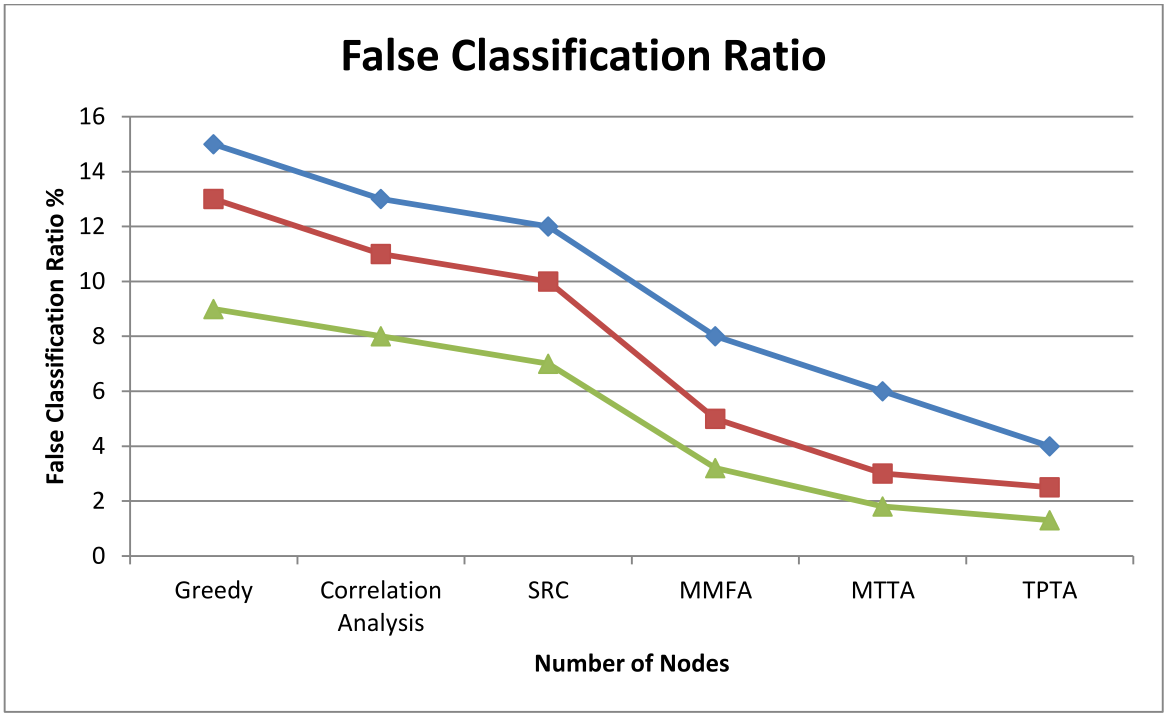
Graph 1: How Intrusion Detection Achieved

The intrusion detection accuracy produced by the proposed TPTA algorithm has been measured. It has been compared with the other methods results on the same set of scenario. The comparison result depicts clearly that the proposed TPTA algorithm has achieved higher accuracy on intrusion detection. The result has been presented in Graph 1.



Graph 2: How Time Complexity Achieved

The time complexity of low rate attack detection has been measured and compared with other methods results on the same test bed. The result has been presented in Graph 2. The result clearly represents the efficiency of the proposed TPTA algorithm in time complexity which reduces the time complexity than other methods on different number of packets considered.



Graph 3: How False Classification Ratio Reduced

The False ratio in classification has been measured and compared with other methods results on the same test bed. In each test bed, the method has produced less false ratio on the classification. This proves that the proposed TPTA algorithm has produced less false classification ratio than other methods. The result has been presented in Graph 3.

Table 2: Comparative Study

Protocol	**Accuracy On Intrusion in %**			**Ratio on False in %**			**Time Complexity in Milli seconds**		
	50 Nodes	**75 Nodes**	**100 Nodes**	**50 Nodes**	**75 Nodes**	**100 Nodes**	**100 packets**	**500 Packets**	**1000 Packets**
Greedy	67	69	71	15	13	9	67	302	746
Correlation Analysis	71	74	76	13	11	8	63	280	710
SRC	77	79	82	12	10	7	56	267	680
MMFA	83	87	99.2	8	5	3.2	42	234	192
MTTA	89	92	99.7	6	3	1.8	31	192	520
TPTA	91	94	99.8	4	2.5	1.3	28	167	478

The performance on various parameters has been measured and presented in Table 2. The comparative study shows clearly that the proposed TPTA algorithm has achieved higher performance in all the parameters considered.

5. Conclusion:

In this paper, an efficient real time predicate based traffic approximation based denial of service attack detection model is presented. The network trace has been taken as input and that has been split into the number of time window considered. With each subset of traces belongs to different time window, different features has been extracted. With the extracted features, different average values on payload, hop count, latency and no of access has been measured. Similarly using the malicious trace, the method estimates the various features. Using all the features extracted, the method generates the predicate closure for different services in each time window. For the classification, the method computes the predicate closure weight. Using the predicate closure weight estimated for the incoming packet the method performs classification of the packet. The method produces efficient results in attack detection and improves the performance as well.

References:

1. Monowar H. Bhuyan , D. K. Bhattacharyya and J. K. Kalita ,Information metrics for low-rate DDoS attack detection: A comparative evaluation, IEEE conference on Contemporary Computing (IC3), 2014.

2. Nazrul Hoque , Dhruba K Bhattacharyya and Jugal K Kalita, A novel measure for low-rate and high-rate DDoS attack detection using multivariate data analysis, IEEE, conference on Communication Systems and Networks (COMSNETS), 2016.

3. Yang Xiang, Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics, IEEE Transactions on Information Forensics and Security, Vol.6, Issue.2, 2011.

4. Lu Zhou, Mingchao Liao, Cao Yuan, and Haoyu Zhang, Low-Rate DDoS Attack Detection Using Expectation of Packet Size, Hindawi, Security and Communication Networks, Vol. 2017.

5. M. Sachdeva and K. Kumar, A traffic cluster entropy based approach to distinguish DDoS attacks from flash event using DETER testbed, ISRN Communications and Networking, vol. 2014.

6. W. Zhou, W. Jia, S. Wen, Y. Xiang and W. Zhou, Detection and defense of application-layer DDoS attacks in backbone web traffic, Future Generation Computer Systems, vol. 38, pp. 36–46, 2014.

7. J. Luo, X. Yang, J. Wang, J. Xu, J. Sun and K. Long, On a mathematical model for low-rate shrew DDoS," IEEE Transactions on Information Forensics and Security, vol. 9, no. 7, pp. 1069–1083, 2014.

8. S. Yu, W. Zhou, W. Jia, S. Guo, Y. Xiang, and F. Tang, Discriminating DDoS attacks from flash crowds using flow correlation coefficient, IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 6, pp. 1073–1080, 2012.

9. P. N.Jadhav and B. M. Patil, Low-rate DDOS Attack Detection using Optimal Objective Entropy Method, International Journal of Computer Applications, vol. 78, no. 3, pp. 33–38, 2013.

10. M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, E-LDAT: a lightweight system for DDoS flooding attack detection and IP traceback using extended entropy metric, Security and Communication Networks, vol. 9, no. 16, pp. 3251–3270, 2016.

11. Sunny Behal , Detection of DDoS attacks and flash events using information theory metrics an empirical investigation, ACM Computer Communication, vol. 103, pp 18-28, 2017.

12. Saied, A., Overill R.E and Radzik, T, Detection of known and unknown DDoS attacks using artificial neural networks, Commun. Comput. Inf. Sci.,vol. 172, pp.385–393 ,2016.

13. Yu, S., Zhou, W., Jia, W., Guo, S., Xiang, Y. and Tang, F., Discriminating DDoS attacks from flash crowds using flow correlation coefficient. IEEE Trans. Parallel Distrib. Syst. vol.23, no.6, pp. 1073–1080, 2012.

14. Zhijun Wu, Liyuan Zhang and Meng Yue , Low-Rate DoS Attacks Detection Based on Network Multifractal, IEEE Transactions on Dependable and Secure Computing, vol.13, Issue.5, 2016 .

15. Chaitanya Buragohain and Nabajyoti Medhi , FlowTrApp:An SDN based architecture for DDoS attack detection and mitigation in data centers, IEEE Conference on Signal Processing and Integrated Networks (SPIN), 2016.

16. P. Xiao, W. Y. Qu, H. Qi, and Z. Y. Li, Detecting DDoS attacks against data center with correlation analysis, Computer Communications, vol. 67, pp. 66–74, 2015.

17. Tomasz Andrysiak, Łukasz Saganowski and Michał Choraś, DDoS Attacks Detection by Means of Greedy Algorithms, Image Processing and Communications Challenges 4, Advances in Intelligent Systems and Computing ,vol.184, pp 303-310, 2013..

18. Andom Ain and Monowar H. Bhuyan, Rank Correlation for Low-Rate DDoS Attack Detection: An Empirical Evaluation, International Journal of Network Security, Vol.18, no.3, pp.474-480, 2016.

19. Zhang Sheng , Zhang Qifei , Pan Xuezeng and Zhu Xuhui, Detection of Low-rate DDoS Attack Based on Self-Similarity Sign In or Purchase, Education Technology and Computer Science (ETCS), 2010.

20. Hamedi-Hamzehkolaie M., Shamani M. J. and Ghaznavi-Ghoushchi, M. B., Low Rate DOS Traceback Based On Sum of Flows. In Proceedings of the Sixth International Symposium on Telecommunication, IST 2012.