A Time Oriented Flow Inference Model Based on Low Rate DDoS Attack Detection for Improved Network Security

*A. Surendar, S. K. Sadulla

Department of Electronics and Communication Engineering, [2] Vignan's Foundation for Science, Technology & Research, University, Vadlamudi-522 213, Guntur, A.P, India
*corresponding Author, Email: surendararavindhan@ieee.org

***Abstract* - Modern network services can be accessed through a number of devices. Any network can present a number of services towards various approached to support network users. The users of the network could access the services to complete their required individual task. However, the network services provided face serious challenges from malicious users. The Distributed Denial of Service, DDoS, attack is a major challenge which can be initiated from various nodes of the network in a distributed manner. There are a number of approaches available to handle the issue of low rate attack but suffer to achieve higher performance. Towards this end, a novel efficient time oriented flow inference model is presented in this paper. The method monitors the flow of packets in the network and logs them to the database. Based on the log available and the flow of current time window, the method performs inference on the current packet to identify the presence of low rate attack. The method estimates the trust weight for the incoming packet to perform low rate attack detection. The proposed method improves the performance of low rate attack detection and reduces the false ratio.**

Keywords - Low Rate Attack, DDoS attack, Flow Inference Model, Time Orient Approach, Network Security.

I. INTRODUCTION

The development of information technology has opened the gate for the users to access various services through number of devices like mobiles, PDA and so on. However, the service accessed by the user has been transferred in form of data packets. The packets generated has been transmitted through number of intermediate nodes. On the fly, the packets would face different type of threats. The presence of malicious node would perform different threat to the network packets. In simple case, the malicious node would drop the packet without knowing anything as eavesdrop attack. On the other side, the malicious node would modify the network packet data to perform modification attack. More than these attacks, the malicious node would involve in Distribute Denial of Service Attack to degrade the performance of the network or the service.

The DDoS attack is performed by more than one nodes which are located in a distribution location of the network. The malicious nodes would generate packets in huge number towards the service point which will be automatically discarded by the service node because of the capacity issue. This type of attack would spoil the generic packet to be delivered to the service point. Similarly, the DDoS attacks can be performed based on the connection strategy.

Unlike the generic DDoS attack, the malicious node would not perform with large number of malicious packets towards the service point. The low rate attacks are one which are generated in low frequency and in general way such low rate attacks cannot be identified. But even the presence of low rate attacks would affect the performance of the networks. Flow inference is the way of identifying the presence of low rate attack according to the flow of packets. Any service would be accessed by different users at each time window. So the number of times the service being accessed would vary at each time window. By analyzing the flow features of any network service, the presence of low rate attack can be identified. This paper present such a flow inference model towards the detection of low rate attack in the networks. The detailed approach is discussed in the next section.

II. RELATED WORKS

There exist numerous techniques to perform low rate attack detection. This section briefs set of approaches towards the detection of low rate attacks. A self-similarity based low rate attack detection algorithm is presented in [1]. The method estimates the trust measure based on Hurst coefficient to detect DDoS on Low-rate. The method has been proposed towards the detection of low rate attack in real time traffic.

In [2], a packet size based low rate attack detection has been presented. The method estimates the distribution size of in various threats like pulsing, constant attack with legitimate traffic. According to the packet size of legitimate traffic, the presence of low rate attack has been identified.

The presence of low rate attack in the web traffic has been detected based on the frequency vectors in [3]. The

method estimates the real time frequency vector of web traffic and based on that the presence of low rate attack detection has been performed.

An mathematical model has been presented in [4] to handle the problem of low rate attack. The method identifies the size of congestion window in TCP packets and based on that the presence of low rate attack is performed. In [5], the traffic pattern has been used as the key to perform low rate attack detection. The method maintains the traffic pattern of various traffic like genuine and malicious. Based on the pattern of the traffic the presence of low rate attack has been identified.

An entropy measure has been adapted to the problem of low rate attack detection in [6], which present a method named ELDAT which uses entropy measure in a extended manner with lightweight. The method uses the covariance measure of both legitimate and malicious traffic values to perform low rate attack detection.

The information metric has been used as the key in the detection of low rate attack in [7]. The method uses the information distance and the entropy values to perform low rate attack detection.

In [8], the multi fractal de-trended fluctuation analysis (MF-DFA) is used to perform low rate attack detection. The method uses wavelet analysis to identify genuine and malicious traffic in the system which has been used to perform low rate attack detection. In [9], the granular computing with entropy measure has been used to perform low rate attack detection. In [10], the RED algorithm with Fourier robust has been adapted to perform low rate attack detection which computes the PSD entropy to perform low rate attack detection. The method also uses the active queue management for the support of detection. In [11], the fast decision tree has been used to perform low rate attack detection.

The correlation measure has been used to perform low rate attack detection in [12]. The method uses both spearmen and partial rank measures in detecting the low rate attack. An multi classifier algorithm for low rate attack detection is presented in [13], which generates ensembles of network traffic. The same has been used to perform classification and uses SVD technique to perform classification.

The correlation analysis with k-nearest neighbor approach is presented in [14]. The method estimates correlation measures with each sample of the traffic with the incoming traffic which has been used to perform classification. For the same purpose, in [15], the same correlation measure has been used for low rate attack detection where the decision has been enforced with artificial neural network.

From the above survey, it is noticeable that the methods suffer to achieve higher performance in low rate attack detection and needs certain strategic approach.

III. TIME ORIENTED FLOW INFERENCE MODEL

The method receives the incoming packet and extracts the packet features like the source node details, and from the network trace the method identifies the list of packets from the same source. Based on them, the method perform inference on the flow of packets from the same source node. Then a trust weight has been measured for the received packet which has been used to perform conclusion on the packet. The detailed approach is discussed in this section.

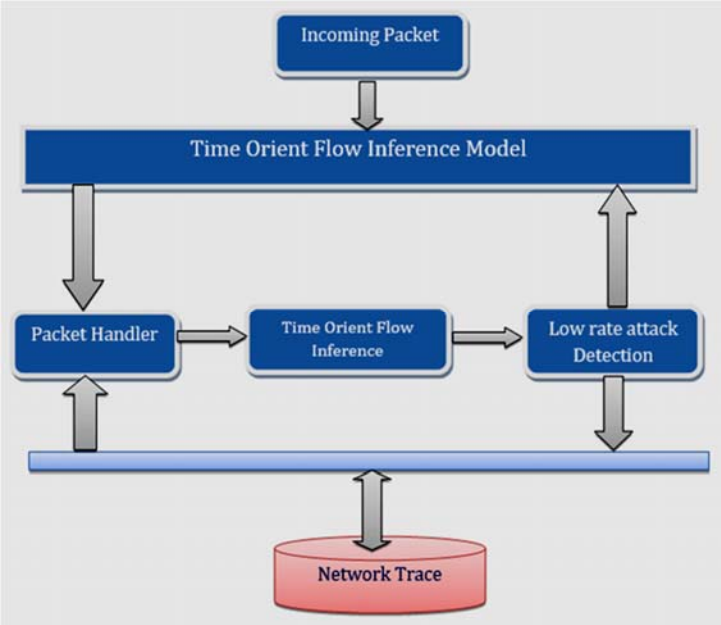


Figure 1: Architecture of Time orient Flow Inference Model

The Figure 1, shows the architecture of time orient flow inference model and its functional components. Each functional component has been discussed in detail in this section.

A. Packet Handler

The packet handler is responsible for the reception of the packet. Whatever the packet being destined towards the service point has been received by the packet handler. The received packet has been extracted for various information like Source Address, Source Port, Payload, Hop Count and so on. The extracted features has been used to perform inference to conclude the trustworthy of the packet.

Algorithm:

Input: Packet P
Output: Feature Set Fs
Start
  Read input packet P.
  Source Address SA = Extract source address from packet P as P.SourceAddress.
  Source Port Sp = Extract source port from packet P.
    Sp = $Source\ Port \in P$
  Estimate payload Pl = $\sum Bytes \in P$
  Compute hop count Hp = $\sum Distinct(Hops) \in P$
  Generate Feature set Fs = {SA,SP,Pl,Hp}
Stop

The above discussed algorithm shows how the feature of the packet has been extracted and converted into feature set.

B. Time Orient Flow Inference

In this stage, the method reads the network trace and the feature set. Based on the details of feature set, the method identifies and extracts the traces belongs the service point and source. The extracted trace has been split into number classes according to the time window. Third for each time window, the method estimates the flow factor and for the current time window it has been measured. Finally using the flow factor, the method estimates the trust weight for the incoming packet. Estimated trust weight has been used to perform low rate attack detection.

Algorithm:

Input: Feature Set Fs, Network Trace Nt.
Output: Trust weight Tw
Start
  Read feature set Fs and trace Nt.
  Identify the traces generated based on the source of feature set.
  User Trace Ut = $\sum_{i=1}^{size(Nt)} NT(i).Source == Fs.Source$
  Split the trace into different time window.
  For each time window Ti
    Time window Trace Twt = $\sum_{i=1}^{Size(Ut)} UT(i).Time == Ti$
    Compute Flow factor Flf = $Size(Twt) / size(Ut)$
  End
  Compute average flow factor Aff = $\frac{\sum_{i=1}^{size(Time\ window)} Flf}{size(Tw)}$
  Compute flow factor of current time window Cff.
    Cff = $\sum_{i=1}^{Size(Ut)} UT(i).Time == CT / size(Ut)$
  Compute trust weight Tw = $\frac{Cff}{Aff}$
Stop

The above discussed algorithm estimates the trust weight for the packet based on the flow features of the packets received. The estimated trust weight has been used to perform low rate attack detection.

C. Low Rate Attack Detection

The presence of low rate attack has been performed based on the result of flow inference. To perform this, the method receives the packet through the packet handler. Then the method estimates the trust weight though time orient flow inference model. Based on the trust weight estimated, the method decides the packet status as genuine or malicious.

Algorithm:

Input: Network Trace Nt
Output: Null
Start
  Read Network Trace Nt
  While true
    P=Receive incoming packet through packet handler
    Tw = Time orient flow inference (P)
    If Tw>Th then
      Genuine
    Else
      Malicious
    End
  End
Stop.

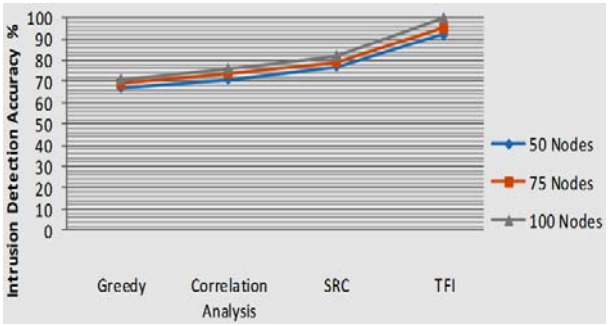
The above discussed algorithm estimates the trust weight for the incoming packet and based on that the method concludes whether the packet is genuine or malicious.

IV. RESULTS AND DISCUSSION

TABLE 1: DETAILS OF SIMULATION

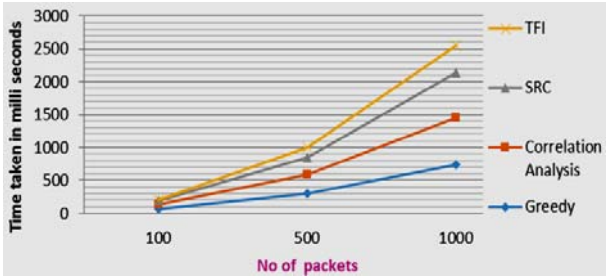
Parameter	Value
Protocol Name	TFI
Number of Nodes	100
Simulation Time	10 Minutes
Tool Used	Advanced Java

The Table 1, shows the simulation details being used to evaluate the performance of the proposed time orient traffic inference model for low rate attack detection.



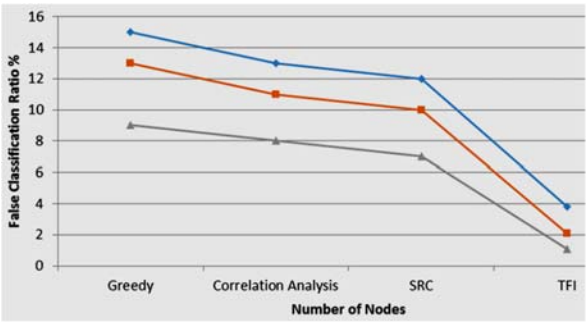
Graph 1: shows the Intrusion Detection Accuracy of malicious packet.

Graph 1, present the comparative result of accuracy in low rate attack detection and shows that the proposed TFI algorithm has produced higher accuracy than other methods.



Graph 2: shows the Time Complexity of the proposed system.

The graph 2 shows the time complexity of the proposed system compare to other methodologies. It shows clearly that the proposed system takes only little time compare to other methods for different number of packets.



Graph 3. Comparison on False Classification Ratio.

The ratio of false classification has been measured for the proposed TFI algorithm and has been compared with the result of other methods. It is highly noticed that the proposed TFI algorithm has produced less false ratio than other methods.

V. CONCLUSION

This paper presented a time oriented flow inference model for the detection of low rate DDoS attacks in any network. The method monitors the network traffic and extracts various features. Then based on the features extracted, the network trace is split into a number of time windows. For each time window the method estimates the trust weight for the user based on the number of access and flow features. Finally a single trust weight is estimated which is used to classify the network packet and to perform low rate attack detection. Our proposed method has been shown to produce higher performance in low rate attack detection up to 96%.

REFERENCES

1. Zhang Sheng, Detection of Low-rate DDoS Attack Based on Self-Similarity, IEEE Educational technology and computer science, 2010.
2. Lu Zhou, Low-Rate DDoS Attack Detection Using Expectation of Packet Size, Hindawi, security and Communication Networks Vol. 2017,2017.
3. W. Zhou, W. Jia, Detection and defense of application-layer DDoS attacks in backbone web traffic, Future Generation Computer Systems, vol. 38, pp. 36–46, 2014.
4. J. Luo, X. Yang, J. Wang, On a mathematical model for low-rate shrew DDoS, IEEE Information Forensics and Security, vol. 9, no. 7, pp. 1069–1083, 2014.
5. T. Thapngam, S. Yu, Distributed Denial of Service (DDoS) detection by traffic pattern analysis, Peer-to-Peer Networking and Applications, vol. 7, no. 4, pp. 346–358, 2014.
6. 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.
7. Yang Xiang, Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics, IEEE Information forensic and security, vol.6, issue 2, 2011.
8. Zhijunwu, Low-Rate DoS Attacks Detection Based on Network Multifractal, IEEE Dependable and Secure Computing, Vol.13, Iss. 5, 2016.

9. Suleman Khan, Abdullah Gani, Feature Selection of Denial-of-Service Attacks Using Entropy and Granular Computing, Arabian Journal for Science and Engineering, Vol 43, Iss. 2, pp 499–508, 2018.
10. Chen, Zhaomin, et al. FRRED: Fourier robust RED algorithm to detect and mitigate LDoSattacks.,ZINC, 2017.
11. RabiaLatif, Haider Abbas, Analyzing Feasibility for Deploying Very Fast Decision Tree for DDoS Attack Detection in Cloud-Assisted WBAN, Springer, Intelligent Computing theory, vol. 8588, pp 507-519, 2014.
12. Andom Ain1 , Monowar H. Bhuyan1, Rank Correlation for Low-Rate DDoS Attack Detection: An Empirical Evaluation, IJNS Vol.18, No.3, PP.474-480, 2016
13. Bin Jia, Xiaohong Huang, A DDoS Attack Detection Method Based on Hybrid Heterogeneous Multiclassifier Ensemble Learning, JECE,Vol 2017, 2017.
14. 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
15. Alan Saied, Detection of known and unknown DDoS attacks using Artificial Neural Networks, Elseveir, Nuro Computing, vol 172, issue 8, pp:385-393,2016.