Journal of Ambient Intelligence and Humanized Computing
https://doi.org/10.1007/s12652-020-02744-y

ORIGINAL RESEARCH

# Low rate DDoS mitigation using real-time multi threshold traffic monitoring system

**M. Baskar[1] · J. Ramkumar[1] · C. Karthikeyan[2] · V. Anbarasu[1] · A. Balaji[3] · T. S. Arulananth[4]**

Received: 15 August 2020 / Accepted: 21 November 2020


**Abstract**
The low rate distributed denial of service (DDoS) attack has been identified as most vulnerable to the network services which has been studied recently. The approaches consider only the high rate DoS attacks and ignore rest in low rate. The existing techniques suffer with poor detection of low rate attacks as they consider only limited features of network traffic. Variety of techniques mitigate such threats using different parameters like amount of data in service packet as payload, number of intermediate nodes, and so on. The previous techniques struggle to detect and mitigate them in efficient way. Towards improving the detection and mitigation performance of low rate threats, the author presents a novel real time traffic monitoring algorithm which uses multi threshold traffic analysis. By considering the payload, hop count, latency, packet counts, the method analyzes the real time traffic. Using the features obtained from the traffic, the method computes the low rate threat measure. Based on computed threat measure, the packets trustworthy have been validated. The method produces higher detection rate in low rate DDoS attack detection and produces efficient results.

**Keywords** Network services · DDoS attack · Low rate attack · Traffic monitoring · Multi threshold analysis

## 1 Introduction

The network communication has been used to access various services provided in the network by various providers. The services are allowed to access for users by generating the service request. The service request has been converted into network packets and transferred through number of intermediate nodes. Because of the service has been available in a network node which may be far away from the user node, it has to be transferred by the intermediate nodes to access the service in success. It is not necessary that all the nodes of the network to be genuine and there may be a presence of malicious nodes in the route of data transmission.

The presence of malicious node introduces various threats to the network services. The presence of malicious node allows analyzing the network service and would perform various malicious activities. The malicious node would perform the network threat in various ways like, Eavesdrop- the packets received towards the servicing node would be simply dropped without mercy, Modification- the malicious node would change the data present in the packet before forwarding, routing attack- the malicious node would perform

✉ J. Ramkumar
ram.kumar537@gmail.com

M. Baskar
baashkarcse@gmail.com

C. Karthikeyan
ckarthik2k@gmail.com

V. Anbarasu
anbarasukv@gmail.com

A. Balaji
balajia1981@gmail.com

T. S. Arulananth
arulanandh.ts@gmail.com

[1] Department of Computer Science and Engineering, School of Computing, College of Engineering and Technology, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, Tamilnadu 603 203, India

[2] Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Deemed To Be University, Vaddeswaram, Guntur, Andhra Pradesh, India

[3] Department of Computer Science and Engineering, KCG College of Technology, Karapakkam, Chennai 600 097, India

[4] Department of Electronics and Communication Engineering, MLR Institute of Technology, Hyderabad, Telangana 500 043, India

Published online: 02 January 2021

routing against the policy of routing protocol. More than this, the DDoS attacks has been generated by the malicious nodes by sending enormous number of packets towards destination at which point service is running with the intension to reduce the service performance. Similarly, the malicious node would send the packets with the higher payload to occupy the entire bandwidth capacity. In earlier scenario, the node tries to occupy the whole capacity of the server and in the second case the malicious node tries to occupy the entire capacity of the network bandwidth. In both the cases, the genuine node has been stopped in accessing the service and affects the service performance.

The DDoS attacks can be identified by monitoring the network traffic in efficient manner. But the presence of low rate attack which is not generated in a consistent manner cannot be identified easily. The low rate attacks are generated by the genuine nodes in a sparse timing and in a least amount. But the intension is same as the malicious node and has to be stopped to improve the service performance. The low rate attacks can be identified with the help of traffic information like payload feature, hop count, latency and number of packet transmission. Number of techniques exists towards mitigating such threats by using payload value and some other would use hop count or other features. However, the does not succeed with the detection of threat in efficient way.

With the motivation to improve the performance in low rate attack detection, a multi threshold traffic monitoring algorithm is presented. The algorithm uses various thresholds in identifying the low rate attacks. With the help of traffic features discussed earlier the method performs traffic analysis and estimates trustworthy measure to perform low rate attack detection.

## 2 Related works

The researchers have discussed several techniques in mitigating the low rate DoS threats. This section explores different approaches towards the problem.

Ain et al. (2016) presented a rank based correlation algorithm towards the detection of low rate Dos attacks, which uses partial and spearman rank correlation measures to detect malformed node. Bhuyan et al. (2015) evaluates different measures and metrics of low rate attack detection like entropy, general entropy, shanon, Hartley entropy. According to the value of different entropy measures, the performance of the approach in the detection has been computed. Bhuyan et al. (2013) discussed a comprehensive survey on denial of service attack tools. The tools has been validated their performance in detecting such threats in Wireless Network.

Bhuyan et al. (2014) analyzed various anomaly detection approaches and recommends different tools toward detecting anomaly in network traffic. Zhang et al. (2010) presented a Hurst coefficient based denial of service attack detection towards low frequency DDoS attacks. The method has produced impacting result in the detection of low rate attacks. Jia et al. (2017) presented a multi classifier heterogeneous ensemble learning approach which uses the SVD technique for the construction of intrusion detection system. The method produces efficient result in detecting such threats.

Luo et al. (2014) presented a mathematical model distributed denial of service attack. The method tracks the behaviors of different victims involved in congestion attack. Based on that the mathematical model performs low rate attack detection. Xiao et al. (2015) classifies incoming data flow with correlation analysis. For the similarity measurement, the k-nearest neighbor algorithm has been used. The grid based approach has been used for training and for the evaluation the same has been used.

Mao et al. (2014) presents a ensemble based multi-classifier approach which combines SVM and Kernel Matching Pursuit Ensemble (KMPs). SVM has been used to construct the trainer and KMP has been used for the evaluation. Hamedi-hamzehkolaie et al. (2012a) presented an ant colony based intrusion detection algorithm. The method uses the network traces collected and based of the flow of packets which is varying, the intrusion detection is performed.

Hamedi-Hamzehkolaie et al. (2012b) presented a trace based approach which measure sum of flows in specific time to detect the threat. The sum of flow defines the number of packets has been sent by any node considered. Andrysiak et al. (2013) A greedy based DDoS attack detection scheme which measure the similarity according to the matching and orthogonal matching schemes. According to the tree structure generated by the algorithms the detection has been performed.

Alomari et al. (2012) presented a detailed survey on the methods available for the detection. The method monitors the application layer traffic and discusses how it can be analyzed to perform DDoS attack detection. Latif et al. (2014) presented an cloud based decision tree approach towards DDoS attack detection. The methods read the network

streams through sensors and analyze them for denial of service attack detection.

Suchithra and Baska (2020) presented a network condition based low rate attack detection approach in multimedia networks which consider the network conditions like traffic, latency, number of routes available and other conditions in finding low rate attack. Baskar et al. (2018) sketch the application of time variant predicate based approach towards low rate attack detection by approximating the traffic in the network.

Baskar et al. (2017a) presents a low rate attack detection scheme which consider the region specific traffic features and its impact in identifying the low rate attacks in detail. Baskar et al. (2017b) performs low rate attack detection by combining different approximation models which analyzes the payload, traffic, route features.

The techniques discussed above introduce poor performance in detecting DDoS low rate attacks which encourages the design of novel scheme to be framed.

## 3 Real time multi threshold traffic monitoring

The real time multi threshold traffic monitoring algorithm reads the network traffic and log. Using the log available the method splits the entire log into different class as based on their time frame. Then for each time frame for the same user, the number of access made, the payload strategies, hop count strategies and their latency are measured. According to the features estimated and the value computed, the low rate threat measure is computed. Using the measure estimated the low rate attack detection is performed.

The real time multi threshold traffic monitoring based intrusion detection approach uses the huge trace of the network. It is necessary to consider the traces belong to different time window. From the large set of network trace, the traces belong to a specific time window can be identified as follows:

Trace Ts $= \sum_{i=1}^{size(tw)} T(i) \cdot Ti == Ti$, Here Tw represent the number of time window being considered and $Ti$ represent a single instance where $T(i)$ represent the single instance of the time window.

Once the traces belongs to the time window has been separated, then it can be used to extract various features namely payload, hop count and latency. The above mentioned features has been used to construct the feature vector. The feature vectors generated has been used to perform the traffic analysis. The traffic has been analyzed in different ways.

The average payload being sent by different nodes has to be considered. Such average payload has been computed using the below formula.

$$\text{Average payload Apl} = \frac{\sum_{i=1}^{size(pv(Ti))} Pv(i) \cdot payload}{size(pv(Ti))}, \tag{1}$$

where Pv represent the feature vector of any trace and Ti represent the time window trace. The average payload of the time window has been computed using the above equation.

However, not all the nodes use the same route to reach the destination and it depends on the network conditions and the genuine of the node involve in the data transmission. So it is necccessary to consider the hop count in performing traffic analysis.

$$\text{Average hop count Ahcount} = \frac{\sum_{i=1}^{size(pv(Ti))} Pv(i) \cdot hopcount}{size(pv(Ti))}. \tag{2}$$

Similarly the number of access plays the vital role in identifying the malicious access. It can be identified using the below formula.

$$\text{Average access Ava} = \frac{size(pv(Ti))}{Numberofusers}. \tag{3}$$

The latency of the packet increases when the middle nodes involve in denial of service attack or any kind of modification. This increases the latency and increases the entire data transmission's latency. It can be computed using the below formula.

$$\text{Average latency Al} = \frac{\sum_{i=1}^{size(pv(Ti))} Pv(i).latency}{size(pv(Ti))} \tag{4}$$

Using the above features considered, the method can compute the threat weight for the packet received. It can be computed as follows:

$$\text{Lrth} = \frac{(Uapl > Apl \&\& Uapl < P.pl)?1 : 0}{Una} \times \frac{(Uahc > Ahcount \&\& Uahc < P.hc)?1 : 0}{Una} \times \frac{(Ulat > Al \&\& Ulat < P.lat)?1 : 0}{Una}, \tag{5}$$

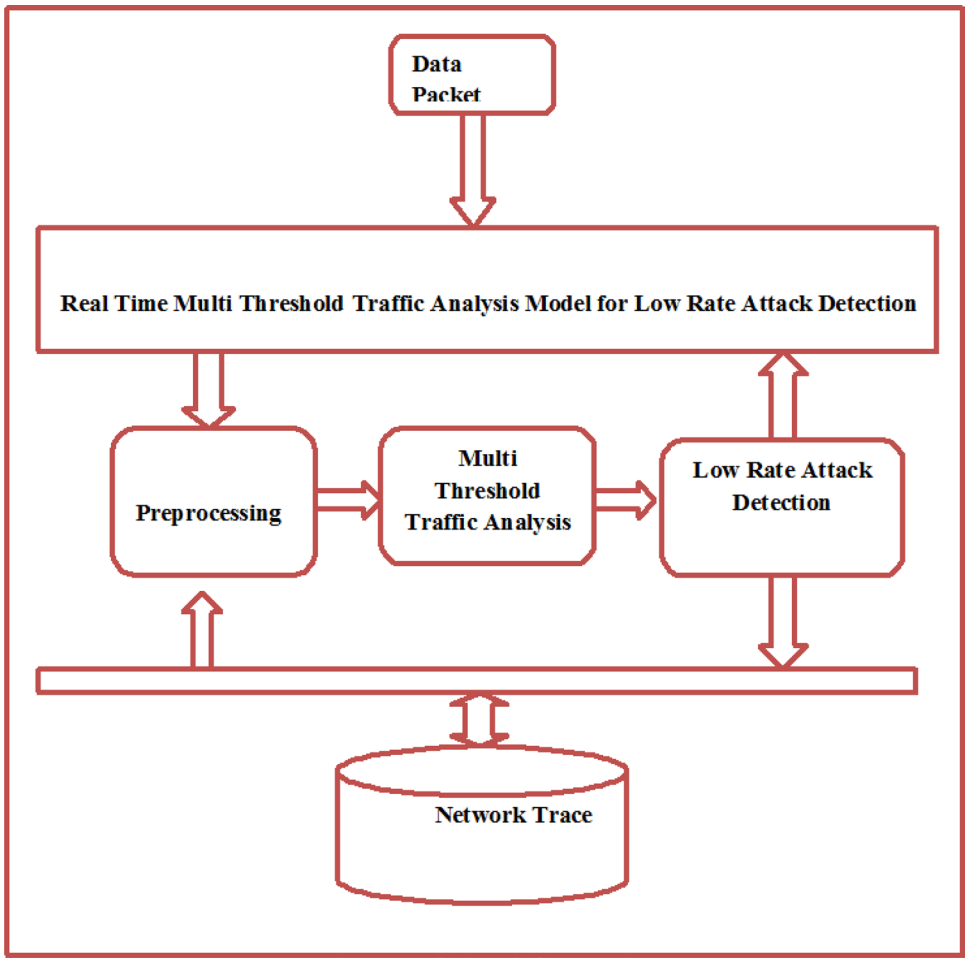



**Fig. 1** Architecture of multi threshold traffic analysis

here Uapl- user average payload, Uahc-user average access count, Ulat- latency.

The estimated, threat weight has been used to perform the denial of service attack detection.

The functional architecture of proposed multi threshold traffic analysis based approach is presented in Fig. 1. The functional components of the model are detailed in this section.

### 3.1 Preprocessing

In this stage, the traces generated by earlier access has been taken and split according to the time stamp they generated. For each time stamp, the logs generated at the time are identified and split into separate group. Then from the logs the method, extracts different features from the log and convert them into feature vector. The extracted features have been applied with traffic analysis to support the mitigation process.

**Algorithm:**

Input: Network Trace Nt.

Output: Preprocessed feature vector Pv.

Start

Read network trace Nt.

Trace T = $\sum Traces \in Nt$

Initialize time window Tw.

Tw = $\sum Time$ - $Window@Total$ - $Time$

Identify and split the entire trace into time window based.

For each time window Ti

Trace Ts = $\sum_{i=1}^{size(tw)} T(i).Ti == Ti$

For each trace Tsi

Extract user Uid = Tsi.Uid

Extract Payload Pl = $size(Tsi(data))$

Extract hop count hc = $\sum Hops \in Tsi(route)$

Compute latency l = hc×μ

Generate feature vector Fv = {Uid, Pl, hc, l}

End

Compute total number of access Ta = size(Ts)

Add feature vectors to preprocessed vector.

End

Stop.

The preprocessing algorithm reads the network trace and split them into number of time stamp. The number of time window is generated by computing the oldest log time available and the current time. The number of time window is computed by splitting the entire time into number of equal duration. In each time stamp log, the features are extracted and utilized to perform analysis to support DDoS attack detection.

## 3.2 Multi threshold traffic analysis

The multi threshold traffic analysis algorithm analyzes the traffic in different way. The user would access the service in a generic way in different time window. They would perform service access in a reasonable number of times and the number of access will be in a limit. But the number of access will vary between time windows. The number of access is highly depending on the time window in which the service being access. According to this, the access pattern also varies between time windows. The multi threshold traffic analysis algorithm, reads the preprocessed feature vector and from them, it computes the number of access, average payload being submitted, average latency being introduced and average hop count being used. The same has been computed for overall users. Based on the values of single user and the other user in the same window, the method estimates the low rate threat weight and based on that a single Boolean will be returned.

**Table 1** Details of Simulation

| Key | Value |
|---|---|
| Protocol name | MTTA |
| Number of nodes | 100 |
| Simulation time | 10 min |
| Tool | Advanced Java |

**MTTA Algorithm:**

Input: Preprocessed feature vector Pv, Packet vector P.

Output : Boolean

Start

Read feature vector pv.

For each time window Ti

Compute average payload Apl = $\frac{\sum_{i=1}^{size(pv(Ti))} Pv(i).payload}{size(pv(Ti))}$

Compute average hop count Ahcount = $\frac{\sum_{i=1}^{size(pv(Ti))} Pv(i).\text{hop}count}{size(pv(Ti))}$

Compute average access Ava = $\frac{size(pv(Ti))}{Number\ of\ users}$

Compute average latency Al = $\frac{\sum_{i=1}^{size(pv(Ti))} Pv(i).latency}{size(pv(Ti))}$

Identify logs of user Ul = $\sum_{i=1}^{size(pv(Ti))} Pv(i).uid = Uid$

Compute user average payload Uapl = $\frac{\sum_{i=1}^{size(Ul} Ul(i).payload}{size(Ul)}$

Compute user average hop count Uahc = $\frac{\sum_{i=1}^{size(Ul} Ul(i).\text{hop count}}{size(Ul)}$

Compute number of access Una = size(ul)

Compute latency of user Ulat = $\frac{\sum_{i=1}^{size(Ul)} Ul(i).latency}{size(Ul)}$

End

Compute low rate threat weight Lrth.

Lrth= $\frac{(Uapl > Apl \,\&\&\, Uapl < P.pl)?1:0}{Una} \times \frac{(Ua\text{hc} > A\text{hcount} \,\&\&\, Ua\text{hc} < P.\text{hc})?1:0}{Una} \times \frac{(Ulat > Al \,\&\&\, Ulat < P.lat)?1:0}{Una}$

//where p.pl – payload of packet. P.hc – hop count of packet, p.lat – latency of packet.

If Lrth>Th then

Return true.

Else

Return false.

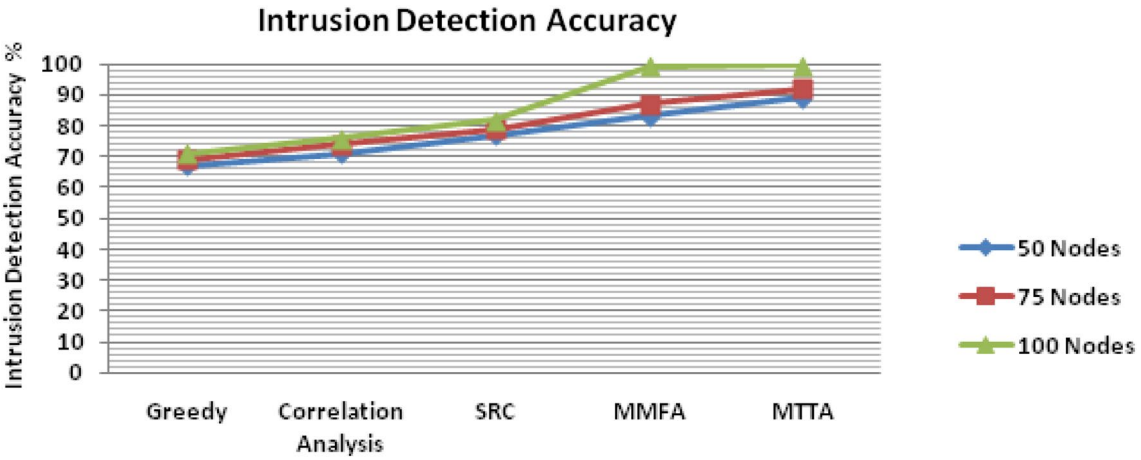
End

Stop.

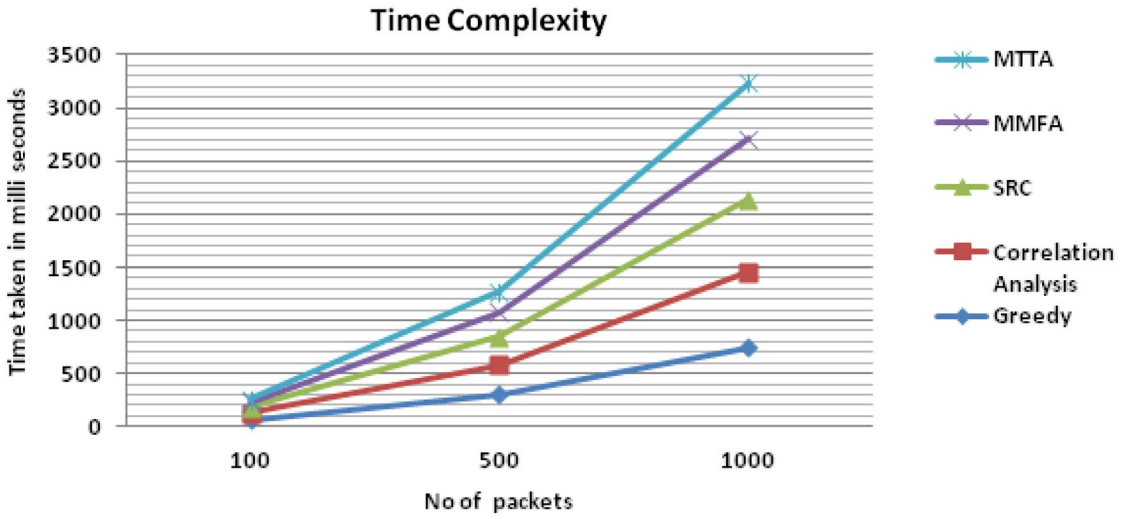
The algorithm presented above reads the preprocessed network feature vector and estimates various measures based on the entire time window log and user orient log. Using the feature estimated the method compute the low rate threat weight and based on that the user trustworthy has been defined. For each time weight the method computes the value of payload, hop count, latency, access and so on. According to the average values of different features, the value of low rate threat weight is measured. If the current value of any feature less than the average value of feature, then a binary 1 is assigned otherwise a binary 0 is assigned to the condition. By assigning the binary values for different conditions the method would compute the low rate threat weight.

**Table 2** Analysis on different performance metrics

| Protocol | Intrusion detection accuracy % | | | False classification ration | | | Time Complexity in Milli seconds | | |
|---|---|---|---|---|---|---|---|---|---|
| | 50 packets | 75 packets | 100 packets | 50 packets | 75 packets | 100 packets | 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 |



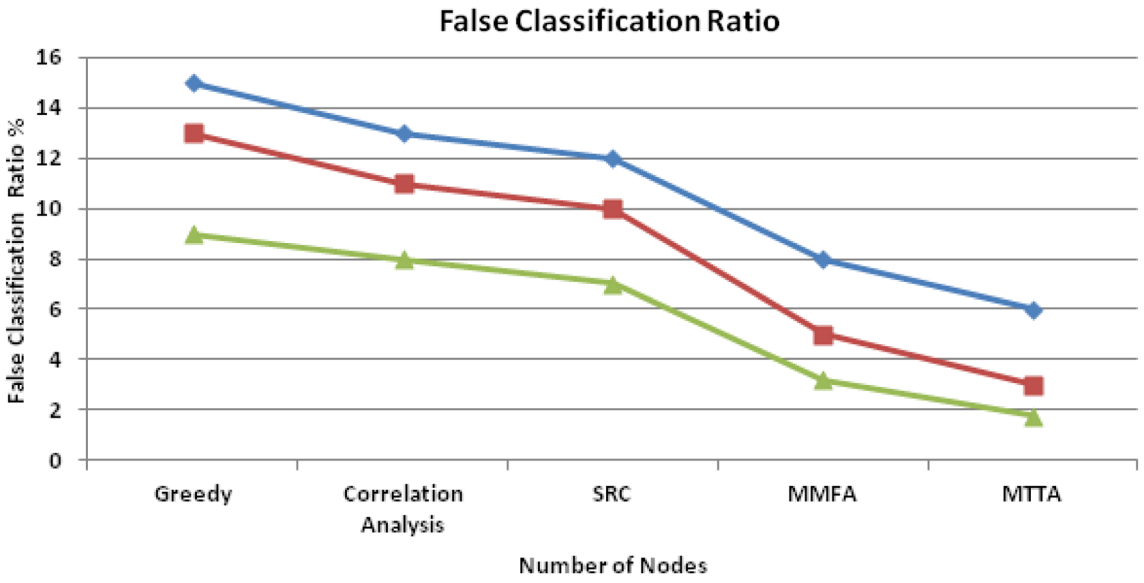

**Graph 1** Analysis on intrusion detection accuracy




**Graph 2** Analysis on time complexity

### 3.3 Low rate attack detection

The multi threshold traffic analysis model performs the detection of low rate attack according to the measures estimated on different time stamp. The user would access the service in particular strategy in each time window but they would perform attack by introducing low level threats. By monitoring the network traffic it can be identified. In this approach, the network traffic has been read and extracts the features in different time window. Using the feature vector belongs to different time window, the method computes various measures like average hop count, payload, latency in




**Graph 3** Analysis on false classification ratio

particular time window. Based on the average values a low rate attack weight has been computed. Based on the value estimated the traffic analysis model return a Boolean value towards the trustworthy of the packet.

**Algorithm:**

Input: Network Packet p, Network Trace Nt

Output: Null

Start

Read network trace Nt.

Pv = Perform preprocessing (Nt).

Boolean b = MTTA (pv,p )

If true

Genuine packet

Else

Malicious

End

Stop.

The attack detection algorithm extracts the packet feature and performs preprocessing. The preprocessed vector has been used to perform multi threshold traffic analysis. Based on the result of traffic analysis the method accepts or deny the packet.

## 4 Result and discussion

The proposed multi threshold traffic analysis (MTTA) approach is implemented using Advanced Java and their performance in mitigating the low rate attacks are monitored and compared with the performance of other methods. The results obtained are presented in this section.

The details of simulation being used to evaluate the performance of proposed MTTA algorithm has been presented in Table 1. According to these details, the methods are evaluated for their performance and presented in this section.

The performance on various performance metrics are measured and compared in Table 2. The proposed MTTA approach has produced higher performance in all the conditions of simulation than other methods (Graph 1).

The accuracy on detecting intrusion attack or low rate attack are measured for different methods by varying the number of packets. In each case, the proposed MTTA approach has produced higher detection accuracy compare to other methods. The proposed MTTA approach has been evaluated for its intrusion detection accuracy at different number of nodes in simulation which yield 89%, 92% and

99.7% in 50 nodes, 75 nodes and 100 nodes in the simulation. Inclusion of MTTA approach in low rate attack detection has supported the improvement of intrusion detection accuracy. As the intrusion detection is performed by measuring low rate threat weight according to different feature values and decides the genuine of the packet according to the threshold used, the performance of intrusion detection gets increased (Grapgh 2).

The value of Time complexity in detecting the attack and classifying the incoming packet has been measured for different methods. The proposed MTTA algorithm has produced less time complexity than any other method compared in each test case. The proposed MTTA approach has produced the result with the time complexity of 31, 192 and 520 s in classifying 100, 500 and 1000 packets.

The ratio of false classification introduced by different methods are measured in different test cases like 100, 500 and 1000 packets are measured and compared in Graph 3. The proposed MTTA approach has produced the false ratio in the ratio 6%, 3% and 1.8% in classifying 100, 500 and 1000 packets. The proposed MTTA approach has produced less false ratio compare to other methods.

## 5 Conclusion

Thus the paper, an efficient real time multi threshold traffic analysis model is presented. The method reads the network trace and split them into number of time window based. At each time window logs, the method extracts various features of the log and converts them into feature vector. Using the feature vector available, the method computes the average values of hop count, payload, number of access and latency. The computed values with the packet feature have been used to estimate the low rate threat weight for the packet received. The weight has been estimated based on various thresholds and computed value has been used to perform classification of the packet. The method produces efficient results in attack detection and improves the performance as well. The proposed MTTA approach has produced intrusion detection accuracy up to 99.7% with the false ratio of 1.8% and the time complexity is greatly reduced than other methods. Further, the method of intrusion detection could be carried forward by incorporating behavior and strike analysis of network services and their features.

## References


Ain A, Bhuyan MH (2016) Rank correlation for low-rate DDoS attack detection: an empirical evaluation. Int J Netw Secur 18(3):474–480

Baskar M, Gnansekaran T (2017a) Developing efficient intrusion tracking system using region based traffic impact measure towards the denial of service attack mitigation. J Comput Theor Nanosci 14(7):3576–3582

Baskar M, Gnansekaran T (2017b) Multi model network analysis for improved intrusion tracing towards mitigating DDoS attack. Asian J Res Soc Humanit 7(3):1343–1353

Baskar M, Gnansekaran T, Frank-Vijay J (2018) Time variant predicate based traffic approximation algorithm for efficient low rate DDoS attack detection. Taga J Graph Technol 14(208):352–368

Bhuyan MH, Kashyap HJ, Bhattacharyya DK, Kalita JK (2013) Detecting distributed denial of service attacks: methods, tools and future directions. Comput J 57(4):537–556

Bhuyan MH, Bhattacharyya DK, Kalita JK (2014) Network anomaly detection: methods, systems and tools. IEEE Commun Surv Tutor 16:303–336

Bhuyan MH, Bhattacharyya DK, Alita JK (2015) An empirical evaluation of information metrics or low-rate and high-rate DDoS attack detection. Pattern Recogn Lett 51:1–7

Esraa A, Manickam S, Gupta BB, Karuppayah S, Alfaris R (2012) Article: Botnet-based distributed denial of service (DDoS) attacks on web servers: classification and art. Int J Comput Appl 49(7):24–32

Hamedi-hamzehkolaie M, Shamani MJ, Ghaznavi-ghoushchi MB (2012a) Article: Ant colony traceback for low rate DOS attack. IJCA Special Issue on Computational Intelligence & Information Security CIIS(1):22–26

Hamedi-Hamzehkolaie M, Shamani MJ, Ghaznavi-Ghoushchi MB (2012b) Low Rate DOS traceback based on sum of flows. In: Proceedings of the Sixth International Symposium on Telecommunication, IST 2012

Jia B, Huang X, Liu R, Ma Y (2017) A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning. J Electr Comput Eng 2017

Luo J, Yang X, Wang J, Xu J, Sun J, Long K (2014) On a mathematical model for low-rate shrew DDoS. IEEE Trans Inf Foren Secur 9(7):1069–1083

Mao SS, Xiong L, Jiao LC, Zhang S, Chen B (2014) Isomerous multiple classifier ensemble via transformation of the rotating forest. J Xidian Univ 41(5):48–53

Rabia L, Abbas H, Assar S, Latif S (2014) Analyzing feasibility for deploying very fast decision tree for DDoS attack detection in cloud-assisted WBAN. Springer Intell Comput Theory 8588:507–519

Suchithra M, Baskar M, Ramkumar JP, Kalyanasundaram B, Amutha (2020) Packet feature with network conditions for efficient low rate attack detection in multimedia networks for improved QoS. J Ambient Intell Human Comput

Tomasz A, Saganowski Ł, Choraś M (2013) DDoS attacks detection by means of greedy algorithms, image processing and communications challenges 4. Adv Intell Syst Comput 184:303–310

Xiao P, Qu WY, Qi H, Li ZY (2015) Detecting DDoS attacks against data center with correlation analysis. Comput Commun 67:66–74

Zhang S, Zhang Q, Pan X, Zhu X (2010) Detection of low-rate DDoS attack based on self-similarity sign in or purchase. Educ Technol Comput Sci (ETCS)