THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

A NOVEL ROUTING MECHANISM USING SNR AND CBDM TECHNIQUE TO DEFEND AGAINST DDOS ATTACK

Sathya Priya[1*] and Bharathi[2]
[1]*Velammal Engineering College, INDIA*
[2]*Panimalar Engineering College, INDIA*

ABSTRACT

The growth of internet technology and increase in network attacks are directly proportional to each other. The internet is always targeted by various types of network threats. Amongst all the other type of attacks, Distributed Denial of Service (DDoS) is considered to be top most network attack. A DDoS attack is an attempt to make a service unavailable or unusable to intend user at intend time and there are no limitations in the number of systems that can launch the attack. Since this type of attack launch attacks by wide range of IP addresses, it is very hard to block and detect at the network firewall level. DDoS attacks remain a serious security problem; the mitigation of threat is very hard to the highly distributed network attacks. In this paper, we proposed DDOS detection using efficient router mechanism with the help of signal to noise ratio deviations and using technique Clustering Based Data Mining (CBDM) to monitor and calculate any deviation from the trained routing data and the same as been alarmed as attack. The evaluation based on anomaly detection using extensive simulations shows effectiveness and low overhead. The proposed work also supports for incremental deployment in real networks.

Published on: 10th– August-2016

KEY WORDS

DDoS, CBDM, Clustering, Anomaly, Score, Multi-Level

INTRODUCTION

The increased development of e-commerce leads to the increased development of security on network resource. DDoS attack aims on total packets on the network, which in turn delay the user from accessing their network resource. The DDoS attack runs on a client machine and tries to compromise other systems in the standard network configurations and makes it as weak configurations.. There are two types of DDoS attack such as flood attack and crash attack. The vast development of internet technology resulted in large scale need of IP routers [1].

Initially attacker tries to gain vulnerabilities of weak network. The attacker tries through computer systems network port to gain unauthorized access. The number of ports that are open, means there are more chance of entry into the network. The compromised machines are now instructed to control another set of compromised machines [2]. These are called the agents or daemons. By doing this it is very difficult to track the actual attacker and place of occurrence of attack on the Internet. Therefore, it is most difficult to provide global security for the entire network. Any deviation in security leads to the loss of information. This unprotected environment results in unsatisfied customers and fall in reputation of organization.

In this paper, we propose a novel mechanism for detecting DDoS using clustering based approach. As our network is large, for earlier and accurate detection we need to sub group our network as finite number of clusters [3]. Each cluster is controlled and monitored by cluster lead. The cluster lead monitors the number of users logging in at particular time duration and the total number of packets sent by each user. Before implementing the actual concept, training has been provided to the network to differentiate between normal packets and the abnormal packets [4].

To distinguish normal packet from abnormal packet it considers the score obtained from the parameters such as number of entries of single user at particular interval of time and number of packets sent by him on that particular time period. For the simulation purpose we considered random amount packets can be sent in 3ms.The fore coming analysis of the work structured as follows. Section 2 gives discussion on related work. Section 3 explains the system model. Section 4 summarizes the computations being performed to detect DDoS at router level. Section 5 provides details about the result discussion. Section 6 concludes with the future work

RELATED WORK

The increased damage caused by DDoS attacks leads to the increased development of attack detection mechanisms. These approaches vary depending on the techniques being used. Many of the methods were implemented based on anomaly detection mechanism. Reyhaneh and Ahmad [5] proposed an anomaly based DDoS detection based on selected features of attacker packets and classified attacks as normal or abnormal, but failed to differentiate the type of attacks. Basheer Nayef [6], computed the correlation difference based on the outgoing and incoming packets of a network to detect DDoS attack.

Thwe Thwe Oo and Thandar Phyu [7], considered a statistical based approach to observe certain features of a network packet. The proposed system implemented novel routing mechanism to detect DDoS. It first calculates the cost function based upon different parameters of packet transmission. Then using the cost function, it measures the signal to noise ratio. Based on the result obtained scores has been set for each transmission. Then the scores are grouped under threshold values to predict the DDoS attack. Moreover, the proposed work also considers the count of each user entry. If the user entry exceeds with in the limit of predefined time duration, then it is identified as initiative of attack. Then it identifies normal and attack packets from matching the data with the predefined database values.

Thwe Thwe Oo and Thandar Phyu [8], the proposed work shows data mining approach to detect DDoS attack. Here, traffic features are calculated from network and then clustered into normal and abnormal attack traffic using data mining approach. This paper performs extensive computations. Now, in our paper, the proposed system is SNR with CBDM presents novel approach of data mining classification algorithm and score computation using mathematical calculation to detect DDoS. The calculation is based on light weight operations being performed in the network routers. The main aim of dividing network as clusters of different levels [9] helps easier identification of attack and also earlier detection of attack. Diagnosis earlier means prevention in future [10]. The proposed method shows better results with low over lead.

Barati et al., [11] proposed architecture of a detection system for DDoS attack. Genetic Algorithm (GA) and Artificial Neural Network (ANN) are deployed for feature selection and attack detection respectively in the hybrid method. Wrapper method using GA was deployed to be selected the most efficient features and then DDoS attack detection rate was improved by applying Multi-Layer Perceptron (MLP) of ANN. Results demonstrated that the proposed method was able to be detected DDoS attack with high accuracy and deniable False Alarm.

Katkar and Bhatia [12] evaluated the effect of various data preprocessing methods on the detection accuracy of DoS/DDoS attack detection Intrusion Detection System (IDS) and proved that numeric to binary preprocessing method performs better compared to other methods. Experimental results obtained using KDD 99 dataset are provided to support the efficiency of proposed combination.

Bhaya and Manaa [13] presented a hybrid approach called centroid-based rules to be detected and prevented a real-world DDoS attacks collected from “CAIDA UCSD" DDoS Attack 2007 Dataset” and normal traffic traces from “CAIDA Anonymized Internet Traces 2008 Dataset” using unsupervised k-means data mining clustering techniques with proactive rules method. Centroid-based rules are used to effectively detect the DDoS attack in an efficient time. The Result of experiments shows that the centroid-based rules method perform better than the centroid-based method in term of accuracy and detection rate. In term of false alarm rates, the proposed solution obtains very low false positive rate in the training process and testing phases. Results of accuracy were more than 99% in training and testing processes. The proposed centroid-based rules method can be used in a real-time monitoring as DDoS defense system.

PROPOSED SYSTEM MODEL

The network is composed of collection of systems under an organizational entity. Each system has edge routers to get connected with the network. Every system in the network communicates with the help of Border Gateway Protocol (BGP). BGP passes information about routes to the routers [14]. At each stage of transmission routing information updating takes place. In the proposed work, we compute path information in router table and pass same to the cluster representatives' who leads the network clusters [15]. For assumption, it is being simulated each cluster can communicate with other clusters using implicit signaling concept. **[Figure -1]** explains the following.

The Proposed system model works in two phases:

- Training/ Computation Phase.
  For training packets sent in TCP connection, offline operations are considered to identify normal user from abnormal user. In order to make implementation easier the network is divided in to sub groups as clusters. The clusters monitors the activity of user with respect to data sent and enter of each user into the network based on the monitoring result the cluster lead checks with predefined value of normal behavior. Deviation in this is noted as attack by cluster and creates score for that particular transmission. Transmission with less congestion will be given high score and vice-versa in order to avoid false alarm [16].
- Detection Phase.
  In the Detection phase cluster lead signals the next level cluster as congestion takes place [17]. Hence it disallows the packet transmission to next router. If the obtained level falls in-between normal and abnormal, at that situation, router gets incremented and same procedure has been followed in next cluster. After the confirmation of actual DDoS takes place, it drops packets. This helps to reduce unnecessary packet drops.

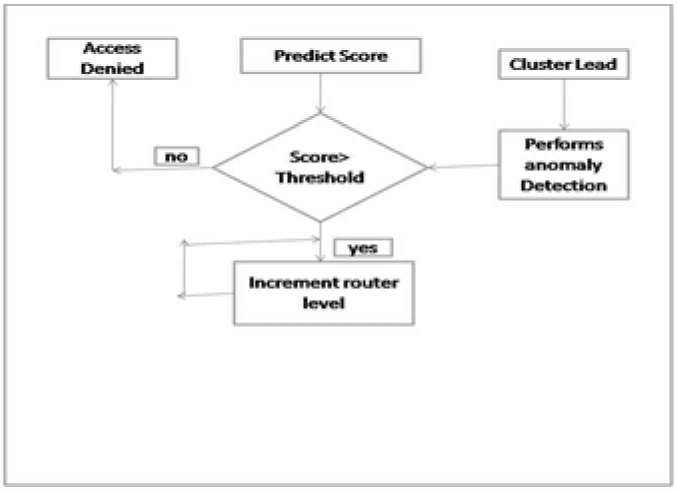

Fig: 1. System Architecture

ANALYSIS AND COMPUTATIONS

Due to the distributed nature, DDoS attack seems to be more severe than all the other type of attack. . It is also not easy to identify the exact point of attack in the network. So in order to detect exact point of attack and necessarily detection at early stage, we aim to divide the network as clusters. The identification of attack in one cluster, which is nearer to ingress router, prevents the whole network from congestion. Earlier detection helps to prevent the server system being shutdown or overflow. In our previous work, we concentrated on detecting DDoS attack at the client side during authentication process. Now we would like to perform computation inside the router network to detect DDoS attack. For the result accuracy, we trained routers based anomaly based attack detection mechanisms.

Depending on the training provided to the user, score has been given to the each user and the same has been marked in the identification field [18]. Deviation is the predefined computed threshold value based on score, results in the rejection or acceptance of the packet from that particular user IP.

Given set of routers in the network R={ r1,r2,r3,…….,rn} where n is the total number of routers. Set of packets traverse through the network is termed as packet size ps={ps1,ps2,ps3,……psn }. The whole network is divided in to finite group called cluster(k). The ith number of cluster is denoted as Ki, hence KI is ki ∈n. The number of packets from single user is recorded with its time duration and the length of the path it traverse. It is determined by Rjy-Rix=dxy, where d is the distance travelled in a network.

Algorithm Inputs

Number of packets sent as packet size (PS)

Time Duration to monitor number of packets received from same IP as TD

Predefined Threshold vale for DDoS attack as Total packet Count FC.

Threshold value computed based on anomaly detection as score S.

Cluster as the group of routers in network as C

p is the probability used for calculation purpose

User with IP address is represented as U for i number of times

The proposed method works as follows:

Step 1. Computation of score Metric.

Score has been computed in each router depending on the number of packets received.

Read: Packet Size PS, Time Duration TD, Total packet Count FC.

Result: Score based on probabilities p

S →TCP (Anomaly Detection Mechanism)

Return S ∀ PS

Each packet contains its source and destination address along with relevant topological information. All the nodes participate in forwarding packets and maintain node strength. The analyzing of packet being traversed is monitored by cluster lead.

Cost function (CF) is calculated, based upon the score given by cluster lead, and the number of packets (FC) being sent in particular time interval (TD), packet size (PS) and score (S).

$$CF = \alpha.PS + \beta.FC + \gamma.\ TD + S. \qquad (1)$$

α, β, γ. Are the expected weights assigned.

Depending on flow of packets under conditions like during attacks and no attacks different values may be assigned to the considered parameter metrics.

The node strength is a measure of sum of weights assigned to and the effects of attacks based on anomaly based detection are to be considered. Each node computes its individual strength by using signal to noise ratio [19]

$$S_{cn}=(1- \alpha)SNR_{ps}+(1- \beta)SNR_{fc}+(1- \gamma)SNR_{td} \qquad (2)$$

Scn is the score provided by the cluster and SNRps,, SNRfc,, SNRtd are the cumulative packet flood obtained over a period of time and the score result has been set to 1 to 10 depending on the parameter considered. That is the range from 6 to 10, no Flood, 4 and 5 initiate for the DDoS attack alarm and 3 means the flood, 2 DDoS flood and 1 is DDoS crash.

When the Scn falls below a critical threshold, it returns score value of 1, 2 and 3 depending on the severity. when the Scn computed based on SNR is within the range of threshold 9 to 10 it proceeds with the successful packet transmission. Scn returns the value of 1 to 10 based on the measure of SNR to tell about the node strength:

$$\begin{aligned} &S=1 \text{ to } 3 \text{ if } CF \geq 100000 \\ &S=4 \ \& \ 5 \text{ if } CF > 50000 \ \& \leq 100000 \\ &S=6 \text{ to } 10 \text{ if } CF \leq 50000 \qquad (3) \end{aligned}$$

Network not only affected by bulk bandwidth to induce DDoS attack but also large number of light weight entry can also flood the network. If a user enter more than the n number of permitted times, then the particular user has been put in blacklist database of cluster lead to keep an eye on particular user in his future transmission.

$$\frac{U= \sigma A(i) * VH(i)}{n}$$

where, n is number of users Scores are updated finally in the score list.

As soon as process gets started, IP address and corresponding physical address of each users are noted [20] .User entry is maintained in A and σ is some constant metric added with user entries. If A, entry is greater than the predefined (n), then access for further transmission is denied. Else, it goes to next vertical cluster [21].

Step 2. Comparison with predefined Threshold.

In anomaly based detection mechanism, it keeps track of all the users entering into the network at the entry point and also counts the total number of packets being sent at particular time duration.

Step 3. Total packet Detection Pseudo code

```
Read: Routers R, Score S
Result: Alarm Signal
1.0→R.
2. ∀ PS in TD  do
        Determine Score  → S based on SNR
        if S falls on Predefined Threshold of PS
//Predefined Threshold of PS (PS && U(i) = max & TD <= admitted value)
       compute SNR
       increment R
       else pause R for some (1-p) probability of time
       end if
       do SNR based on CF
       compute threshold
       signal Ci
       Ci alarms and warns Ci+1
       end do
       End.
3.End
```

Depending on the following parameters, scores has been fixed for the router loop execution.

Table: 1. Score Metric Calculation

User Entry	Packet Size	Distance Traversed in router (Hop Count)	Score
10.1.125.44	110000	15	1
54.121.54.11	10500	40	5
69.12.56.89	9500	15	8
58.129.102.9	76500	20	4
55.12.13.56	97800	14	2
54.121.55.6	82500	10	4
10.1.75.22	3600	15	3
10.1.25.11	77800	13	3
56.12.33.55	55000	30	5
45.23.66.78	4500	45	7

Whenever same user entry and number of packets sent are high and Distance traversed is less than the score provided will be less. High Score will be given chance of further transmission through the network [22]. **[Figure - 2], [Figure - 3]** shows network model and cluster formation.

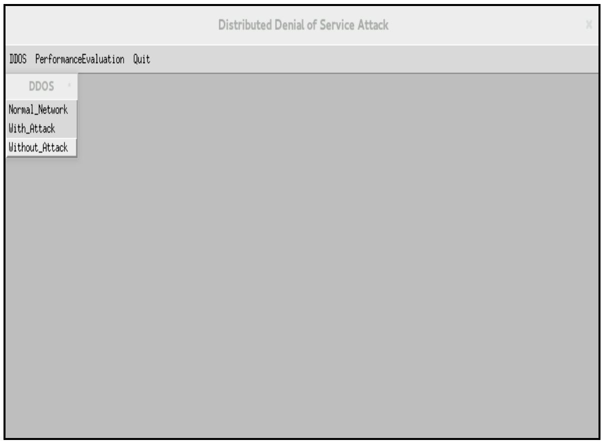
Distributed Denial of Service Attack
DDOS PerformanceEvaluation Quit
DDOS
Normal_Network
With_Attack
Without_Attack

Fig: 2. Model Simulation

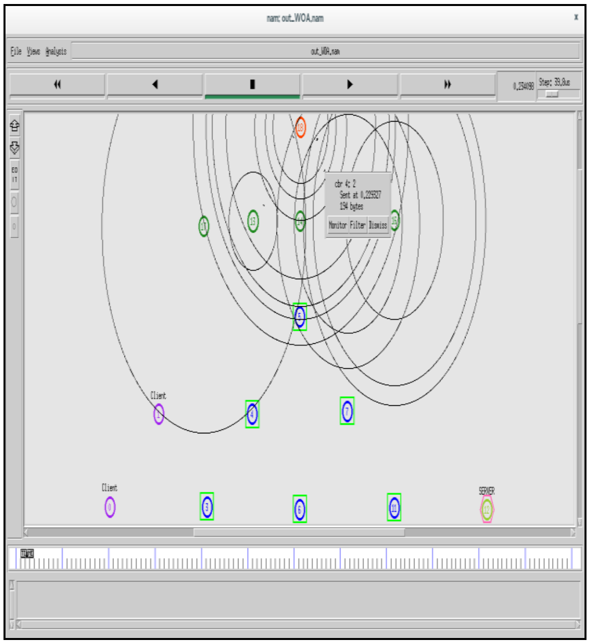

Fig: 3.Cluster Communications

RESULTS AND DISCUSSIONS

Rank with highest number will be given chance to allow packets to the next level router. Performance measure based on cluster based data mining technique to detect DDoS shows better results with false positive and false negative. The Complexity of mechanism is less as it involves only a set of iterative same simple light weight operations. Until the predefined threshold value exceeds, it continues looks up and computation being performed by cluster lead. Also by considering different parameters at light weight computation rate and monitoring at different levels ensure accuracy in attack detection. The Proposed method can easily detect DDoS attack from flash crowd. The **[Figure - 4]** simulated the detection procedure with attack and without attack with respect to data loss and data delivery rate.

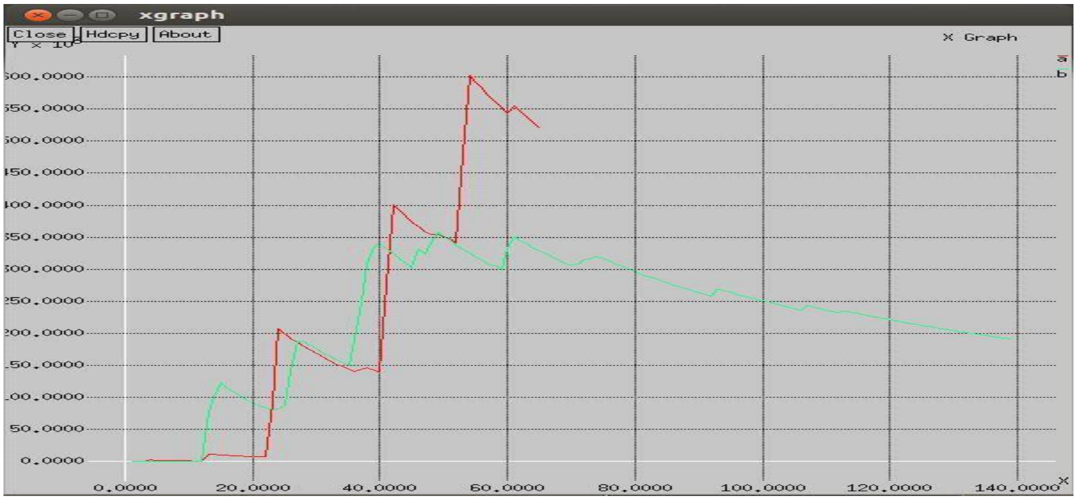

Fig: 4. Data loss with attack

CONCLUSION

In this paper, we have proposed a data mining approach for the DDoS attack detection by using clustering based network. Before performing the actual implementation, we proposed to train the network for anomaly based detection as done in the real practical network detection approach. We considered the parameters such as packet count, time duration, hop count. The approach also very effective to be implemented under mobile adhoc network with very less over lead. We simulated the concept under both the normal case and the attack case. We mounted the most powerful DDoS attack changing attack types, so we could get the attack traffic of various types. As the outcome of experiment, we compared the misbehavior user from normal one at early stage by clustering the network as different level of cluster. Score calculation based on different parameters at different level shows the proposed approach is more effective compared with the existing multiple computations method. The future works focus on comparative experiments using different data mining technologies and statistic approach.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

The authors report no financial interests or potential conflicts of interest.

REFERENCES

[1] Elliott Karpilovsky, Mathew Caesar, Jennifer Rexford, Aman Shaikh, Jacobus van der Merwe.[2012]Practical Network-Wide Compression of IP Routing Tables, *IEEE trtansactions on Network and Service Management*, 9(.4).

[2] Boswell Steven, Calvert, Ben and Campbell, Paul. [2003]Security+ Guide to Network Security Fundamentals. *Thomas Course Technology: Canada*,

[3] Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, Sehun Kim.[2007] DDoS attack detection method using cluster analysis, Expert Systems with Applications, *Elsevier*, 34(3):1659-1665.

[4] Thwe Thwe Oo, and Thandar Phyu, Analysis of DDoS Detection System based on Anomaly Detection System, *International Conference on Advances in Engineering and Technology* (ICAET'2014) March 29-30, 2014 Singapore

[5] K Reyhaneh, F Ahmad.[2011] An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks, International Conference on Network and Electronics Engineering *IPCST* vol.11, IACSIT Press, 2011, Singapore.

[6] AD Basheer Nayef.[2005] Mitigation and traceback countermeasures for DDoS attacks" , Iowa State University,

[7] Thwe Thwe Oo, Thandar Phyu.[2013] A Statistical Approach to Classify and Identify DDoS Attacks using UCLA Dataset" , *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* 2(5).

[8] Thwe Thwe Oo, Thandar Phyu.[2013 DDoS Detection System based on a Combined Data

THE IIOAB JOURNAL ISSN: 0976-3104

mining Approach",*4 th International Conference on Science and Engineering*,

[9] Jérôme François, Issam Aib, and Raouf Boutaba.[2012] FireCol: A Collaborative Protection Network fortheDetection of Flooding DDoS Attacks, IEEE/ACMTRANSACTIONSONNETWORKING 20(6).

[10] A El-Atawy, E Al-Shaer, T Tran, and R Boutaba.[2009] Adaptive early packet filtering for defending firewalls against DoS attacks ," in Proc. *IEEE INFOCOM*, pp. 2437–2445,

[11] Barati M, Abdullah A, Udzir NI, Mahmod R, Mustapha N. [2014] Distributed Denial of Service detection using hybrid machine learning technique. In Biometrics and Security Technologies (ISBAST), 2014 International Symposium on (pp. 268-273). *IEEE*.

[12] Katkar VD, Bhatia DS. [2014] Lightweight approach for detection of denial of service attacks using numeric to binary preprocessing. In Circuits, Systems, Communication and Information Technology Applications (CSCITA), 2014 International Conference on (pp. 207-212). *IEEE*.

[13] Bhaya W, Manaa ME. [2014]. A Proactive DDoS Attack Detection Approach Using Data Mining Cluster Analysis. *Journal of Next Generation Information Technology*, 5(4): 36.

[14] Stefano Vissicchio, Laurent Vanbever, Cristel Pelsser, Luca Cittadini, Pierre Francois, and Olivier Bonaventure.[2013] Improving Network Agility With Seamless BGP Reconfigurations,IEEE/ACMTRANSACTIONSONNETWORKING, 21(3).

[15] Wesam Bhaya, Mehdi Ebady Manaa.[2014] Review Clustering Mechanisms of Distributed Denial Of Service Attacks, *Journal of Computer Science, Science Publications*, 10(10): 2037-2046

[16] Hari Om, Aritra Kundu.[2012] A Hybrid System for Reducing the False Alarm Rate of Anomaly Intrusion Detection System, in proceeding of the international conference on *Recent Advances in Information Technology (RAIT)*, pp. 15-17.

[17] Basappa B Kodada, Gaurav Prasad, Alwyn R Pais, Protection Against DDoS and Data Modification Attack in Computational Grid Cluster Environment ,I.J. *Computer Network and Information Security*, 12-18, 2012.

[18] Wu Xin-Wen, Zi Lifang, Yearwood John.[2010]daptive Clustering with Feature Ranking for DDoS Attacks Detection, in proceeding of the international conference on Network and System Security (NSS). 281-286,

[19] R Dube, CD Rais K.-Y. Wang and SK Tripathi. [1997]Signal stability-based adaptive routing (SSA) for ad hoc mobile net-works, *IEEE Personal Communications*, 4(1): 36–45,

[20] A Sardana, R Joshi, and T hoon Kim.[2008] Deciding optimal entropic thresholds to calibrate the detection mechanism for variable rate DDoS attacks in ISP domain, in Proc. ISA, 270–275

[21] Koutepas F, Stamatelopoulos and B Maglaris.[2004] Distributed management architecture for cooperative detection and reaction to DDoS attacks, *J Netw Syst Manage*, 12:73–942010

**DISCLAIMER: *This article is published as it is provided by author and approved by guest editor. Plagiarisms and references are not checked by IIOABJ.*