Journal of Soft Computing Paradigm (JSCP) (2019)
Vol.01/ No. 02
Pages: 80- 90
http://irojournals.com/jscp/
DOI: https://doi.org/10.36548/jscp.2019.2.003

SOFT COMPUTING BASED AUTONOMOUS LOW RATE DDOS ATTACK DETECTION AND SECURITY FOR CLOUD COMPUTING

S. R. Mugunthan,

Associate Professor, Department of computer science and engineering,

Sriindu College of engineering and technology,

Hyderabad, India.

Email id: srmugunth@gmail.com

Abstract: The fundamental advantage of the cloud environment is its instant scalability in rendering the service according to the various demands. The recent technological growth in the cloud computing makes it accessible to people from everywhere at any time. Multitudes of user utilizes the cloud platform for their various needs and store their complete details that are personnel as well as confidential in the cloud architecture. The storage of the confidential information makes the cloud architecture attractive to its hackers, who aim in misusing the confidential/secret information's. The misuse of the services and the resources of the cloud architecture has become a common issue in the day to day usage due to the DDOS (distributed denial of service) attacks. The DDOS attacks are highly mature and continue to grow at a high speed making the detecting and the counter measures a challenging task. So the paper uses the soft computing based autonomous detection for the Low rate-DDOS attacks in the cloud architecture. The proposed method utilizes the hidden Markov Model for observing the flow in the network and the Random forest in classifying the detected attacks from the normal flow. The proffered method is evaluated to measure the performance improvement attained in terms of the Recall, Precision, specificity, accuracy and F-measure.

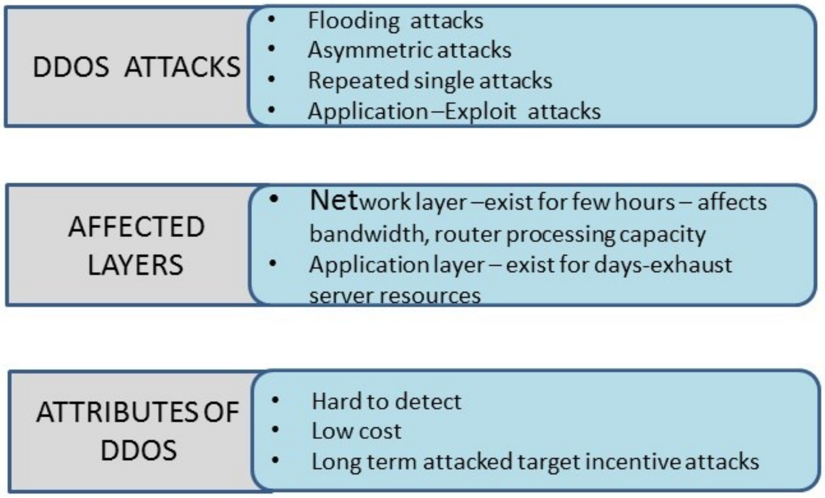
Keywords: Soft Computing, Low Rate DDOS, Attack Detection. Security Measure and Cloud Computing

1. INTRODUCTION

The cloud computing enables the people to share; it's the resources, services and the information. It equips the organization with the architecture that is flexible ensuring an effective computing network for the concern. The effective way of service provisioning by the cloud computing has made it more attractive among a wide range of organizations. The increased popularity of the cloud computing is leading to more and more organization to get adapted to cloud. The multitudes adopting towards the cloud results with high risks and challenges that cause security threats to the cloud computing. The distributed denial of service is also one such vulnerability that affects the services and the resources of the cloud. The distributed denials of services are more sophisticated and continues to progress at a rapid pace overthrowing all the identification and the counter measures.

The dos attacks have remained as a as a security threat to the internet and has caused many problems since its emergence. They are illegitimate activities in which the person who attacks causes interruption to the resources as well as the services of the system and also disturbs network access, the social accounts and other sources and the elements that are associated with the network. Counter measures where developed to stop the dos attacks and was found convincing. The illegal action later emerged with a more sophisticated attack named as the distributed DOS, this involved the multitudes of computer located at various parts of the world and was controlled by same attacker [1].

The DDOS is so mature that it remains as very dangerous form of attempt, creating intrusion into the network, making the network unavailable to its legal user, by interrupting or suspending the network service. The attacks are propelled through the well framed network that is distributed and controlled remotely using numerous of computer system that are compromised. These computers used by the attackers are known as the zombies or bots. The zombies are used in   continuously sending a huge set of attacks to the destined system that is aimed to be attacked. The main objective of the DDOS attack is to cause unusual behavior in the network either in form of inability or unavailability in the accessing of the network. So this makes the target system to respond slowly or get crashed completely. They disrupt the in the connectivity and services of the legal users in various layers. The fig.1 below shows the types of DDOS attacks, their attacks in different layers of the network and the attributes of the DDOS attacks. The DDOS mostly attacks the network layer and the application layer of the seven layers in the network. In which the attack on the network layer exists only for few hours, and the attack on the application layer exist for days. Though many promising methods have aroused to mitigate the severity of the DDOS attacks still the attacker continue develop new and methods and the aids to thwart the counter measure.



DDOS ATTACKS

- Flooding attacks
- Asymmetric attacks
- Repeated single attacks
- Application–Exploit attacks

AFFECTED LAYERS

- Network layer –exist for few hours – affects bandwidth, router processing capacity
- Application layer – exist for days-exhaust server resources

ATTRIBUTES OF DDOS

- Hard to detect
- Low cost
- Long term attacked target incentive attacks

Fig.1 DDOS Attacks Types and Attributes

The DDOS attacks the cloud architecture and affects the resources and the services of the cloud bringing down the speed and the elasticity in the service provisioning. Since the DDOS attacks are long term attacks and appear to be normal flow in the network the identifying of the attacks is a challenging task. So in orders mitigate the DDOS attacks in the cloud architecture, the paper provides the soft computing approach to identify the attacks and prevent them.

The paper utilizes the Hidden Markov Model combined with the Renyi entropies enumerated for the IP of data packets to observe the flow and extract the features and uses the random forest in classifying data flow in the network as either normal or abnormal.

The rest of the paper is arranged with the related works in section 2, proposed work in section 3, experimental results in section .4 and conclusion in section 5.

2. RELATED WORKS

Bravo, et al [1] presents the “systematic review of aspects of DDoS attacks detection." The author provides the complete detail of the deterioration caused by the DDOD attacks in the network. Behal, et al [2] provides the genral review on the “Characterization and Comparison of DDoS Attack Tools and Traffic Generators” the fig .2 given below shows the categories of the DDOS tools used in generating attacks.

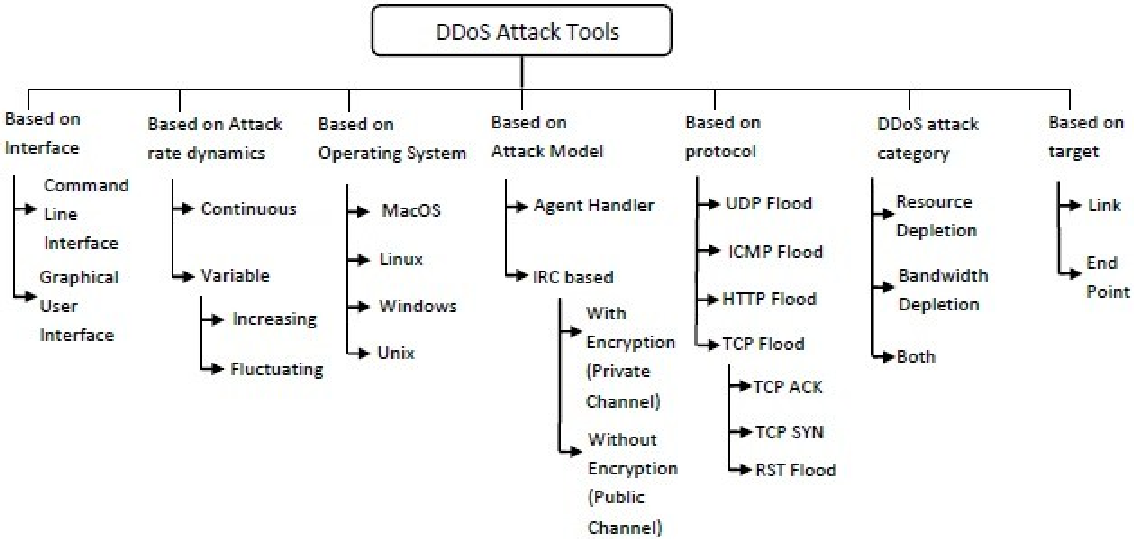


Fig.2 DDOS Tools [2]

Dong, et al [3] elaborates the "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments." Sherazi, et al [4] details the “DDoS attack detection in the sustainable communication in internet of vehicles." Kumar, P. et al [5] provides the "Distributed denial of service attack detection using an ensemble of neural classifier." Devi, et al [6] presents the "A comparative analysis of security methods for DDoS attacks in the cloud computing environment."

Zekri et al [7] explores the "DDoS attack detection using machine learning techniques in cloud computing environments." "A survey on security issues in cloud computing." Is provided by the author Bhadauria, et al [8] ,the author Ravinder, et al [9] presents the "Prevention of IP spoofing attack in cyber using artificial Bee colony and artificial neural network." Agrawal et al [10] explores the "Defense Mechanisms available against DDoS Attacks in a Cloud Computing Environment" Verma et al [11] provides "An Adaptive Threshold-Based Attribute Selection to Classify Requests Under DDoS Attack in Cloud-Based Systems."

Atif, et al [12] and Lara, et al [13] elaborates the "Soft Computing Techniques for Dependable Cyber-Physical Systems." and the "Trends on Computer Security: Cryptography, User Authentication, Denial of Service and Intrusion Detection" respectively. Ko, et al [14] provides the "Feature dynamic deep learning approach for DDoS mitigation within the ISP domain." Samaria, et al [15] uses the "Hidden Markov Model in the facial identification and the feature extraction" Rényi, et al [16] in his paper explores the "foundations of the probability" and details the Renyi's entropy. Wani et al [17] explores the "machine learning techniques in the analysis and the detection of the DDOS attacks in the cloud environment."

3. PROPOSED WORK

The average traffic flow of the low-rate DDOS attacks is much lower when compared to the conventional DDOS attacks, and resembles almost the normal traffic causing great challenges in detecting and preventing of the attacks in the cloud architecture. This necessitates a more effective solution to detect and prevent the attacks in the cloud architecture. So the proposed method utilizes the Hidden Markov model to observe the features of the traffic flow in the network, the features observed are used in the training of the random classifier to detect with the abnormal flow in the network. The block diagram in the fig .3 details the process in the proposed method of Low rate –DDOS detection in the cloud data centers.

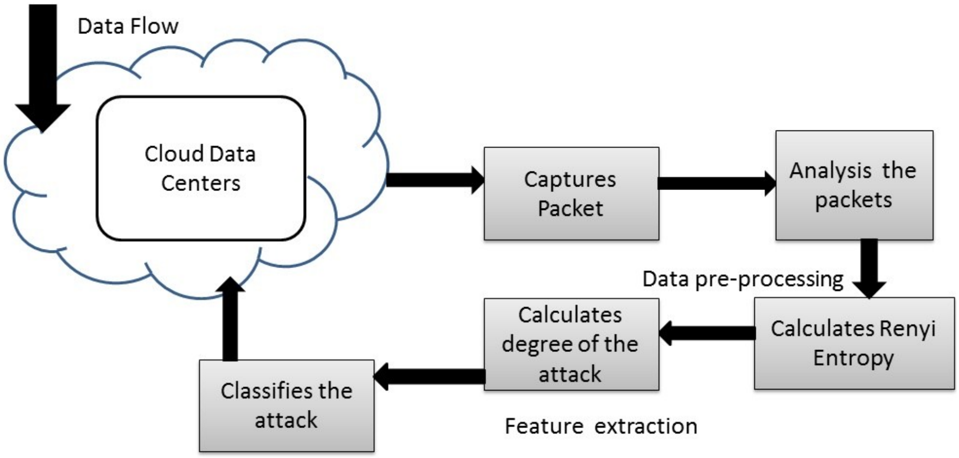


Fig.3 Proposed Block Diagram

The attack in the real time does not seem to be stable at all time. There is always a variation in the probability of the events happening in the network before and after the attacks. The probability of the events decrease with the attacks and increases when there is no attack so the Renyi entropy [16] is added to proffered method to enumerate the probability of the events, according to the attack rate. In case of the Low rate –DDOS the probability of the Low rate –DDOS goes high when the attack rate goes high. So the Renyi entropy enables to differentiate between the normal and the attack flow. It has several entropies forms such as the maximum (M), minimum (m) and Shannon (S).The following equation's (1, 2, and 3) shows the different entropy forms of the Renyi.

$$M_{entropy} = maximum\,\left(H_{\alpha}(x)\right) = \log(n) \text{ For } \propto = 0 \qquad (1)$$

$$m_{entropy} = Minimum\,(-\log(p_i)) = -\log(maximum\,(P_i)) \text{ For } \propto = \infty \qquad (2)$$

$$\lim_{\propto=1} H_x(\propto) = \textstyle\sum_{i=1}^{n} p_i * \log_2(p_i) \text{ For } \propto = 1 \qquad (3)$$

All Renyi entropies for the random variable that follows the uniform distribution remain the same, but differ in the effects of detection.

The Hidden-MM [15] is stochastic model that is used to predict the probabilities of the attack. It composed of two states hidden state (h_s), observational state (o_s). The probability transformation matrix for the h_s and the $o_s$are represented as TM_{hs} and TM_{os} respectively. In Low rate –DDOS the Hidden-MM is used remove the noises in the flow and fully observe the features of the traffic flow and defines the states based on the degrees of the attacks. The following equation (4) and (5) is framed in this regard.

$$TM_{hs} = [TM_{hs_{xy}}]_{n*n} TM_{hs_{xy}} = P\left(i_{t+1} = s_{ty} \middle| i_t = s_{tx}\right) x \geq 1, y \leq n \tag{4}$$

$$TM_{os} = [TM_{os_{xy}}]_{n*n} TM_{os_{xy}} = P\left(j_{t+1} = s_{ty} \middle| j_t = s_{tx}\right) 1 \leq x \leq n, 1 \leq y \leq n \tag{5}$$

Where, the s_{tx} is the prevailing moment in the state, the xy is the next state moment, TM_{os} the decides the generation method of the observations made and decides the way to generate the observed sequence. The TM_{hs} along with the initial time probability of every state is used in enumerating the hidden Markov chain and produces the state sequence of the unobserved.

The degrees of the attack obtained from the output of the Hidden-MM and used to train the Random Forest [17] along with the normal traffic to identify the abnormal behavior in the network. The attributes of the random forest makes it easy and flexible to use and as well as produce improvised results in all cases.

It operates by building numerous of the decision trees during the training phase and produces the classification output in form of single tree. The training for the detection of the abnormal traffic flow in the network is based on the bootstrap aggregation technology. It utilizes the degrees of the attack and the normal flow observed from the output of the Hidden-MM and applies trees to the data set and predicts the attack. The equation (6) gives the prediction average ($Pred_{avg}$) observed from the entire individual regression tree ($T_r{'}$)

DOI: https://doi.org/10.36548/jscp.2019.2.003

$$Pred_{avg} = \frac{1}{b_t} \sum_{T_r{}'=1}^{b_t} Pred_{avg}\ b_t\ (T_r{}') \tag{6}$$

Where, b_t is the bagging time. The uncertainties existing in the observations can be enumerated applying the standard deviation

4. EXPERIMENTAL RESULTS

The proposed frame work is tested using the KDD-Cup99 data set and evaluated to measure the accuracy, precision f-measure and the recall, the table.1 below provides the degree of the attack ratio obtained for the different entropies of the Renyi entropy. The Renyi entropy provides the probabilities of the attacks and the Hidden-MM provides the degree of the attacks reducing the noises in the flow. The table.1 below provides the observed and the hidden degree of the attacks.

Order of entropy	Attack ratio	Degree of attacks
[redacted]	[redacted]	[redacted]
α =3	0.01	11
[redacted]	[redacted]	[redacted]
α =8	0.01	13

Table.1 Order of Entropy, Attack Ratio, Degree of Attacks

The fig.4 shows the accuracy, precision and the F-measure and the Recall of the HMM-RF (proposed method) with the other methods such as the ABC-ANN [9] and the ATBA [11]. The result obtained shows that the proposed method provides a 97.34% accuracy and 95.45% of precision in detection of the low-rate DDOS in when compared with the other methods.

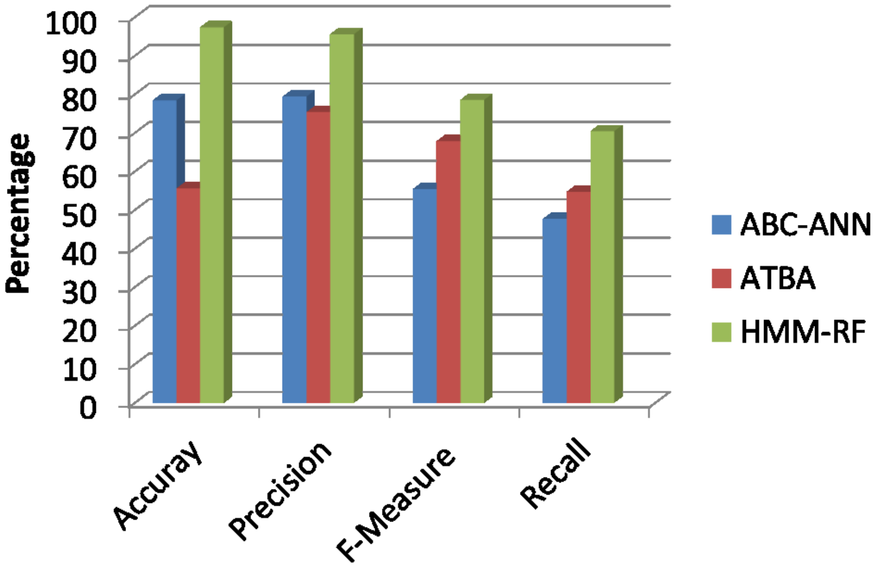


Fig .4 Results observed

5. CONCLUSION

The proposed HMM-RF for the identifying the low rate- DDOS in the cloud data centers utilizes the Hidden Markov model to observe the features of the traffic flow in the network, the features observed are used in the training of the random classifier to detect with the abnormal flow in the network. The Renyi entropy provides the probabilities of the attack and the Hidden–MM predict the degree of the attack. The based on the degree of the attack predicted the RF is trained using the bootstrap aggregation technology to classify the normal traffic form the attacked flow. The evaluation of the HMM-RF using the KDD CUP 99 data set highlights the improved classification accuracy of the proposed model when compared with the other model ABC-ANN and the ATBA.

References

[1] Bravo, Silvia, and David Mauricio. "Systematic review of aspects of DDoS attacks detection." *Indonesian Journal of Electrical Engineering and Computer Science* 14, no. 1 (2019): 162-176.

[2] Behal, Sunny, and Krishan Kumar. "Characterization and Comparison of DDoS Attack Tools and Traffic Generators: A Review." *IJ Network Security* 19, no. 3 (2017): 383-393.

[3] Dong, Shi, Khushnood Abbas, and Raj Jain. "A survey on distributed denial of service (DDoS) attacks in SDN and cloud computing environments." *IEEE Access* 7 (2019): 80813-80828.

[4] Sherazi, Hafiz Husnain Raza, Razi Iqbal, Farooq Ahmad, Zuhaib Ashfaq Khan, and Muhammad Hasanain Chaudary. "DDoS attack detection: A key enabler for sustainable communication in internet of vehicles." *Sustainable Computing: Informatics and Systems* 23 (2019): 13-20.

[5] Kumar, P. Arun Raj, and S. Selvakumar. "Distributed denial of service attack detection using an ensemble of neural classifier." *Computer Communications* 34, no. 11 (2011): 1328-1341.

[6] Devi, BS Kiruthika, and T. Subbulakshmi. "A comparative analysis of security methods for DDoS attacks in the cloud computing environment." *Indian Journal of Science and Technology* 9, no. 34 (2016): 1-7.

[7] Zekri, Marwane, Said El Kafhali, Noureddine Aboutabit, and Youssef Saadi. "DDoS attack detection using machine learning techniques in cloud computing environments." In *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, pp. 1-7. IEEE, 2017.

[8] Bhadauria, Rohit, Rituparna Chaki, Nabendu Chaki, and Sugata Sanyal. "A survey on security issues in cloud computing." *arXiv preprint arXiv:1109.5388* (2011): 1-15.

[9] Singh, Ravinder, Kashish Thakur, Gurpreet Singh, and Shaina Gupta. "Prevention of IP spoofing attack in cyber using artificial Bee colony and artificial neural network." In *Proceedings of the Third International Conference on Advanced Informatics for Computing Research*, p. 16. ACM, 2019.

[10] Agrawal, Neha, and Shashikala Tapaswi. "Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges." *IEEE Communications Surveys & Tutorials* (2019).

[11] Verma, Priyanka, Shashikala Tapaswi, and W. Wilfred Godfrey. "An Adaptive Threshold-Based Attribute Selection to Classify Requests Under DDoS Attack in Cloud-Based Systems." *Arabian Journal for Science and Engineering* (2019): 1-22.

[12] Atif, Muhammad, Siddique Latif, Rizwan Ahmad, Adnan K. Kiani, Junaid Qadir, Adeel Baig, Hisao Ishibuchi, and Waseem Abbas. "Soft Computing Techniques for Dependable Cyber-Physical Systems." *IEEE Access* (2019).

[13] Lara, Pablo Daniel Marcillo, Daniel Alejandro Maldonado-Ruiz, Santiago Daniel Arrais Díaz, Lorena Isabel Barona López, and Ángel Leonardo Valdivieso Caraguay. "Trends on Computer Security: Cryptography, User Authentication, Denial of Service and Intrusion Detection." *arXiv preprint arXiv:1903.08052* (2019).

[14] Ko, Ili, Desmond Chambers, and Enda Barrett. "Feature dynamic deep learning approach for DDoS mitigation within the ISP domain." *International Journal of Information Security* (2019): 1-18.

[15] Samaria, Ferdinando, and Frank Fallside. *Face identification and feature extraction using hidden markov models*. Olivetti Research Limited, 1993.

[16] Rényi, Alfred. *Foundations of probability*. Courier Corporation, 2007.

[17] Wani, Abdul Raoof, Q. P. Rana, U. Saxena, and Nitin Pandey. "Analysis and Detection of DDoS Attacks on Cloud Computing Environment using Machine Learning Techniques." In *2019 Amity International Conference on Artificial Intelligence (AICAI)*, pp. 870-875. IEEE, 2019.