International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

An Artificial Intelligence (AI) Framework for Detection of Distributed Reflection Denial of Service Attacks

[1]Dr. Jaideep Gera, [2]Dr.Venkata Kishore Kumar Rejeti, [3]Dr.G.RajeshChandra, [4]Dr.K.Jagan Mohan, [5]D.Anand, [6]Kotha Chandana

[1]Associate Professor, Department of CSE, ST. Mary's Group of Institutions Guntur, AP, India.
[2,3]Professor, Department of CSE, KKR & KSR Institute of Technology and Sciences, Guntur, AP, India.
[4]Professor, Department of CSE-AI, KKR & KSR Institute of Technology and Sciences, Guntur, Andhra Pradesh, India.
[5]Assistant professor, Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India.
[6]Assistant Professor, Department of IT, R.V.R & J.C College of Engineering, Guntur, AP, India.

Abstract

In the contemporary digital world, cyber space is growing continuously witnessing amalgamation of different technologies associated with telecommunications, networking and sensing to mention few. This has enabled Service Oriented Architecture (SOA) to realize distributed applications that cater to the needs of enterprises in the real world. With the advantages of such environments, there has been increased number of instances of cyber-attacks. Distributed Denial of Service (DDoS) is the large-scale attack targeting critical digital infrastructure to make it useless for certain amount of time. Such attacks have several implications and lead to collapse of businesses unless there are countermeasures to detect it and handle it properly. Distributed Reflection Denial of Service (DRDoS) is a variant of such attacks which is more destructive in nature. It is more so in the presence of Internet of Things (IoT) devices deployed in cyber space in large scale. The existing DDoS countermeasures do not work to solve the problem of DRDoS directly. We propose an Artificial Intelligence (AI) framework for detection of DRDoS attacks. We propose an algorithm known as Machine Learning based DRDoS Attack Detection (ML-DAD) for effective detection of attacks. The prototype service built in Python monitors such attacks and take necessary steps to defeat it. The empirical results revealed that the proposed framework has superior performance improvement over the stat of the art. The research in this paper leads to new ideas in the area of detection and prevention of DRDoS attacks.

Index Terms – Cyber-attacks, DDoS attacks, DRDoS attack detection, artificial intelligence, ML based DRDoS detection

1. INTRODUCTION

Denial of Service (DoS) attacks when made in large scale in distributed environments, they are named as Distributed Denial of Service (DDoS) attacks. There are different kinds of such attacks found in the cyber space. One such attack is known as Distributed Reflection Denial of Service (DRDoS) which tricks different servers to send large amount of data as response to requests to the victims. Source address IP spoofing is the strategy followed by attackers [8]. Of late, Internet community has suffered from DRDoS attacks and these attacks are made by exploiting UDP protocol vulnerabilities. As the attacks are made in large scale, they result in exhaustion of servers' resources and depletion of energy as well. In the attack process, an attacker makes use of compromised bots with spoofed target's IP, in order to launch attack on different servers that give large volumes of data to the victim. The servers are tricked or cheated in fact to send such responses to victims. The responses are very larger than the requests so as to make the servers busy besides ensuring that victim's resources are consumed badly. In order to increase the effect of attacks, attackers often make use of the phenomenon known as amplification. There are two kinds of amplifications known as Bandwidth Amplification Factor (BAF) and Packet Amplification Factor (PAF) and these are used to measure the amplification in terms of payload and number of packets respectively.

There are many kinds of approaches to detect DRDoS attacks. They are basically used to either to protect a target system or to detect in a wide range. The former has detection approaches namely detection at individual routers and detection at the victim. The latter has approaches known as detection at reflectors and analysing traffic that comes from multiple routers [8]. There are many researchers contributed towards detection of the attacks. As explored by Fraiwan et

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

al. [1], a store and forward kind of DRDOS attack has different phases such as crawling stage, storing stage, flooding stage and service outage stage. The defence strategy is based on the attack's modus operandi. SDN based mechanism is proposed in [3] while machine learning based detection is provided in [8] and [15]. An IoT measuring based phenomenon is employed in [9] while actionable knowledge based visualization method is used in [10]. Store and flood kind of DRDoS are explored in [1], [5] and [14] while NTP DRDoS is investigated in [11]. From the literature, it is understood that there are different kinds of approaches. However, the usage of Artificial Intelligence (AI) is a promising solution as there is knowledge built in the form of training samples. In this paper, therefore, an AI framework is proposed and implemented to detect DRDoS attacks. Our contributions in this paper is are as follows.

1. We proposed an AI framework for detection of DRDoS attacks. The framework has underlying mechanisms to deal with early detection of attacks.
2. We proposed an algorithm known as Machine Learning based DRDoS Attack Detection (ML-DAD) for detection of attacks.
3. A prototype service is built using Python data science platform for monitoring network flows for early detection of DRDoS attacks.

The remainder of the paper is structured as follows. Section 2 presents different approaches that are used by researchers to detect DRDoS attacks. Section 3 presents the proposed framework that is based on AI with underlying ML based algorithm. Section 4 presents experimental results that provide the efficiency of the proposed framework when compared with existing methods. Section 5 concludes the paper and gives directions for future work.

2. RELATED WORK

This section reviews relevant literature on countermeasures of DRDoS attacks. Fraiwan et al. [1] proposed a methodology for detection of DRDoS attacks of store and forward nature. Such attacks are found to store the data in Peer to Peer (P2P) networks that are distributed in nature. They are also found to more destructive than DDoS attacks. Attack analysis based on attack timeline is made in order to detect attacks. Liu et al. [5] also studied the store and forward kind of DRDos attacks with three stages in the attack such as preparation stage, storing stage and flooding stage. Fachkha et al. [2] studied intelligence pertaining to DRDoS attacks and prevention measures. They proposed a methodology based on K-Means clustering and expectation maximization technique in order to predict DRDoS campaigns. They analysed DNS amplification process to arrive at the prediction and validated with real world case studies pertaining to DNS DRDoS attacks. Their work could show mitigation of such attacks. Lukaseder et al. [3] proposed an SDN-based methodology for defence against RDDoS attacks. As the SDN is a centralized approach and transparent to attack target, it is found to be effective in dealing with such attacks. It is also found to be good for defence and also protocol-agnostic in nature. Their mitigation architecture has differentiator and mitigation system. There are certain practical approaches to detect distributed attacks on netflows as studied in [4].

Kumar et al. [6] introduced a threshold based technique that is used to isolate DDoS attack in an IoT use case. Jing et al. [7] on the other hand focused on amplification attacks and mitigating such attacks using a reversible sketch-based approach. It could handle large volumes of attack traffic and detect such attacks. The analysis is based on Chinese Reminder Theorem that is used as part of the technique for detecting and mitigating attacks. Gao et al. [8] proposed an approach based on ML to detect DRDoS attacks. The solution contains different operations such as feature extraction, observation of packets and classification and detection of attack. Huraj et al. [9] proposed a measuring technique for detection of DRDoS attack that us UDP based. Their measure is based on IoT scenario where IoT devices are involved in launching attacks in distributed environments. Their methodology is used to detect attacks based on the IoT measuring phenomenon. Aupetit et al. [10] proposed a method that can be used by Internet Service Providers (ISPs) in order to have actionable intelligence that leads to mitigation of DRDoS attacks. They focused on data-driven approach in experimentation and visualization as well.

Sassani et al. [11] explored on a kind of DRDoS attack that is based on Network Time Protocol (NTP). They developed a defence mechanism in order to detect such attacks. Cloud based DDoS attack prevention methods are explored in [12] and [15]. Diao et al. [13] proposed an algorithm to detect DRDoS attacks based on protocol free detection and flow correlation coefficient. Near victim cloud, they analysed basic traffic correlation to detect such attacks. Liu et al. [14] investigated on DRDoS attack of store and flood kind besides its counter measure. They developed a prototype to demonstrate such attack and show the prevention measure that could detect the attack. Li et al. [16] proposed an entropy based approach for DDoS attack detection. Su et al. [17] used Splunk platform to have a prototype application that detects DRDoS attacks. Both flooding and amplification attacks are demonstrated with countermeasures. Their methodology is integrated with existing tools like Wireshark in order to

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

mitigate DRDoS attacks. Fujinoki [18] proposed a cloud based approach as a mechanism to defend DRDoS attacks. Their approach has two phases such as monitoring phase and detection phase and the solution is available at each server. Shangytbayeva et al. [19] focused on different kinds of attacks on computer networks including DRDoS kind of attacks. They proposed a solution to DRDoS attack based on the traffic analysis and correlation methods. Alieyan et al. [20] covered different DDoS attacks that are based on DNS that has vulnerabilities. They found that amplification attacks are most frequent and quite damaging in nature. From the literature, it is understood that there are different kinds of approaches. However, the usage of Artificial Intelligence (AI) is a promising solution as there is knowledge built in the form of training samples. In this paper, therefore, an AI framework is proposed and implemented to detect DRDoS attacks.

3. PROPOSED ARTIFICIAL INTELLIGENCE BASED FRAMEWORK

The proposed method based on AI and it takes data of networks in distributed environments. A network flow has different number of packets. Each packet has both source IP and destination IP. It is also associated with source and destination ports besides the payload it carries. In a given time, interval, there is need to be feature extraction process at different layers of network. Large number of packets pertaining to requests will emerge when attacker launches DRDoS attack. In the same fashion, large number of response packets arise from the reflectors as well. For each IP address, it is essential to count the request and response packets in order to identify vulnerabilities as expressed in Eq. 1.

$$\forall_{(S_i,D_i,T_i,P_{si},P_{di})}\{\begin{matrix} W_q[S_i]= W_q[S_i]+1 & \text{if } T_i \text{ is a request packet to VSD} \\ W_r[D_i]= W_r[D_i]+1 & \text{if } T_i \text{ is a responce packet from VSD} \end{matrix} \quad (1)$$

We compute volume per unit time of both request and response packets for source and destination IPs as expressed in Eq. 2 and Eq. 3 respectively.

$$\forall_{M_k \in M}\{\begin{matrix} V_{qk} = \frac{Q_q\,[M_k]}{\Delta t}, & \text{if } M_k \text{ exists in } Q_q \\ V_{qk} = 0, & \text{otherwise} \end{matrix} \quad (2)$$

$$\forall_{M_k \in M}\{\begin{matrix} V_{rk} = \frac{Q_r\,[M_k]}{\Delta t}, & \text{if } M_k \text{ exists in } Q_r \\ V_{rk} = 0, & \text{otherwise} \end{matrix} \quad (3)$$

If there is any abnormality, it is reflected in V_{qk} indicates the probability of DRDoS attack. With respect to packet's source and destination ports, the amount at ports is also considered for possible detection of attack. These commutations at the ports are made using Eq. 4 and Eq. 5.

$$\forall_{M_k \in M}\{\begin{matrix} P_{qk} = \left|\left|J_q[M_k]\right|\right|, & \text{if } M_k \text{ exists in } J_q \\ P_{qk} = 0, & \text{otherwise} \end{matrix} \quad (4)$$

$$\forall_{M_k \in M}\{\begin{matrix} P_{rk} = \left|\left|J_r[M_k]\right|\right|, & \text{if } M_k \text{ exists in } J_r \\ P_{rk} = 0, & \text{otherwise} \end{matrix} \quad (5)$$

Where the P_{qk} and P_{rk} the two features reflecting attack index. Feature values are analysed in order to detect attack source, victim and internal nodes. Once features are extracted, it is possible to have an AI method that employs learning process followed by detection of such attack. Different existing ML techniques such as Random Forest, KNN and SVM are used to as detection models.

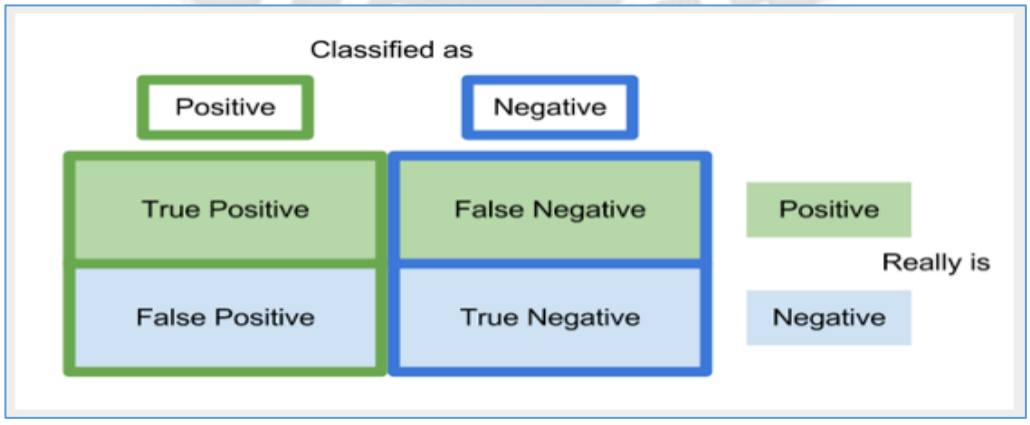

Figure 1: Confusion matrix

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

As shown in Figure 1, the performance of AI based approach is evaluated using how the algorithm detected a particular vulnerability when compared with ground truth.

Algorithm: Machine Learning based DRDoS Attack Detection (ML-DAD)
Input: Traffic from distributed network P, training flows T
Output: DRDoS attack detection and defence

1. Start
2. Initialize feature vector F
3. Initialize vulnerabilities vector V
4. F← FeatureExtraction(T)
5. Train a classifier C
6. For each network flow t in T
7. Compute source packet count
8. Compute destination packet count
9. Update V
10. End For
11. For each v in V
12. If v is found vulnerable Then
13. Drop the packet
14. End If
15. End For
16. Return
17. Stop

Algorithm 1: Machine Learning based DRDoS Attack Detection (ML-DAD)

As presented in Algorithm 1, there are mechanisms as discussed in the methodology that help in detection of DRDoS attacks. The dataset taken from [8] is subjected to feature extraction and then a classifier is trained in order to have a DRDoS detection and defence. Then the vulnerabilities are assessed to determine the presence of DRDoS attacks. Several performance metrics such as false alarm rate, missing rate and detection rate are used to evaluate the performance of the proposed system. These metrics are based on the confusion matrix presented in Figure 1 and they are expressed in Eq. 6, Eq. 7 and Eq. 8 respectively.

$$DR = \frac{TN}{TN+FN} \quad (6)$$

$$MR = \frac{FN}{TN+FN} \quad (7)$$

$$FAR = \frac{FP}{TP+FP} \quad (8)$$

Detection rate indicates a classifier's probability of detecting actual attack flows. Missing rate is on the contrary to DR while false alarm rate denotes the probability of normal traffic flows identified as attack flows.

4. EXPERIMENTAL METHODS

Experiments are made with a python service that monitors traffic flows. The results of the proposed algorithm ML-DAD are evaluated in terms of the performance metrics such as false alarm rate, detection rate and missing rate. The results also compared with existing ML techniques such as SVM, RF and KNN. Request packet (b_r) and response packet (b_s) bandwidths are differed in experiments and they are measured in Mbps.

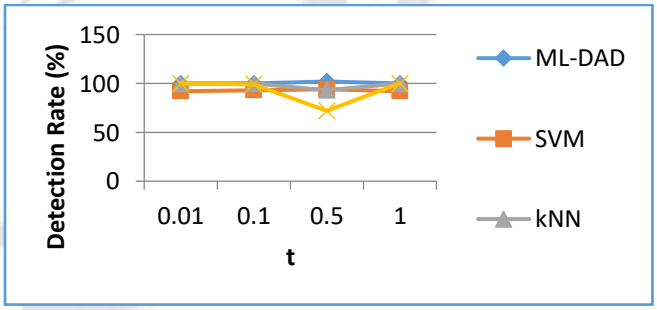

Figure 2: Detection rate comparison with b_r = 1 and b_s = 100

As presented in Figure 2, the time value is presented in horizontal axis while the vertical axis shows the detection rate %. The results revealed that there is influence of time on the detection rate. At the same time, it is clear that the proposed method ML-DAD outperforms the existing ML techniques. It reveals the fact that the feature extraction approach of ML-DAD is causing improved performance over the state of the art.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

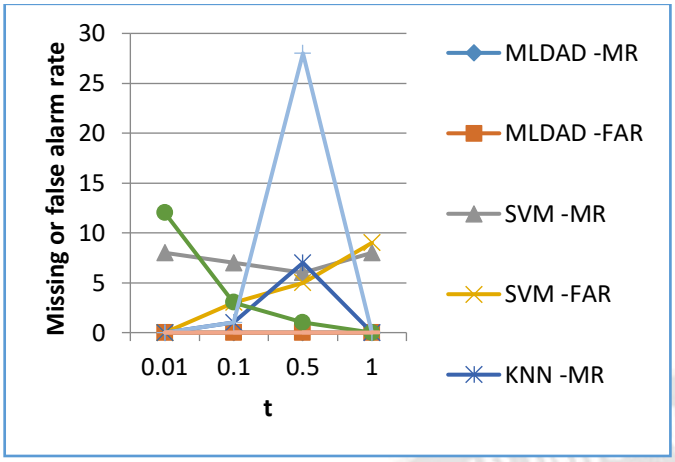

Figure 3: Missing or false alarm rate comparison with b_r = 1 and b_s = 100

As presented in Figure 3, the time value is presented in horizontal axis while the vertical axis shows the missing or false alarm rate %. The results revealed that there is influence of time on the detection rate. At the same time, it is clear that the proposed method ML-DAD outperforms most of the existing ML techniques. It reveals the fact that the feature extraction approach of ML-DAD is causing improved performance over the state of the art in terms of reducing missing or false alarm rate.

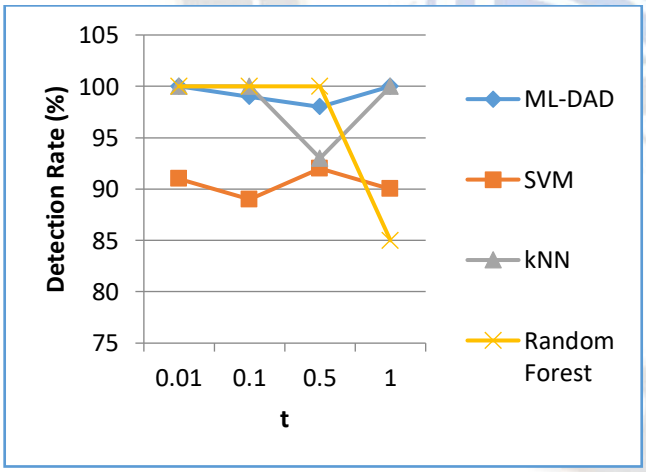

Figure 4: Detection rate comparison with b_r = 20 and b_s = 500

As presented in Figure 4, the time value is presented in horizontal axis while the vertical axis shows the detection rate %. The results revealed that there is influence of time on the detection rate. At the same time, it is clear that the proposed method ML-DAD outperforms the existing ML techniques. It reveals the fact that the feature extraction approach of ML-DAD is causing improved performance over the state of the art.

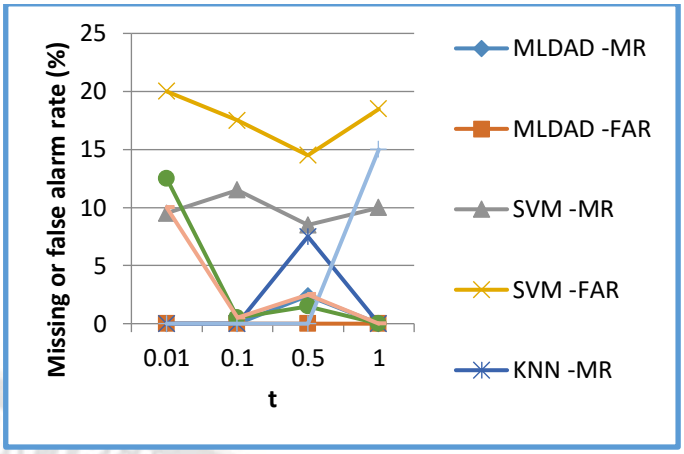

Figure 5: Missing or false alarm rate comparison with b_r = 20 and b_s = 500

As presented in Figure 5, the time value is presented in horizontal axis while the vertical axis shows the missing or false alarm rate %. The results revealed that there is influence of time on the detection rate. At the same time, it is clear that the proposed method ML-DAD outperforms most of the existing ML techniques. It reveals the fact that the feature extraction approach of ML-DAD is causing improved performance over the state of the art in terms of reducing missing or false alarm rate.

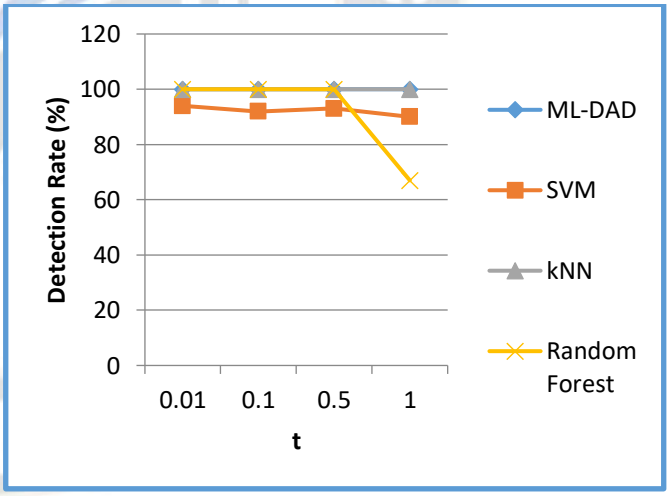

Figure 6: Detection rate comparison with b_r = 100 and b_s = 100

As presented in Figure 6, the time value is presented in horizontal axis while the vertical axis shows the detection rate %. The results revealed that there is influence of time on the detection rate. At the same time, it is clear that the proposed method ML-DAD outperforms the existing ML techniques. It reveals the fact that the feature extraction approach of ML-DAD is causing improved performance over the state of the art.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

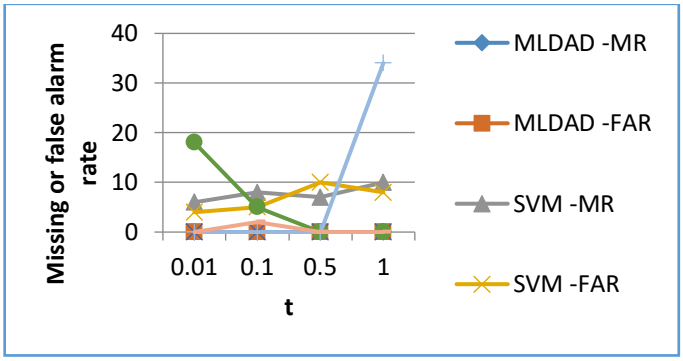

Figure 5: Missing or false alarm rate comparison with b_r = 100 and b_s = 100

As presented in Figure 5, the time value is presented in horizontal axis while the vertical axis shows the missing or false alarm rate %. The results revealed that there is influence of time on the detection rate. At the same time, it is clear that the proposed method ML-DAD outperforms most of the existing ML techniques. It reveals the fact that the feature extraction approach of ML-DAD is causing improved performance over the state of the art in terms of reducing missing or false alarm rate.

5. CONCLUSION AND FUTURE WORK

In this paper, we proposed a framework known as Artificial Intelligence (AI) framework for detection of DRDoS attacks. We propose an algorithm known as Machine Learning based DRDoS Attack Detection (ML-DAD) for effective detection of attacks. The prototype service built in Python monitors such attacks and take necessary steps to defeat it. As there are increasing IoT scenarios and connected devices, there is increase in the DRDoS attacks. The AI based mechanism in this paper provides defence against such attacks. Different features are extracted from the traffic in order to have analysis and find statistically the probability of attack. Different measures such as false alarm rate, missing rate and detection rate are used to evaluate the performance of the proposed system. A dataset collected from [8] is used in order to have AI based detection mechanism. The solution involves feature selection, detection and classification based on the threat index. The ML-DAD algorithm is evaluated against different state of the art methods. The experimental results revealed the significance performance improvement of the proposed method. The results are a step forward in the research of DRDoS attacks. In future, we enhance the framework with deep learning methods fusion based approaches for effective detection of DRDoS attacks.

References

[1] Fraiwan, M., Al-Quran, F., & Al-Duwairi, B. (2018). Defense Analysis Against Store and Forward Distributed Reflective Denial of Service Attacks. 2018 International Conference on Innovations in Information Technology (IIT). p111-116.

[2] Fachkha, C., Bou-Harb, E., & Debbabi, M. (2015). Inferring distributed reflection denial of service attacks from darknet. Computer Communications, 62, p59–71.

[3] Lukaseder, T., StOlzle, K., Kleber, S., Erb, B., & Kargl, F. (2018). An SDN-based Approach For Defending Against Reflective DDoS Attacks. 2018 IEEE 43rd Conference on Local Computer Networks (LCN). p299-302.

[4] Jungtae Kim/Ik-Kyun Kim and Koohong Kang (2016). Practical Approaches to the
DRDoS Attack Detection based on Netflow Analysis. The Eighth International Conference on Evolving Internet, IARIA, P20-25.

[5] Liu, B., Berg, S., Li, J., Wei, T., Zhang, C., & Han, X. (2014). The store-and-flood distributed reflective denial of service attack. 2014 23rd International Conference on Computer Communication and Networks (ICCCN). p1-8.

[6] Naveen Kumar, Nitin Mittal and Yogendra Naryan. (2019). Isolation of Distributed Denial of Service Attack using Threshold Based Technique in Internet of Things. International Journal of Recent Technology and Engineering. 8, p87-93.

[7] Jing, X., Zhao, J., Zheng, Q., Yan, Z., & Pedrycz, W. (2019). A reversible sketch-based method for detecting and mitigating amplification attacks. Journal of Network and Computer Applications. p15-24.

[8] Gao, Y., Feng, Y., Kawamoto, J., & Sakurai, K. (2016). A Machine Learning Based Approach for Detecting DRDoS Attacks and Its Performance Evaluation. 2016 11th Asia Joint Conference on Information Security (AsiaJCIS). p80-86.

[9] Huraj, L., Simon, M., & Horak, T. (2018). IoT Measuring of UDP-Based Distributed Reflective DoS Attack. 2018 IEEE 16th International Symposium on Intelligent Systems and Informatics (SISY). p209-214.

[10] Aupetit, M., Zhauniarovich, Y., Vasiliadis, G., Dacier, M., & Boshmaf, Y. (2016). Visualization of actionable knowledge to mitigate DRDoS attacks. 2016 IEEE Symposium on Visualization for Cyber Security (VizSec). P

[11] Sassani, B. A., Abarro, C., Pitton, I., Young, C., & Mehdipour, F. (2016). Analysis of NTP DRDoS

attacks' performance effects and mitigation techniques. 2016 14th Annual Conference on Privacy, Security and Trust (PST). p1-7.

[12] Fakieh, Khalid. (2016). An Overview of DDOS Attacks Detection and Prevention in the Cloud. International Journal of Applied Information Systems. 11. 25-34. 10.5120/ijais2016451628.

[13] Xiao, L., Wei, W., Yang, W., Shen, Y., & Wu, X. (2016). A protocol-free detection against cloud oriented reflection DoS attacks. Soft Computing, 21(13), p3713–3721.

[14] Liu, B., Li, J., Wei, T., Berg, S., Ye, J., Li, C., … Han, X. (2015). SF-DRDoS: The store-and-flood distributed reflective denial of service attack. Computer Communications, 69, p107–115.

[15] Kamboj, Priyanka & Trivedi, Munesh & Yadav, Virendra & Singh, Vikash. (2017). Detection techniques of DDoS attacks: A survey. 675-679. 10.1109/UPCON.2017.8251130.

[16] Li L., Zhou J., Xiao N. (2007) DDoS Attack Detection Algorithms Based on Entropy Computing. In: Qing S., Imai H., Wang G. (eds) Information and Communications Security. ICICS 2007. Lecture Notes in Computer Science, vol 4861. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-540-77048-0_35

[17] Su, T.-J., Wang, S.-M., Chen, Y.-F., & Liu, C.-L. (2016). Attack detection of distributed denial of service based on Splunk. 2016 International Conference on Advanced Materials for Science and Engineering (ICAMSE). p397-400.

[18] H. Fujinoki Southern Illinois University Edwardsville, Edwardsville, IL.. (2018). Cloud-Base Defense Against DRDoS Attacks. IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). p1-2.

[19] Gulmira Asaugalikyzy Shangytbayeva, Bahytzhan Srazhatdinovich Akhmetov, Mikolaj Petrovich Karpinski, Roza Nuralievna Beysembekova and Erbol Amangazyevich Ospanov. (2015). Research Distributed Attacks in Computer Networks. BIOSCIENCES BIOTECHNOLOGY RESEARCH ASIA,. 12 (1), p734-744.

[20] Alieyan, K., Kadhum, M. M., Anbar, M., Rehman, S. U., & Alajmi, N. K. A. (2016). An overview of DDoS attacks based on DNS. 2016 International Conference on Information and Communication Technology Convergence (ICTC). p276-280.