International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7559
***Article Received**: 05 April 2023 **Revised**: 30 May 2023 **Accepted**: 26 June 2023*

A Generalized Renyi Joint Entropy Method for the Detection of DDoS Attacks in IoT

Jeethu Mathew[1], Dr. Jemima Priyadarsini R[2]
[1]Dept. of Computer Science
Bishop Heber College Trichy
Affiliated to Bharathidasan University Trichy
jithumap@gmail.com
[2]Associate Professor
Dept. of Computer Science
Bishop Heber College Trichy
Affiliated to Bharathidasan University Trichy
jemititus@gmail.com

Abstract— Internet of things connects all the smart devices with internet and gain more information in comparison with other systems. Since different types of objects are connected, privacy and security of the users must be ensured. Because of the decentralised nature, IoT is prone to different types of attacks which are either active or passive. Since internet is the main part of IoT, the security issues present in Internet will be available in the Internet of Things too. Distributed denial of service is a major threat of this type and a critical threat. It reduces the performance of the complete network even it breaks entire communication. For this reason many researches have been made in this area to detect Distributed Denial of Service attack. Entropy-based approaches to identify DDoS attacks in the internet of things are discussed in this research. This new approach is based on the GRJE method, which stands for generalised Renyi joint entropy. Renyi joint entropy is used in the suggested approach to analyse network traffic flow. The suggested method is put into practise and evaluated against other methods based on a few factors. Results from an analysis of the suggested system's effectiveness in NS2 are reported in this study.

Keywords- IoT, DDoS attack, Entropy, Renyi joint entropy.

I. INTRODUCTION

Internet of Things is defined as the network of all the things which are connected such as physical objects, devices, automobiles, people, appliances, etc. The sensors and actuators are the main components of IoT. It is calculated that there are 35.82 billion connected devices are there. These devices exchange data through internet. Today IoT is related even in the minutest levels of human life. Hence it is associated with automation, integration and analysis of the data and the entire system. It has different levels of applications and benefits in human life. It provides enormous services to the humankind which are applicable in the areas of social, political and economic aspects. Huge amount of data is produced in each second. These data must be handled quickly and efficiently [1]. Security is the major concern in IoT environments. It is very difficult to ensure security and privacy to the users and data because different types of devices are connected. Hence many researches are concentrated in this area.

Because fresh data is generated every second, especially when new devices are linked to the network, security issues are the main IoT concern. Data privacy is a significant consideration. The risk is rising as the number of devices linked to the Internet rises every day [2]. Network vulnerabilities, security threats, and security breaches are all possibilities. An attacker can use a variety of tactics within an IoT context. As a result, some nodes can be destroyed or the entire network can be broken. Hence, there must be a security mechanism to protect the IoT devices which addresses most of the security threats. Since all the connected devices are light, the solution must be also a lightweight model which is suitable for the entire IoT environment.

II. DDOS ATTACKS IN IOT

IoT devices have simple, power-efficient computing. It poses a serious problem. These attacks come in a variety of forms. One of them is denial of service. The intruder chooses to attack the system via a denial-of-service attack. By flooding the target with traffic, the system and its resources become unavailable to the intended consumers. The entire network has been altered or disabled. The systems, network, services, or resources are off-limits to authorized users. Denial of service attacks come in a variety of types.

A type of DoS attack known as distributed denial of service happens when numerous systems are used to attack a single

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7559
***Article Received**: 05 April 2023 **Revised**: 30 May 2023 **Accepted**: 26 June 2023*

system. DDoS attack comes from multiple systems. A system is attacked by different other systems. Because of flooding of requests, the system of the network will be hampered. The internet bandwidth, RAM, CPU will be collapsed. The system completely stops its functioning. Mainly there are two broader types of attacks. First one is related with the network centric attacks and the second one is application layer attacks [3]. Hence it is a key issue in IoT. This kind of attack destroys the entire system. Today IoT has different applications. All these are related with different areas of human life. So, these are vital. Any harm to these systems directly affects human life. Hence IoT systems must be protected from these kinds of attacks. The first step here is to detect the DDoS attack.

III. RELATED WORK

For the detection of DoS and DDoS attacks in the Internet of Things, Shruti Kajwadkar and Vinod Kumar Jain suggested an innovative algorithm [4]. The method is intended for early DDoS attack detection and mitigation. It works well with constrained networks. The two performance matrices for evaluation are malicious packet delivery ratio and valid packet delivery ratio.

Pooja Redekar and Madhumita Chatterjee proposed a novel hybrid approach for detection of detection of DDoS attack. The proposed method is a hybrid approach which combines misuse- based and anomaly-based detection [5].

An effective method for detecting DDoS attacks by entropy variations was proposed by V. Sushma Reddy et al. The suggested approach is fundamentally distinct from commonly employed packet marking approaches because it is based on the entropy variation between regular and DDoS attack traffic. It has a larger scalability. According to this method the attack can also be blocked [6].

For Internet of Things devices, Akshat Gaurav et al. proposed a fog-layer based DDoS attack detection technique. It is a technique based on fog layers. To find fraudulent IoT nodes, a clustering and entropy-based approach is used. Statistical factors are used to analyze the effectiveness [7].

A new approach to DDoS attack isolation in the Internet of Things was put forth by Upendra Kumar et al. Their research suggests that a mutual authentication system that can identify and remove harmful nodes from a network. The execution time was kept to a minimum. A few variables are assessed [8].

An entropy-based approach to network anomaly identification was put out by Przemyslaw Berezinski et al. An entropy-based strategy is ideal to identify contemporary botnet-like malware based on aberrant network patterns, according to their suggested methodology [9].

DDoS attack detection algorithm based on IP entropy model was proposed by Wang Xintong et al. It correctly recognises DDoS assaults. It distinguishes between expected traffic and DDoS flow. The important variables are assessed [10].

In order to combat distributed denial of service, Abhinav Bhandari et al. presented a destination address entropy-based detection and tracking technique. According to their research, a packet-based entropy technique can detect DDoS issues that are caused by flooding. To identify the edge routers from where the entire attack traffic is entering the domain, an entropy-based traceback method is used [11].

Early detection of DDoS assaults on SDN controllers was suggested by Marc St-Hilaire and Seyed Mohammad Mousavi. According to their theories, DDoS attacks can deplete controller resources and offer a way to identify them based on the entropy variation of the target IP address. They assert that within the first 500 packets of the assault stream, they are capable to identify DDoS attacks [12].

Entropy-based methodology was suggested by Mohammad Aladaileh et al. to identify DDoS attacks on software defined networking controllers. This study suggests a technique that can identify assaults on SDN controllers independent of the quantity of victims or hackers. The parameters were satisfactorily evaluated [13].

IV. PROPOSED METHOD

The suggested method is based on entropy. Here the algorithm is introduced to detect DDoS attack. Before getting into the algorithm some key terms defined below.

A. Entropy

Entropy is a useful indicator of unpredictability. The chance of an event occurring in relation to the overall number of events is measured by entropy. It is identified using Shannon. For instance, if a network has 70 nodes, each node has a chance to accept new packets from other nodes. High entropy is the effect of this. Low entropy is caused by reduced randomness, which happens when a small number of nodes receive the majority of incoming packets [14]. Here, we make use of entropy. Entropy has a threshold value set here, and if the value is below the threshold value, an attack has occurred. This threshold value can also be modified when the network configuration is altered.

Understanding flow is necessary to comprehend entropy. The flow of packets via a router is made up of those with the same destination address. The probability of the flow is determined using the following equation, and the frequency of the flow is then estimated. The probability mass function is,

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7559
***Article Received**: 05 April 2023 **Revised**: 30 May 2023 **Accepted**: 26 June 2023*

$$P(x) = Pr\{X=x\}, x \in \mu \quad (1)$$

Where X be the discrete random variable.

The entropy of the flow using the subsequent formula, is determined.

$$H(x) = -\sum_{i=1}^{n} P_i * log_2 P_i \quad (2)$$

Here n is the number of packets, Pi be the probability of each element.

The randomness is measured in entropy. Because entropy can gauge the randomness or uncertainty of incoming packets to the network, it is utilized to identify DDoS attacks. The entropy increases with increasing randomness. Also, entropy decreases with decreasing randomness. There are two techniques to identify DDoS using entropy: (i) window size, and (ii) threshold value. The total amount of packets or the duration of the time determines the window size. To determine the level of ambiguity in the incoming packets, entropy is estimated inside the window. An attack detection, threshold is required. Entropy calculations are used to identify the attack. Entropy is a very typical technique for DDoS identification.

B. Generalized Renyi Joint Entropy

One of the primary indicators of attacks using DDoS is the existence of randomness in the communication. Some detection techniques that employ the Shannon entropy technique consistently produce incorrect results. Particularly for elaborate DDoS operations involving numerous nodes, the outcome could be a poor detection rate and a large false positive rate. As the input single packet header feature is used to calculate the entropy. Here a static value is used as a threshold value.

The basis of Ranyi joint entropy is joint entropy and Renyi. Two random variable x and y are measured here. Here, the source IP address and a destination IP address of a packet header are illustrated. Here, the source IP and the destination IP are used to generate the probability distribution. The threshold value in this case is dynamically set. This dynamic nature aids in identifying DDoS attacks and recognizing the randomness of the flow. This formula helps to detect lower rate and higher rate DDoS attacks.

$$H_{RJ\alpha}(x) = \frac{1}{1-\alpha}\ log_2\left(\sum_{i=1}^{N}\sum_{j=1}^{M} P(x_i y_i)^{\alpha}\right)$$

Here $P(x_i y_j)$ is the probability of the event ($x=x_i$, $y=y_j$), i=1,2,3, …., N and j=1,2,3, …, M is the positive parameter. In conclusion, Renyi joint entropy $H_{RJ\alpha}(x, y)$ is a statistical technique for determining the randomness of incoming network traffic flows to identify UDP DDoS attacks. The probability of the source IP address and the destination IP address must be considered (15).

V. PROPOSED DETECTION METHOD

It is typically exceedingly challenging to distinguish malicious traffic from regular traffic patterns. Additionally, getting a decent scheme detection is exceedingly challenging, especially when there are numerous hosts. Network traffic that exhibits unusual behavior is a major source of DDoS attacks. There are different types of approaches which highlights the strategies for detecting DDoS attacks. But we cannot attain a maximum accuracy because of the varying traffic rate. The suggested method therefore makes use of the Renyi joint entropy method, which has notable features with changeable threshold values. It helps to improve the efficiency of the method.

Here Renyi joint entropy method is used because it has some benefits over Shannon entropy method. Reduces low-rate and high-rate attacks as well as the amount of packet header features in order to distinguish between legitimate data and malicious traffic. It more precisely identifies attacks. It has the ability to gauge how random the packets are.

Here two concepts are combined, joint entropy and Renyi method. Here, the source IP address and destination IP address are two random variables. X and Y, respectively, serve as their representations. The recommended Renyi joint entropy equation

$$H_{RJ\alpha}(x) = \frac{1}{1-\alpha}\ log_2\left(\sum_{i=1}^{N}\sum_{j=1}^{M} P(x_i y_i)^{\alpha}\right)$$

Here the entropy is based on α which helps to calculate the probability of incoming packets. The probability is derived using the source and destination IP frequencies. Maximum Renyi joint entropy occurs when the probability distribution is dispersed evenly among all of the endpoints. On the other way, minimum value is occurred when the probability is distributed to some of the destination hosts.

The probability of each destination IP (y_i) address and source IP(x_i) address forms the basis of the Renyi joint entropy. Here we provide the equations for calculating the probability of x_i and y_i.

$$Px_i = \frac{xi}{n}$$

$$Py_i = \frac{yi}{n}$$

Here, x_i stands for the frequency of visits to each unique source IP address, y_i for visits to each unique destination IP address, and *n* stands for the total amount of packets. Here, it's important to note that the probability of regular traffic and attack traffic differ from one another. The source IP and the

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7559
***Article Received**: 05 April 2023 **Revised**: 30 May 2023 **Accepted**: 26 June 2023*

destination IP are variables in the running joint entropy method. We can determine the degree of randomness and unpredictability in these two variables by calculating their probability. If there is a high uncertainty then there will be high Renyi joint entropy. It helps to detect DDoS attacks in network.

The *algorithm* is described as follows.

Input: Arriving packets

Output: whether the packet is harmful or authorized.

Start

For every incoming packet [Source IP, Destination IP]

Step 1 **If** source IP ∈ BlackIPList then

Drop Packet

End

Step 2 **Else**

Compute the probability of source IP(x_i) and destination IP(y_i), p($x_i y_i$)

Step 3 **If** $0 < p(x_i y_i) \leq 1$ then

Calculate the frequency of source and destination IP;

Calculates Renyi joint entropy value $H_{Rj\alpha}(x, y)$;

Step 4 **If** $H_{Rj\alpha}(x, y) > Th$ then

DDoS attack detected;

Add source IP address to the BlackIPlist.

End

Step 5 **Else**

Normal flow

End

End

Step 6 **Else**

Go to step 2

End

End

VI. RESULTS

The GRJE method's primary goal is to identify DDoS attacks in IoT networks. NS2 was used to implement the system. Analysis and comparison of the suggested system's effectiveness with currently used techniques are conducted. The primary factors in a fog-layer-based DDoS attack detection method for Internet of Things devices are detection rate, precision, packet delivery ratio, true negative rate, and false positive direction. [16].

Precision

It means the accuracy of the method. The malicious nodes are identified in our system and blacklisted. As a result, the level of precision is increased. It is represented in figure 1.

Detection rate

According to the simulation, the GRJE methodology has a reliable detection of attacks strategy. In IoT networks, it can detect both high- and low-rate DDoS attacks. The suggested approach is contrasted with the current methods. It is described in figure 1.

Packet delivery ratio

It is the proportion between the entire quantity of packets sent from the source to the entire amount of packets received at the destination. In this case, the most packets are received. This is seen in figure 1.

True negative rate

It provides the system's rejection rate for attack packets. Here, in suggested system the number of packets discarded by the blacklisted IPs and the method, the true negative rate is increasing. This is plotted in figure 1.

False positive detection

The proposed method has high false positive rates when compared to the existing methods. The reduction in false positive rate is because of the usage of dynamic threshold value instead of static one. It is more flexible and it improves the detection rate. It is illustrated in figure 1.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 6
DOI: https://doi.org/10.17762/ijritcc.v11i6.7559
***Article Received**: 05 April 2023 **Revised**: 30 May 2023 **Accepted**: 26 June 2023*

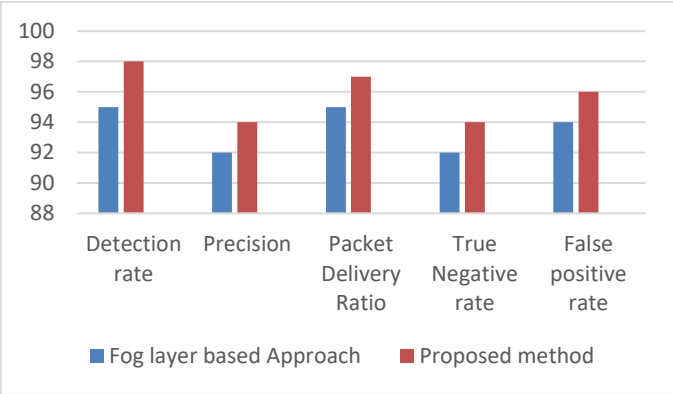

Fig 1: Comparison of the existing system with the proposed method.

VII. CONCLUSION

Here, Renyi entropy is the foundation of the suggested method. The network suggests a novel approach. This technique aids in the network identification of DDoS attacks. Early detection might lessen the victim's adverse effects of the harm. It is applicable to many IoT applications. The packet header is used to extract the source and destination IP addresses. These data are used to determine the Renyi entropy, which is then compared to the dynamic threshold value. Entropy beyond the threshold value indicates a malicious packet, which is why it is discarded. The proposed approach is statistically assessed, and comparisons with other current methods are made. The accuracy rate is greater than the current ones. Hence the proposed system works efficiently.

REFERENCES

[1] A. Zanella , N. Bui, A. Castellani, L. Vangelista, & M. Zorzi, “Internet of things for smart cities”, IEEE Internet of Things Journal, Vol.1, Issue 1, pp. 30–34, 2014.

[2] J. Mathew, R. J. Priyadarsini, “A Review on DoS Attack on IoT”, Solid State Technology, Vol. 63, Issue. 4, pp. 8000-8009, 2020.

[3] L. Liang, K. Zheng, Q. Sheng, & X. Huang, “A denial of service attack method for an IoT system”, 8th international conference on information technology in medicine and education, Vol. 5, pp. 1–3, 2016.

[4] S. Kajwadkar, and K. J. Vinod, "A Novel Algorithm for DoS and DDoS Attack Detection in Internet of Things.", 2018 Conference on Information and Communication Technology (CICT), IEEE, 2018.

[5] P. Redekar, and C. Madhumita, "A Novel Hybrid Approach for Detection of DDoS Attack.", International Conference on Intelligent Data Communication Technologies and Internet of Things. Springer, Cham, 2018.

[6] V. S. Reddy, K. D. Rao, and P. S. Lakshmi, "Efficient detection of DDoS attacks by entropy variation." IOSR Journal of Computer Engineering, Vol 7,Issue. 1, pp.13-18, 2012.

[7] A. Gaurav, et al. "Fog Layer-based DDoS attack Detection Approach for Internet-of-Things (IoTs) devices", 2021 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2021.

[8] U. Kumar, et al. "Isolation of DDoS attack in IoT: A new perspective." Wireless Personal Communications, Vol. 114, pp. 2493-2510, 2020.

[9] P. Bereziński, J Bartosz, and S. Marcin, "An entropy-based network anomaly detection method." Entropy, Vol. 17, Issue.4, pp.2367-2408, 2015.

[10] X. Wang, et al. "DDoS Attack Detection Algorithm Based on IP Entropy Model.", Proceedings of the 2015 International Industrial Informatics and Computer Engineering Conference, pp.179-182, 2015.

[11] A. Bhandari, A. L. Sangal, and K. Krishan K, "Destination address entropy based detection and traceback approach against distributed denial of service attacks", International Journal of Computer Network and Information Security, Vol 7, Issue. 8, pp. 9-20, 2015.

[12] S. M. Mousavi, and M. St-Hilaire, "Early detection of DDoS attacks against SDN controllers", 2015 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2015.

[13] Kim, H. ., Jeong, Y. ., Seo, S. ., Youn, J. ., & Lee, D. (2023). A Study on Radiant Heat Application to the Curing Process for Improvement of Free-Form Concrete Panel Productivity. International Journal of Intelligent Systems and Applications in Engineering, 11(4s), 157–164. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2583

[14] M. Aladaileh, et al. "Entropy-Based Approach to Detect DDoS Attacks on Software Defined Networking Controller", CMC-COMPUTERS MATERIALS & CONTINUA, Vol. 69, Issue. 1, pp. 373-391, 2021.

[15] Martínez, L., Milić, M., Popova, E., Smit, S., & Goldberg, R. Machine Learning Approaches for Human Activity Recognition. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/146

[16] S. M. Mousavi, and M. St-Hilaire. "Early detection of DDoS attacks against SDN controllers." 2015 International Conference on Computing, Networking and Communications (ICNC). IEEE, 2015.

[17] A. Gaurav, et al. "Fog Layer-based DDoS attack Detection Approach for Internet-of-Things (IoTs) devices." 2021 IEEE International Conference on Consumer Electronics (ICCE). IEEE, 2021.

[18] S. Kajwadkar, and K. J. Vinod, "A novel algorithm for DoS and DDoS attack detection in internet of things", 2018 Conference on Information and Communication Technology (CICT), IEEE, 2018.