Entropy Based Deep Attention Mechanism (EDAM) To Mitigate Denial of Service (Dos) Attack Orchestrated Through Idempotent Operation

S.Vijayalakshmi[1], Dr.V.Prasanna Venkatesan[2]

[1] Research Scholar, Department of Banking Technology, Pondicherry University, Pondicherry, India.
[2] Professor, Department of Banking Technology, Pondicherry University, Pondicherry, India.

Correspondence should be addressed to S.Vijayalakshmi; samvijirajesh1980@gmail.com

ABSTRACT- Measuring entropy in a system represents the degree of uncertainty that characterizes the smooth, free and fair conduct of the network operations. The change in quantum of entropy value raises an alarm of the unscrupulous behavior in the vicinity of the network. The continuous inspection of network characteristics and internet flow profiling maintains a constant vigil of the state, behavior and actions performed by the participating hosts in the network. The traffic flow from the multiple senders to either same/different receiver evinces a significant entropy escalation trend as the network composition at any timestamp is a rightful mixture of quality transmission attributes like source IP address, destination IP address, Sequence no. This suffers a setback when the senders camouflaging as legitimate ones tries to fool the network administrators of the impending threat viz. DoS (Denial of Service) attack that the adversary may wish to coordinate via an idempotent HTTP Get Request operation. A request method is considered idempotent if the intended effect on the destination server with multiple identical requests is the same as the effect for a single such request. It produces the same result when executed over and over again. This ambiguous request operation directed from multiple/single sender to the intended receiver generates a broadcast storm that dampens the network services to the core. The ability of the idempotent nature is to generate as many genuine requests as possible and swamp the receiver with HTTP Get request packets. The receiver believes that the same host connection metric per flow count is generated by multiple senders but the reality is reverse. The proposed solution to this problem is to aggregate and maintain a time stamp based and granular based flow attributes reserved for future entropy synchronization at several intermediate routers which will serve as evaluation checkpoints for the receiver. This Entropy based Deep Attention Mechanism (EDAM) coupled with DES (Deferred Entropy Synchronization) acts as a determinant for receiver to perform multi-level cross verification at different time instants and perform deferred synchronization with the reserved values. The performance of this deep attention based entropy synchronization approach witness a deep spike in prediction accuracy and this is plotted with no. of idempotent attackers in the x axis and the improved accuracy in Y axis.

KEYWORDS- Entropy, Denial of Service Attack, Deep Attention, Idempotent Operation.

I. INTRODUCTION

The entropy is a measure of uncertainty/randomness that exists in a given composite system to validate the genuinity of the participating elements that exhibits the goal oriented behaviour in complete sense to promote the smooth and complete conduct of the network operations to the core [1]. An attack free network has negligible divergence from the established Baseline Behavior Profile (BBP) and it reflects the true composition of heterogeneous activities occurring between different valid source IP address and destination IP address witnessing an increase in entropy value [2][3].

The escalating trend in entropy values guarantee the proper functioning of the network with free and fair resource allocation to the participating entities. The idempotent operation has the effect in producing similar/same result even when performed for several times. Big challenge rests with uncovering idempotent operation that launches a stealthier DoS attack without it being explicitly noticed by the genuine nodes present in the network. The BBP is dynamically tuned in accordance with the current network traffic features and it helps in determining the initial and subsequent values of the flow attributes by using the concept of adaptive threshold [4].

The infected network with any of the attack class manifest unidirectional transmission of packets from the source flooding to the same destination culminating to clogging of network resources like bandwidth, computation, communication and storage ability. The system under attack spree promulgates homogenous network actions yielding to deteriorating entropy value attesting the occurrence of illegitimate activities targeting a gullible victim node [5].

The cumulated entropy of the flow features of the system are considered for several epochs and a DES operation performed on it shows either a steady declining/improving trend. The witnessed improving trend promises free and fair network activities with minimal/zero intervention by the attackers [6][7].

The declining trend in the entropy value reiterates the presence of intruder in the system deliberately molesting the network and its associated resources. The granular entropy weight calculation for diverse flow features executed for several epochs either reflects the consistent increment in variation signaling the network traffic to be normal ie multiclass or declining trend in variation depicts the traffic to be abnormal and categorized to the same attack class [8][9].

The calibration of entropy aggregation and variation of different flow features helps to detect the early occurrence of attack and the influential feature that leverages the detection rate to a greater extent. A thorough causality study of potential routing flow features and their glaring variational impact in robust mining of the presence of DoS intruder in the network is conducted [10].

The enormous amount of generated big data traffic encourages deep attention-based entropy calculation and hierarchical processing of different features. This deep attention technique assists in intermittent storing, verifying, validating and deferred synchronizing of the aggregated entropy values of the potential flow features used to disclose the identity of the attacker. In a bid to maintain an unwavering entropy value despite the attacker's presence and its malevolent attitude of disrupting the normal network conduct by launching an idempotent HTTP Get Request operation. The stealthy sender deliberately launches a Denial of Service attack on the receiver by flooding with Bogus HTTP Get Request Operation generated through idempotent mode [11][12].

The sender under the pretext of forwarding legitimate route request to the receiver performs scrupulously the idempotent operation with HTTP Get Request metric. The implementation time of this idempotent operation serves as a buffer/cushion variable for the network to analyze the impending and incumbent vulnerable intruders to the system based on large scale feature variations [13] [14]. Thus with this idempotent operation, the source node impersonating as legitimate node conceals the orchestration and implementation of the DoS attack.

II. LITERATURE SURVEY

Wang. et al (2020) [1] recommends the adoption of Multi Layer Perceptron (MLP) based sequential feature selection to expedite the intrusion detection process with minimal delay and error and an effective feedback mechanism to reconstruct/renovate the error prone detector producing an high false alarm rate. The validation of the effectiveness of this method is compared with some related works and the results showed that our method could yield comparable detection performance and correct the detector when it performed poorly. Kaur. Et al (2017) [2] proposes a classification of detection approaches against DDoS attacks with an aim to go deep insight into the DDoS problem for the beginners in this research area. The detection approaches have been explained along with their pluses and minuses. Further, this review paper includes the different functional classes to which the detection approaches belong to. In the end, a comparison of signature-based, anomaly-based and hybrid detection approaches is depicted in tabular form. Aamir. et al (2019) [3] recommends the adoption of feature engineering approaches like backward elimination, chi2 and information gain score to reduce the dimensionality of datasets and apply supervised machine learning models over it to enable faster detection with less error rate. This feature-engineered dataset is likely to produce a better DDoS detection accuracy with KNN algorithm. Low dimensions dataset of discrete features produce better results with Random Forest as compared to high dimensions of numerical features. The reduced feature space will offer a better accuracy with less processing overhead and high detection efficiency.

Corin. Et al (2020) [4] reiterates the applicability of Convolutional Neural Network in to the DDoS detection that requires the deployment of lightweight, practical deep learning model with dataset-agnostic preprocessing mechanism to produce traffic observations and an activation analysis for LUCID's DDoS classification. This model is empirically validated on a resource-constrained hardware platform matching the state-of-the-art detection accuracy with 40x reduction in processing time and overhead.

David. Et al (2015) [5] discusses the applicability of Fast entropy, flow-based analysis and adaptive threshold algorithm being concurrently deployed to produce better detection accuracy of DDoS attack when the network activities and user's behavior continuously changes over time. Fast entropy of request per flow is considered and the difference in the entropy values between the discrete, instant point and mean value of the entropy at the particular time interval if greater than adaptive threshold signaling the presence of DDoS intruder. The adaptivity nature of threshold is attributed to reflect the current traffic pattern/condition.

Singh. et al (2016) [6] highlights the objective of the paper in detecting DDoS attack using MLP as classification algorithm and Genetic algorithm as learning algorithm. The parameters selected are HTTP GET request count, entropy and variance for every connection. The proposed model can provide a better accuracy of 98.31%, sensitivity of 0.9962, and specificity of 0.0561 when compared to other traditional classification models.

Tritilanunt. et al (2010) [7] analyses the detection mechanism based on a technique of entropy-based input-output traffic mode detection scheme. The experimental results demonstrate that this approach is able to detect several kinds of denial-of-service attacks, even small spike of such attacks. The usage of volume-based schemes to detect attacks fails miserably to inspect short-term DoS attack and cannot distinguish between heavy load from legitimate users and huge number of bogus messages from attackers. Basicevic. et al (2015) [8] opines that Cumulative sum control chart (CUSUM) algorithm is deployed for change-point detection. CUSUM based monitoring of entropy of several packet distributions, source and destination ports, number of packets and bytes transferred, synchronize sequence numbers (SYN) packets escalates the generalizability perspective as it assists in detection of many different types of attacks and network anomalies. Khan. et al (2019) [9] advocates the selection of potential attributes that truly characterize the DDoS attack based on computed weight for each of the attributes using entropy calculation. However, this mechanism fails to capture/identify the potential attributes that needs to be addressed on its early occurrence. The selection of potential attributes based on user-defined chosen granulation is also given using NSL KDD dataset. Gupta. Et al (2018) [10] opines the adoption of blended Machine learning approach with chosen Feature selection algorithm and classification algorithm to maximize the attack prediction accuracy to 99.83%. Once the Weighted Ranked Feature Selection (WRFS) algorithm is deployed the network traffic to the established socket is captured and analyzed for any attack instance. This trained model is optimized to finetune the minimal attributes to define the attack class to which the packet belongs. Idhammad. et al (2018) [11] proposes a detection system of HTTP DDoS attacks in a Cloud environment based on Information theoretic entropy and random forest ensemble learning algorithm. Network header features of the incoming network traffic are analyzed using time-based sliding window algorithm. The preprocessing and classification tasks are triggered when the estimated entropy exceeds its normal range. The proposed approach achieves satisfactory results with an accuracy of 99.54%, a FPR of 0.4%, and a running time of 18.5s. Nayaz. et al (2013) [12] highlights the idea of merging Entropy based System with Anomaly detection System for providing multilevel Distributed Denial of Service (DDoS). Detection algorithms running within the network allows only legitimate users inside the network. Confirmation algorithms deployed in router present in the cloud site checks for the threshold value to label it as either genuine or intruder in the environment.

Altaher. Et al (2011) [13] recommends the adoption of real time anomaly detection system based on relative entropy. The proposed system uses adaptive filter and relative entropy to dynamically determine the traffic changes in the captured network traffic and examines it as normal or anomaly. The experimental results show that the proposed system is efficient for on-line anomaly detection, using traffic trace collected in high-speed links. Ujjain. Et al (2021) [14] discusses the idea of proposing a generalized entropy calculation by combining Shannon and Renyi entropy to decipher the potential distributed features of DDoS traffic. It also helped the Software Defined Networking (SDN) controller to meticulously thwart the heavy malicious traffic. Stacked Auto Encoder (SAE) and Convolutional Neural Network (CNN) models were improvised using entropy-based features to attain a progressive growth in detection accuracy. Quantitative results demonstrated SAE achieved relatively higher detection accuracy of 94% with only 6% of false-positive alerts, whereas the CNN classifier achieved an average accuracy of 93%.

III. A BRIEF STUDY ON ENTROPY AND DEEP ATTENTION MECHANISM

A. Entropy

Entropy is a information theoretic concept used to measure randomness and uncertainty of a random variable. The high degree of randomness of a variable signifies a high entropy and vice versa. Shannon entropy is a type of generalized information entropy used to quantify the diversity of the randomness or uncertainty of a system. It is also an important metric in statistics for calculating the uncertainty index. Appreciating widespread application in diverse fields like mass oscillators, acoustic emission detection, image randomness, fuzzy setting, fuzzy concept lattice and finance, this has potential usability in detecting DDoS attack by analyzing/measuring the randomness of packets generated during the attack.

B. Deep Attention Mechanism

Attention is direct application of the keen focus at something and taking greater notice of it. The attention mechanism in Deep Learning is attributed to the concept of coordinating and directing your focus to some specific/special information in intelligent processing of data that derives comprehensible knowledge and latent patterns which aids in value addition of the data. Attention can also be described as a discrete component of a network's architecture that manages and quantifies the interdependence between the input and output elements (General Attention) and within the input elements (Self-Attention). Attention Mechanism has a wider application in diverse fields of deep learning such as Computer Vision, Self-driving cars, Automatic machine translation and Automatic text generation but its main breakthrough and success comes from its application in Natural Language Processing (NLP) tasks [15].

This mechanism allows the model to focus and place more "Attention" on the relevant parts of the input sequence as needed and retains the most important and the hidden/forgotten context/states that aids in sensible semantic reconstruction of the decoder that unpacks an intelligent translation of the text that is fed to the encoder. The applicability of this mechanism in intrusion detection system is encouraged by its power of intellectual selection of important/potential flow features and its retainment capacity that truly characterize the attack scenario and classifies it to any of the multi class attack types [16].

C. Deep Learning

Deep Learning (DL) a derivative of Machine Learning with a deeper network of neurons in multiple layers has come to the rescue with its automated dynamic feature learning ability to decipher/mine the features obviating the need for a domain expertise. Deep learning is a derivative of ML models where it exploits the cascaded layers of data processing stages in a hierarchical structure for Unsupervised Feature Learning (UFL) and pattern recognition [17].

DL based Classifier has made remarkable strides in maximizing the attack detection accuracy and classification efficiency of IDS. It attempts to represent the world as a nested hierarchy of concepts with higher level concepts explained in terms of lower-level concepts.

D. Idempotent Operation

Idempotence is an important concept in the HTTP specification that states idempotent HTTP requests will result in the same state on the server no matter how many times that same request is executed. The multiple identical requests should have the same effect as a single request [18]. Methods GET, HEAD, OPTIONS and TRACE, being prescribed as safe, should also be idempotent, as HTTP is a stateless protocol. Figure 1 illustrates the conceptual diagram of idempotent operation leading to Denial of Service Attack.

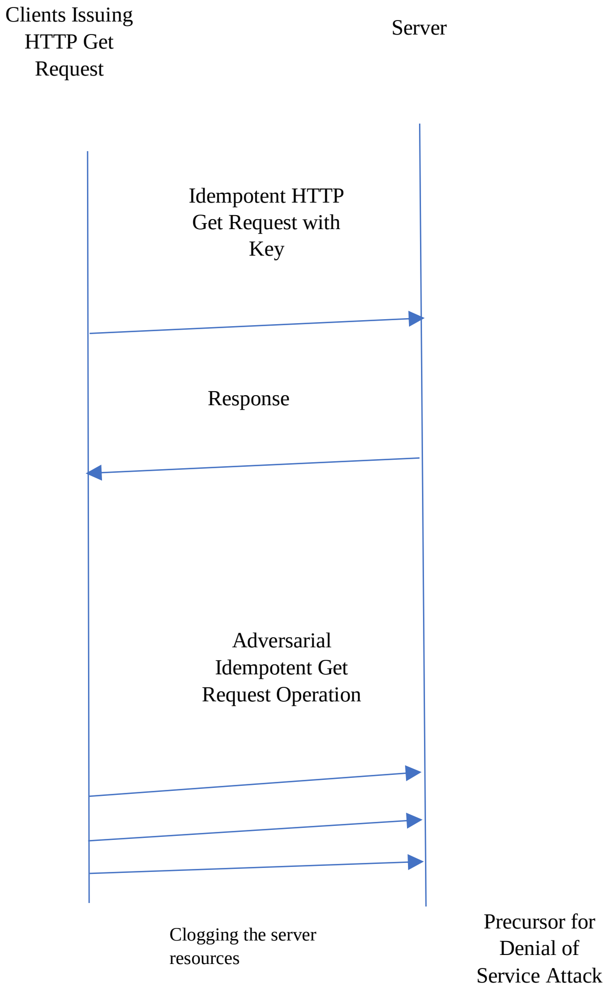
Clients Issuing HTTP Get Request
Server
Idempotent HTTP Get Request with Key
Response
Adversarial Idempotent Get Request Operation
Clogging the server resources
Precursor for Denial of Service Attack

Fig 1: Diagram Illustrating Idempotent Operation.

IV. EDAM OPTIMIZER USING DES

This resource contentious receiver deploys a tricky mechanism to outwit the unscrupulous senders intending to clog them by pumping extraneous HTTP Get request packets using idempotent operation. The receiver has to apportion a part of its network resources to continuously inspect the reserved RREQ packets for any breach of the established/baseline communication procedure.

The entropy weight aggregation (granular) of flow features of the HTTP Route request packets at the bifurcation point in the application gateway interface/router is reserved for future validation by the receiver. The handicap of the destination node in effectively discerning the genuine and idempotent HTTP Get Request operation compels the deployment of EDAM optimizer in churning out the attacker that orchestrates idempotent operation. The deciphering of this idempotent activity by consistently validating the discrepancy between the stored entropy value at diverse points and the actual entropy value received by the receiver rests with the construction of intelligently configured entropy estimation table depicting the aggregated flow features. Two-fold aggregations of the HTTP RREQ packets at each network checkpoint on intermediate router is performed with time and destination IP address as underlying attribute. Chronological based multi-level feature aggregator serves as a catalyst to mitigate the impact of idempotent HTTP Get Request operation attributing to DoS attack. Differential mapping of the computed entropy values of flow features stored at intermediate routers during the routing process with the received features at the destination end clearly signifies the presence of an intruder intending to embark on and implant DoS attack in the network.

The potential features to be analyzed includes source and destination port and address, Number of bytes and packets sent to remote hosts, Number of bytes packets received by the local host, TCP flags, especially SYN, RST and FIN flags and duration of the connection. The recommendation of deploying flow features in granular level relaxes the computation overhead and processing time than incurred for individual feature processing at every checkpoint. The disparity existing between the aggregated features viz. No. of RREQ packets with respect to a particular time and destined receiver node and the actual features in the receiver node gives demographic details of the entropy variation in a concrete manner uncovering the latent idempotent operation. The flow-based analysis for a given time window/interval represent a skewed nature of this considered metric aimed at knocking out the particular receiver with a flood of RREQ packets.

Table 1: Initial Entropy Estimation Table (EET)
Client

Source IP	Destination IP	No. of Bytes Sent/Received	Sequence No.	Initial Entropy	Timestamp
A	B	155	5	0.9	T0
				(Estimated entropy between source and destination node)	

Table 2: EET for Router 1- Intermediate Router 1

Source IP	Destination IP	No. of Bytes Sent/Received	Sequence No.	Timestamp	Router 2	Last Hop Router	GE2
A	B	155	5	T2	Router 2	Router 3	0.3

Table 3: EET for Router- Intermediate Router 2

Source IP	Destination IP	No. of Bytes Sent/Received	Sequence No.	Timestamp	Last Hop Router	Receiver	GE3
A	B	155	5	T3	Router 3	Server	0.3

Table 4: EET for Router 3- Intermediate Router 3

Server

Source IP	Destination IP	No. of Bytes Sent/Received	Sequence No.	Intermediate First Hop Router	Intermediate Next Hop Router	Granular Entropy (at diverse intermediate routers)	Deferred Entropy Synchronization	Timestamp	Genuine/Fake Request (Deferred Entropy Analysis)
A	B	255	5	Router 1	Router 2	0.3	0.5	T1	
				Router 2	Router 3	0.3	0.6	T2	
				Router 3	Server	0.3	0.5	T3	Server Entropy (Received) – 1.6 (Actual) – 0.9
Classified as									Idempotent DoS Attack

Table 5: Final Entropy table assessing the integrity of HTTP Request Operation

Source IP	Destination IP	No. of Bytes Sent/Received	Sequence No.	Timestamp	First Hop Router	Router 2	Aggregated/Granular Entropy (GE1) at Router 1
A	B	155	5	T1	Router 1	Router 2	0.3

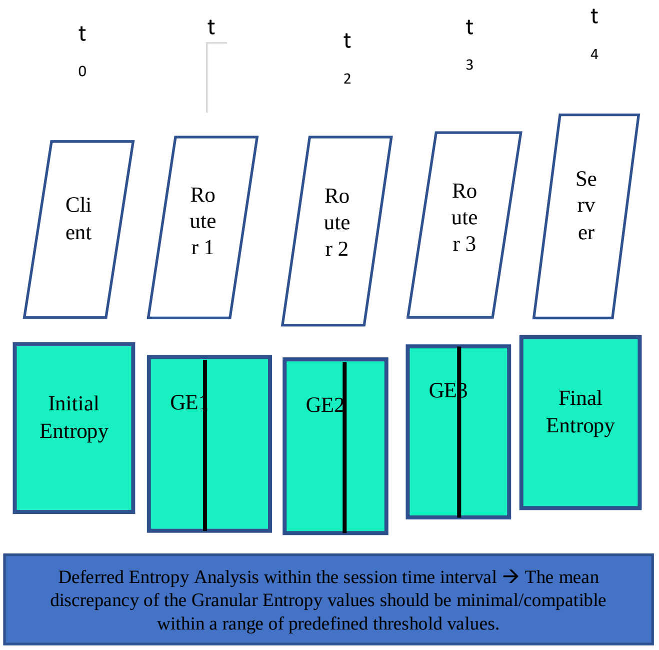
t 0
t
t 2
t 3
t 4
Client
Router 1
Router 2
Router 3
Server
Initial Entropy
GE1
GE2
GE3
Final Entropy
Deferred Entropy Analysis within the session time interval → The mean discrepancy of the Granular Entropy values should be minimal/compatible within a range of predefined threshold values.

Fig 2: Diagram Showcasing the Calibration of Granular Entropy and Deferred Entropy Analysis

Figure 2 showcases the calibration of granular entropy and deferred entropy analysis. Table 1 highlights the initial Entropy Estimation Table (EET) for client invoking HTTP Request operation. Tables 2 through 4 represents the EET for the Intelligent Intermediate Routers 1,2,3. Table 5 represents the Final Entropy table assessing the integrity of HTTP Request Operation.

V. SIMULATION STUDY

The deployment of deep attention mechanism in routing feature's entropy calculation behaves as a detrimental force in curbing out the HTTP Get Request DoS attack operated through idempotent fashion. The idempotent operation has an inherent latent potential in causing an avalanche/cascading effect on the routing process and slowing down the server in offering uninterrupted service to the legitimate users of the network. The outcome of idempotent execution remains constant invariant to the number of operations executed at different time instants. EDAM optimizer helps to weed out the hidden idempotent operation by performing deferred entropy synchronization of received potential features like Destination IP address, No. of bytes sent/received, Timestamp, Granular entropy in the receiver with the intermediate aggregated values stored in the Intelligent/smart Network checkpoints. The glaring difference in the entropy values of the selected features indicates the presence of an intruder performing Idempotent DoS operation in a stealthy mode. Iteration of this two-fold EDAM synchronization for several epochs trains proactively the network in distinguishing the legitimate and illegitimate route request aimed at launching a DoS attack by leveraging the idempotent ability. Graphs are plotted with increasing EDAM optimizer nodes in the x axis and attack detection accuracy in the y axis as shown in Figure 3. The higher the genuine nodes partaking in EDAM optimization process the higher is the attack detection rate and accuracy. The participation of more and influential flow features in EDAM and DES process invigorates the attack classifier to be more resilient and robust.

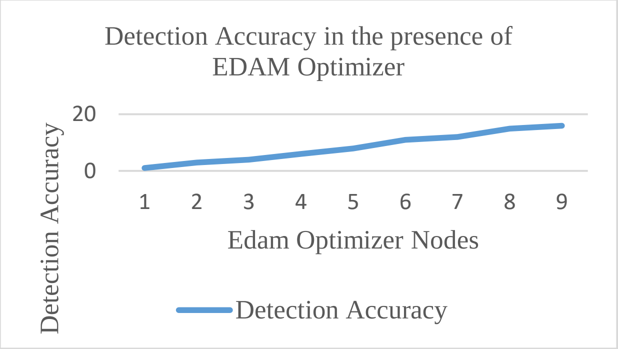

Fig. 3: Detection Accuracy in the presence of EDAM optimizer

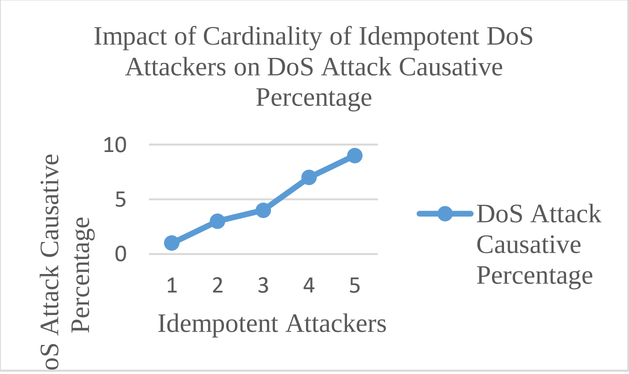

Fig. 4: Impact of cardinality of Idempotent DoS Attackers on DoS Attack Causative Percentage

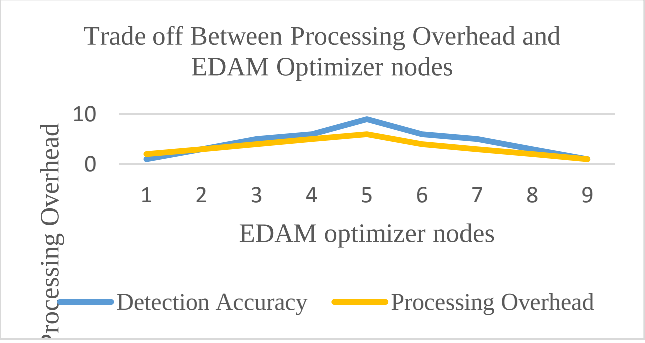

Fig. 5: Trade-off between Processing Overhead and EDAM Optimizer nodes.

The more the number of Idempotent DoS attackers induces a spike in attack causative percentage as witnessed in figure 4. The more nodes partaking in EDAM synchronization results in increased detection accuracy with increased processing overhead as shown in figure 5.

VI. CONCLUSION

The receiver's agility serves as a precursor for intelligently validating the genuinity of HTTP Route Request packets in syphoning off the perils of DoS attack and its impact. The significant variation in flow-based features and its associated entropy calibration has a high telling effect on the smooth conduct of network operations. The smart hacker tries to intellectually deceive this entropy variation by performing network operations through idempotent manner. The proposed method requires the intelligent destination node to perform a deferred entropy synchronization of the received flow features with the actual aggregated entropy of the features that had been forwarded through intelligent routers in the routing path established between the source and destination. Chronological based multi feature aggregation based on destination IP address and timestamp of the originated route request calculated at several intermediate checkpoints are reserved for future synchronization and comparison. The disparity in entropy synchronization values between the destination node and the intermediate aggregated values uncovers the presence of idempotent operations disrupting the normal conduct of network operations. Graphs are plotted to showcase and validate the research contributions of this work in routing process empowerment against stealthy idempotent operation and offers seamless adversary free routing between the sender and the receiver.

CONFLICTS OF INTEREST

The authors declare that they have no conflicts of interest.

REFERENCES

[1] Wang, M., Lu, Y., Qin, J., "A dynamic MLP-based DDoS attack detection method using feature selection and feedback", Elsevier, Computers and Security (88), 2020.

[2] Kaur, P., Kumar, M., Bhandari, A., "A review of detection approaches for distributed denial of service attacks", Systems Science & Control Engineering, pp. 301-320, DOI: 10.1080/21642583.2017.1331768.

[3] Aamir, M., Mustafa,S., " DDoS attack detection with feature engineering and machine learning: the framework and performance evaluation", International Journal of Information Security (2019) pp. 761–785 https://doi.org/10.1007/s10207-019-00434-1, Springer Nature 2019.

[4] Corin, R.D., Millar, S., Hayward, S.S., Rincon, M., Siracusa, D., "LUCID: A Practical, Lightweight Deep Learning Solution for DDoS Attack Detection" IEEE Transactions on Network and Service Management, t https://doi.org/10.1109/TNSM.2020.2971776.

[5] David, J., Thomas, C.," DDoS Attack Detection using Fast Entropy Approach on Flow Based Network Traffic", 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

[6] Singh, K.J., Thongam, K., De, T., "Entropy-Based Application Layer DDoS Attack Detection Using Artificial Networks", MDPI, Entropy 2016, 18, 350; doi:10.3390/e18100350

[7] Tritilanunt, S., Sivakorn, S., Juengjincharoen, C., Siripornpisan, A., "Entropy-based Input-Output Traffic Mode

Detection Scheme for DoS/DDoS Attacks", 978-1-4244-7010-5/10/2010 IEEE

[8] Basicevic, I., Ocavaj, S., Popovic, M., "Evaluation of entropy-based detection of outbound denial-of-service attacks in edge networks", Security and Communication Networks, Security Comm. Networks 2015; pp. 837–844,

[9] Khan, S., Gani, A., Wahab, A.W.A. *et al.* Feature Selection of Denial-of-Service Attacks Using Entropy and Granular Computing. *Arab J Sci Eng* **43,** 499–508 (2018). https://doi.org/10.1007/s13369-017-2634-8

[10] Gupta, A. (2018). Distributed Denial of Service Attack Detection Using a Machine Learning Approach (Unpublished master's thesis). University of Calgary, Calgary, AB doi:10.11575/PRISM/32797

[11] Idhammad, M., Afdel, K., Belouch, M., " Detection System of HTTP DDoS Attacks in a Cloud Environment Based on Information Theoretic Entropy and Random Forest", Security and Communication Networks Volume 2018, https://doi.org/10.1155/2018/1263123

[12] Nayaz, A.S.Syed, Sangeetha, V., Prabhadevi, C., "Entropy based Anomaly Detection System to Prevent DDoS Attacks in Cloud", International Journal of Computer Applications (0975 – 8887) Volume 62– No.15, January 2013.

[13] Altaher, A., Ramadass, S., Almomani, A., "Real Time Network Anomaly Detection Using Relative Entropy", 978-1-4577-1169-5/11/$26.00 ©2011 IEEE

[14] Ujjan, R.M.A., Zeeshan Pervez, Z., Dahal, K., Khan, W.A., Khattak, A.M., Hayat, B., "Entropy Based Features Distribution for Anti-DDoS Model in SDN", Sustainability 2021, 13, 1522. https://doi.org/10.3390/su13031522 https://www.mdpi.com/journal/sustainability.

[15] https://wiki.pathmind.com/attention-mechanism-memory-network

[16] https://blog.floydhub.com/attention-mechanism/

[17] Kim, K., Aminanto, M.E., "Deep Learning in Intrusion Detection Perspective: Overview and Further Challenges", IWBIS 2017 978-1-5386-2038-0/17/$31.00 c 2017 IEEE

[18] https://tools.ietf.org/id/draft-idempotency-header-00.html

ABOUT THE AUTHORS

Mrs. S. Vijayalakshmi an M.C.A., M.Phil. graduate currently pursuing Ph.D. in Dept. of Banking Technology, Pondicherry University. Her research interest includes Artificial Intelligence, Cyber security, Deep Learning and applications of DL models in security engineering mainly on domains such as Intrusion/Anomaly Detection System. I have 12 years of teaching and research experience and have scholarly publications in international repute conferences and erudite blind peer-reviewed journals.

Dr. V. Prasanna Venkatesan, Professor, Dept. of Banking Technology, Pondicherry University has research thrust on domains like software architecture, service oriented architecture, Business Intelligence, Smart Banking, Banking Technology. Eleven scholars have successfully earned their Ph.D degree under his able guidance and support. He has 27 years of teaching and research experience to his credit. He has meticulously completed one project and has 127 publications in peer-reviewed international conferences and journals.