Adaptive Self Organizing Maps Inspired SDN-Based DDoS (ASOM-SDN-DDoS) Mitigation Framework

Pillutla Harikrishna, A. Amuthan

Abstract: The integration of cloud computing with Software Defined Networking (SDN) has improved several features like scalability, flexibility, cost saving, sustainability and quality control. But similar to other network, SDN- based cloud is susceptible to various kinds of security issues like Distributed Denial of Service, Data Breaches and Phishing. Out of these security issues Denial of Service causes major harm to SDN-based cloud. In order to classify a normal traffic with that of malicious traffic three types of Self Organizing Maps namely Fuzzy Self Organizing Maps (FSOM), Rival Model Penalized Self Organizing Maps (RMPSOM) and Convolution Recursively Enhanced Self Organizing Map (CRESOM) have been used. The comprehension description of the proposed Adaptive Self Organizing Maps inspired SDN-Based DDoS (ASOM-SDN-DDoS) mitigation framework with its role and applications that focuses on effective detection and isolation of DDoS attacks in SDN-based cloud computing environment is presented in this paper. The option of integrating three categories of the SOM-based DDoS attack mitigation mechanisms that derives the merits of FSOM, RMPSOM and CRESOM into this adaptive framework. The predominance of the proposed ASOM-SDN-DDoS mitigation framework when compared with baseline DDoS attack mitigation frameworks investigation using simulation experiments are portrayed. In addition, the proposed ASOM-SDN-DDoS mitigation framework with its suitability and applicability is also explored and highlighted.

Index Terms: DoS, DDoS attack, DDoS framework, Self Organizing Maps, Cloud Computing, Software Defined Networking, SDN based Cloud

1 INTRODUCTION TO ASOM-SDN-DDOS FRAMEWORK

THE existence of the DDoS attack [1],[2],[3] in the SDN-based cloud computing [4] is considered as the serious threat, since the hosts that are controlled by attackers are forced to send huge amount of data to the victims without any essential purpose. This DDoS attack is responsible for creating great imbalance in the cloud environment through the minimization of processing ability of the network systems and servers that directly reduces its processing potential due to maximum exhaustion. Most of the DDoS mitigation frameworks [5] contributed in the literature essentially necessitates a separate entity for the collection and exploration of data traffic such that stochastic and machine learning-based investigation can be facilitated in an efficient manner. The existing frameworks maximally utilized additional space for classifying the cloud data traffic into genuine and malicious data traffic. The existing frameworks were also operated in the offline mode for effective determination of attack source that initiated the maliciousness in the cloud computing environment. However, Software Defined Networking (SDN) [6],[7],[8] is the potential perspective that wide opens the option of incorporating the process of significant monitoring and network resources by separating the data plane from the control plane. This option of separating the data plane and control plane in SDN facilitates potential configuring, managing, monitoring and controlling of network resources through the enforcement of software routines that are stored in the controller. Further, SDN [9],[10],[11],[12] using OpenFlow is another significant enhancement that aids in sustaining the connection between the control and data plane such that messages could be sent and received from the controller and the open switches. The utilization of OpenFlow also aids in collecting network-associated factors from the SDN such that it helps in detecting and responding to the DDoS attacks in the cloud computing environment. Furthermore, the utilization of multiple classifier using variant self-organizing maps in SDN is determined to be significant in potential detection of DDoS attacks. In addition, the adaptation of botnet tracking and reactive action response in DDoS defence is estimated to improve the rate of detection with improved accuracy. Thus, an Adaptive Self Organizing Maps inspired SDN-Based DDoS (ASOM-SDN-DDoS) mitigation framework that incorporates the utilization of multiple classifier using variant self-organizing maps in SDN with flexible botnet tracking and reactive action response in DDoS is proposed for enhancing the rate of detection with improved accuracy. In FSOM [13],[14] novel fuzzy rules were generated to detect a malicious traffic from a normal traffic. RMPSOM [15] deals about conserving the topological structure for the input data. Based on the topological structure the neighboring neurons can be detected more seamlessly. The addition of constant learning rate improves the detection between normal and malicious traffic much faster. For improving the initialization process CRESOM [16] makes use of merging and splitting. The merging and splitting process is helpful in facilitating the discovery of high-density area. With the help of discovery of high- density area, a different topology is created that would be helpful in reducing the adaptation rate of the neurons. To prove the performance improvement of the proposed ASOM-SDN-DDoS mitigation framework, it is compared with three existing frameworks namely: OVERWATCH-SDN-DDoS [17], COLLABORATIVE-SDN-DDoS [18] and BSSGC-DDoS [19] mitigation frameworks. In OVERWATCH-SDN-DDoS, a cross-layer DDoS attack is detected and mitigated. This framework makes use of the cooperative intelligence that is shared between the data plane and the control plane. In order to be more potent, Overwatch makes use of two separate algorithms for DDoS detection. For the DDoS attack detection, Overwatch uses a coarse-grained flow monitoring algorithm that has been implemented on the data plane as well as a fine-grained machine learning- based attack classification algorithm implemented on the control plane. For DDoS defence strategy, Overwatch employs

- *Pillutla Harikrishna is currently pursuing his PhD in Department of Computer Science and Engineering at Pondicherry Engineering College, Pondicherry, INDIA, Email: pillutlaharikrishna@yahoo.co.in.*
- *A. Amuthan is Professor in Department of Computer Science and Engineering at Pondicherry Engineering College, Pondicherry, INDIA, Email: amuthan@pec.edu*.

different defence applications that are implemented on various controllers and switches which is helpful for faster DDoS attack reaction along with accurate location of the botnet. The COLLABORATIVE-SDN-DDoS makes use of a secure and robust (C-to-C) controller-to-controller protocol. Using this (C to C) protocol the communication that takes place between SDN controllers in different autonomous systems (AS) is more secure. Another benefit of this protocol is that the attack information could also be transferred between different AS. It also helps in the providing a potent filtering mechanism closer to the origin of the attack. In BSSGC (Bifold SDN based Solution using Genetic algorithm and Covariance matrix)-DDoS mitigation framework, a bitfold approach is used to differentiate between a normal and an abnormal traffic. The preliminary decision regarding whether the traffic is normal or not is made by using the genetic algorithm. The genetic algorithm preliminary decision is further evolved by making use of a covariance matrix. The highlights of the paper are mentioned as follows. Section 2 deals about the detailed description of the proposed architecture. The sustainability and application of the proposed framework is mentioned in section 3. The significance of the proposed framework is presented in section 4. In section 5, the simulation results and discussions of the proposed framework is mentioned.

2 DETAILED DESCRIPTION OF THE PROPOSED ASOM-SDN-DDOS MITIGATION FRAMEWORK

The proposed ASOM-SDN-DDoS mitigation framework consists of two separate planes such as control plane and data plane for effective DDoS attack detection as depicted in Figure 1. The mechanisms such as FSOM, RMPSOM and CRESOM are used as the DDoS classifiers in the control plane. This control plane includes the botnet tracker that comprises of tracking thread and topology viewer. The botnet tracker and the proposed DDoS classifiers are connected with the SDN classifier that are in turn connected to the DDoS defence Library and the history repository. The data plane and the control plane of the proposed framework are connected through the OpenFlow like south bound interface. Further, switches acts as the sensor and actuators are used in the data plane for facilitating its connection with the victim server and botnets in the cloud environment. This architecture of the proposed ASOM-SDN-DDoS Mitigation framework is motivated through the merits of the knowledge plane in the SDN. The proposed ASOM-SDN-DDoS mitigation framework includes a defence actuator library, a botnet tracker and DDoS attack classifier that are essential for identifying the sources of the attack generating traffic and its corresponding attacker is incorporated in the control plane. Moreover, the data plane switches of the proposed framework comprise of sensor and actuators for detecting the DDoS attack in this SDN [20]. Further, the sensor in the data plane starts the running process for constantly monitoring each and every flow in the SDN-based networking. The data plane switches are responsible for notifying the existence of DDoS attack traffic in the network using alert messages for determining the attack characteristics such that abnormal flow is detected through the control plane. The proposed framework leverages the option of including the attack characteristics in the control plane in order to detect DDoS attack categories and its attack sources in a global dimension. Then, the defence actuator library is requested by the SDN controller for employing particular kind of defence actuators over the switches that has closest proximity to the botnet detector.

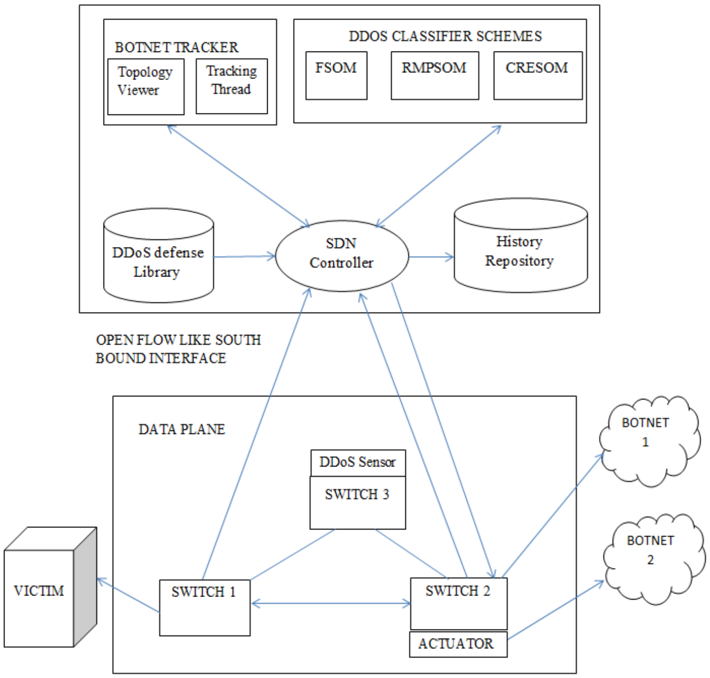


Figure 1: *Architecture view of the proposed ASOM-SDN-DDoS Mitigation framework*

Finally, each kind of DDoS attacks are mitigated through the use of loaded actuator that gets executed depending on the particular kind of switches considered for detection and response. Hence, the core objective of the proposed ASOM-SDN-DDoS mitigation framework focuses on the detection of DDoS attacks in order to respond to them reactively with accuracy in the network. In addition, the proposed ASOM-SDN-DDoS mitigation framework needs the essentiality of including the potential in the data and control plane in an effective and efficient manner.

2.1 Enhancement in the design of data plane and control plane

The data plane considered in the proposed framework does not only possess entities that play the role of forwarding, but they also utilize a collection of sensors and actuators that are responsible for detecting and responding to DDoS attacks. This utilization of sensor and actuators widely opens the option of improving the significant characteristics of the SDN switches in an effective manner. The switches of the data plane are improved with maximum potential for extracting the core features of the DDoS attacks. Then, the response functionalities are transformed from the control plane to the data plane in a reactive manner after the response actions to DDoS attacks is enforced by the control plane. Finally, the actuators are executed in the data plane for filtering out packets that are maliciously introduced by the attackers in the SDN. The control plane used in this proposed ASOM-SDN-DDoS mitigation framework is considered as the brain, since it plays the key role of exploring and reactively identifying the defence strategy that could be deployed for mitigating the existing types of DDoS attacks based on its detected traces. The heart of the control plane in the proposed framework is its intelligent significance that aids in investigating various types of recent DDoS attacks such that they are classified and precisely tracked based on botnets. Thus, the control plane of this proposed ASOM-SDN-DDoS mitigation framework is responsible for attack categorization, botnet tracking and attack response.

2.2 Enforcement of DDoS attack defence actuators

The DDoS attack defence actuators are enforced for detecting the deviation between the normal traffic and malicious traffic. The utilization of actuators is responsible for invoking possible set of strategies that could be used in the control plane for detecting and responding to the influence of the DDoS attacks in the cloud computing environment. The defence actuators in the data plane inspires the working principle of OFX, but a quite number of significant differences also exists in them during the investigation of the parameters that attribute towards DDoS detection process. In this framework, the defence actuators do not maintain any flow table for reducing the number of packets being redirected to the SDN controller. The defence actuators only redirects the packets to the SDN controller only when they satisfy the requirements of the metadata considered in the flow. First, the defence actuator source code is first loaded into the SDN controller for considering a designated switch as a local memory. Then, the source code of the controller is included with the operating system (generally Linux-based) for effective enforcement of DDoS defence. Further, the agent process receives designated identifiers are sent by the actuator registers that are uniquely assigned to each of the actuators considered in the data plane. Further, the actuator forwards the standard data to its associated agent process before the commencement in execution of its initiation function. This process of forwarding standard data is mainly for denoting the potential kind of data packets that are essential to be processed by the SDN-based controller. This process of forwarding standard data enhances the priority rule that could be used for the hardware match that corresponds to the agent process in order to include the metadata for investigating the factors of the data flow into the hardware.

2.3 Incorporated SOM-based DDoS Attack Categorization

In this proposed ASOM-SDN-DDoS framework, the benefits of SOM-based DDoS attack detection approaches such as FSOM, RMPSOM and CRESOM are considered for enhancing the accuracy of detection with minimized false positive rate during the classification of diversified kinds of malicious traffic in the network. These FSOM, RMPSOM and CRESOM approaches are used for determining the type of attack by extracting potential traffic characteristics that are further integrated into an autoencoder for facilitating superior classification using Softmax. The methods of FSOM, RMPSOM and CRESOM approaches are contextually used, depending on the number of features considered for classification. The utilized autoencoder comprises of input layer, hidden layer and output layer that are trained using backpropagation algorithm. This proposed framework uses two autoencoders that are combined with each other in order to facilitate the option of feeding the output of first hidden layer as the input of the second hidden layer. Then, the output of second hidden layer is feeded into the Softmax classifier [21] for effective DDoS attack classification process. Thus, this utilized SOM-based DDoS Attack Categorization process determines the type of DDoS attack depending on the output vector derived from the hidden layers when the collected traffic features are fed as the input vector. The first autoencoder used in thus framework comprises of three layers that pertains to the input (collection of features), hidden and output layers corresponding to the number of nodes used for reconstructing the input vector in an optimal manner. The network determines the weight matrix-based optimal values and bias vector for integrating them in order to discover the significant patterns of the input DDoS attack record considered as input. Then, the second encoder considers the output of first encoder as input and starts computing the second optimal weight matrix with its associated bias vector. Then, the Softmax classifier is responsible for establishing a mapping association between the hidden layer of the second autoencoder to the possible types of DDoS attack features extracted from the data traffic. Again, the network estimates the third optimal weight matrix with its associated bias vector for determining its closeness to the real DDoS type characteristics. In addition, the utilized model can be used for categorising attacks using run traffic record after training them with the past DDoS attack dataset.

2.4 Cooperative Botnet Tracking

The cooperative botnet tracking [22], [23] strategy of the proposed ASOM-SDN-DDoS framework focuses on localizing the switches that has close proximity with the botnets. This localization is essential for improving the potential of defence actuators for ensuring predominant defence over DDoS attacks in the SDN. The botnet tracker algorithm is considered as the cooperative botnet tracking scheme that identifies botnets based on the cooperation between control and data plane such that they are integrated into a built-in module. First, the important requirements for implementing this cooperative botnet tracking strategy relates to the storing of the comprehensive network information (rules used for data forwarding, topology information and link state) on the controller. Secondly, the comprehensive network information stored by the controller has to visible to the other interacting built-in applications. The aforementioned requirements for the enforcement of cooperative botnet tracking strategy is achieved based on the utilization of an improved topology viewer. In particular, cooperative botnet tracking strategy concentrates on the estimation of last hop that is related to the sampled packet, because the determination of last hop aids in extracting vital MAC address that helps the controller in localizing the nearest switch closer to the botnet.

2.5 DDoS attack Reaction Process

Finally, the process of DDoS attack Reaction Process is initiated when the botnet locations and attack categories are determined. In this proposed ASOM-SDN-DDoS framework, the control plane enforces reaction process by triggering particular kind of defence actuators over the data plane entities. In this context, the DDoS defence library that contains different source codes for attack actuators is responsible for registering the reaction process to the event listener. When the DDoS attack is detected, a two tuple Identifier is generated and sent to the event manager to emphasize the data path identity in the SDN-based cloud environment. This two tuple Identifier also highlights the kind of defence strategy used as the response for each category of DDoS attacks initiated by the built-in applications of cloud environment. Further, the two tuple Identifier is forwarded to the defence library and it loads the source code that correlates to the attack characteristics of actuator used in the framework. Finally, the actuator is loaded into each of the switches through the channel of southbound.

3 SUITABILITY AND APPLICABILITY OF THE PROPOSED ASOM-SDN-DDOS MITIGATION FRAMEWORK IN ANALYSING DATA TRAFFIC FLOWS

This proposed ASOM-SDN-DDoS mitigation framework is suitable for analysing the data traffic flow for effective and efficient detection, because volume features and asymmetry features are considered for identifying the difference between the deviation of the flow that enters and leaves the server. This deviation needs to be determined because the large traffic rate estimation is considered to be the significant feature that aid in better detection of DDoS attacks in the cloud computing environment. The efficient large traffic rate estimation parameters used in the proposed ASOM-SDN-DDoS mitigation framework are packer per second, byte count per second, byte count symmetry and packet count symmetry. The proposed framework uses a prediction-based algorithm for capturing the deviation between the normal traffic and the malicious traffic based on the packer per second, byte count per second, byte count symmetry and packet count symmetry metrics. This proposed framework aids in leveraging samples of the history-aware samples of each and every traffic flow for determining the possible range of future values. This proposed framework confirms the traffic flow as normal when they lie in between the low and high range of threshold considered for the large traffic rate estimation parameters. Else, the difference between the observed and forecasting values exhibits the confirmation towards the detection of malicious flow by a DDoS attack source in the cloud environment. In particular, the method of Weighted Moving Average is considered for computing the forecasting value of each metric considered for investigation. In addition, the merits of Enhanced Pauta criterion is considered with Gaussian distribution for achieving a suitable prediction level in the cloud environment.

4 SIGNIFICANCE OF THE PROPOSED ASOM-SDN-DDOS MITIGATION FRAMEWORK

The proposed ASOM-SDN-DDoS mitigation framework is considered as the potential cross plane inspired defence framework that exploits the inherent cooperative intelligence existing between the control and data plane for enhancing the efficiency in ensuring defence. This proposed framework is determined to be potent, since it inherits an adaptive and capable defensive approach that is embedded in the switches and controllers for faster attack response and precise botnet tracking process. This proposed ASOM-SDN-DDoS mitigation framework is considered to be significant than the existing defence frameworks as they enforce the process of cross plane optimization in the data plane of the SDN. This proposed ASOM-SDN-DDoS mitigation framework also resolves the possible issues that are encountered by the southbound interface that separates control plane from data plane in SDN. In addition, the proposed framework handles the issues that could hurdle the enforcement of cooperative botnet tracking process, when it is interfaced with the OpenFlow-based southbound that aids in integrating the advantages of control plane and data plane in SDN.

5 SIMULATION RESULTS AND DISCUSSIONS OF THE PROPOSED ASOM-SDN-DDOS MITIGATION FRAMEWORK

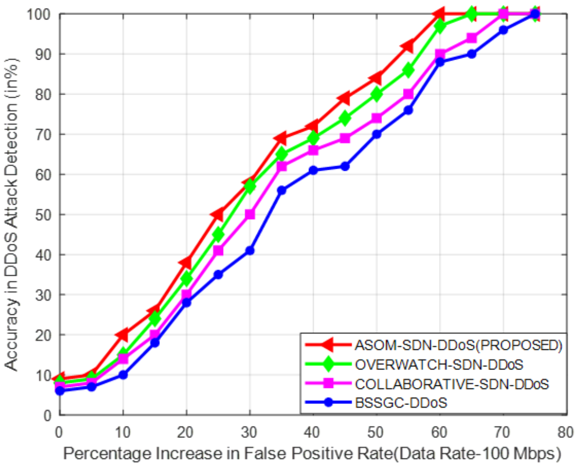
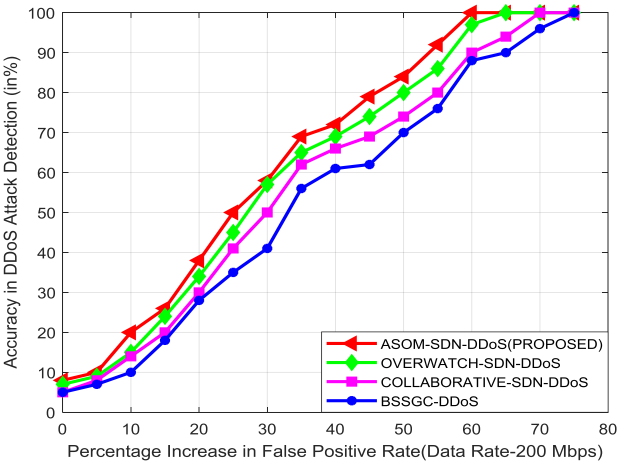


***Figure 2**-ASOM-SDN-DDoS framework-classification accuracy under false positive rates (Data Rate-100 Mbps)*

The simulation setup, parameters considered for investigating the proposed ASOM-SDN-DDoS mitigation framework with the compared OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks is similar to the set up used for implementing the FSOM, RMPSOM and CRESOM-based DDoS detection schemes. In the investigation, first the predominance of the proposed ASOM-SDN-DDoS Mitigation Framework is examined based on accuracy in DDoS detection under increasing rate of false positive determined under different data rates of 100 Mbps, 200 Mbps, 300 Mbps, 400 Mbps and 500 Mbps respectively. Further, the excellence of the proposed ASOM-SDN-DDoS mitigation framework is investigated using precision, recall value and F-score by varying the number of data traffic flows in the network. Furthermore, the remarkable performance of the proposed ASOM-SDN-DDoS mitigation framework is investigated using CPU utilization, memory utilization, number of bits per second and communication overhead by varying size of data packets used in the network. Finally, the superior performance of the proposed ASOM-SDN-DDoS mitigation framework is investigated using CPU utilization, memory



utilization, number of bits per second and communication overhead by varying the number of data traffic flows in the network. Initially, Figure 2 and 3 emphasizes the accuracy in DDoS attack detection of the proposed ASOM-SDN-DDoS mitigation framework estimated under varying levels of false positive rate with data rate considered as 100 Mbps and 200 Mbps respectively. The accuracy of the proposed ASOM-SDN-DDoS mitigation framework is determined to be enhanced by 12%, 10% and 7% superior compared to the existing OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks investigated under increasing levels of false positive degree with data rate of 100 Mbps. Then, the accuracy of the proposed ASOM-SDN-DDoS mitigation framework is determined to be enhanced by 11%, 9% and 6% superior compared to the existing OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks investigated under increasing levels of false positive degree with data rate of 200 Mbps. Figures 4, 5 and 6 emphasizes the accuracy in DDoS attack detection of the proposed ASOM-SDN-DDoS mitigation framework estimated under varying levels of false positive rate with data rate considered as 300 Mbps, 400 Mbps and 500 Mbps respectively. The accuracy of the proposed ASOM-SDN-DDoS mitigation framework is determined to be enhanced by 10%, 8% and 5% superior compared to the existing OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks investigated under increasing levels of false positive degree with data rate of 300 Mbps. Furthermore, the accuracy of the proposed ASOM-SDN-DDoS mitigation framework is determined to be enhanced by 9%, 7% and 4% superior compared to the existing OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks investigated under increasing levels of false positive degree with data rate of 400 Mbps. In addition, the accuracy of the proposed ASOM-SDN-DDoS mitigation framework is also concluded to be enhanced by 8%, 6% and 3% superior compared to the existing OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks investigated under increasing levels of false positive degree with data rate of 500 Mbps. Hence, the proposed ASOM-SDN-DDoS mitigation framework is considered to be maximum even when the data rates are varied from 100 Mbps to 500 Mbps, since they utilize a cooperative reaction mechanism for counteracting the impacts of the DDoS attacks in cloud computing.

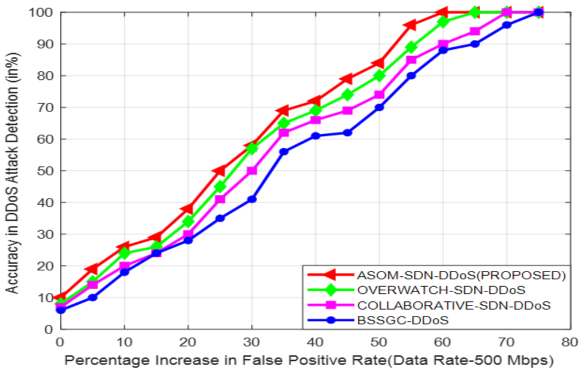


Figure* 3-*ASOM-SDN-DDoS framework-classification accuracy under false positive rates (Data Rate-200 Mbps)

ation accuracy under false positive rates (Data Rate-100 Mbps)

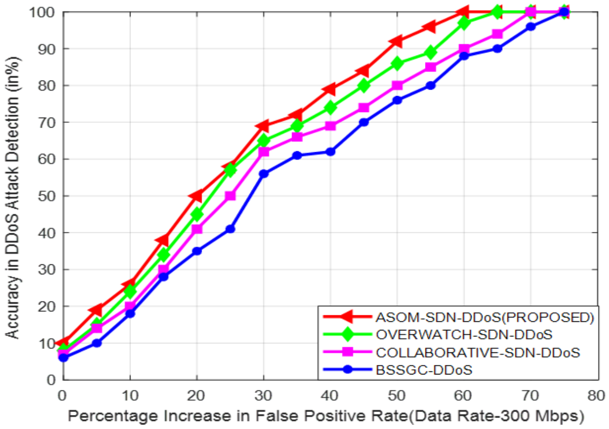


Figure* 4-*ASOM-SDN-DDoS framework-classification accuracy under false positive rates (Data Rate-300 Mbps)

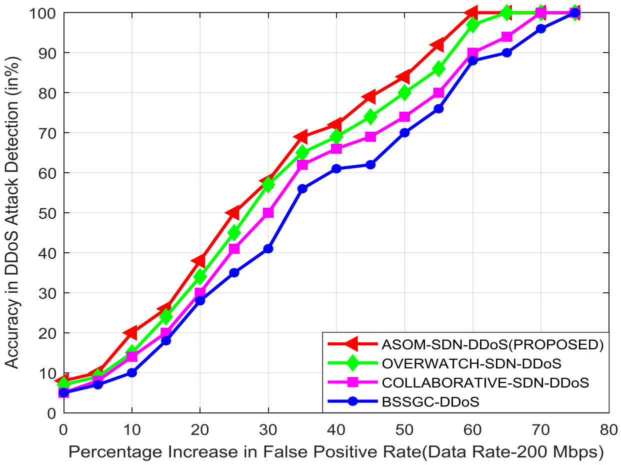


Figure* 5-*ASOM-SDN-DDoS framework-classification accuracy under false positive rates (Data Rate-400 Mbps)

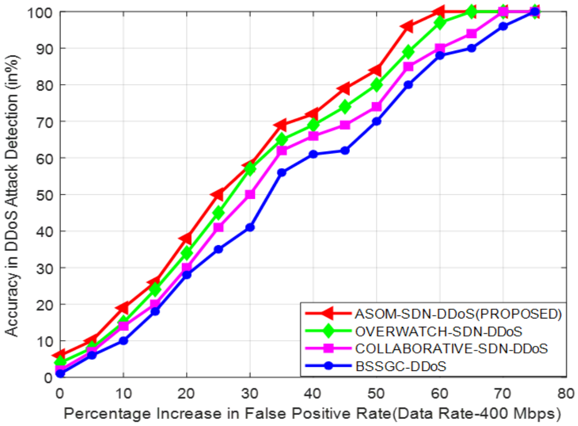


Figure* 6-*ASOM-SDN-DDoS framework-classification accuracy under false positive rates (Data Rate-500 Mbps)

Further, Figure 7, 8 and 9 highlights the predominance of the proposed ASOM-SDN-DDoS mitigation framework quantified based on precision, recall value and F-score by increasing the number of data traffic flows in the cloud computing environment. The precision of the proposed ASOM-SDN-DDoS mitigation framework is estimated to be improvised by 12%, 15% and 18% compared to the existing OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks. The recall value of the proposed ASOM-SDN-DDoS mitigation framework is estimated to be enhanced 14%, 17% and 19% compared to the existing DDoS mitigation frameworks used for exploration. The F-score of the proposed ASOM-SDN-DDoS mitigation framework is also confirmed to be enhanced 13%, 15% and 18% compared to the existing OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks. This realized enhancement in precision, recall value and F-score of the proposed ASOM-SDN-DDoS mitigation framework under increasing the number of data traffic flows is mainly determined due to the incorporation of adaptive SOM classifier used for detection process.

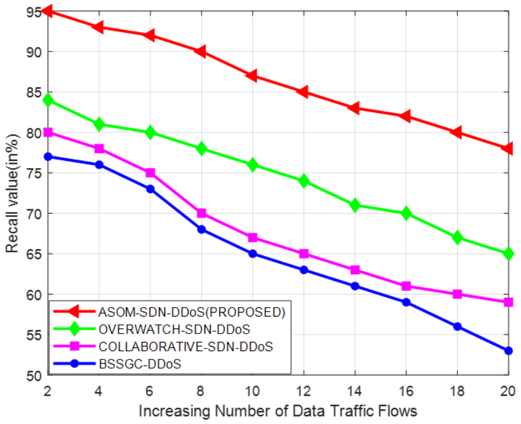


***Figure 7** -ASOM-SDN-DDoS framework-Precision under increasing data traffic flows*

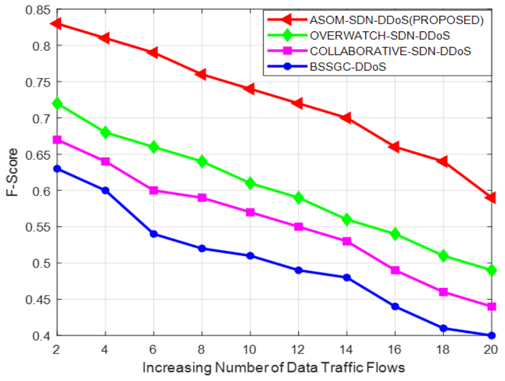


***Figure 8**-ASOM-SDN-DDoS framework- Recall Value under increasing data traffic flows*

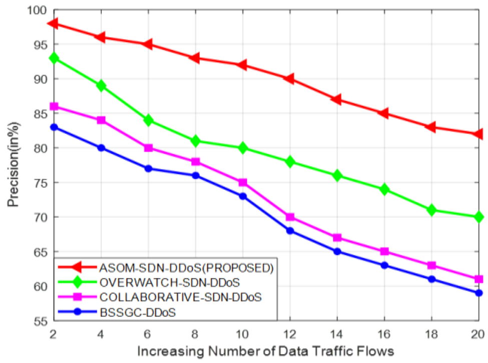


***Figure 9**-ASOM-SDN-DDoS framework- F-Score under increasing data traffic flows*

Further, Figure 10 and 11 portrays the potential of the proposed ASOM-SDN-DDoS mitigation framework quantified using CPU utilization rate and memory utilization rate by increasing size of data packets. The CPU utilization rate of the proposed ASOM-SDN-DDoS mitigation framework seems to be 16%, 13% and 10% excellent to the benchmarked OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation schemes considered for investigation. The memory utilization rate of the proposed ASOM-SDN-DDoS mitigation framework is proven to be reduced by 14%, 12% and 8% compared to the baseline OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation schemes considered for investigation. Furthermore, Figure 12 and 13 present the results of the proposed ASOM-SDN-DDoS mitigation framework evaluated in terms of number of bits per second and percentage decrease in communication overhead analysed under increasing size of data packets. The number of bits per second determined for the proposed ASOM-SDN-DDoS mitigation framework seems to exhibit maximum enhancement of 11%, 9% and 7% compared to the baseline OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation schemes considered for investigation.

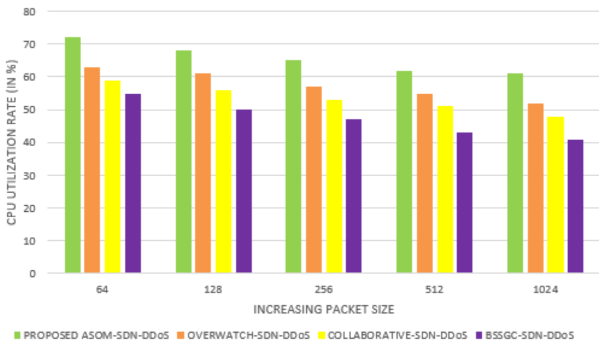


***Figure 10**-ASOM-SDN-DDoS framework- CPU utilization under* varying packet size

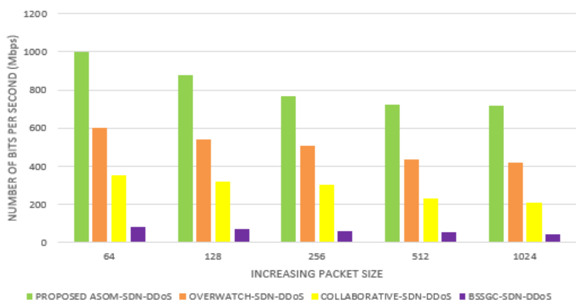


Figure 11*-ASOM-SDN-DDoS framework- Memory Utilization under varying packet size*

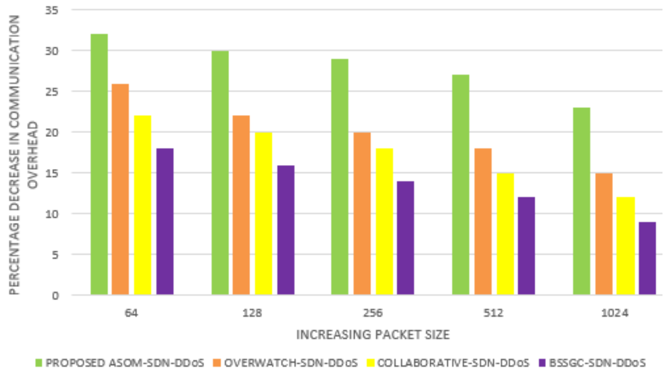


Figure 12*-ASOM-SDN-DDoS framework- bits per second under increasing packet size*

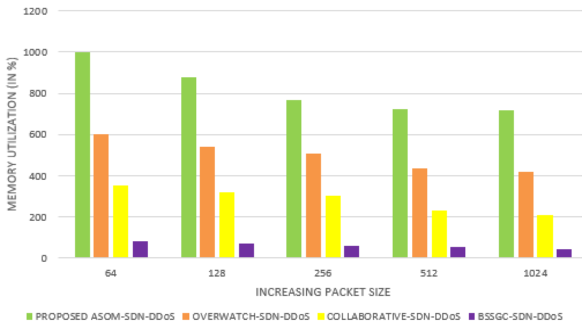


Figure 13*-ASOM-SDN-DDoS framework- communication overhead under increasing packet size*

The percentage decrease in communication overhead is also estimated to be highly minimized by 13%, 11% and 18% compared to the baseline OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation schemes considered for investigation. This visualized improvement in number of bits per second and percentage decrease in communication overhead of the proposed ASOM-SDN-DDoS mitigation framework is mainly determined due to the enhancement introduced in the control and data plane characteristics of the utilized botnet detection strategies. Finally, Figure 14 and 15 highlights the performance of the proposed ASOM-SDN-DDoS mitigation framework quantified using CPU utilization rate and memory utilization rate by increasing the number of data traffic flows. The CPU utilization rate of the proposed ASOM-SDN-DDoS mitigation framework seems to be 16%, 13% and 10% excellent to the benchmarked OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation schemes considered for investigation. The memory utilization rate of the proposed ASOM-SDN-DDoS mitigation framework is proven to be reduced by 14%, 12% and 8% compared to the baseline OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation schemes considered for investigation.

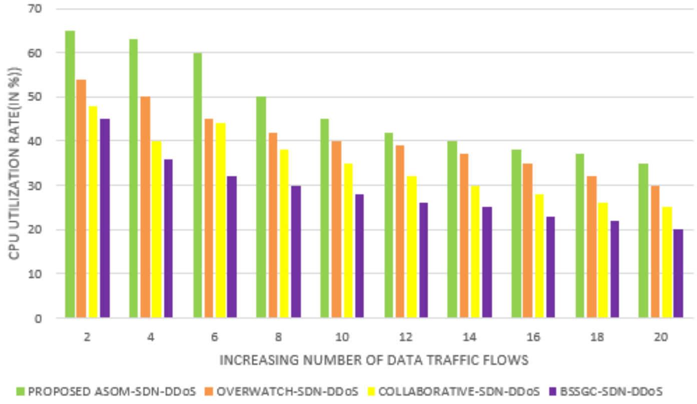


Figure 14*-ASOM-SDN-DDoS framework- CPU utilization per second by varying flows*

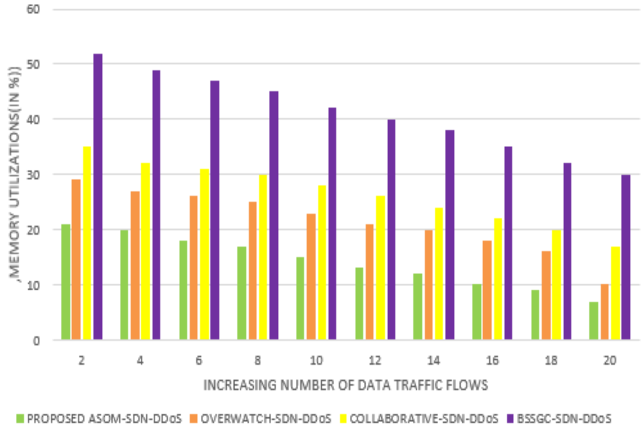


Figure 15*-ASOM-SDN-DDoS framework- memory utilization* under increasing flows

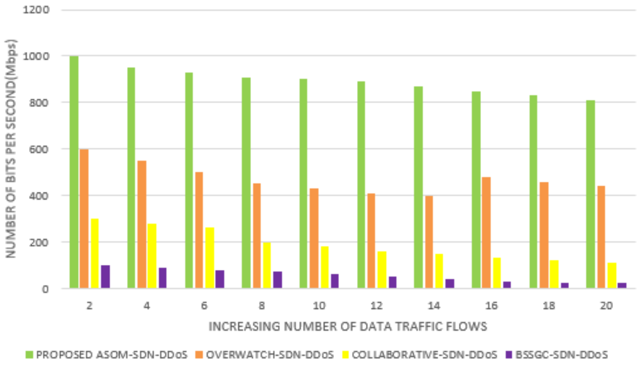


Figure 16*-ASOM-SDN-DDoS framework- bits per second under increasing flows*

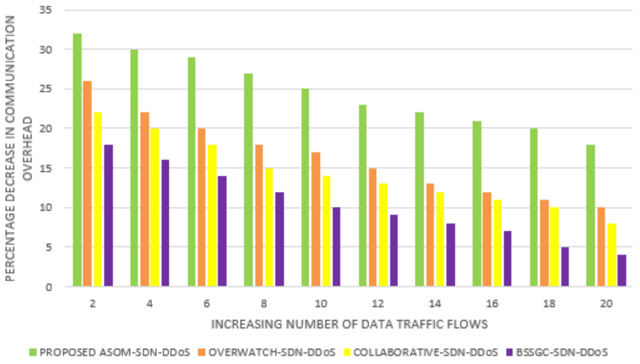


***Figure 17**-ASOM-SDN-DDoS framework- percentage decrease in communication overhead under increasing flows*

In addition, Figure 16 and 17 present the results of the proposed ASOM-SDN-DDoS mitigation framework evaluated in terms of number of bits per second and percentage decrease in communication overhead analysed under increasing number of data traffic flows. The number of bits per second determined for the proposed ASOM-SDN-DDoS mitigation framework seems to exhibit maximum enhancement of 11%, 9% and 7% compared to the baseline OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation schemes considered for investigation. The percentage decrease in communication overhead is also estimated to be highly minimized by 13%, 11% and 18% compared to the baseline OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation schemes considered for investigation. This visualized improvement in number of bits per second and percentage decrease in communication overhead of the proposed ASOM-SDN-DDoS mitigation framework is mainly determined due to the enhancement introduced in the control and data plane characteristics of the utilized botnet detection strategies.

6 CONCLUSION

This paper has presented the key significances and detailed architecture view of the proposed ASOM-SDN-DDoS mitigation framework with its improvised characteristics over the compared baseline OVERWATCH-SDN-DDoS, COLLABORATIVE-SDN-DDoS and BSSGC-DDoS mitigation frameworks considered for investigation. This chapter presented the simulation experiments and results of the proposed ASOM-SDN-DDoS mitigation framework for confirming its superiority in enhancing the accuracy under DDoS detection by increasing the percentage of false positive rate considered under DDoS mitigation process. This paper also has presented the predominance of the proposed ASOM-SDN-DDoS mitigation framework evaluated using CPU utilization rate, memory utilization rate, number of bits per second and communication overhead under increasing packet size and data traffic flows.

REFERENCES

[1] Q. Yan, F. R. Yu, Q. Gong and J. Li, “Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges,” IEEE Communications Surveys & Tutorials, vol. 18, no. 1, pp. 602-622, First quarter 2016.

[2] H. Pillutla and A. Arjunan, “A Survey of Security Concerns, Mechanisms and Testing in Cloud Environment,” 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), Coimbatore, 2018, pp. 1519-1524.

[3] J. Smith-perrone and J. Sims, “Securing cloud, SDN and large data network environments from emerging DDoS attacks,” 2017 7th International Conference on Cloud Computing, Data Science & Engineering - Confluence, Noida, 2017, pp. 466-469.

[4] D. S. Linthicum, “Software-Defined Networks Meet Cloud Computing,” in IEEE Cloud Computing, vol. 3, no. 3, pp. 8-10, May-June 2016.

[5] Amuthan A., Harikrishna P. (2019) Mean Availability Parameter-Based DDoS Detection Mechanism for Cloud Computing Environments. In: Zungeru A., Subashini S., Vetrivelan P. (eds) Wireless Communication Networks and Internet of Things. Lecture Notes in Electrical Engineering, vol 493. Springer, Singapore.

[6] B. A. A. Nunes, M. Mendonca, X. Nguyen, K. Obraczka and T. Turletti, “A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks,” in IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617-1634, Third Quarter 2014.

[7] Jim Doherty, SDN and NFV Simplified A Visual Guide to Understanding Software Defined Networks and Network Function Virtualization, Pearson Education, 2016.

[8] I. Ku, Y. Lu, and M. Gerla, “Software-defined mobile cloud: Architecture, services and use cases,” in Proc. IEEE IWCMC, pp. 1–6. Aug. 2014.

[9] R. Cziva, D. Stapleton, F. P. Tso, and D. Pezaros, “SDN-based virtual machine management for cloud data centers,” in Proc. IEEE Int. Conf. CloudNet, pp. 388–394, Oct. 2014.

[10] A. Akella and K. Xiong, “Quality of service (QoS)-guaranteed network resource allocation via software defined networking (SDN),” in Proc. Int. Conf. DASC, pp. 7–13, Aug. 2014.

[11] Y. Lin, D. Pitt, D. Hausheer, E. Johnson and Y. Lin, “Software-Defined Networking: Standardization for Cloud Computing's Second Wave,” in Computer, vol. 47, no. 11, pp. 19-21, Nov. 2014.

[12] T.-C. Yen and C.-S. Su, “An SDN-based cloud computing architecture and its mathematical model,” in Proc. IEEE Int. Conf. ISEEE, vol. 3, pp. 1728–1731, Apr. 2014.

[13] H. Pillutla A. Arjunan “Fuzzy self organizing maps-based DDoS mitigation mechanism for software defined networking in cloud computing” J. Ambient Intell. Humanized Comput. vol. 10 no. 4 pp. 1547-1559 Apr. 2019.

[14] H. Pillutla and A. Arjunan, "A Brief Review of Fuzzy Logic and Its Usage Towards Counter-Security Issues," 2018 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), Chennai, 2018, pp. 1-6.

[15] Pillutla Harikrishna, A.Amuthan, “Rival-Model Penalized Self-Organizing Map enforced DDoS Attack Prevention Mechanism for Software Defined Network-based Cloud Computing Environment,” unpublished.

[16] Pillutla Harikrishna, A.Amuthan, “Convolution Recursively Enhanced Self Organizing Map-based DDoS Attack Mitigation Scheme for Software Defined Networking cloud

environment," unpublished.

[17] B. Han, X. Yang, Z. Sun, J. Huang and J. Su, "OverWatch: A Cross-Plane DDoS Attack Defence Framework with Collaborative Intelligence in SDN," Security and Communication Networks, vol. 2018, pp. 1–15, 2018.

[18] Sufian Hameed and Hassan Ahmed Khan, "SDN Based Collaborative Scheme for Mitigation of DDoS Attacks," Future Internet, vol. 10, no. 3, p. 23, 2018.

[19] T. V. Sindia and Dr. Julia Punitha Malar Dhas,"A Bifold Software Defined Networking based Defence Mechanism for DDOS Attacks in the Cloud Environment," International Journal of Applied Engineering Research, vol. 12, no. 20, pp. 9467-9474, 2017.

[20] X. Yang, B. Han, Z. Sun, and J. Huang, "Sdn-based ddos attack detection with cross-plane collaboration and lightweight flow monitoring," in Proceedings of the Global Communications Conference, 2017.

[21] X. Qi, T. Wang and J. Liu, "Comparison of Support Vector Machine and Softmax Classifiers in Computer Vision," Second International Conference on Mechanical, Control and Computer Engineering (ICMCCE), pp. 151-155, Dec. 2017.

[22] R. Dinita, A. Winckles and G. Wilson, "A software approach to improving cloud computing datacenter energy efficiency and enhancing security through Botnet detection," IEEE 14th International Conference on Industrial Informatics (INDIN), , pp. 816-819, Jul. 2016.

[23] M. Eslahi, R. Salleh and N. B. Anuar, "Bots and botnets: An overview of characteristics, detection and challenges," IEEE International Conference on Control System, Computing and Engineering, pp. 349-354, Nov. 2012.