International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Software Defined Networking Based Protection against DDOS in IoT

P. J. Beslin Pajila, P. Jenifer, C. Karpagavalli, A. Angeline Valentina Sweety, R. Muthu Lakshmi

Abstract: ***Safety has become enormously important with the proliferation of internet of Things(IoT) technologies. Most of the IoT devices are linked with the DDoS attack, there are many risk nowadays for IoT because of DDoS attack.The new software-defined everything(SDx) model offers a way to handle IoT devices securely. The proposed S-IOT framework consists of a pool that includes S-IoT controllers, S-IoT switches and IoT devices. A new ENeFS algorithm is proposed to identify and reduce the DDoS attack. The proposed algorithm uses neuro fuzzy instruct rule to identify the DDoS attack and the number of data packets count also considered for the identification. The simulation results shows that the proposed algorithm performs better to improve the reliability of the IoT with different and unsafe gadgets.***

Key words: Software defined Internet of Things (S-IoT), Distributed Denial of Service (DDoS), attack identification, attack reduction, neuro fuzzy instruct rule.

I INTRODUCTION

Internet is an emerging technique, and it is available in wearable devices, home and vehicle. The devices like wearable equipment, public facilities, medical equipment, home appliances and other appliances are interconnected in IoT they need networking. So it is vulnerable to many attacks. There is no user interface, no security protocol and no computing and storage capacity. Since all the devices are connected in internet, Internet of Things (IoT) becomes more favourite. Devices that are connected with IoT are vulnerable. Even the firewall and diagnosis tool cannot identify the vulnerability because the device that is connected with network does not have any user interface, storage capacity, security protocol etc [1]. IoT comprises of more weak components for example sensors, RFID tags equal or more than the strong components like laptops, computers etc. The weak components are accomplished with distinct technologies with distinct thought in cost [2]. In recent developing world, all the devices emerge as brilliant and can transform information with other gadgets as well. These smart devices which are connected with the network does not have security protocol, user interface and repository quantity to make use of diagnostic tool and firewalls. There are many obstacles to securing the global privacy because of the advancement of Internet of Things in various streams like smart hospital, smart home etc. DDoS attack is one of the malicious attacks that may abuse the human life directly or indirectly and even cause death. All the computed system is compromised previously. Many issues should be defeated to make IoT more feasible [3, 4].Now a days DDoS attacks show that loopholes are everywhere in IoT. Without security safeguards, most of IoT gadgets may unconsciously move toward becoming assistants to DDoS attacks.

Software-defined anything (SDx) is the only solution for the DDoS attacks. There are many categories under SDx paradigm they are Software Defined Networking (SDN), Software Defined Radio(SDR),Software Defined Data Centre (SDDC),Software Defined World(SDW) and Software Defined Infrastructure(SDI).Software Defined Networking is truly the ultimate perceived technology, and the partition of data plane and control plane is the main focus of this technology. It is adaptable with any kind of network traffic. R. Huo *et al* [5] concentrated on the organization of caching, networking and computing of SDN for the next generation green wireless networks. J. Zhang et al [6] concentrated on the forthcoming 5G wireless networks. K. Wang et al [7] mentioned a unique idea, for the calculation of various intercommunication networks. The analysis of computation variance in the developing networking paradigms like C-RAN, SDN, and MCC was done. A box-covering-based routing algorithm (BCR) was proposed by L. Zhang et al in [8] for the large scale networks like SDNs. The source code for the BCR algorithm is embedded inside the controller of SDN. The merging of SDN and IoT furnish a probably feasible result to enhance management and check the effectiveness of the IoT network. The SDN architecture was suggested for IoT and inspected about the resource allocation problem in the SDN IoT network. A Relative Value iterative algorithm (RVI) was implemented for determining solution for the SMDP problem [9]. Jiaqiang Liu[10] put forward about the SDIoT architecture. It is separated into physical infrastructure, control and application layer. SDIoT is mainly used for the smart urban sensing, Southern interface exist between Physical infrastructure and control layer, and Northern interface exist between control layer and Application layer.

Revised Manuscript Received on March 30, 2020.
* Correspondence Author
P. J. Beslin Pajila, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.
E-mail: beslin.kits@gmail.com
Jenifer P., Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.
E-mail: jeniferjebavaram@gmail.com
Karpagavalli C.*, Department of Computer Science and Engineering, St.Mother Theresa Engineering College, Tuticorin, India.
E-mail: ckvalli08@gmail.com
Angeline Valentina Sweety A., Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.
E-mail: valentinaraj1997@gmail.com
Muthu Lakshmi R., Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, India.
E-mail: muthulakshmitha@gmail.com

The control layer has mainly data acquisition service, Sensor states monitoring and Manage and optimization.

II. RELATED WORK

M. E. Ahmed and H. Kim [10] propose a SDN Open flow that will weaken DDos before it reaches the innocent network. It is possible for the SDN network infrastructure to beat the recent threats. The DDoS attack originates from huge number of compromised host that can be guarded before it makes the innocent server nonexistent. Bawany et al [12] discussed about SDN and proposed a DDoS safeguard framework that is used to identify and reduce DDoS attack. This framework was proposed for the smart cities because it is composed of many complex systems. Architecture was designed for the ProDefense framework mainly to eradicate the ddos attack in the smart city to secure it. S.Lim et al [13] proposed a scheme called scheduling based architecture that protects the SDN controller against the DDoS attack. The SDN controller will handle the flow request; the DDoS attack will send more flow request to the controller and flood it,to make it more slower in responsiveness. Martin Vizv´ary et al [14] discussed about how the DDoS attacks will affect the legitimate user and the reduction of the attack based on SDN. DDoS is the worst attack in the modern days. SDN has data plane and control plane, the data plane has devices like switches and the control plane has controller. The controller will manage the overall network as well the devices that is available in the data plane. The switch will forward the traffic based on the rules that is available in the flow table, if there is any contradiction the device will intimate to the controller. Wu et al. [15] mentioned the possibilities of DDoS attack in the data plane. Mostly DDoS attack will affect the controller by using the flooding attack, one of the type of DDoS.But there is a possibilities of intrusion of DDoS attack in the data plane. Neelam et al [16] discussed about various DDoS attack issue that occurs in SDN. SDN faces the challenges against attacks. But still since it is a controller, it is concern about the DDoS attack. The challenges faced by the SDN and the solution for that particular problem was also discussed. Switches are available inside the data plane, so it is unsafe to attacks. S. M. Mousavi and M. St-Hilaire [17] proposed a new SDN based on entropy to detect the attack. It fixes a threshold value with very low value. The packet enters into the controller at that time if the threshold value is below the range then there exist an attack. If the threshold value is high, then there exists no attack. The ddos attack is detected based on the threshold value. Moreover the incoming packets are counted. If the same packets are entered into the controller more times it means that the randomness drop. Lei Wei et al [18] proposed a concept to reduce the ddos attack and to improve the service to the legitimate user. The request from different users is prioritized based on a prioritized algorithm known as flowranger. It will prioritize the entire request based on the trust value. If the particular request have high trust value, it will be processed first and intimate a message to the switch. The entire request from the user is queued based on job prioritization. R. T. Kokila et and al [19] proposed a new SVM, it will produce a correct classification based on the samples. It is mainly used to detect the DDoS. N.-N. Dao et [20] and al proposed a method that will identify the ddos attack based on the ip address and by the number of packets a user send to the forwarding device. A new table was used instead of the flow table called as temple table(T table). If the number of IP address inside the T table is greater than or equal to the number of the packets to the particular connection then collect the count from the switch(s). If the values of s is less than or equal to the number of packets in the connection(n) then the particular packet should be blocked. Q. Yan [21] proposed a 'Multislot algorithm' to protect the request from the legitimate user. They have used three switches to detect the and eradicate the ddos attack so earlier and easily. Also the comparison between the multiQ and singleQ algorithm has been done. R. Wang et al [22] proposed three main concept for detecting and filtering ddos attack. They are entropy based detection method, trace back mechanism and source filtering. A drop rule is set in the switch to filter the traffic and it the simplest method to prevent the network from the ddos attack. Wang Xiulei et al [23] proposed a new algorithm to detect the ddos attack called Shiryaev–Roberts detection algorithm. This is an enhancement of the SR detection algorithm. An experimental observation was done in [23] to make the detection more accurate. For the observation they have used three networks, one with the controller inside the control plane and it also has open flow switches. The second network has Tribe Flood Network 2000, it is used to create the ddos attack ie., a malicious traffic to affect the working of the controller. The third one has two generators to create the other traffic. DFA algorithm is also used to filter the ddos attack. B.Wang and al [24] proposed DaMask architecture that is mainly used to detect and mitigate ddos attack. The collision of ddos attack that affects both SDN and cloud computing was effectively maintained by the DaMask architecture. Uncoupling of the network from the traffic can be done be done by virtual network. The ddos attack will mostly affect the cloud computing, SDN is the solution to mitigate the attack. Because of the fast evolution of botnets, the ddos attacks affect the cloud computing in the faster rate [25]. Q. Yan et al [26] classified the ddos attack based on the location where the protection mechanism was installation. The origin of ddos attack and the detection of the ddos attack were discussed. The ddos attack is classified into different categories. The effective and useful feature of the SDN to detect the ddos attack was discussed. SDN also a victim for the ddos attack, the solution for the problem also discussed. The link services of the controller in the control plane were the important services that are used to protect the controller from the ddos attack and also it more vulnerable to the attack. Because LLDP packets are used to find the links between the switch-to-switch that is available in the Data plane layer. The link spoofing attack will make the switch-to switch link more vulnerable. The proposed hybrid counter measures method for the link spoofing attack will prevent the controller from the attack. The fake links can be identified by the HMAC signature [27].

In [28] an optimal reconfiguration algorithm was proposed to deal with the non-patchable vulnerability, the optimal topology is calculated. Two methods were mentioned they are optimal method and heuristic method.SDN architecture will overcome the most attacks that occur in IoT, similarly because of the implementation of the central controller of the SDN, new attacks will occur. The SDN architecture has three layers; they are application layer, control layer and data layer.

The Control layer will manage all the traffic flow in the network by using the controller. Data layer contains the switches, devices and other heterogeneous devices.
Application layer perform many security and business operations [29].

An enhanced algorithm to detect and mitigate the ddos attack is very faster than the previous algorithm. Newly proposed has a neuro fuzzy system for measuring from multiple inputs. The enhanced algorithm is loaded inside SDN-Controller.

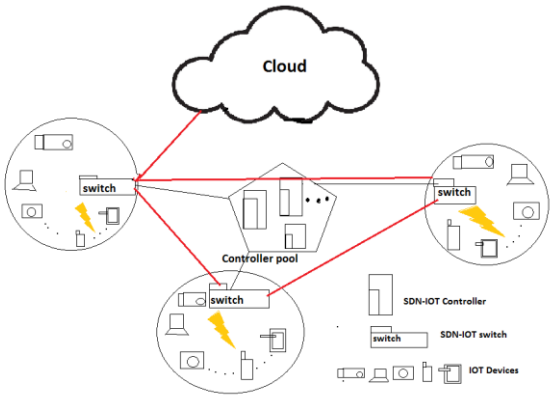


Figure 1 S-IOT Framework

III. SDN-IOT WITH DDOS ATTACK

The future generation SDN will control the hardware using software. The main component for SDN is switches and controller. The controller will control the entire network and switches operate the devices in the network based on the instructions given by the controller. The software alone needs to be updated for up gradation of the network and it minimizes the cost. DDoS was mitigated using fuzzy based in [31], a separate security device is inhibited to protect the system from the attack. This device has a threshold value and the attack is eliminated based on the threshold value. The fuzzy technique will make easier to mitigate the attack even the lookup table have more number of rules. It picks the proper rules from the table to eradicate the attack more quickly than the previous architecture. The SDN software gives commands to the whole networks. Controller plays an important role in giving commands to the various networking components using programs. This quality strengthens the overall achievement, good reliability and energy saving. Different layers in the SDN are coupled using the APIs. The SDN controller job is to finds the performance of the SDN. So DDoS attack's main aim is to eradicate the SDN controller. There is a drawback in programmable SDN ie., it is unsafe from the attacks like ddos attacks, intrusion attacks etc. During energy utilization in devices as well in infrastructures, SDN provides to reduce the utilization. SDN controller has rules, it was managed by it and the network components will flow the rule to reduce the network traffic.SDN uses a Data centers for storage purpose that can be enlarged and shrink based on its needs [32].

A.SDN Structure

The below figure shows the structure of the SDN, it has three layers application layer, control layer and infrastructure layer. Controller is available in the control layer, that is responsible for identifying and to diminish the ddos attacks. The controller has a security device deployed within it which is responsible for the destruction of ddos attacks. Single controller will act as a centralized controller and to manage the security process [33].

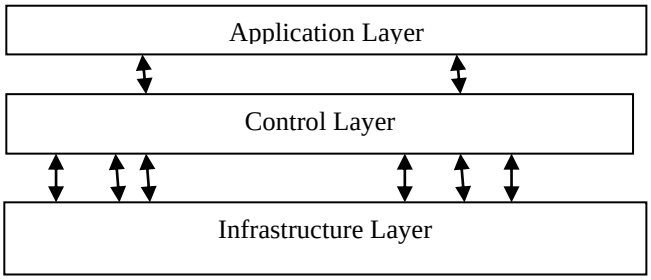


Figure 2 SDN structure

IV. ENHANCED DDOS ATTACK DETECTION ALGORITHM BASED ON NEURO FUZZY SYSTEM

The Neuro fuzzy system is used detect the ddos attack since it used to learn about the attack from the multiple inputs. A new algorithm is proposed ENeFS (Enchanced Neuro Fuzzy System) Algorithm and it is used by the S-IoT controller to proactively work against the ddos attack.

A. Neural Network System:

The single perceptron layer, supervised training approach is practice to keep track the network in [34]:

$$Wgt_i(t-1) = Wgt_i(t) + \varphi \times (Oput_T - Oput_A) \times Ï$$

Where Wgt_i be the weight, i be the number of inputs, φ be the learning rate, $Oput_T$ and $Oput_A$ be the output of the system and chosen output simultaneously. Finally Ï be the parameter used for the input cell initial variable.

The weight can adjust by using the following Equation.

$$Wgt_{new} = Wgt_{old} + N \times \varphi \times Iput_p \times (Oput_T - Oput_A)$$

Where

$$\Delta Wgt = N \times \varphi \times Iput \times (Oput_T - Oput_A)$$

N is the active neuron, $Iput_p$ be the input to the active neuron from the preceding layer.

Output rate in each layer is expressed as

$func_1(Iput_1 \times Wgt_1)$
$func_2(Iput_2 \times Wgt_2)$
$func_3(Iput_3 \times Wgt_3)$
....
$func_n(Iput_n \times Wgt_n)$

Algorithm 1: Perceptron instruct rule.

Input ln = {L1,L2,…Ln}
Initialize $L_i = 0$ or 1.
Output Go= 0 or 1.
While {Perfect output}
Input ln = (L1,L2,…Ln).
Ro ←lo.
If{Not recommended output}
$W_i := W_i + Pr (Oput – Ro)K_t$
t := t − O(Oput – Ro)
Go ← Oput.

Weight change rule:

If Ro = 0, and Oput =1,
Diminish threshold and strengthen W

If lo = 1, Oput = 0
Rise threshold and diminish W
If Ro=1, Oput = 1, or Ro = 0 ,Oput = 0,
No adjustment in weights or thresholds.
Where Go – perfect output, Ro – Perceptron output, Pr – positive instruct rate.

The perceptions instruct rule is used by the S-IoT controller to learn about the ddos attack. The algorithm is used to analyze about the attacks from the inputs from switches. The IoT devices will send packets to the switches. It transforms the packets to the S-IoT controller.Many S-IoT Controllers are available inside Controller pool. Each every S-IoT controller inside the pool has the separate learning algorithm. As soon as the S-IoT controller receives the data packets from the S-IoT switches it checks whether the data packet is from the legitimate user or malicious user. Because the ddos attack will keep on sending data packets with forged source IPaddress and with destination address and MAC source address.

The system has inputs. Neural network instruct the inputs of the sensor nodes such as received signal strength residual energy. This denotes a network of energy usage as a continuous parameter. The Best quality node contact is determined by the frequency of the radio signal identified by formula [35].

Trust Factor (R_f) :

The Cluster Header (CR) will packets fell consecutive and the number of packets dropped was used to evaluate the True Factor (R_f)

$$E_x(b, y) = h_x(b, y) + C_y$$

Where M= number of packets fell consecutive by the CR

$$R_f = 100 * y^{\log 2 (M)}$$

Eventually, the effective quality of the link as well as the total energy sets are trained to select powerful nodes for unpredictable cluster heads which are the secure transmission between endpoints. This input is linked to the neural network's first n inputs. The next input is the base station location which is valued discreetly and feedback output if the third input. In different situations, three inputs make various scenarios. For linear value, the first two neurons have fixed weights. The next two neurons have weights need to train and it is used in the Fuzzy-based neural network's sigmoid function. A range of inputs can be plotted to a desired output. This sensor network has been equipped in situations such as the base station at the middle of the surrounding area. To direct the network to acquire preferred output, a single layer perceptron has been used. Algorithm 1 represents the Perceptron instruct rule and weight alter rule. Trained network as well as maps outputs using the earlier learning process. The proposed neuro fuzzy networks learn about the attack and prevent the S-IoT controller from the ddos attack. The network is more efficient because prevent the attack in reaching the S-IoT controller.

i

ENeFS Algorithm:

Train with instruct rule without any attack as well as with attacks.

If pkt_in data reach **then**
Check the data using Perceptron instruct rule.
Instruct rule verify whether the data is ddos attack or not
If found then
Discard the attack and also don't allow any pkt_in data from that particular host.
Endif

V. SIMULATION RESULTS

The performance of the proposed system is evaluated after the experimental analysis in the laboratory surroundings. The proposed ENeFS algorithm used neuro fuzzy system for making the S-IoT controller more secure from the DDoS Attack.

The results are analyzed based on the count in the S-IoT switches flow table, based on the packets transfer to the S-IoT controller from the S-IoT switches and the amount of data packets accepted based on the three algorithms by the S-IoT controller.

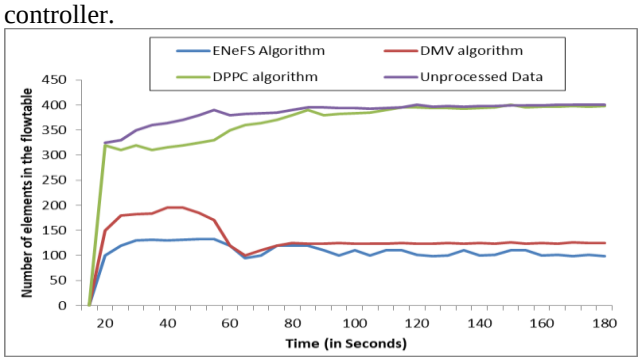


Figure 6: Number of elements in the flow table

A. Elements in the flow table

The effect of time based on the amount of units in the flow table in S-IoT switch is shown in figure 6. The curves are very sharp and has big slant in the initial. The proposed ENeFS algorithm, DVM algorithm[1] and the DPPC algorithm [20] and the unprocessed data the elements in the flow table gradually raise to 200 , 218 and 347 commonly. The curve of DPPC algorithm is constant after 10s because the *timeout_idle* is fixed to 10s, but there is no decrement after 20s.Therefore there is no experimental effect towards this algorithm because it won't identify any ddos attack. In DVM algorithm the ddos attack is identified after 5s in the S-IoT switch so that the switch does not forward any data packet to the S-IoT controller after 5s.The controller still process the message from the S-IoT switch and the transfer the flow table elements to the S-IoT switch. But there is a huge variation in the count of the elements of the flow table. The elements are less in number between 5s to 10 s than 0s to 5s. Based on the DVM algorithm, the data packets will get removed after 5s. Because DVM algorithm has effect only after 5s so the ddos attack is identified and eradicated only after 5s. The proposed ENeFS algorithm has more effect, it identify and eliminate the ddos attack before 3s by using the fuzzy instruct rule. The learning process has more effect in identification of the attack.

B. Packets transfer to S-IoT controller

The effect of time based on the data packets transfer by S-IoT switch to the S-IoT controller is shown in the figure 7. Over time the amount of data packets messages transfer to the S-IoT controller by the S-IoT switch raise. Among the three curves plotted in the graph, our ENeFS algorithm specifies a minimum amount of improvement.

The improvement of ENeFS algorithm is 17.09 percent of the unprocessed data and 17.77 percent of the DPPC algorithm and 5 percent of the DVM algorithm in [1].

Our proposed algorithm makes the S-IoT switch to learn about the attacks using neuro fuzzy system. So that it can able to identify the attack better than the previous approaches. The S-IoT switch transfer very limited amount of the data packets to the S-IoT controller afterwards. The DPPC algorithm in [20], still transfer very less amount of data packets to the S-IoT controller and DVM algorithm in [1], send large amount of packets so that the curve is very hilly.

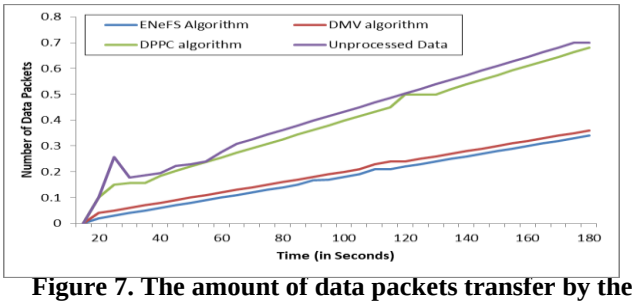


Figure 7. The amount of data packets transfer by the S-IoT switch to S-IoT controller.

C. Packets Accepted by S-IoT controller

The effect of time based on the amount of data packets accepted by the S-IoT controller is shown in the Figure 8.The range of the amount of improvement of the packets transfer from the S-IoT switches to the S-IoT controller is similar as shown in Figure 7. The improvement of the our proposed algorithm is just 5 percent of that of the DMV algorithm, 17.55 percent than the unprocessed data and 18.83 percent than the DPPC algorithm. There are greater growth rates of data packet accepted by the S-IoT controller in Figure 8 compared to the data packets in Figure 7.The inconsequential variation is occurred by the neuro fuzzy system instruct rule.

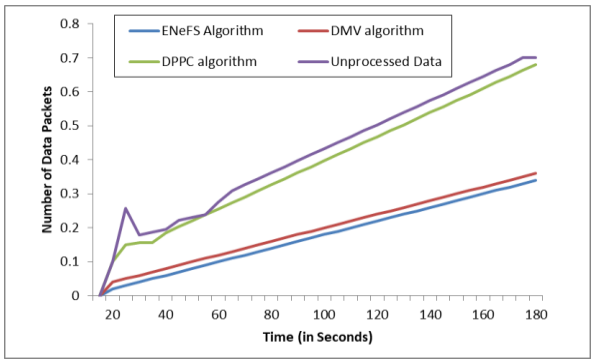


Figure 8. The amount of data packets accepted by the S-IoT controller

D. Bandwidth of S-IoT CS channel

The effect of time based on the bandwidth between the medium of the controller and switch in the S-IoT is represented in Figure 9. For our ENeFS algorithm, the hike in the bandwidth rate is very quick between 0s and 3s.Because the S-IoT switch will reject the packet with DDos attack within 3s when ENeFS algorithm installed in the S-IoT controller. So that the S-IoT controller receives only a limited amount of data packets, since S-IoT transfer very few data packets to S-IoT controller. The rate of the data packets accepted by the S-IoT controller moderately decreases very low until it is fixed. The bandwidth rate of the DMV algorithm in [1] is very fast between 0s to 5s.The S-IoT switch will eliminate the data packets with attack only after 5s.After that the S-IoT controller receives limited amount of data packets. The small variation is due to unblock of normal flow. It means the S-IoT switch transfer the data packets to the S-IoT controller slowly with limited data packets. The DMV algorithm [1] does not identify the DDoS attack profitably and it was not success. The count of the elements in the flow table is less compared to the DPPC algorithm. Similarly, the number of the data packets transfer and received by the S-IoT Switch and S-IoT controller is less compared to the DPPC algorithm. But the DMV algorithm does not identify the DDoS attack accurately. For the unprocessed data, the rate of the data packets accepted by the S-IoT controller was highest at 10s after that it become constant slowly. In the graph there is upward and downward variation due to the DDoS attack and the normal flow. The DPPC algorithm [20], the data packets rate accepted by the S-IoT controller is very high till 20s and is stable afterwards.

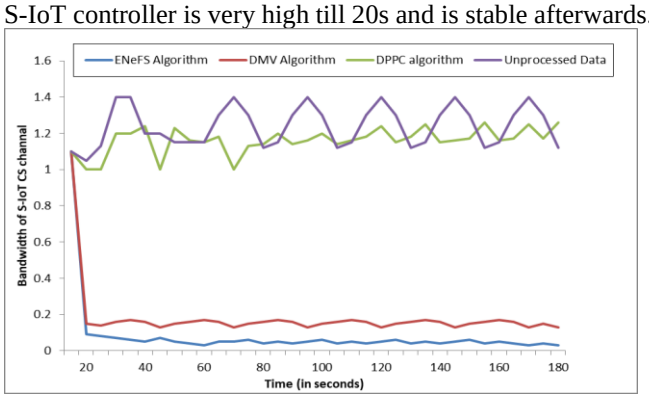


Figure 9. Bandwidth of S-IoT CS channel

The proposed ENeFS Algorithm performs better than the other algorithms like DMV algorithm [1] and DPPC algorithm [20].The count of elements in the flow table, data packets transfer by the S-IoT switch and data packets accepted by the S-IoT controller very less than the other two approaches. That shows, our algorithm performs well because it uses neuro fuzzy instruct rule to identify the ddos attack. It makes IoT to function more better under DDoS attack. ENeFS Algorithm performs better than DVM algorithm about 5 % because very less amount of data is accepted by the S-IoT controller.

VI. CONCLUSION

In this paper, S-IOT framework was described that has a pool woth S-IoT controller and S-IoT switches and IoT gadgets. A new ENeFS Algorithm was proposed to identify and reduce the DDoS attack. In the proposed algorithm, Neuro fuzzy instruct rule is used to identify and reduce the DDoS attack based on the threshold value in the algorithm.From the analysis it is clear that the proposed algorithm identifies and removes the DDoS attack quickly than the previous methods. As a future work the load balancing algorithm is constructed and achieved in the controller pool to minimize the response time and increase the throughput.

REFERENCES

1. Da Yin1, Lianming Zhang, And Kun Yang, (Senior Member, Ieee) ,"A DDos Attack Detection and Mitigation With Software-Defined Internet of Things Framework", Special Section On Security And Trusted Computing For Industrial Internet Of Things, Volume 6, 2018.
2. H. Ma, L. Liu, A. Zhou, and D. Zhao, ``On networking of Internet of Things: Explorations and challenges," *IEEE Internet Things J.*, vol. 3,no. 4, pp. 441_452, Aug. 2016.
3. K. Sonar and H. Upadhyay, ``A survey: DDoS attack on Internet of Things," *Int. J. Eng. Res. Develop.*, vol. 10, no. 11, pp. 58_63, Nov. 2014.
4. U. Lindqvist and P. G. Neumann, ``The future of the Internet of Things,"*Commun. ACM*, vol. 60, no. 2, pp. 26_30, Jan. 2017.
5. R. Huo *et al.*, ``Software de_ned networking, caching, and computing for green wireless networks," *IEEE Commun. Mag.*, vol. 54, no. 11,pp. 185_193, Nov. 2016.
6. J. Zhang, X. Zhang, M. A. Imran, B. Evans, Y. Zhang, and W. Wang, ``Energy ef_cient hybrid satellite terrestrial 5G networks with software de_ned features," *J. Commun. Netw.*, vol. 19, no. 2, pp. 147_161,Apr. 2017.
7. K. Wang, K. Yang, H.-H. Chen, and L. Zhang, ``Computation diversity in emerging networking paradigms," *IEEE Wireless Commun.*, vol. 24, no. 1,pp. 88_94, Feb. 2017.
8. L. Zhang, Q. Deng, Y. Su, and Y. Hu, ``A box-covering-based rout-ing algorithm for large-scale SDNs," *IEEE Access*, vol. 5, no. 1,pp. 4048_4056, Mar. 2017.
9. X. Xiong, L. Hou, K. Zheng, W. Xiang, M. S. Hossain, and S. M. M. Rahman, ``SMDP-based radio resource allocation scheme in software-defined Internet of Things networks," *IEEE Sensors J.*, vol. 16, no. 20, pp. 7304_7314, Oct. 2016.
10. J. Liu, Y. Li, M. Chen, W. Dong, and D. Jin, ``Software-defined Internet of Things for smart urban sensing," *IEEE Commun. Mag.*, vol. 53, no. 8,pp. 55_63, Sep. 2015.
11. C. G. Krishnan, K. Sivakumar and E. Manohar, "An Enhanced Method to Secure and Energy Effective Data Transfer in WSN using Hierarchical and Dynamic Elliptic Curve Cryptosystem," 2018 International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2018, pp. 1-7.
12. C. Krishnan, A.Rengarajan and R.Manikandan, "Delay Reduction by Providing Location Based Services using Hybrid Cache in Peer to Peer Networks," KSII Transactions on Internet and Information Systems, vol. 9, no. 6, pp. 2078-2094, 2015. DOI: 10.3837/tiis.2015.06.006.
13. P.S.Apirajitha, C.Gopala Krishnan, G.Aravind Swaminathan, E.Manohar(2019) "Enhanced Secure User Data on Cloud using Cloud Data Centre Computing and Decoy Technique", "International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8 Issue-9, July 2019"
14. M. E. Ahmed and H. Kim, ``DDoS attack mitigation in Internet of Things using software de_ned networking," in *Proc. IEEE 3rd Int. Conf. Big Data Comput. Service Appl.*, Apr. 2017, pp. 271_276.
15. N. Z. Bawany, J. A. Shamsi, and K. Salah, ``DDoS attack detection and mitigation using SDN: Methods, practices, and solutions," *Arabian J. Sci.Eng.*, vol. 42, no. 2, pp. 425_441, Feb. 2017.
16. S.Lim, S.Yang,Y. Kim, and S.Yang, ``Controller scheduling for continued SDN operation under DDoS attacks," *Electron. Lett.*, vol. 51, no. 16,pp. 1259_1261, Aug. 2015.
17. M. Vizvary and J. Vykopal, ``Future of DDoS attacks mitigation in soft-ware de_ned networks," in *Proc. IFIP Int. Conf. Auto. Infrastruct., Man-age. Secur.*, Jul. 2014, pp. 123_127.
18. X. Wu, M. Liu, W. Dou, and S. Yu, ''DDoS attacks on data plane of software-defined network: Are they possible?'' Secur. Commun. Netw., vol. 9, no. 18, pp. 5444–5459, Dec. 2016.
19. N. Dayal, P. Maity, S. Srivastava, and R. Khondoker, ``Research trends in security and DDoS in SDN," *Secur. Commun. Netw.*, vol. 9, no. 18,pp. 6386_6411, Feb. 2016.
20. S. M. Mousavi and M. St-Hilaire, ``Early detection of DDoS attacks against SDN controllers," in *Proc. Int. Conf. Comput., Netw.Commun. (ICNC)*, Feb. 2015, pp. 77_81..
21. L. Wei and C. Fung, ``FlowRanger: A request prioritizing algorithm for controller DoS attacks in software de_ned networks," in *Proc. IEEE Int.Conf. Commun.*, Jun. 2015, pp. 5254_5259.
22. R. T. Kokila, S. T. Selvi, and K. Govindarajan, ``DDoS detection and anal-ysis in SDN-based environment using support vector machine classi_er," in *Proc. 6th Int. Conf. Adv. Comput.*, Dec. 2015, pp. 205_210.
23. N.-N. Dao, J. Park, M. Park, and S. Cho, ``A feasible method to combat against DDoS attack in SDN network," in *Proc. Int. Conf. IEEE Inf. Netw. (ICOIN)*, Aug. 2015, pp. 309_311.
24. Q. Yan, Q. Gong, and F. R. Yu, ``Effective software-de_ned networking controller scheduling method to mitigate DDoS attacks," *Electron. Lett.*, vol.53, no.7, pp.469_471, Mar.2017.
25. R. Wang, Z. Zhang, L. Ju, and Z. Jia, ``A novel OpenFlow-based DDoS fooding attack detection and response mechanism in software-defined networking," *Int. J. Inf. Secur. Privacy*,vol.9,no.3,pp.21_40,Jul.2015.
26. X. Wang, M. Chen, X. Wei, and G. Zhang, ``Defending DDoS attacks in software de_ned networking based on improved Shiryaev_ Roberts detection algorithm," *J. High Speed Netw.*,vol.21,no.4,pp.285_298,Nov.2015.
27. B.Wang, Y. Zheng,W. Lou, and Y. T. Hou, ``DDoS attack protection in the era of cloud computing and software-de_ned networking," *Comput. Netw.*,vol. 81, pp. 308_319, Mar. 2015.
28. Q.Yan and F.Yu, ``Distributed denial of service attacks in software-defined networking with cloud computing," *IEEE Commun. Mag.*, vol. 53, no. 4,pp. 52_59, Apr. 2015.
29. 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 Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 602_622, 1st Quart., 2016.
30. T. H. Nguyen and M. Yoo, ``A hybrid prevention method for eavesdropping attack by link spoo_ng in software-de_ned Internet of Things controllers,"*Int. J. Distrib. Sensor Netw.*, vol. 13, no. 11, pp. 1_9, Nov. 2017.
31. M. Ge, J. B. Hong, S. E. Yusuf, and S. K. Dong, ``Proactive defense mechanisms for the software-de_ned Internet of Things with non-patchable vulnerabilities," *Future Generat. Comput. Syst.*, vol. 78, no. 2,pp. 568_582, Jan. 2018.
32. D. B. Rawat and S. R. Reddy, ``Software dened networking architecture, security and energy efciency: A survey," IEEE Commun. Surveys Tuts.,vol. 19, no. 1, pp. 325346, 1st Quart., 2017.
33. R. Kandoi and M. Antikainen, ``Denial-of-service attacks in OpenFlow SDN networks," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage.*,May 2015, pp. 1322_1326.
34. Tuyen Dang-Van, Huong Truong-Thu**,"**A Multi-Criteria based Software Defined Networking System Architecture for DDoS-Attack Mitigation", REV Journal on Electronics and Communications, Vol. 6, No. 3–4, July–December, 2016.
35. D. B. Rawat and S. R. Reddy, ``Software defined networking architecture, security and energy efficiency: A survey," *IEEE Commun. Surveys Tuts.*,vol. 19, no. 1, pp. 325_346, 1st Quart., 2017.
36. A. Hakiri, P. Berthou, A. Gokhale, and S. Abdellatif, ``Publish/subscribe- enabled software de_ned networking for ef_cient and scalable IoT communications," *IEEE Commun. Mag.*, vol. 53, no. 9, pp. 48_54, Sep. 2015.
37. Golden Julie, E., & Tamil Selvi, S. (2016). Development of energy efficient clustering protocol in wireless sensor network using neuro-fuzzy approach. The Scientific World Journal 2016, Article ID 5063261, 1–8.
38. YH Robinson, EG Julie, S Balaji, A Ayyasamy,"Energy aware clustering scheme in wireless sensor network using neuro-fuzzy approach ",Wireless Personal Communications 95 (2), 703-721.

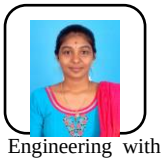
AUTHORS PROFILE

P. J. Beslin Pajila, Assistant Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India. She received his B.E., M.E.,degrees in Computer Science and Engineering. Her Academic Research was Internet Of Things. Her Research Interest is Machine Learning.. She has eight publications. She has attended five seminars, five conferences, five workshop and has delivered a lecture.

Jenifer P., Assistant Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India. She received his B.E., M.E.,degrees in Computer Science and Engineering. Her Academic Research was Fog Computing. Her Research Interest. She has Thirty One publications. She has attended four seminars, nine conferences, five workshop and has delivered a lecture.

Karpagavalli C., Professor, Department of Computer Science and Engineering, St.Mother Theresa Engineering College, Tuticorin, Tamilnadu, India. She received her B.E and M.E degrees in Computer Science and Engineering. Her Academic Research is Cloud based IoT. She has two publications and two conferences. She has attended 5 seminars and 7 workshops. She applied for Short Term Training Programme for the faculties through AICTE schemes.

Angeline Valentina Sweety A., received the B.E degree in Computer Science and Engineering from Franics Xavier Engineering College, Affiliated to Anna University, Tirunelveli, Tamil Nadu, India in 2018. She is currently pursuing the M.E degree in Computer Science and Engineering with Francis Xavier Engineering College, An Autonomous Institution, Tirunelveli ,Tamil Nadu, India



MuthuLakshmi R., received the B.E degree in Computer Science and Engineering from Franics Xavier Engineering College, Affiliated to Anna University, Tirunelveli, Tamil Nadu, India in 2017.. She is currently pursuing the M.E degree in Computer Science and Engineering with Francis Xavier Engineering College, An Autonomous Institution, Tirunelveli ,Tamil Nadu, India.