A Hybrid Mechanism to Detect DDoS Attacks in Software Defined Networks

Afsaneh Banitalebi Dehkordi[1*], MohammadReza Soltanaghaei[2], Farsad Zamani Boroujeni[3]
1- Department of Computer Science,Payame Noor University(PNU),P.OBOX,19395-4697 ,Tehran,Iran
Email: banitalebi97@gmail.com(Corresponding author)
2- Department of Computer Engineering, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran.
Email: soltan@khuisf.ac.ir
3- Department of Computer Engineering, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran.
Email: f.zamani@khuisf.ac.ir

Received: June 2020 Revised: August 2020 Accepted: October 2020

ABSTRACT:
DDoS (Distributed Denial-of-Service) attacks are among the cyberattacks that are increasing day by day and have caused problems for computer network servers. With the advent of SDN networks, they are not immune to these attacks, and due to the software-centric nature of these networks, this type of attack can be much more difficult for them, ignoring effective parameters such as port and Source IP in detecting attacks, providing costly solutions which are effective in increasing CPU load, and low accuracy in detecting attacks are of the problems of previously presented methods in detecting DDoS attacks. Given the importance of this issue,the purpose of this paper is to increase the accuracy of DDoS attack detection using the second order correlation coefficient technique based on Ø-entropy according to source IP and selection of optimal features.To select the best features, by examining the types of feature selection algorithms and search methods, the WrapperSubsetEval feature selection algorithm, the BestFirst search method, and the best effective features were selected. This study was performed on CTU-13 and ISOT datasets and the results were compared with other methods. The accuracy of the detection in this work indicates the high efficiency of the proposed approach compared to other similar methods.

KEYWORDS:Ø-Entropy, WrapperSubsetEval, Second orderCorrelation Coefficient , SDN, DDoS attack.

1. INTRODUCTION

One of the important goals of SDN networks is to be able to design automated security controls that work without interference or at least human intervention. These security controls can respond to network changes and security threats in real time[1].

Since, according to Fig. 1, in SDN networks large flows transmit between hosts, controllers, and switches, these networks can be classified as dynamic networks. SDNs have many advantages, but due to their nature, they can face many challenges and be subjected to various cyberattacks such as DDoS. DDoS attacks are more dangerous in SDN networks compared to classical networks because there is a central controller in them; and if it is attacked, the whole network will be disrupted[2].

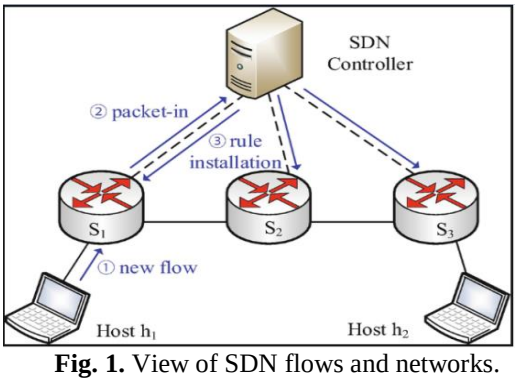

Fig. 1. View of SDN flows and networks.

DDoS attacks are abundant in cyberspace today. Since the beginning of 2020, due to the outbreak of Covid-2019 epidemic, most people's lives have moved towards cyberspace and the web. There is a lot of work, study, shopping, and entertainment in the web world. This has led to an increase in DDoS attacks on virtual systems, especially medical organization sites, games, and educational sites. The attackers have tried hard to

Paper type: Research paper
DOI: https://doi.org/10.29252/mjee.15.1.1
How to cite this paper: A. Banitalebi Dehkordi, M. R. Soltanaghaei and F. Zamani Boroujeni, **"A Hybrid Mechanism to Detect DDoS Attacks in Software Defined Networks"**, *Majlesi Journal of Electrical Engineering*, Vol. 15, No. 1, pp. 1-8, 2021.

hack the health ministries of some countries. The purpose of this attack is to deprive citizens of knowledge about the actions taken. Cybercriminals tried to disable the infrastructure of medical institutions. As a result, hospital staff and remote patients were unable to use corporate applications and emails for some time. However, the attackers could not paralyze the entire organization[3].

According to the information and reports collected on the cybersecurity site, the DDoS attacks will reach about 14.5 million by 2022[4].

Ignoring real attacks and turning to simulated attacks, using only machine learning methods and spending a lot of time training the relevant model, using many features to detect the attack and increasing the controller and CPU load, high cost of implementing some methods are of the problems seen in previous works. In this paper, we try to provide a statistical approach based on the second order correlation coefficient to increase the accuracy of DDoS attack detection in SDN networks and in addition to low cost of software implementation and cost-effectiveness of the proposed approach compared to costly methods like Deep Learning, by choosing the optimal features, we attempted to decrease the workload on the CPU and reduce attacks by decreasing and eliminating the attack flow using the rules of openflow switches.

The rest of the research is listed in the following order: In Section 2, the research related to the detection of DDoS attacks and their methods are discussed. Section 3 presents a proposed approach for investigating attacks and detecting DDoS attacks in this study. Section 4 introduces the implementation and simulation environment. The results are evaluated in Section 5. In Section 6, a comparison of the proposed approach with other methods proposed in previous research works is performed. Finally, Section 7 provides conclusions and suggestions for future work. For the convenience of the authors, the abbreviations of the words used are mentioned in Table 1.

Table 1. Abbreviations.

Symbol	Explanation
DDoS	Distributed Denial Of Service
SDN	Software Defined Network
PR	Precision
F1	F-Measure
IP	Internet Protocol
TP	True Positive
TN	True Negative
FP	False Positive
FN	False Negative
TPR	True Positive Rate
FPR	False Positive Rate
AC	Accuracy
IDS	Intrusion Detection System
CRPS	Continuous Ranked Probability Score
ES	Exponentially Smoothing
T-EHO	Taylor-Elephant Herd Optimization
DC	Data Control
Tr	Threshold

2. RELATED WORK

So far, various solutions have been proposed to detect DDoS attacks, each of which has attempted to increase the accuracy of attack detection. Examples of these solutions are given below:

In the article [5] , the author and colleagues examine the proposed features to detect HTTP attacks, which constitute a large percentage of application layer attacks. In this method, instead of using the captcha technique, it uses different waiting times on the pages, which is more efficient due to the independent nature of the content of the pages. The proposed method is compared with the previous methods under different attacks; and it is examined in terms of the requests sent, the response time and the time period of the request sent, and other factors.

In the research [6] , the author has used the SVM technique, which is one of the machine learning techniques, to detect DDoS attacks. To do this, DDoS attacks are detected through an attack pattern obtained from the database. Online attacks are not detectable in this way. Using the SVM method, which is one of the machine learning techniques, requires a training process. Since this process is slow, it is not suitable for timely detection. It is one of the disadvantages of machine learning methods. Since it acts more as a binary category, it does not provide more information about the type of attack.

In the research [7] , an IDS was provided for the control section in the SDN network. This method uses a set of fuzzy methods, and Deep Neural Networks (DNNs) that are related to machine learning methods. The reason for using this collective technique and deep learning is the high accuracy of these methods in classification and the low FPR. In this method, KDD CUP 99 dataset is used for performance evaluation. Deep learning methods are expensive methods and require special GPUs which are expensive and require expertise in this field.

In paper [8] , a system called T-CAD is proposed to detect and reduce threshold-based DDoS attacks. This method calculates the entropy of router flows. After calculation, this entropy is compared with different thresholds to identify attack flow or normal flows. OMNeT ++ and INET software were used to evaluate the proposed method. The results show the low accuracy of T-Cad system performance.

In [9], the author introduces a hybrid method called CRSP-ES, which consists of a Continuous Ranked Probability Score (CRPS) and anExponential Smoothing (ES) pattern, to detect DDoS attacks. In this method, the new observed flow is compared with the normal traffic distribution, and by quantifying the difference between the two, it tries to detect attacks. This method uses a multiple decision threshold to compare the flows. Failure to check the properties of packages is one of the problems of this method.

In the article[10], introducing a multi-layer intrusion detection system, the authors try to detect and prevent attacks on 5G networks by using cloud computing and artificial intelligence. The 5 layers of the proposed method include: data acquisitionlayer, switch layer, domain controller layer, intelligent controller layer, and intelligence layer; it is tried to detect attacks with the help of these 5 layers. In the first layer, users are validated using the Q-Q algorithm. In the DC layer, packets are examined and flows are divided into attack or normal using the Shannon entropy statistical method. In the switch layer, the game theory method is used to manage the workload of switch tables. In the proposed ML-IDP system, NS3.26 is also used to detect various attacks. Examining the method in the DC layer through Shannon entropy alone does not have the power to detect all DDoS attacks and it is better to use other methods along with it.

In the article[11], the author examines and detects software-defined network attacks and considers the separation of data sheets from the control panel as a factor to increase security challenges such as DDoS attack and MITM attack. Providing software capabilities to manage these networks, software-defined networks have provided solutions to increase the security of these networks and prevent computer attacks.

In the paper[12], a fuzzy method called (T-EHO) based on DBN classification algorithm is presented for detecting DDoS attacks. The method of learning fuzzy rules was evaluated when the FT-EHO algorithm was used instead of the genetic algorithm. The proposed method in this paper examines the cloud environment and uses a standard database to evaluate system performance. The detection accuracy of 93.81 indicates the not very high efficiency of the proposed method.

In the paper[13] , Karan et al. proposed a system with integrated openstack firewall and raw socket programming to monitor network traffic; they are compared to algorithms such as decision tree, the k-nearest neighbor,Naive Bayes, and the deep neural network based on a dataset generated in a DDoS attack environment. In this model, DDoS attacks are detected and the private sector manager is notified. Failure to check all the features of the input packets is one of the problems of the mentioned method.

Although the researches are trying to increase the accuracy of DDoS attack detection, there are some problems in these methods that have been raised. The proposed approach tries to provide a statistical approach based on Ø-entropy according to Source IP and second order correlation coefficient, which is cost-effective and has a high speed in calculation because the SDN networks are based on software; examining the characteristics of the input flows and with high detection accuracy, the problems mentioned in these methods are eliminated and the detection accuracy of DDoS attacks and the efficiency of the detection approach are increased.

3. THE PROPOSED METHOD

The approach proposed in this paper for detecting DDoS attacks is based on coefficient correlation. The similarity of the parameters in normal flows and attack flow can be determined with this approach. The similarity between the two variables causes them to be placed in the same cluster and the correlation coefficient between them increases. The distance between two variables is obtained by different methods such as Euclidean distance and Minkowski distance[14]. A correlation coefficient-based method using Shanon Entropy in classical networks is presented in [15]. In the mentioned study, by calculating the correlation coefficient by considering Shannon entropy in each time period for normal flows, it has been concluded that the value of correlation coefficient for normal flows is close to zero and Shannon entropy has constant values in this case which is independent of its values in the present time compared to the past time, but the values of the correlation coefficient for the attack flows were above zero, which are more pronounced in the second order correlation coefficient. In this paper, by upgrading this method, a new approach based on Ø-entropy, Source-IP and second order coefficient correlation is introduced to detect DDoS attacks in SDN networks based on the optimal feature selection algorithm. The flowchart in Fig. 2 presents more details of the proposed approach.

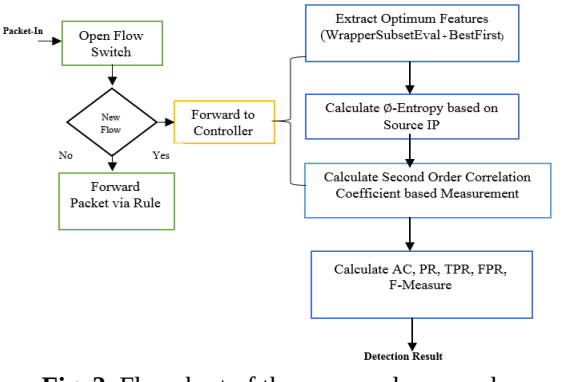

Fig. 2. Flowchart of the proposed approach.

In this flowchart, by considering a period of time, the flows related to that period of time that enter the switch are examined and analyzed. An application module is designed in the controller to collect flows and extract the desired properties. When a host tries to establish a connection with another host, the first packet is sent to the controller; this packet is stored with the details of the sender's IP, sender's port, receiver's IP, receiver's port, packet byte number, and packet arrival time. This is done for all packet-in messages; in this section, the desired properties are extracted according to the received input data. Each flow is considered as a edge; the hosts of the two ends of this flow are graph nodes. To extract these features, each IP is considered as a node at first, then all the connections that those two nodes have with other nodes are used to obtain the features. 8 features have been considered for this task, the initial values of which are different for each data and in each time period. These features include:

- Number of neighboring nodes in relation to the source node
- Number of neighboring nodes in relation to the destination node
- Package size of each flow
- Entropy of the number of flows per second
- Number of the requests that reach the switch in each time period
- Number of flow in the data layer
- The amount of bandwidth consumed over the time period
- Number of two-way flows sent between the source node and the destination node
- Class: This parameter displays the flow class, which is divided into two classes of Normal Flow and DDoS Flow.

In this paper, different feature extraction techniques [16] such as CfsSubsetEval, Classifier Subset Eval, Principal Components and WrapperSubsetEval, and search methods such as Genetic Search, Greedy Stepwise, Ranker, and BestFirst have been used to extract the optimal features. WrapperSubsetEval technique and the BestFirst search method yielded results with higher accuracy in detecting attacks.
After applying the mentioned algorithm to select the optimal features, the following features were selected as optimal:

- Number of neighboring nodes associated with the source node
- Entropy of the number of flows per second
- Number of requests that reach the switch in each time period
- The amount of bandwidth consumed over the time period
- Number of two-way flows sent between the source node and the destination node

The mentioned features are the ones related to flows and can be extracted through the flow statistics message received by the controller. After extracting the optimal features from the proposed features, Ø-entropy is calculated based on Source IP and then the second order correlation coefficient between the extracted features is obtained using Ø-entropy. The presence of attack flows in traffic can increase the value of the second order correlation coefficient. The proposed Ø-entropy metric is defined based on source IP as (1)[17]..

$$H_{\phi}(Src-IP) = -\frac{1}{\sinh(\alpha)}\left(\sum_{i=1}^{n}\left(P_{(Src-IP_i)}\right)^{\sinh(\alpha \log_2 P_{(Src-IP_i)})}\right) \quad (1)$$

Where $\alpha \geq 0$ and $\alpha \neq 1$ and P is the possibility of the number of hosts with the desired source-IP for all the hosts.

According to research[18], new metrics such as Ø-entropy have a higher convergence rate to reach a solution for detecting DDoS attacks compared to α-entropy and Shannon entropy, so they can be used to achieve much better results.

This paper tries to increase the amount of attack detection accuracy by considering the Ø-entropy instead of Shannon entropy and calculating the value of second order correlation coefficient instead of correlation coefficient which has higher accuracy in detecting attacks.

Equation 2 calculates the second order correlation coefficient $A_k^{'}$ in phase i.

$$A_k^{'} = \frac{\sum_{i=0}^{N-1-k}(A_i - \bar{A})(A_{i+k} - \bar{A})}{\sum_{i=0}^{N-1}(A_i - \bar{A})^2} \quad (2)$$

In this relation A_k, the correlation coefficient k is from 0 to N-1 which is calculated according to (3) as follows.

$$A_K = \frac{\sum_{i=1}^{N-K}(H_{\phi(src-ip_i)} - \bar{H}_{\phi(src-ip)})(H_{\phi(src-ip_{i+k})} - \bar{H}_{\phi(src-ip)})}{\sum_{i=1}^{N}(H_{\phi(src-ip_i)} - \bar{H}_{\phi(src-ip)})^2} \quad (3)$$

In (4), if the values of the second order correlation coefficient are higher than Threshold according to (5), the attack flow is detected.

$$A_k^{'} > Tr \quad (4)$$

In (5), the threshold relationship is introduced.

$$Tr = (1-r)\hat{\mu}_{H_{\phi(src-ip)}} + 0.5\hat{\sigma}_{H_{\phi(src-ip)}} \quad (5)$$

Where, μ calculates the mean Ø-entropy value according to (6), and σ is calculated according to (7).

$$\hat{\mu}_{H_{\phi(src-ip)}} = E\left(H_{\phi(src-ip)}\right) = \frac{1}{N}\sum_{i=1}^{N} H_{\phi(src-ip_i)} \quad (6)$$

$$\sigma_{H_{\phi(src-ip)}} = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left[H_{\phi(src-ip_i)} - \mu_{H_{\phi(src-ip)}}\right]^2} \quad (7)$$

In this equation, N indicates the length of the time period. After calculating the threshold and comparing its value, DDoS attack detection and its accuracy are checked. After the attack is detected, the controller sets the values of the idle timeout and hard timeout of the desired flow to zero to prevent the attack from continuing. The proposed approach algorithm is shown in Fig. 3.

Algorithm 1: The Algorithm for DDoS Attack Detection

1: Procedure DDoS Detection System
2:Input: α, N,P, Δt,r
3:Output: DDoS attack detection Result
4: Set

Δt = Sampling Period Time

T_r =DDoS|Attack Detection Threshold

5: For each flow f_i during the Period Time (Δt), calculate the statistical of network Traffic using flow statistics message Module and extract packet header features, then add f_i to the List of Flows.
6. Use WrapperSubsetEval technique and Best-First Search Method to extract best Features.
7: Compute the Ø-entropy based on Source IP and best selected features for incoming flows as follows:

$$H_{\phi}(Src-IP) = -\frac{1}{\sinh(\alpha)}\left(\sum_{i=1}^{n}(P_{(Src-IP_i)}\sinh(\alpha\log_2 P_{(Src-IP_i)})\right)$$

8: Compute the Correlation between features in flows via Ø-entropy :

$$A_K = \frac{\sum_{i=1}^{N-K}(H_{\phi(src-ip_i)}-\bar{H}_{\phi(src-ip)})(H_{\phi(src-ip_{i+k})}-\bar{H}_{\phi(src-ip)})}{\sum_{i=1}^{N}(H_{\phi(src-ip_i)}-\bar{H}_{\phi(src-ip)})^2}$$

9. Compute the second order correlation coefficient as follows:

$$A_k^{'} = \frac{\sum_{i=0}^{N-1-k}(A_i-\bar{A})(A_{i+k}-\bar{A})}{\sum_{i=0}^{N-1}(A_i-\bar{A})^2}$$

10. The threshold is calculated as follows:

$$Tr = (1-r)\hat{\mu}_{H_{\phi(src-ip)}} + 0.5\hat{\sigma}_{H_{\phi(src-ip)}}$$

$$\hat{\mu}_{H_{\phi(src-ip)}} = E\left(H_{\phi(src-ip)}\right) = \frac{1}{N}\sum_{i=1}^{N} H_{\phi(src-ip_i)}$$

$$\sigma_{H_{\phi(src-ip)}} = \sqrt{\frac{1}{N-1}\sum_{i=1}^{N}\left[H_{\phi(src-ip_i)} - \mu_{H_{\phi(src-ip)}}\right]^2}$$

11. If the second order correlation coefficient is more than threshold as shown in equation, a DDoS attack will be detect.

$A_k^{'} > Tr, 2 < K < N$

12.Set Flag =Attack
13. If Flag = Attack then mitigate Attack:
Idle -time out = 0
hard- time out=0
14:Compute Accuracy ,TPR,FPR,F-Measure, Precision
15: end if
16: end Procedure

Fig. 3. Proposed algorithm.

In this algorithm, different stages of the module implemented in the floodlight controller are discussed.

4. IMPLEMENTATION AND SIMULATION ENVIRONMENT

In SDN networks, the computer network can be easily managed through software. Attack tools such as hping3 can be used to simulate an attack[19].

These tools can be used to specify the attacker host, the type of attack and the victim host. In node and host number 1, using the Xterm h1 h2 command, host h1 can attack the host h2 by injecting dataset. With the TCPdump command, it can calculate the packet information sent between hosts and transmit their information to the controller. In this paper, the floodlight controller is used to implement the controller in the SDN network. In the controller, the packet is received in the commandreceive section and parsed with the packet parser () module. By doing this, the packet information is extracted and using the statistics collector () module in the floodlight, the packet information and the information of each of them are calculated by the controller, and the DDoS attack detection and reduction operation is performed by the module mentioned in Fig. 3. The switches used in this article are OpenvSwitch virtual switches that support the openflow protocol. After receiving the packet in the switch, a flow-entry with the flow add method is written in the tables related to the switch. The following command is used to view the flow-entries.

Sh ovs-ofctl dump-flows s1 which is used to check the flow-entries added in this implementation. After implementing and registering the module in the Eclipse environment, the values of Ø-entropy, second order correlation coefficient and threshold are considered and the accuracy of attack detection is calculated regarding different values of α and variable r in different time periods. After identifying and detecting the attack in SDN networks, using the controller in openflow switches and by zeroing the idle-time out andhard timeout value, the detected packets and attack flow are prevented.

To evaluate the proposed approach, we used the datasets that have been examined in this paper.

4.1. Datasets

In this research, the CTU-13 dataset[20], which is one of the largest datasets, has been used along with the ISOT dataset. The CTU-13 dataset includes attack traffic and normal traffic and was produced at the Czech Technical University. This dataset contains 13 scenarios with different botnets. This dataset is a real attack, not a simulated attack. The ISOT dataset [21] is a combination of several existing normal and abnormal datasets. The dataset includes Storm and Waledace botnets selected from the Traffic Laboratory at Ericsson Research in Hungary and the Lawrence Berkeley National Laboratory.

4.2. Performance Measure

Accuracy, Precision, F-Measure, TPR, and FPR from Equations (8) to (12) are used to evaluate the proposed approach. In these equations

- TP: the number of samples of attack flows that have been correctly detected.
- TN: the number of normal flows that are correctly identified as normal flows in this system.
- FP: the number of normal flowsthat are incorrectly identified as attackflowsin this system.
- FN: the number of attack flowsthat are incorrectly identified as normal flowsin this system.
- Accuracy(AC): it examines the ratio of the number of classes of normal and attack flows that are correctly detected and calculates this ratio to the total number of classes according to (8).

$$\frac{TP+TN}{TP+FN+TN+FP} \quad (8)$$

- Precision(PR): it considers the ratio of the number of classes of normal and attack flows that are correctly detected in this system to the total number of samples of attack flows according to (9).

$$\frac{TP}{TP+FP} \quad (9)$$

- Recall: the ratio of the classes that are correctly detected in this system to the total number of normal flow classes according to (10).

$$\frac{TP}{TP+FN} \quad (10)$$

- F-measure(F1): it considers both Precision and Recall to calculate accuracy and can be interpreted as a weighted criterionaccording to (11).

$$. \frac{2\times Precision\times \mathrm{Re}call}{\mathrm{Pr}ecision+\mathrm{Re}call} \quad (11)$$

- TPR: it calculates the rate of the number of classes that has correctly detected the attack flows`according to (12).

$$. \frac{TP}{FN+TP} \quad (12)$$

- FPR: the rate of the classes that are incorrectly detected as an attack flow according to (13).

$$. \frac{FP}{FP+TN} \quad (13)$$

The results of the proposed approach are evaluated on the dataset in the following.

5. RESULTS OF THE EXPERIMENTS

In this section, the results of the proposed method for the proposed dataset are mentioned. After multiple performances for different time periods, with different values of the parameter α for different Ø-entropies in the range (2-10) and considering the values of r to calculate different thresholds for each α, in the range of (-5-5), using the floodlight controller module, different results were obtained; in Tables 2 and 3, the best values obtained in terms of detection accuracy, are listed for different time periods and are obtained separately for each dataset.

The results in the diagrams in Figs. 5 and 7 show the accuracy of the proposed method for the mentioned cases.

Table 2. Evaluation in CTU-13.

Period Time	**α**	H_{ϕ}	A'_{α}	r	Tr	AC
10	3	0.3	0.6	0.5	0.54	98.35
20	2	1.3	0.87	1.5	0.41	99
25	3	1.6	0.84	1	0.64	99.13
30	4	0.7	0.65	2.5	0.74	99.81
35	5	0.64	0.74	2	0.47	98.34
45	6	1.2	0.63	1.5	0.65	99.34
60	7	0.9	0.26	3	0.34	96.76

Analysis of the results shows that at values of r <3, high attack detection accuracy is obtained for different values of Ø-entropy. Fig. 4 examines the relationship between the mean entropy values at different time periods and the threshold for the CTU-13 dataset.

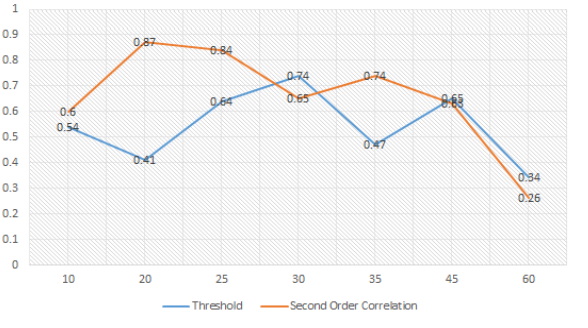

Fig. 4. Examining the mean values of second order correlation coefficient and threshold in different time periods.

This figure shows the mean values of the second order correlation coefficient and threshold at different time periods. Attacks are detected in cases where the second order correlation coefficient is higher than the threshold. The degree of detection accuracy at these time periods for the CTU-13 dataset is shown in Fig. 5.

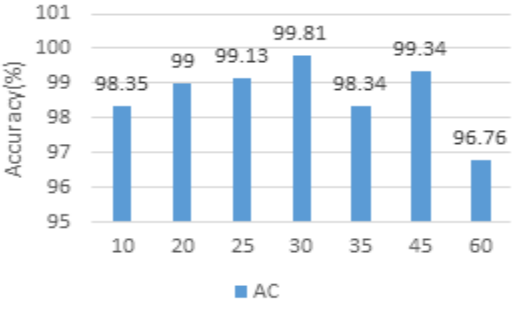

Fig. 5. Comparison of detection accuracy in different time periods in CTU-13.

The accuracy of detection in the time period of 30 seconds with 99.81% accuracy has the highest percentage of detection compared to other time periods. The results for the ISOT dataset are shown in Table 3.

Table 3. Evaluation in ISOT.

Period Time	**α**	H_{ϕ}	$A_{\alpha}^{'}$	r	Tr	AC
10	3	0.9	۰/۸۵	3	0.34	97.65
20	2	0.54	0.43	2	0.54	98.35
25	3	0.75	0.87	2	0.82	99.87
30	2	0.83	0.98	4	۰/۶۳	97.78
35	5	0.73	0.69	1.5	0.9	99.42
45	6	0.25	۰/۷۹	2	0.53	99.54
60	4	0.64	0.39	2.5	0.98	99.12

By the analysis of the results, it is clear that, like the CTU-13 dataset, at values of r <3, high attack detection accuracy is obtained for different values of the second order correlation coefficient. Fig. 6 examines the relationship between the mean entropy value at different time periods and the threshold for the ISOT dataset.

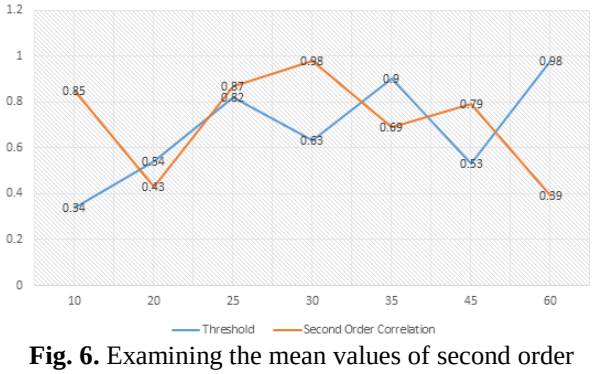

Fig. 6. Examining the mean values of second order correlation and threshold in different time periods.

This figure shows the mean values of second order correlation coefficient and threshold at different time periods. Attacks are detected in cases where the second order correlation coefficient is higher than threshold. The accuracy of detection at these time periods for the CTU-13 dataset is shown in Fig. 7.

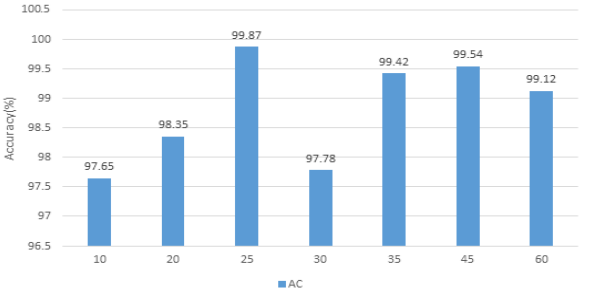

Fig. 7. Comparison of the accuracy of attack detection at different time periods in ISOT.

The accuracy of detection in the time period of 25 seconds with 99.87% accuracy has the highest percentage of detectioncompared to other time periods.

6. COMPARISON OF THE PROPOSED APPROACH WITH PREVIOUS METHODS

In this section, the results of research in the field of DDoS attack detection are compared with the proposed approach in Table 4. For the proposed approach, the results are mentioned for two different datasets.

Table 4. Comparison of the proposed method with other methods.

Techniques	AC(%)	FPR(%)
T-CAD	96	4
CRPS-ES	98.40	3.27
ML-IDP	96.08	2.5
FT-EHO	93.81	-
This Method(CTU-13)	99.81	0
This Method(ISOT)	99.87	0

Fig. 8 also shows a comparison between the results.

.

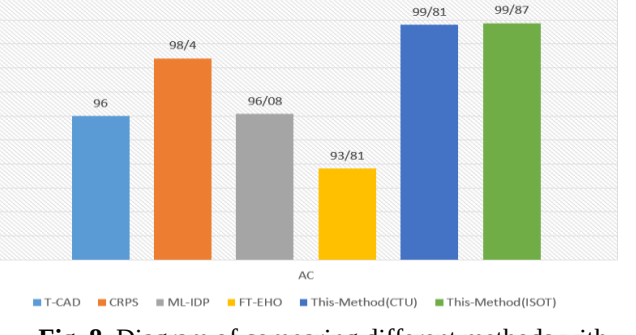

Fig. 8. Diagram of comparing different methods with the proposed method.

In this diagram, the results are compared with each other. This comparison shows that the proposed approach is more efficient than the previous ones.

7. CONCLUSION

In this study, a statistical method based on features correlation coefficient is presented for detecting DDoS attacks. To do this, the second order correlation coefficient is combined with the SourceIp-based ∅-entropy method and the optimal features are selected based on the WrapperSubsetEval algorithm and the BestFirst search method. The datasets used are CTU-13 and ISOT and the results of the proposed approach are presented on these two datasets. Then, the results of the proposed approach were compared with several other studies under the same conditions. The results show the superiority of the proposed approach over the other methods presented. Although there are various cyber attacks on computer networks, in this study, only DDoS attacks on SDN networks have been investigated and other attacks have been skipped. Analyzing other attacks on these networks can be considered as a research work in the future.

REFERENCES

[1] Yadav, A., et al., **"SDN Control Plan Security in Cloud Computing Against DDoS Attack"**. IJARIIE, Vol. 2, No. 3, pp. 426-430, 2016.

[2] Dayal, N., et al., **"Research Trends in Security and DDOS in SDN".** *Security and Communucation Networks*, Vol. 9, No. 18, pp. 6386-6411, 2017.

[3] Kupreev, O., E. Badovskaya, and A. Gutnikov. **"DDoS attacks in Q1 2020"**. *2020; Available from*: https://securelist.com/ddos-attacks-in-q1-2020/96837/.

[4] Morgan, S. **"CyberCrime Magazine"**. 2020; *Available from*: https://cybersecurityventures.com.

[5] Mirvaziri, H., **"A new method to reduce the effects of HTTP-Get Flood attack"**. *Future Computing and Informatics Journal*, pp. 87-93, 2017.

[6] Kirubavathi, G. and R. Anitha, ***"Botnet detection via mining of traffic flowcharacteristics".*** *Computers and Electrical Engineering*, 2016.

[7] Anbarsu, S., A.X. Annie Rayan, and V. Vetrian, **"Software-Defined Networking for the Internet of Things: Securing home networks using SDN"**, ed. R.-T.D.A.f.L.S.S. Data. 2020.

[8] Singh, K., K. Dhindsa, and D. Nehra, *T-CAD:* **"A threshold based collaborative DDoS attack detection in multiple autonomous systems".** *Journal of Information Security and Applications*, 2020. **51**.

[9] Bouyeddou, B., et al., **"DDOS-attacks detection using an efficient measurement-based statistical mechanism".** *Engineering Science and Technology, an international Journal* 2020.

[10] Abdulqadder, I., et al., **"Multi-layered Intrusion Detection and Prevention in the SDN/NFV Enabled Cloud of 5G Networks using AI-based Defense Mechanisms".** *Computer Network*s, 2020.

[11] Pradhan, A. and R. Mathew. **"Solution to Vulnerabilities and Threts in Software Defined Networking(SDN)".** in *Third International Conference on Computing and Network Communications(CoCoNet'19)*. 2020.

[12] Velliangiri, S. and H.M. Pandey, ***"Fuzzy-Taylor-elephant herd optimization inspired Deep Belief Network for DDoS attack detection and comparison with state-of-the-arts algorithms"***. *Future Generation Computer Systems*, Vol. 110, pp. 80-90, 2020.

[13] Virupakshar, K., et al., **"Distributed Denial of Service (DDoS) Attacks Detection System for OpenStack-based Private Cloud"**. *Procedia Computer Science*, 2020.

[14] Fuente, D., A. Romero, and P. Torres, **"Existence and extendibility of rotationally symmetric graphs with a prescribed higher mean curvature function in Euclidean and Minkowski spaces".** *Journal of Mathematical Analysis and Applications*, Vol.. 446, No. 1, pp. 1046-1059, 2017.

[15] LIU, H., **"A collaborative defense framework against DDOS Attacks in networks".** 2013, WASHINGTON STATE University.

[16] Xu, Z., et al., **"Software defect prediction based on kernel PCA and weighted extreme learning machine".** *Information and Software Technology*, Vol. 106, pp. 182-200, 2019.

[17] Bolly, F. and I. Gentil, *"***∅-entropy inequalities for diffusion semigroups".** *Journal de Mathématiques Pures et Appliqués*. Vol. 93, No. 5, pp. 449-473.

[18] Song, Y., et al., **"Divergence-based cross entropy and uncertainty measures of Atanassov's intuitionistic fuzzy sets with their application in decision making"**. *Applied Soft Computing*, 2019. 84.

[19] Hoque, N., et al., **"Network attacks: Taxonomy, tools and systems".** *Journal of Network and Computer Applications*, , 2014. 40.

[20] Yavanoglu, O. and M. Aydos **"A review on cyber security datasets for machine learning algorithms"** in *IEEE International Conference on Big Data (Big Data)* 2017. Boston, MA, USA

[21] Bhamare, D., et al., **"Feasibility of Supervised Machine Learning for Cloud Security",** in *International Conference on Information Science and Security (ICISS)* 2016: Pattaya, Thailand