How to Cite:
Kaur, G., & Gupta, P. (2022). An investigation of different DDOS attack detection methods in software-defined networks. *International Journal of Health Sciences*, *6*(S1), 1088-1108. https://doi.org/10.53730/ijhs.v6nS1.4863

An Investigation of Different DDOS Attack Detection Methods in Software-Defined Networks

Gaganjot Kaur
Assistant Professor, Department of Computer Science and Technology, Manav Rachna University, Faridabad, India

Prinima Gupta 2
Professor, Department of Computer Science and Technology, Manav Rachna University, Faridabad, India

***Abstract*---**Software-Defined Network is more vulnerable to more frequent and severe security attacks. Distributed Denial of service (DDoS) spasms corrupt network along with hinder efficiency and performance significantly. DDoS spasms lead to exhaustion of network means, thereby stopping the controller and impeding normal activities. Detection of DDoS attacks requires different classification techniques that provide accurate and efficient decision-making. Various techniques to detect the attacks are proposed in the existing literature. However, analysis of various works reveals various shortcomings of different techniques. In this paper, the existing techniques are analyzed in terms of their accuracy and MSE, and seven methods are compared with regards to suitability to counter DDoS attacks efficiently. Analysis of the results shows limitations and sets the tone for future studies on the topic. Overall, it is suggested to continue looking for better techniques to improve upon the existing learning and experiences gained and provide more accurate results.

***Keywords*---**Software-Defined Network, Distributed denial-of-service, SVM, DENFES, BPNN, Network security.

Introduction

As innovation progresses, software-defined networks (SDN) are developing an organization that allows for a vivacious network flow. As a result of this adaptive structure, all of the organization's arrangements may be accessed from any computer in the globe. SDN engineering is legitimately programmable as it is being decoupled. The organization traffic is dynamically transformed allowing to

International Journal of Health Sciences ISSN 2550-6978 E-ISSN 2550-696X © 2022.
***Corresponding author**: Kaur, G.; Email: gaganjot@mru.edu.in*
Manuscript submitted: 27 Nov 2021, Manuscript revised: 18 Feb 2022, Accepted for publication: 09 March 2022

the necessities of the customers. In addition to holding up a global view on the organisation as it is seen halfway, programming defined network includes an additional component. As a result, the organization's theoretical viewpoint is consumed. SDN is required in the present systems administration as autonomous advancements are needed at each layer. SDN is a financially economical worldwide utilized organization for systems administration that is non-massive and cheap because it involves source programming. The information or bundles that have been sent to the organization plane are when all is said in done utilizing an open stream switch, which gives access to follow the organization way over an organization of switches. There is just one open switch convention that is supervised distantly and is available on a large scale internationally. This makes the organization plan less complex as the SDN regulators give them directions instead of the sellers who explicitly plan the gadgets and conventions.

In standard frameworks organization, the control plane and data plane exist on each contraption. SDN abstracts this thought and confines the two planes. The control plane is arranged clearly on an SDN regulator to provide versatility, a Linux worker running. Arrangement of the real or virtual switch is used for SDN programming and data plane operations. The SDN regulator transforms to form an essential portion to enable changes in the best way in order to propel data bundles. The two planes can grant through a show, for instance, OpenFlow. Despite allowing a versatile framework, SDN also conveys programmability and ease to the framework heads. Since singular defenselessness can lead to significant errors, security should be a principal fragment consolidated with SDN. Other than the current assault vectors on conventional frameworks, the regulators and the relationship with the control plane cause novel challenges associated with the security unique to the SDN. SDN is a novel framework organization plan that might be vulnerable to face DDoS spasms. In a rejection of Service (DOS), all bits of SDN network can be impacted. By launching a DoS, an aggressor can bring about a reduction or make the unsettling influence of SDN organizations.

Moreover, artificial intelligence (AI) is being used on a huge scale in current programming networks. Facebook's News Feed is a popular model. The News Feed uses modified sorting out some way to individualize each customer's channel. Suppose a section occasionally stops in order to scrutinize or like a particular person's post. In that case, the news line begins to depict a highly prominent estimate of the partner's growth preceding the channel. The item undertakes the authentic assessment and examines judiciously to acknowledge customer's data plan and also uses monitors to populate the newsfeeds. Also, Virtual assistant growth is also computerized through AI. Sophisticated business partners combine two important learning models to decipher trademark talk and get appropriate settings (like a customer's own personalised strategy and as of late described tendencies) and take action, such as booking an aeroplane ticket or pulling up an online driving school course.

Literature review

The world is developing at a very fast pace, and the world online or the internet is equally progressing at a fast pace. In the modern era, life seems imaginable

without access to the internet and most of the daily activities are completely dependent on the internet. People use the internet primarily for communication, data sharing, research purposes, sales, online purchasing, and many more activities; these activities involve the simultaneous sharing of important information and data. As this is extended towards a vast platform accessible worldwide, maintaining data secrecy and internet security is necessary. Intrusion Detection System (IDS) ensures the safety of this global connection of networks. IDS monitors and analyses the data traffic and distinguishes intrusions from normal to spam. Currently, there is an immense focus on advanced wireless transmission, wireless networks, and Bluetooth connections. In such cases, the proper use of the IDS facilitates providing security of wireless networks. It is used to detect and supervise abnormal behavior of the network. To tell whether data or network is abnormal, an IDS compares it with already stored intrusion records to identify the abnormality and intrusion.

Research is going on to detect newer attacks in every possible and better way. For attacks, SDN is a large logical point of communication. DDoS attacks have become a cause of serious concern growing in frequency, number, and severity. The approach for DDOS detection is to identify and relieve identified and obscure DDoS spasms in continuous environments.

In the assessment of network IDS, the selection of the required data set has a strong influence. However, most of the data sets that are publicly accessible are not practical and lack a variety of attacks to cover all developments seen today on the internet. This lack is mainly due to the reason that the service providers disclose their network details on security and confidentiality issues, explaining that many data sets being used with intrusion systems do not provide reasonable accuracy. Numerous datasets are available for IDSs like KDDCUP'99, CICIDS2017, ISCX2012, Kyoto, LBNL, UMASS, CDX, ADFA, and DEFCON (Hettich, 1999; Sharafaldin et al., 2018; Canadian Institute for Cybersecurity,2012; Song, 2011; Nechaev et al., 2004; Sangster et al., 2009; Creech and Hu, 2013). Such publicly opened datasets like DARPA, KDD, NSL-KDD, and ADFA-LD are sometimes considered to be the standards. Table 1 summarizes various features of the datasets (Creech and Hu, 2013).

Software-Defined Networking (SDN) is a superb network architecture. In it, the network control is vital, achievable, adjustable, and location-wise distant from forwarding devices (Khraisat et al., 2019). The SDN architecture has 3 layers consisting of infrastructure (Data plane) and Control layer (Control Plane), as shown in Figure 1.

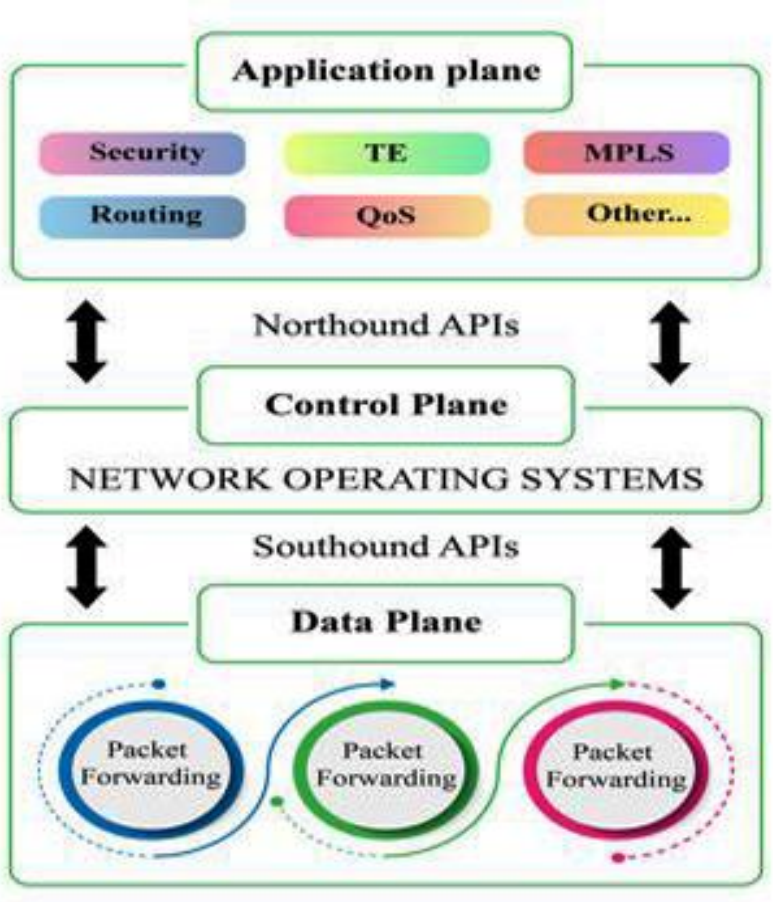

Figure 1. Features of the application plane and data plan

Figure 2 shows a comparative profile for mean squared error (MSE) for seven different logarithms. These seven algorithms are Support Vector Machine (SVM), Transductive Confidence Machines for K-Nearest Neighbors (TCM-KNN), adaptive binary tree-based multi-class support vector machine (ABTSVM), random neural network and an artificial bee colony algorithm (RNN-ABC), dynamic evolving neuro-fuzzy inference system (DENFIS), and Back Propagation Neural Network (BPNN). Fig. 2 shows SVM maximum value of MSE (0.10%) followed by RNN-ABC, KNN-ACO with BPNN showing least errors, showing maximum accuracy of BPNN algorithm.

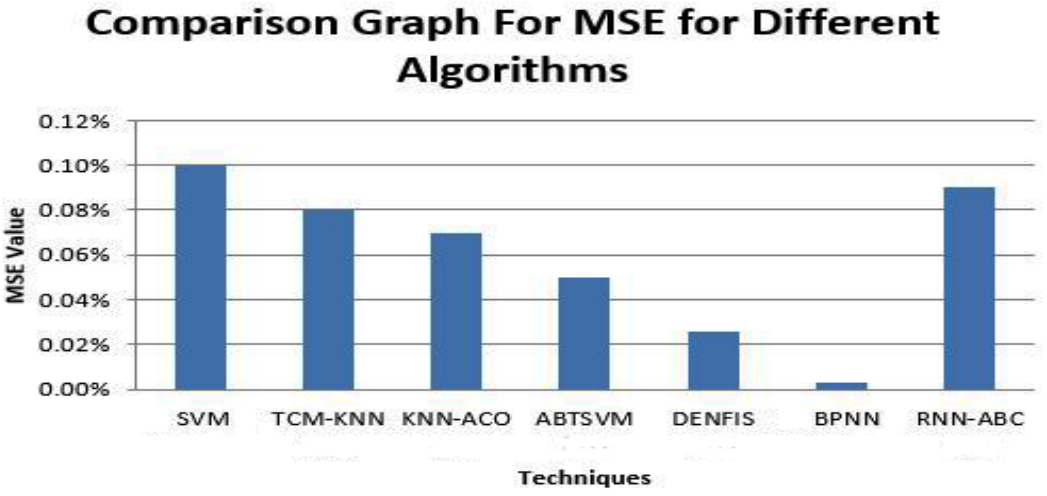

Figure 2. Comparison Graph for MSE for different logarithm

Materials and Methods

Figure 3 shows the accuracy levels of seven algorithms. It shows BPNN, DENFIS at 98% accuracy levels. The accuracy percentage of five other methods- SVM, TCM-KNN, ABTSVM, RNN-ABC are 90, 92, 93,95, and 91, respectively. This shows that the SVM method is the least accurate and BPNN is the most accurate.

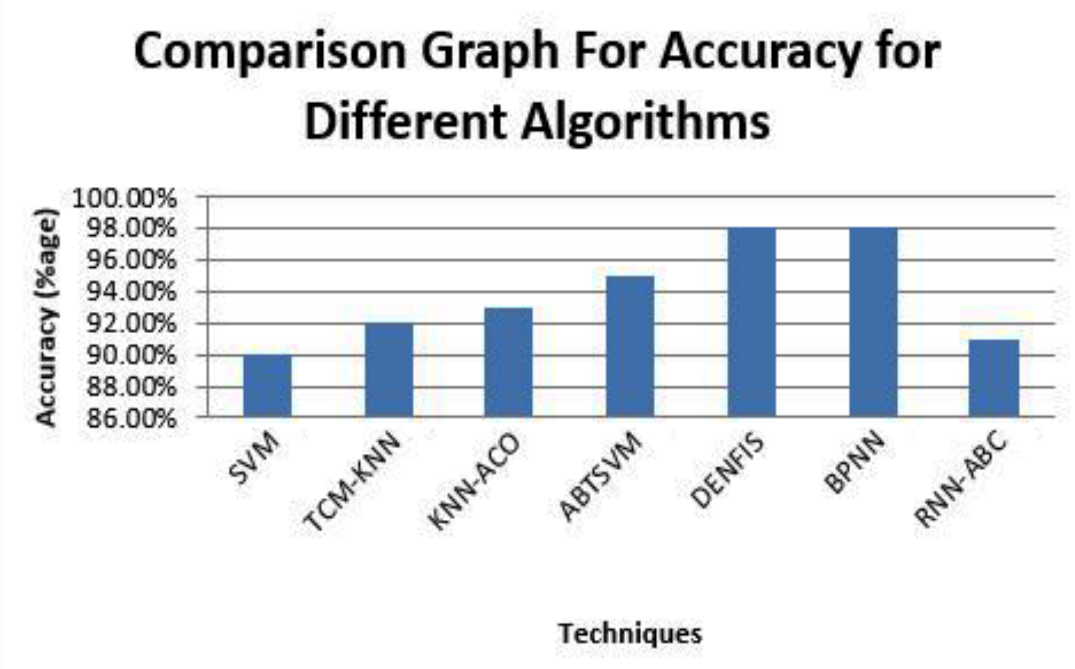

Figure 3. Comparison Graph for accuracy of different logarithms

Table 1 below shows a comparison of different datasets of network connection.

Table 1
Comparison of different datasets

Dataset	Realistic Traffic	Label data	IoT traces	Zero-day attacks	Full packet captured	Year
DARPA 98	√	√	×	×	√	1998
KDDCUP 99	√	√	×	×	√	1999
CAIDA	√	×	×	×	×	2007
NSL-KDD	√	√	×	×	√	2009
ISCX 2012	√	√	×	×	√	2012
ADFA-WD	√	√	×	√	√	2014
ADFA-LD	√	√	×	√	√	2014
CICIDS2017	√	√	×	√	√	2017
Bot-IoT	√	√	√	√	√	2018

Analysis of these datasets in Table 1 reveals that all have good traffic anagement and data handling characteristics. The current review further shows that out of 11 datasets only 4 datasets: ADFA-WD, ADFA-LD, CICIDS2017, Bot-IoT reported zero-day attacks. The only BoT showed IoTtraces. Rest all the 10 datasets had negative IoT traces. Kaur and Gupta in their study reported that all the categorized and unorganized methods could assist indetecting the unspecified flow on the foundation of definite frameworks as packet flow, precision rate as well as time duration. These investigators applied Bayesian Network, Wavelets, SVM, as well as KNN for identifying D.D.O.S strikes (Canadian Institute of Cybersecurity).

Comparison of the above all datasets of network connections show BoT-IoT to be the best datasets on the chosen nine parameters: traffic, IoT, trace, day attack, and full packet capture. Table 2 shows the comparison of all seven techniques, their limitations, and findings of studies in the literature on those methods to avert DDoS attacks.

Table 2
Comparison of the existing techniques

Authors Name	Technique name	Findings	Limitations
(Li and Wang, 2017)	SVM	SVM classification techniques analysis shows that the method's average precision rate is 95.24% with a limited amount of flow collection.	Has high false alarm rates to different degrees.
(Li and Guo, 2008)	TCM KNN	TCM for K-Nearest Neighbors (TCM-KNN) was developed for guided device interruption discovery. They used a know-how method of identifying irregularities based on TCM-	The algorithm has faults with the detection points of an anomaly.

		KNN and stressed improvement on the components.	
(Tavallaee et al., 2009)	KNN ACO	This paper integrates the KNN algorithm with the ACO (ant colony optimization) algorithm; on this basis, the KNN-ACO was suggested and uses an ID3 algorithm (decision tree) to decrease features.	Weak scalability, low accuracy, and low performance for large and speedy data flows
(Burai P et al., 2014)	ABTSVM	The adaptive parallel tree SVM (ABSVM) classifier was created in agreement with the standard of SVM. This paper explores characterization strategies (MLC, SVM) utilizing highlight extraction that can segregate among species and clones of vitality trees.	
(Saad et al., 2014)	DENFIS	ICMPv6 Flood Attack Identification using DENFIS algorithm was proposed for the Detection of DOS strike on IPv6 networks. The suggested data showed that ICMPv6 Flood Attack could be detected by a low-root MSE of about 0.26.	This research aimed at the flooding attacks of an ICMPv6 packet that is "ICMPv6 ECHO challenge" from 1000 to 1500 pings with various flood rates. Therefore, it becomes difficult to detect attacks of DDoS and DoS in other ICMPv6 communications.
(Saad, et al., 2016)	BPNN	A smart ICMPv6 DDoS flood-attack detection system using back-neural propagation ((v6IIDS)) in the IPv6 network was presented. In this study, the precision of the proposed v6IIDS System was also discussed and analyzed. The results showed that ICMPv6 DDoS flood spasms at a finding precision of 98.3% could be detected within the proposed system.	The authors used the same dataset as in his previous research that included only one attack, which is the overflowing of messages from the "ICMPv6 ECHO Order" and the training models from these works.

(Qureshi et al., 2020)	RNN-ABC	The algorithm of Artificial Bee Colony (ABC) was used to shape the device based on the Random Neural Network (RNNABC). The device proposed was trained and checked for unseen data on the NSL-KDD Train+. Experimental findings showed that new attacks with a precision of 91.65 percent can be effective with swarm intelligence and RNN.	The approach must also be strengthened and the training time for the neural network model reduced.

Review of methods in Table 2 shows that these methods have the following disadvantages

RNN-ABC takes more time that needs to be reduced.
KNN-ACO method suffers from weak scalability, has low accuracy, and shows low performance for large and speedy data flows.
SVM shows high false alarm rates to different degrees.
Furthermore, SVM shows a precision rate of 95.24 percent against 98.30 percent demonstrated by BPNN. From this table we can conclude that out of the above methods, BPNN appears most accurate method.

The study of DDoS spasms and numerous detection methods to identify these attacks requires in-depth analysis. Also, since SDN is a recent subject, more research on its safety issues is not yet available. Several studies have highlighted the vulnerability of an SDN controller to DDoS attacks and proposed policing packets for the controller (Yan et al., 2015; Ankali and Ashok 2011).
Some of the studies are reviewed here. Data mining (DM) as well as Machine learning (ML) approaches are developed and hit immensely for identifying detection. Suresh and Anitha assessed several ML algorithms for DDoS attacks (Suresh and Anitha,2010).

After the emergence of SDN, various methods to models the attack actions based on the SDN controller in a deep learning algorithm have developed. However, current approaches, like the neural network algorithm, have some issues in their delivery of proper outcomes. In this study, we constructed the SDN environment via the mininet and lighting fixture simulation platform, extracted six-fold feature values by switch flow table, and then built DDoS spasm pattern through the combination of SVM classification techniques (Ye et al., 2018). The analysis showed that the proposed method's average precision rate was 95.24%, with a limited flow collection. This proposed work on detecting DDoS attacks in SDN is of good value.

The Support Vector Machine (SVM) is an popular data mining method. SVM techniques reveal the inadequacy of previous knowledge for the detection of anomalies (Li and Wang, 2017). The accuracy of classification is fine, but together

SVM and neural networks demonstrated high false alarm rates (FAR) to different degrees.

The KNN algorithm (k-Nearest Neighbor) is another popular common data mining anomaly detection technique (Burai et al., 2014). This is popularly used as it is an advanced theory, relatively cheap retraining, high accuracy, and high real-time performance, and also adds to incremental learning.

Li and Guo in their study introduced the TCM-KNN algorithm and the collection and optimized weighting process for functions (Li and Guo, 2008). The original algorithm based on the KNN algorithm's closest neighbor principle analyses the anomalies among detection points and regular workouts by determining p values to identify the recognition points.

In TCM for K-Nearest Neighbors (TCM-KNN) was developed for guided device interruption discovery(Li and Guo, 2008). This study used a know-how method of identifying irregularities based on the TCM-KNN method and stressed improvement on the components. It used the weight system to enhance TCM-KNN as an effective lightweight and online specification recognition procedure to cut device costs and increase its position execution. Commitment and highlighting of weight systems were included. An advance in analyses using remarkable interruption discovery data set KDD Cup 1999 demonstrates suitability of the projected technique.

Before development of the TCM-KNN, an enhanced KNN-ACO idea was further evolved for interruption recognizable evidence through the use of KDDCUP'99 (Tavallaee et al., 2008). Jaiswal et al. (2016) integrated the KNN algorithm with the ant colony optimization (ACO) algorithmand suggested that KNN-ACO uses an Iterative Dichotomiser 3 (ID3) algorithm (decision tree) to reduces the number of anomalous features. The algorithm was verified by conducting tests on the KDD CUP99 data sets in order to determine greater precision in the attack detection. Though having anomaly flow in conventional networks, these detection processes have a specific SDN security safety reference value, weak scalability, low accuracy, and poor performance for large and speedy data flow. Hence, SDN-based irregular detection has gradually become an evaluative subject in past years.

Ye et al. established a parallel adaptive tree adaptive boosting SVM (ABSVM) classification in compliance with the SVM method (Ye et al., 2018) and examined the characterization techniques that highlight extraction to separate vitality trees from animal species and clones, such as the support vector machines (SVM) as well as maximum likelihood classifier (MLC). Because of the location confines, the analyzed trees show comparable features. Based on the SVM guideline, an SVM tree paired classifier was defined using the plane characteristics of selected classes. The flexible SVM (ABSVM) double tree provided more detailed results than those after applying the multi-class SVM strategy. This research links the techniques used to support vector machines (SVM) to evaluate plant species or clones.

Internet Control Message Protocol version6 (I.C.M.Pv6) Flood Attack Identification using the active neural-fuzzy inference system (D.E.NF.IS) algorithm was proposed to detect DOS attacks on IPv6 networks, as presented in a previous study (Saad et al., 2014). The authors created an application called C # to dispatch flood attack packets ICMPv6. Various attack rates were produced for flood packets, from 1000 to 1500 pings, and for each ICMPv6 packet, the usual traffic packets are calculated by various ping rate as 10 to 15 pings. The dataset includes 2000 data collected and divided into 2 sets. The proposed data showed that a low-root MSE of about 0.26 could detect an ICMPv6 Flood Attack.

This study aimed at the flooding spasms of an ICMPv6 packet that is "ICMPv6 ECHO challenge" from 1000 to 1500 pings with various flood rates. Therefore, as the attacks are not included in this study, it could not detect DDoS and DoS attacks in other ICMPv6 communication systems.

Saad et al. presented a smart ICMPv6 DDoS flood-strike assessment system using back-neural propagation (v6IIDS) in the IPv6 network (Saad et al., 2016). Herein, they discussed and analyzed the precision of the proposed v6IIDS System. By applying real data sets acquired by National Advanced IPv6 Center (NAv6) facility, usefulness of ICMPv6 DDoS flooding-attack discern setup utilising back-propagation neural network (V6IIDS) system was shown. The traffic of data sets was focused on a testbed environment established on certain input limits used to create a new data set. It was revealed that ICMPv6 DDoS flood strikes at a perceived rate of 98.3% could be detected within the proposed system. However, the authors' data set included only one attack: the overflowing of messages from the "ICMPv6 ECHO Order" and the training models from these works.

Larijani et al. suggested a technique to secure sensitive information and identify new cyber-attacks on an anomaly-based intrusion(Larijani et al., 2019)and employed Artificial Bee Colony (ABC) algorithm to shape the device based on the Random Neural Network- artificial bee colony (RNNABC). The device proposed was checked for any suspicious and unseen data on the NSL-KDD Train+. Experimental findings revealed that new attacks with a precision of 91.65 percent could be effective with swarm intelligence and recurrent neural network (RNN). However, it is suggested to strengthen the approach and reduce the training time for the neural network model.

Table 2 shows the above-reviewed techniques combined with their findings and limitations. The performance of these techniques is further analyzed, and their effects are analyzed to indicate the usefulness of the method. The performance analysis is discussed in the next section.

Different Techniques for DDoS detection

There are several methodologies and techniques for DDoS detection. In this section, we elaborate on them correlating with SDN as well and make a comparative study. Well-known ML techniques for detecting DDoS attacks are an Support Vector Machine (SVM), artificial neural network (ANN), Decision Tree, Fuzzy Logic, Evolutionary Algorithm, Marine Bayes, and clustering algorithms.

Different studies have reviewed the above techniques. One study reported that a meld type of SVM and Fuzzy logic resulted in superior intrusion perceiving perfection and an improved SVM with firefly algorithm with FPR of 8.6% and FNR (false negative rate) of 2.2% yielded optimum outcomes (Shah and Issac, 2018; Kabanda, 2020).

A Bayesian Network model constructed using supportive artificial intelligence techniques such as autonomous robotic vehicles, machine learning techniques, Random Forests, Artificial Neural Networks (ANN), Decision Tree C4.5 and Support Vector Machines and fuzzy logic has proven one of the effective machine learning algorithms. In some mobile cognitive radio networks, a malevolent primary user emulation (PUE) may attempt to copy main user signal for making mental network released used channel, resulting in rejection of service. In such a situation, a support vector machine (SVM) method, that differentiates receiving signal uses SNR and Rényi entropy of an energy signal like an input to SVM to distinguish between a main or malevolent primary user emulation signal., has proved effective method (Cadena et al., 2020).

Fuzzy c-means groping provides superior precession in the detection of the strikes. IDSs are popularly used in a wireless sensor network (WSN) for safeguarding the network from insider strikes by applying a definite trust-based method. Malicious nodes initiate strikes in the category of the maximal harm model can be easily identified. Hackers can resort to other spasms like passive message fingerprint attacks (Li et.al.,2016).

CAIDA: This dataset type of DOS attack impedes ongoing traffic of an identified network by over-powering the latter with enormous network packets and thereby disrupting the traffic to arrive at the requisite place (Hick et al., 2020). During participation in finding performance, the area of every SDN is needed for providing a huge chunk of real traffic data, by which private evidence might be disclosed(Zhu et al., 2018). A DDoS attack can be easily revealed by the SDN because of its central based monitoring ability and network accessibility. Sahoo et al. concluded as information distance metric could efficiently evaluate DDoS traffic concerning other metrics at advanced precession (Sahoo et al., 2017).

Despite numerous solutions available, DDoS attacks are increasing in their frequency, volume, and severity gradually, throwing a spanner to network security specialists to address current overwhelming dangers. Software-defined networking (SDN) has acquired a lot of friction from several analysts concerning its ability to direct the burgeoning requirements of present data stations (Bawany et al., 2017). Software-Defined Networking focuses on the function of the software to monitor networks. There are multiple mechanisms by which SDNs identify specific types of strike such as DDoS by enhanced features, better legacy network, more error detection percentage (AlEroud and Alsmadi, 2017).

Undoubtedly, Software Defined Networking (SDN) assists in making the network agile, flexible, and programmable. Its centralized control plan monitors the entire network. Distributed Denial of Service (DDoS), very well-known cyber strike leads to emptying of the system holdings, thereby making the system not available to serve authorized activities (Karan et al., 2018). SDNs in combination with cloud

computing have also proven effective in tackling DDoS attacks, though the latter has emerged to become a better severe strike into the SDN-Cloud (Misra et al., 2021).

Open flow is most standard SDN methods that facilitates communication among the controller and the switches, but its dynamism poses several security challenges such as spoofing attacks, scanning, DoS attacks (Li et al., 2016). In DDoS attacks, SDN may face anomalies and intrusions. Major SDN anomaly detection mechanisms have been categorized in several schemes: flow counting, information-based, entropy-based, hybrid scheme, and deep learning (Jafarian et al., 2021).

Software-Defined Networks (SDN) makes the network design easier and offers a stage for network application growth in a configurable way and is employed in different topologies so that the new network design can have more capable configuration, improved performance, and better flexibility (Krishnan and Oliver, 2019). Singh and Bhandari reported as an new-flow-based DDoS spasm shows a crucial security predisposition to confiscate and take hold of the rare resource of data plane as well as control plane in SDN network (Singh and Bhandari, 2020). Another study stated that reviewed circulated denial-of-service (DDoS) spasms detecting in SDN networks by using three datasets (e.g., UNB-ISCX, CTU-13, and ISOT) and by applying a specific static threshold method can enhance accuracy in detecting DDoS spasms in the software-defined network (Dehkordi et al., 2021). Table 4 shows the accuracy levels of all seven methods. It shows BPNN to be the most accurate (98%) against SVM, the least accurate method (90%).

Table 3
Accuracy for different techniques

Technique	Accuracy (%age)
SVM	90%
TCM-KNN	92%
KNN-ACO	93%
ABTSVM	95%
DENFIS	98%
BPNN	98%
RNN-ABC	91%

Dynamic evolving neural fuzzy inference system (DENFES): Noori et al. in their study on the DENFES method in optical fiber transmission concluded that nonlinear DENFIS equalization scheme could better the established distorted signal from a mode division multiplexer (MDM) with improvised precision as compared to earlier linear equalization schemes like recursive-least-square (RLS) algorithm(Noori et al., 2019). This finding strengthened the findings in the current review whereas as above in Tables 2, 3 and 4, the DENFES method shows one of the highest (98%) accuracy rates. This shows that in our review, DENFES and Backpropagation neural network (BPNN) rank among the best methods to counter distributed denial-of-service attack with both having about 98% precision level.

Table 4
Validation Error (MSE) for different techniques

Technique	MSE
SVM	0.10
TCM-KNN	0.08
KNN-ACO	0.07
ABTSVM	0.05
DENFIS	0.026
BPNN	0.0030683
RNN-ABC	0.09

Backpropagation neural network (BPNN): Liu stated that the network controller employs the PSO-back spread neural network to identify if a dispersed denial-of-service spasm occurs by additional extracting the flow features of the abnormal switch in the network (Liu et al., 2019).

Wang et al., in their study, mentioned the defend scheme (SGS) for defending the control plane against the spread rejection of service spasms and argued that key feature of SGS is the use of multi-controller in the control plane via gathering. They categorized the SGS steps into two parts: anomaly traffic recognition and controller dynamic defense (Wang et al., 2019). This study shows that using well-designed methods for considering all parameters we can have efficient mechanisms to defend in opposition to distributed denial of service attack along with can also achieve superior high detection accuracy on par with excellent network resource utilization.

Discussion

Our research shows that Software-Defined Network (SDN) is cost-effective and along with being a flexible tool. Nowadays, DDoS is among the highly risky strikes and warnings to SDN. Traffic volumetric, traffic entropical, and traffic flow analysis techniques are commonly used to address the challenge of increasing and more disruptive spread rejection of service spasms in SDN (Arivudainambi et al., 2019). Software-Defined Networks has occupied the role of a future communication network architecture that had bright scope in decoupling network control and forwarding certain characteristics including central control and programmability to counter the dangerous combat against a spread denial-of-service attack (Luo et al., 2015).

Comparative evaluation of different methods reviewed in this paper makes it clear that despite its becoming a very instrumental tool to counter hackers, attackers, and other malicious agents, systems, and entities, Software-Defined Network has itself faced persistent onslaughts from Distributed Denial-of-Service attacks, this occurs primarily due to the reason that all SDN layers have some inherent vulnerabilities to the robustattacks. In a distributed denial-of-service attack the maximum attractive and easy attack is the logically centralized controller of a software-defined network (Sahoo et al., 2018). Therefore, it becomes very important to develop the fastest and most accurate possible detection model to identify and thwart the control layer attack traffics at an initial phase itself.

Interestingly, despite software-defined networking bringing a lot of profits through decoupling the control plane from the data plane, a conflicting association among software-defined networking and distributed denial-of-service attacks has been established (Yan and Yu, 2015). The inherent abilities of software-defined networking enable it to feasibly detect and take quick action against any distributed denial of service attack. Conversely, the separation of the control plane from the data plane of SDN generates fresh strikes. Therefore, SDN can also be a prey of DDoS strikes.

Wang et al. proposed an entropy-based lightweight DDoS flooding spasm recognition model running in the OF edge switch. This model realized a distributed anomaly detection in SDN and decreased the flow gathering overload to the controller in a software-defined network (Wang et al., 2015). This model has the advantage of an elaborate algorithm and having a low calculation overload that can be feasibly used in programmable switch, as in the case of Open vSwitch and NetFPGA.

Efforts are underway to continuously improve the systems, software, techniques, methods, and various models to offer a full-proof and robust technique to thwart any sort of distributed denial of service attacks around the world. Sood constructed a queueing theory-based optimization framework in a distributed software-defined network architecture that offered the advantage of QoS-guaranteed flow-balancing in pro-active operations of software-defined network controllers.

As reviewed in the previous section, the techniques presented in few studies (Jaiswal et al., 2016;Li and Guo, 2008; Tavallaee et al., 2009;Larijani et al., 2009; Saad et al.,2016) have shown efficient results but they suffer from some disadvantages. Now, the results-oriented performance analysis of these techniques is performed. We have used the following metrics to evaluate the techniques, including classification Accuracy Mall et al, 2019; Mall and Singh, 2022 and mean squared error (MSE). These parameters are illustrated as under:

$$Accuracy = (\mathrm{TP}+\mathrm{TN})/\mathrm{N} \quad \text{.....(1)}$$

In this equation, TP and TN denote True Positive and True Negative rates, respectively; N represents the number of cases. Here, the TP Accuracy of various classifiers is being compared. Kernels used for SVM are Binary Radical Basis Function kernels that were changed into a multi-class classifier wherein various attacks depict the class. These attacks have been detected by the representation of class by specifying the elapsed time used for detection. The accuracy of the model is classified as ratio negatives divided by the total number of cases.
Mean Square Error (MSE):

$$E_{MSE} = E\left[\left|e_{\min}(n)\right|\right]^2$$
$$Where, e_{\min}(n) = r(n) - y_i(n)$$

Where e_min is the minimum MSE based on the normal output and desired output r(n).

For the analysis part TCM KNN, KNN ACO, ABSTVM SVM, DENFIS, BPNN, and RNN-ABC are considered. Mean Squared Error and Accuracy are considered a parameter for evaluation, as shown in Table 3 and Table 4, respectively. The graph shows that DENFIS and BPNN have the lowest MSE value among the considered techniques, followed by ABSTVM, KNN-ACO, TCM-KNN, RNN-ABC, and SVM. These values thus imply that among different techniques, SVM has the highest validation error (0.10) and DENFIS has the least validation error (0.026). And thus, the least validation error results in high accuracy. The corresponding values for different classifiers are presented in Table 3.

SVM shows a higher validation error than other algorithms because most of these algorithms are tested on a very small subset of the KDD dataset. The larger the value of the data record is, the more accurate the data logarithm is, resulting in an implementation of this algorithm on a larger data set Narayan and Daniel, 2021; Narayan and Daniel, 2021; Narayan and Daniel, 2021; Narayan and Daniel, 2022; Table 4 exhibits the corresponding values for the different classifiers.

Thus, a technique is required that can give a better accuracy rate at large data set compared to all other approaches. Based on the results, the conclusion is drawn to have better accuracy. Future work can be done on combining a good portion of the algorithm. The integration of techniques can be done to give us consistent results and better accuracy in the larger dataset. Also, it was seen that most of current identification techniques are poor in real-time. The presented techniques also provide results only for a small footprint of the dataset, leading to over-fitting the classifier. Thus, a technique is required to provide a way to avoid over-fitting. Thus, these aspects consider combining different efficient robust techniques such as a technique with eager learning algorithms and that deal much better with the training data, especially SVM.

In a nutshell, we would like to highlight that so far under all attack parameters and conditions in a DDoS no method in any country has proven entirely successful. Each has its pros and cons, advantages and disadvantages. BPNL and DENFES have comparatively shown greater accuracy levels. There is a need to develop a hybrid method or that is robust for which several organizations, countries, and leading academia should join hands.

Conclusions

Overall, in the current paper, several popular techniques for identifying DDoS spasms in the SDN network are analyzed. They include TCM-KNN, KNN-ACO, ABTSVM, SVM, DENFIS, BPNN, and RNN-ABC. On analyzing the findings of these techniques, the limitations of these various techniques are also revealed and have been documented above. Besides, the presentation of these techniques is inspected with respect to different parameters such as MSE, precision.

In addition, the results showed that DENFIS, BPNN has the highest accuracy, and SVM has the lowest one. However, the variant of SVM such as ABTSVM provided higher accuracy than that by SVM and KNN variant techniques (TCM-KNN and KNN-ACO). Therefore, it implies that using the variant of SVM with some other

techniques can further enhance the accuracy rate of the system and lower the MSE. Therefore, there is a scope of modification in the existing works that can enhance the system performance even at large data sets. By considering this, for future work, a new effective classifier is to be designed using a hybrid approach of TCM and SVM that will decrease the error rate, providing less attack in software-defined networks. However, there are some shortcomings with this algorithm, which involves a decision based on the relative variance if an abnormal point serves as a boundary between usual and abnormal points. The detection points must be further strengthened since the algorithm has faults with the detection points of the anomaly.

Overall, the authors would like to highlight that SVM methods need to further finetuned on account of their low accuracy levels. Considering the challenge of DDoS and daily new attacking techniques and advanced software being used by attackers, SDN needs to constantly on a real-time basis must anticipate the attacks through different warming signals and DDoS attacks can be better countered as early as possible they are detected and required security measures are initiated.

The authors of this exhaustive rich study are optimistic to develop in future robust methods to identify and mitigate the most dreaded DDoS attacks. Furthermore, it is hoped that this study will go a long way in giving much-needed direction on appropriate modeling and devising methods and techniques to counter DDoS. This paper will contribute to existing literature and will enrich the researchers, scientists, professionals, and network security specialists in India, the USA, and other leading IT superpowers to devise more robust methods and techniques in the years ahead.

References

AlEroud, A., Alsmadi, I. (2017) 'Identifying cyber-attacks on software-defined networks: An inference-based intrusion detection approach', *Journal Network Computer Application*, Vol. 80, pp. 152-164. https://doi.org/10.1016/j.jnca.2016.12.024.

Ankali S.B., Ashoka D.V. (2011) 'Detection architecture of application-layer DDoS attack for the internet', *International Journal Adventure Network Application*, Vol. 3, No.1, 2011, pp. 984-990.

Arivudainambi, D., KA, V.K. and Chakkaravarthy, S.S., (2019) 'LION IDS: A meta-heuristics approach to detect DDoS attacks against software-defined networks,' *Neural Computing and Applications*, Vol.31, No.5, pp.1491-1501. doi:10.1007/s00521-018-3383-3387.

Bawany, N. Z., Shamsi, J. A., Salah, K. (2017) 'DDoS attack detection and mitigation using SDN: methods, practices, and solutions. *Arabian Journal Science Engineering*, Vol.42, No.2, 425-441. https://doi.org/10.1007/s13369-017-2414-5.

Benzekki, K., El Fergougui, A. and ElbelrhitiElalaoui, A.(2016) 'Software-defined networking (SDN): a survey. *Security and communication networks*, Vol. 9, No.18, pp.5803-5833.https://doi.org/10.1002/sec.1737.

Bhuyan, M.H., Bhattacharyya,D.K. and Kalita, J.K. (2013) 'Network anomaly detection: methods, systems, and tools,' *IEEE Communications Surveys &*

Tutorials, Vol. 16, No.1, pp. 303-336. https://doi.org/10.1109/SURV.2013.052213.00046.

Burai, P., Beko, L., Lenart, C. and Tomor, T. (2014) 'Classification of energy tree species using support vector machines', *WHISPERS IEEE,* https://doi.org/10.1109/WHISPERS.2014.8077499.

Cadena Muñoz, E., Pedraza Martínez, L.F. and Ortiz Triviño, J.E. (2020) 'Detection of malicious primary user emulation based on a support vector machine for a mobile cognitive radio network using software-defined radio,' *Electronics*, Vol. 9, pp.1282.

Canadian Institute for Cybersecurity [online] Intrusion detection evaluation dataset (ISCXIDS2012) http://www.unb.ca/cic/datasets/ids.html (accessed 21 October 2020).

Creech, G. and Hu, J. (2013) Generation of a new IDS test dataset: time to retire the KDD collection. IEEE Wireless Communications and Networking Conference.

DEFCON (The Shmoo Group, 2000): Generated in 2000, DEFCON-8 ... create profiles to generate real traffic for HTTP, SMTP, SSH, IMAP, POP3, and FTP ... [21] DEFCON 8, 10 and 11, The ShmooGroup http://cctf.shmoo.com, (2000).

Dehkordi, A. B., Soltanaghaei,M., Boroujeni, F. Z.(2021) 'The DDoS attacks detection through machine learning and statistical methods in SDN,' *Journal of Supercomputer*, Vol.77, pp. 2383-2415. doi:10.1007/s11227-020-03323-w

Dev, S., Wen, B., Lee, Y.H., Winkler, S. (2016) 'Ground-based image analysis: A tutorial on machine-learning techniques and applications,' *IEEE Geoscience and Remote Sensing Magazine*, Vol.4, No.2, pp.79-93. https://doi.org/10.1109/MGRS.2015.2510448.

Hettich, S The ucikdd archive (1999) http://kdd.ics.uci.edu (accessed 29 may 2020).

Hick, P., Aben, E., Claffy, K. Polterock, J. (2010) 'The CAIDA "DDoS attack 2007" dataset' http://www. caida. org. (Accessed on 15 April 2020).

Jafarian, T., Masdari,M., Ghaffari, A., Majidzadeh, K.(2020) 'A survey and classification of the security anomaly detection mechanisms in software-defined networks,' *Cluster Computers*, Vol. 24, No.2, pp. 1235-1253. https://doi.org/10.1007/s10586-020-03184-1.

Jaiswal, S., Saxena, K., Mishra, A. and Sahu, S.K.(2016) 'A KNN-ACO approach for intrusion detection using KDDCUP'99 dataset', *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 628-633. IEEE, 2016.

Kabanda, GA. Bayesian Network Model for a Zimbabwean Cybersecurity System 2019 https://www.researchgate.net/profile/Gabriel-Kabanda/publication/339357040_Bayesian_Network_Model_for_a_Zimbabwean_Cybersecurity_System/links/5e53a9f4299bf1cdb945762b/Bayesian-Network-Model-for-a-Zimbabwean-Cybersecurity-System.pdf. (accessed 15 April 2020)

Karan B. V., Narayan D. G. and Hiremath P. S. (2018) 'Detection of DDoS attacks in software-defined networks', *CSITSS IEEE*. https://doi.org/10.1109/CSITSS.2018.8768551.

Khraisat, A., Gondal, I., Vamplew, P. and Kamruzzaman, J. (2019) Survey of intrusion detection systems: techniques,datasets and challenges. *Cybersecurity*, Vol.2,No.1 pp. 1-22. https://doi.org/10.1186/s42400-019-0038-7.

Krishnan, S. and Oliver, J. J. E. (2019) 'Mitigating DDoS Attacks in Software Defined Networks,' (ICOEI) IEEE. https://doi.org/10.1109/ICOEI.2019.8862589.

Larijani, H., Javed, A., Mtetwa, N. and Ahmad, J. (2019) 'Intrusion detection using swarm intelligence,' UCET.

Li W., Meng W. and Kwok, L. F. (2016).A survey on OpenFlow-based Software Defined Networks: Security challenges and countermeasures. *Journal Network Computer Application*, Vol. 68, pp.126-139. https://doi.org/10.1016/j.jnca.2016.04.011.

Li, D., Wang, A. (2017) 'Improved KNN algorithm for the scattered point cloud', (IAEAC) *IEEE*. https://doi.org/10.1109/IAEAC.2017.8054336

Li, W., Meng, W., and Ip, H. H. S. (2016). PMFA: toward passive message fingerprint attacks on challenge-based collaborative intrusion detection networks. In International Conference on Network and System Security (pp. 433-449). Springer, Cham.

Li, Y. and Guo, L. (2008) 'TCM-KNN scheme for network anomaly detection using feature-based optimizations', SAC ACM. https://doi.org/10.1145/1363686.1364194.

Lima Filho, F.S.D., Silveira F.A., de Medeiros Brito Junior A., Vargas-Solar G. and Silveira L.F. (2019) 'Smart detection: an online approach for DoS/DDoS attack detection using machine learning', *Security and Communication Networks*, pp. 1-15. https://doi.org/10.1155/2019/1574749.

Liu, Z., He, Y., Wang, W. and Zhang, B. (2019) 'DDoS attack detection scheme based on entropy and PSO-BP neural network in SDN', *China Communication*, Vol. 16, 144-155. doi: 10.23919/JCC.2019.07.012.

Luo, S., Wu, J., Li, J. and Pei, B., (2015) A defense mechanism for distributed denial of service attack in software-defined networks. *Ninth International Conference on Frontier of Computer Science and Technology*, pp. 325-329, https://doi.org/10.1109/FCST.2015.11.

Mall, P. K., and Singh, P. K. (2022). BoostNet: a method to enhance the performance of deep learning model on musculoskeletal radiographs X-ray images. International Journal of System Assurance Engineering and Management, 1-15.

Mall, P. K., Singh, P. K., and Yadav, D. (2019, December). GLCM based feature extraction and medical X-RAY image classification using machine learning techniques. In 2019 IEEE Conference on Information and Communication Technology (pp. 1-6). IEEE.

Masdari, M. and Jalali, M.A. (2016) 'survey and taxonomy of DoS attacks in cloud computing', *Security Communication Network*, Vol. 9, pp. 3724-3751. https://doi.org/10.1002/sec.1539.

Meng, W., Li, W., Su, C., Zhou, J. and Lu, R. (2017) 'Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data', *IEEE Access*, Vol.13, No.6, pp.7234-7243. doi: 10.1109/ACCESS.2017.2772294.

Mishra A., Gupta, N. and Gupta, B. B. (2021) Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. Telecommunication System, Vol. 77, No.1,pp. 47-62. doi: 10.1007_s11235-020-00747-w.

Nechaev, B., Allman, M., Paxson, V. and Gurtov, A. (2004) Lawrence berkeley national laboratory (lbnl)/icsi enterprise tracing project. Berkeley, CA: LBNL/ICSI.

Noori, A., Amphawan, A., Ghazi, A. and Ghazi, S. A. (2019) Dynamic evolving neural fuzzy inference system equalization scheme in mode division multiplexer for optical fiber transmission. *Bulletin in Electrical Engineering Information*, Vol.8, No.1,. https://doi.org/10.11591/eei.v8i1.1399

Nwosu C.S., Dev S., Bhardwaj P., Veeravalli B. and John D. (2019) 'Predicting stroke from electronic health records', EMBC IEEE.

Qureshi, A.U.H.,Larijani, H., Yousefi, M., Adeel, A. and Mtetwa, N. (2020) 'An Adversarial Approach for Intrusion Detection Systems Using Jacobian Saliency Map Attacks (JSMA) Algorithm', *Computers*, Vol. 9, No.3, pp. 58. https://doi.org/10.3390/computers9030058.

Saad R. M., Anbar M., Manickam S. (2018) 'Rule-based detection technique for ICMPv6 anomalous behavior', *Neural Computer Application*, Vo. 30, No.12, pp. 3815-3824. https://doi.org/10.1007/s00521-017-2967-y.

Saad, R.M., Almomani, A., Altaher, A., Gupta, B.B., Manickam, S. (2014) 'CMPv6 flood attack detection using DENFIS algorithms', *Indian Journal Science Technology*, Vol.7, No. 2, pp. 168.

Saad, R.M., Anbar, M., Manickam, S. and Alomari, E. (2016) 'An intelligent icmpv6 DDoS flooding-attack detection framework (v6iids) using back-propagation neural network,' *IETE Technical Review*, Vol. 33, No 12, pp.244-255. https://doi.org/10.1080/02564602.2015.1098576.

Sahoo, K. S., Panda, S. K., Sahoo, S., Sahoo, B., Dash, R. (2019) 'Toward secure software-defined networks against distributed denial of service attack', J*ournal supercomputers*, Vol.75. No. 8, pp. 4829-4874. https://doi.org/10.1007/s11227-019-02767-z.

Sahoo, K. S., Puthal, D., Tiwary, M., Rodrigues, J. J., Sahoo, B., and Dash, R. (2018). An early detection of low rate DDoS attack to SDN based data center networks using information distance metrics. Future Generation Computer Systems, 89, 685-697.

Sangster, B., O'Connor, T. J., Cook, T., Fanelli, R., Dean, E., Morrell, C. and Conti, G. J. (2009) Toward Instrumenting Network Warfare Competitions to Generate Labeled Datasets. In CSET.

Shah, S. A. R. and Issac, B. (2018) 'Performance comparison of intrusion detection systems and application of machine learning to Snort system', *Future Generation Computer Systems*, 80, 157-170.

Sharafaldin, I., Lashkari, A.H. and Ghorbani, A.A. (2018) 'Toward generating a new intrusion detection dataset and intrusion traffic characterization', ICISSp.

Singh, K., Singh, P. and Kumar, K. (2017) 'Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges', *Computer Security*, Vol. 65, pp. 344-372. https://doi.org/10.1016/j.cose.2016.10.005.

Singh, RS., Prasad, A., Moven, R.M. and Sarma, H.K.D. (2017) 'Denial of service attack in wireless data network: A survey', *(DevIC) IEEE*, https://doi.org/10.1109/DEVIC.2017.8073968.

Singh. M. P. and Bhandari. A. (2020) 'New-flow-based DDoS attacks in SDN: Taxonomy, rationales, and research challenges', *Computer Communication*, Vol.154 pp. 509-527. https://doi.org/10.1016/j.comcom.2020.02.085

Song, J., Takakura, H., Okabe, Y., Eto, M., Inoue, D. and Nakao, K.(2011) 'Statistical analysis of honeypot data and building of Kyoto 2006+ dataset for

NIDS evaluation', *Proceedings of the first workshop on building analysis datasets and gathering experience returns for security*. https://doi.org/10.1145/1978672.1978676.

Suresh M. and Anitha, R. (2010) 'Evaluating machine learning algorithms for detecting DDoS attacks', *CNSA*. https://doi.org/10.1007/978-3-642-22540-6_42.

Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A. (2009) 'A detailed analysis of the KDD CUP 99 data set', CISDA IEEE. https://doi.org/10.1109/CISDA.2009.5356528.

Narayan, V., & Daniel, A. K. (2021). A novel approach for cluster head selection using trust function in WSN. Scalable Computing: Practice and Experience, 22(1), 1-13.

Narayan, V., & Daniel, A. K. (2022). CHHP: coverage optimization and hole healing protocol using sleep and wake-up concept for wireless sensor network. International Journal of System Assurance Engineering and Management, 1-11.

Narayan, V., & Daniel, A. K. (2021). RBCHS: Region-Based Cluster Head Selection Protocol in Wireless Sensor Network. In Proceedings of Integrated Intelligence Enable Networks and Computing (pp. 863-869). Springer, Singapore.

Narayan, V., & Daniel, A. K. (2021, October). IOT Based Sensor Monitoring System for Smart Complex and Shopping Malls. In International Conference on Mobile Networks and Management (pp. 344-354). Springer, Cham.

Wang, R., Jia, Z. and Ju, L. (2015) An entropy-based distributed DDoS detection mechanism in software-defined networking. In 2015 IEEE Trustcom/BigDataSE/ISPA, Vol. 1, pp. 310-317. IEEE.

Wang, Y., Hu T., Tang, G., Xie, J., Lu, J. (2019) SGS: Safeguard scheme for protecting control plane against DDoSattacks in software-defined networking. *IEEE Access*, Vol.7, pp. 34699-34710. https://doi.org/10.1109/ACCESS.2019.2895092

Yan, Q., Yu, F.R. (2015) 'Distributed denial of service attacks in software-defined networking with cloud computing', *IEEE Communications Magazine*, Vol.53, pp.52-59. DOI: 10.1109/MCOM.2015.7081075.

Yan, Q., Yu, F.R., Gong, Q. and Li, J. (2015) 'Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments: A survey, some research issues, and challenges', *IEEE Communication Survey Tutor*, Vol.18, No.1, pp. 602-622. https://doi.org/10.1109/COMST.2015.2487361

Ye J., Cheng X., Zhu J., Feng L., Song L. (2018) 'A DDoS attack detection method based on SVM in a software-defined network,' *Security Communication Network*. https://doi.org/10.1155/2018/9804061.

Zargar, S.T., Joshi, J. and Tipper, D.A. (2001) 'survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks', *IEEE Communications Surveys and Tutorials*, Vol. 5, No.4, pp. 2046-2069. https://doi.org/10.1109/SURV.2013.031413.00127.

Zhu, L., Tang, X., Shen, M., Du, X. and Guizani, M. (2018) 'Privacy-preserving DDoS attack detection using cross-domain traffic in software defined networks,' *IEEE Journal on Selected Areas in Communications*, Vol. 36, No. 3, pp.628-643.

Zuech, R., Khoshgoftaar, T.M. and Wald, R. (2015) 'Intrusion detection and big heterogeneous data: a survey', *Journal of Big Data*, Vol. 2, pp.1-41. https://doi.org/10.1186/s40537-015-0013-4.

Fischli, A. E., Godfraind, T., & Purchase, I. F. H. (1998). Conclusions and Recommendations. Pure and Applied Chemistry, 70(9), 1863-1865. https://doi.org/10.1351/pac199870091863