Received February 26, 2020, accepted April 21, 2020, date of publication May 20, 2020, date of current version July 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2995820

An Effective Mechanism to Mitigate Real-Time DDoS Attack

RANA ABUBAKAR[1,2], (Graduate Student Member, IEEE), ABDULAZIZ ALDEGHEISHEM[3], MUHAMMAD FARAN MAJEED[4], (Member, IEEE), AMJAD MEHMOOD[5,6], (Senior Member, IEEE), HAFSA MARYAM[7], NABIL ALI ALRAJEH[8], CARSTEN MAPLE[5], (Member, IEEE), and MUHAMMAD JAWAD[6]

[1]Department of Computer Science, University of Sahiwal, Sahiwal 57000, Pakistan
[2]Department of Computer Science, Virtual University, Lahore 54000, Pakistan
[3]Traffic Safety Technologies Chair, Urban Planning Department, College of Architecture and Planning, King Saud University, Riyadh 11574, Saudi Arabia
[4]Department of Computer Science, Shaheed Benazir Bhutto University Sheringal, Sheringal 18000, Pakistan
[5]WMG, University of Warwick, Coventry CV47AL, U.K.
[6]Institute of Computing, Kohat University of Science and Technology, Kohat 26000, Pakistan
[7]Department of Computer Science, COMSATS University, Islamabad 45550, Pakistan
[8]Biomedical Technology Department, College of Applied Medical Sciences, King Saud University, Riyadh 11633, Saudi Arabia

Corresponding author: Amjad Mehmood (dramjad.mehmood@ieee.org)

EP/N510129/1 (The Alan Turing Institute) and EP/S035362/1 (PETRAS National Centre of Excellence for IoT Systems Cybersecurity).

ABSTRACT Computer networks are subject to an unprecedented number and variety of attack, the majority of which are distributed denial of service (DDoS). The nature and mechanisms employed in these DDoS attacks continually change, creating a significant challenge for detection and management. To address this evolving nature of attacks, approaches are required that can effectively detect and mitigate emerging attacks. In this paper, we provide a mechanism that not only detects the presence of a DDoS attacks but also identifies the route of attack and commences a process of mitigation at the initial stage of identification. The proposed research involves an optimized SVM classification algorithm integrated with SNORT IPS to provide prevention mechanisms for the entire network when subject to DDoS attack. The proposed IPS method allows traffic identified as legitimate to pass through the network, whereas suspect traffic is flagged and has to go through an identification system. We present the algorithm with experimental results that show better performance than simple Snort IPS, Probabilistic Neural Network (PNN), Back Propagation (BP), Chi-square, and PSO-SVM in terms of accuracy, exposure and specificity. These results show that the average accuracy rate of our method is 97 percent.

INDEX TERMS DDoS, network attacks, IP networks, security, dataset.

I. INTRODUCTION

A DDoS attack is a malicious type of attack that sends malicious traffic to a specific node or a large number of nodes via a large number of distinct computers, which form part of a system (bot) that the attacker controls legitimately or not. In the main, the machines that are the source of an attack are not legitimately controlled by the attackers, but are rather machines that have been compromised by the attacker and are now, often unknown to the legitimate controller of the machine, used to launch the attack. These compromised hosts send many packets to the target to flood the network and block services. The result of such an attack is that resources are overwhelmed handling illegitimate packets, and are unable to effectively deliver legitimate service requests.

In case of cloud platforms, auto-scaling mechanisms are designed to provide some defense by adding or removing machines to respond to varying load, setting the scaling size factors and an upper CPU utilization threshold values [1]. Using software-defined networking (SDN) principles and the OpenFlow protocol (OFP) can assist in load-balancing thereby improving performance of cloud computing platforms, based on path switching and perceived user quality of experience (QoE) [2]. The DDoS attack techniques have frequently changed over recent years. These attacks are prominent against networks and websites of organizations,

The associate editor coordinating the review of this manuscript and approving it for publication was Jenny Mahoney.

governments and private firms that have been targeted on the basis of the significance of accessibility. The requirement for multi-layered barrier and collaboration is fundamental. A DDoS attack becomes effective by utilizing the Internet to break into computers and utilizing them to attack a network. Hundreds or a huge number of PC frameworks over the Internet can be transformed into zombies and used to attack another framework or site.

A group of already infected devices is used to execute the DDoS attack. These devices can be IoT-based systems. The security threats in IoT exploit vulnerabilities found in many modules such as applications, interfaces of an application, software, network components, firmware, and physical hardware existing at different levels [3]. These devices are organized in a way that they simultaneously transfer large number of packets without any break to some special victim who feels that these are original transmissions. For this, the host must communicate with many devices at the same time across the network with different type of packets. This attack can paralyze both a network and a single host on a network, while using some other networks as infected zombies. Different types of network packet services are used as a source during the attack. Mostly zombie agents are self-controlled Trojans that are installed on attackers' sites as malware or are controlled remotely [4]. DDoS can result in hazardous security concern that could hamper organization's processing time, money, assets, and even the reputation [5], [6]. It sometimes results in loss of credentials, important data and stored information too. The most frequently used technique is a DDoS attack scan, which has myriad functionalities [7]. The DDoS architecture can be divided into two models: proxy (zombies) - based on Handlers model and Internet Relay-Chat (IRC) model [5].

In a successful DDoS attack, the communication between the handler/zombie and the attack is usually hidden (for example, the channel is encrypted). This makes the DDoS architecture invisible and difficult to detect. Many attackers use spoofing methods to override their source address (which is used to hide the attacker's IP or MAC address by generating a random IP/MAC address or using a trusted device source identifier [8]. DDoS handlers and zombies are geographically distributed across different networks. Therefore, any attempt to find them may be tedious and difficult. If the author of the design and implementation of the attack is not published, no other person or organization knows that the attack (zero-day) is quite dangerous [4]. This leads to a lack of awareness of an attack and does not allow for any preparations to stop it. Attacks will not be discovered unless the author publishes them or unless they are accidentally identified by a third party. If the signature of the attack is not included in the database of the detection system, the signature-based detection system will not find a zero-day (unknown) attack. McAfee and Kaspersky are popular signature detection systems that use a regular signature database to detect different attacks [8], [9]. A trace-back of an IP in a DDoS attack depends on packet marking which is frequently mentioned as a Probabilistic Packet Marking (PPM) approach where packets are probabilistically set apart with fractional path data as they are sent by routers. PPM is a general method which the routers can use to uncover inward network data to end-hosts or destinations. Such data is probabilistically set by the routers in headers of regular IP packets on their approach to goals. Various potential applications have been distinguished such as IP trace-back, robust routing algorithms, congestion control, dynamic network reconfiguration, Internet bottle-necks locating, and so forth. In our research, we worked with a general probabilistic packet marking mechanism with an extensive variety of potential applications which would be helpful for finding IP trace-back and internet bottle-necks as two agent cases to show its viability. This approach worked just a solitary bit overhead in the IP packet headers. Even more critically, it fundamentally diminishes the quantity of IP packets required to pass on the applicable data when contrasted with the earlier best-known plan. We introduced smart routing-based on DDoS attack detection and mitigation using latest datasets.

Anomaly-based IDS, in principle, makes the detection of data packets in the network traffic and analyzes packets of data that do not fit in the normal profile that has been created. The Support Vector Machine (SVM) is an algorithm that uses classification to filter incoming traffic and forwarded it to the expert model. The SVM is a sort of learning technique that tries to find a comprehensive solution to the optimal value of non-linear classification problems [10]. A few researches showed that SVM has a good detection accuracy on anomaly-based IDS [10], [11].

TABLE 1. DDoS attack history

Ref	Victim	Details
[33]	Hong Kong (2014	400 GB DDoS attack recorded
[34]	Spamhaus (2014)	400 Gbit/s attack traffic
[35]	BBC (2015)	Attack reached 602Gbps
[36]	GitHub (2015)	500 GB attack recorded
[37]	GitHub (2018)	1.35 TB of attack traffic

The comparison between optimized SVM, SVM and ANN algorithms is not found which use all the dataset attributes. In addition to some research on PSO_SVM, SVM and ANN, have different dataset attributes and parameters. Most scholars use the technique of dataset feature selection in which many attributes are removed that hide network traffic behavior and affect the network traffic to detect attacks in real time. This research compares the performance of the detection accuracy of optimized SVM algorithms and SVM using the same parameters and attributes, using dataset KDDCup99 for training and testing, and use all the attributes of the dataset to better describe the traffic in a real time environment, to know which classification algorithm is better in terms of detection accuracy by using all parameters of datasets. Table 1 shows some very destructive recent DDoS attacks.

II. RELATED WORK

In this section, we discuss DDoS attack detection and mitigation, traceability's, statistics, protocol infrastructure, data

mining algorithms based on artificial intelligence approaches, and how these could potentially have effects on an attack's behavior. Different mechanisms and approaches have been implemented to reduce the attacks' strength. Focus of this research is that we have individually studied and reviewed the researches related to DDoS defense approaches presented by researchers and organizations.

Alsirhani *et al.* [12] proposed a DDoS detection system that is helpful in detecting attack. Their proposed method contains three ideas: algorithms classification, computing parallelism and fuzzy logic techniques. The classification algorithms are used to classify and predict network traffic behavior. The concept of parallelism is used to accurately increase speed of the execution of the classification algorithms utilization. The fuzzy logic techniques are used to select which of the algorithms is to be used in classification. They have proposed this technique to work in the cloud as a service and it can be used in any network. The evaluation of the algorithms classification shows that there is a trade-off between the delay and accuracy.

Shah *et al.* [13] compared the behavior of two open-source intrusion detection systems, the SNORT IPS and the Suricata IPS. They have used many machine learning algorithms and SVM algorithms as a SNORT adoptive plugin. Their analysis and results show that SNORT utilizes less computational resources as compared to Suricata. While Suricata handled huge number of packets per second as compared to SNORT, both have high false positives alarms. The SNORT triggered 55.2% FPR matched as compared to Suricata's 74.3% FPR which is too high with default rules. The evaluation of the system showed that because Suricata has capabilities to perform multi-threading functions, it requires more memory and CPU resources than SNORT. Their evaluation shows that the 4 cores CPU utilization of Suricata is higher than that of Snort utilization. The Suricata used an average of 3.8GB memory which tops SNORT utilization of memory which is 600 MB at 10 Gb of network resource.

Xuan *et al.* [6] suggested a DeepDefense model. It's a deep learning-based approach, to detect DDoS attack and the performance detection of DDoS attack. They convey the DDoS attack detection issue as a series of classification issues and convert the packet-based DDoS detection with detection of a Windows-based approach. The DeepDefense model is a collection of Recurrent Neural Network (RNN), CNN, and entirely connected layers of ANN. The RNN can learn features better than other machine learning approaches, especially longer historical structures. The LS-TM and GRU are used to exclude scaling problems when trace of the history from previous packets of RNN are used. The RNN similarly has improved performance in generalization as compared to random forest.

Shahbaz *et al.* [14] use a efficiency enhanced IDS detection system. They report the problem of dimensionality reduction by suggesting an effective features extraction of datasets by using an algorithm that considers the correspondence between a features subset and the class label behavior.

Peraković *et al.* [15] developed a DDoS detection and classification system which is based on ANN. In their model of DDoS detection, network traffic is classified in four classes, DNS DDoS attack traffic, HTTP DDoS attack, UDP DDoS attack or normal attack. The parameters are IP address source and destination, and protocol validation and packet size. Because of the communication of the features of UDP level attack and normal attack, the detection accuracy and classification of UDP DDoS attacks is slightly lower.

Researchers Aishwarya and Malliga [16] described a shield that responds transport layer threats (SYN). This method associates clients with malicious ACKs. These malicious ACKs are then ignored. It also checks the spoofed packets. Another layer of security is added as encoding of SYN packet. This encoded packet can only be deciphered by authenticated users. This method builds up various probes. The structure can be progressively used to gather security data at various cloud levels for investigation of attacks on the cloud. IP spoofing is proposed in different procedures by scientists to protect from it. This can be comprehensively ordered into host oriented, switch oriented, and a hybrid scheme [7]. Host-oriented can be either passive or active schemes on the other hand, the switch based methods can be fundamental or distributed methods.

Jia *et al.* [17] proposed a detection system that is a mixture of several multi-classifiers by using Singular Value Decomposition (SVD). The making of different classifiers delivers better accuracy than using fixed classifiers. It would be exciting to evaluate the performance of their technique when applied with datasets of huge traffic. Their evolution shows an impressive result when compared to the K-NN algorithm results.

Singh *et al.* [18] introduced an approach in which they adopted a systematic way to exhaustively audit and order 275 works of research representing an existing IP trace-back routing research. The paper likewise gives a top to bottom investigation of various IP trace-back routing methodologies, their useful classes, and the assessment measurements. In the light of the research review, they additionally addressed an arrangement of research inquiries related to IP trace-back latest trends. Different issues, difficulties and roads for future research in the zone of IP trace-back are additionally observed in this paper.

Lu and Wang [19] proposed an approach on the source-based guard system against DDoS flooding attack botnet based through joining the force of SDN (Software-Defined Networking) and SFLOW (Sample Flow) technology. Firstly, they defined a metric to quantify the fundamental components of this kind of attack, which implies distribution and coordinated effort. At that point, they outlined a basic discovery algorithm in light of a factual inferring model along with a reaction scheme through the capacities of SDN (Software Defined Networking). At last, they built up an application to understand their thought furthermore and tried its impact on replicating network with genuine network traffic. The outcome demonstrates that their instrument could successfully

differentiate a DDoS flooding attack, which begins in SDN environment and recognizes that attack, which flows for evading the damage of attack spreading to target from outside. They advocate the pros of SDN in the region of safeguarding DDoS attacks since it is troublesome and unrelenting to sort out a narrow-minded and undisciplined conventional distributed network to stand up to community DDoS flooding attacks.

Cha *et al.* [20] planned a three-layer identification strategy. The principal observing stage utilizes a framework. This framework pre-processes already identified DDoS patterns. It contains another part that describes loads on nodes by utilizing time-series model. Traffic Volume over the system is partitioned on the base of nodes volumes. A Bayesian procedure analyzes the DDoS threat and its possible candidates. The last stage utilizes an anomaly to distinguish both unknown pattern of DDoS this uses an unsupervised method.

Shiaeles *et al.* [21] described FHSD solution the FHSD stands for ''Fuzzy hybrid spoofing detection.'' It is a multi-layered spoofing identification system. It uses MAC address, counts hops and the web client. It uses the empirical rules for detection of malfunctioned traffic and its mitigation. This strategy accompanies its own disadvantages as it features values that are stored in files, which is cumbersome when it comes to database. Another method is Hop Count Filtering (HCF). It utilizes the TTL estimation of the source header to recognize the DDoS threat.

Guenane *et al.* [22] exhibited a method that is based on a firewall. This method lessens impact of a DDoS. This is described as Security-as-a-Service. This is a hybrid scheme comprised of two sections: A virtual and a physical part. Firewalls are the virtual part that execute basic protection. This protection includes checking, breaking down and resource provisioning. Physical part is responsible for resource planning to get a security service offered by the supplier. The DDoS mitigation framework diverts and balances the load on firewalls. The redirected stream is sent to the firewall which is overseen by the virtual part to accomplish the two key targets of selecting the solution and accessibility performance.

Teng *et al.* [9] described coordinated IDS E-CARGO to protect against DDoS threats. Their system is layered in four parts. The main layer generates events and gathers system data traffic and creates suspicious events. The detector layer works as Snort, and is utilized to isolate events that are malicious. The ''statistical indicator'' utilizes the data traffic to decide the probability of event occurrence. If the quantity of packets acquired inside a specific time is higher than the limit set, it is an attack. Another layer is a fusion layer that is responsible for pre-processing, space-time description in a combine's manner and collection of contents. Results and analysis demonstrated that the strategy is a practical answer for DDoS threats checking. A hierarchical method utilizes security tests to gather and break down data at various cloud structure levels. The connections of intrusions are described using ontology and knowledge driven method.

Dou *et al.* [26] employ a filtering technique that uses statistical correlations between different attributes. This uses both the attack situation and the situation when there is no attack. When there is no attack, normal pattern is analyzed using attribute pairs from the transport layers of the network packets. The recurrence of events in these sets is extricated and used to find the confidence value of the stream. The attributes that exist between these two layers were utilized to decide the authenticity of a packet. During the attack, the same confidence value is used to find whether an incoming packet is valid or not. The procedure utilizes the Confidence score to learn the authenticity of an incoming packet with comparing it to a threshold. If confidence limit is satisfied then access is granted to this packet.

Lonea *et al.* [27] described DDoS identification through fusion method. They used the IDS evidence obtained from VMs in the cloud data center. They described that the VM-oriented IDS alert as some threat comes. These data are stored in a database for further processing. The data is save in cloud fusion unit. This unit is further analyzed by a quantitative method through the DST method. DST stands for Dempsters Combination Theory. Along with DST the other techniques are used as fault tree analysis for deciding about flooding attacks. The described answer mixes DST rules with independent sources to decide about the traffic. They state that we must not discard packets as it can also throw off valid traffic. A firewall can be used as an alternate to ACL for safety. It helps in filtering the known attacks and the protocol analysis. However, the DDOS is going to be more complex to detect over the time. The filtration cannot be used against ''SYN and SYN/ACK'' attacks. Another suitable method is use of router end ''URPF-Unicast Reverse Path forwarding.'' This method blocks the malicious IPs that belong to same network. However, the spoofed subnet usage by the attacker is still another issue for this method. In this situation, the valid traffic will be stopped and attacked will continue with spoofed traffic.

Krishnan and Chatterjee [24] described design of an intelligent system that was based on the characteristics of anomaly-based learning systems. These are used against cloud DDoS threats. This method has an agent for service, an agent for alert, an agent for storage, an agent for communication and a couple of nodes. This method is intended to enhance the accuracy of detection by bringing down the false positives. The framework likewise actualizes an alert grouping. The analyzer module has the responsibility of differentiating the false positives and in-valid nodes.

Modi *et al.* [25] outlined a hybrid interruption method to distinguish cloud DDoS threats. Snort is a signature based supervised algorithm. This is an open-source strategy that consists of two parts. The first is a database of DDoS threats patterns, the second is a Bayesian classifier for prediction of system likelihood for being malicious. Eucalyptus is also a cloud for test set-up, where the IDS framework was introduced on all controller nodes. All the ports of the testing system are opened for this testing reason. Another packet

TABLE 2. Comparison of particular related work

Authors/Year	Year	ML Technique	Application
Alsirhani et al. [12]	2018	Classification & fuzzy	Cloud
Shah et al. [13]	2017	SVM	Network
Jia et al. [17]	2017	Multi Classifier	Network
Xuan et al. [6]	2017	ANN	Network
Shahbaz et al. [14]	2016	Classification	Network
Perakovi_ et al. [15]	2016	ANN	Network
Shiaeles et al. [21]	2015	Fuzzy	Network
Beitollahi and Deconinck [23]	2012	Classification	Network
Krishnan & Chatterjee [24]	2012	Classification	Network
Mordi et al. [25]	2009	Classification	Cloud

control system is Scapy to produce and encode many packets to create custom data traffic.

Xu *et al.* [28] propose a Trust-based Adversarial Scanner Delaying (TASD) approach for mitigation of Yo-Yo attack which works effectively and proactively on the cloud-based auto-scaling platforms. The cloud-based platforms have the ability by system design to auto scale-up and scale-down the underlying cloud network resources as per network traffic load. Cloud auto-scaling features can largely enhance cloud elasticity and scalability. The cloud auto-scaling feature introduce new security threats for cloud platforms. The Yo-Yo attack is one of the example of cloud auto-scaling which targets cloud auto-scaling feature. This attack is a newly discovered attack. In order to damage the auto scaling mechanism, attacker sends periodical bursts of traffic towards cloud platforms to oscillate between scale up and scale down which decreases cloud performance and hence leads to financial loss.

Phan *et al.* [29] proposed a DDoS attacks' efficient method in SDN-based cloud platform. They proposed a hybrid machine learning model based on SVM algorithm. To improve network traffic classfication, it uses self-organizing map algorithms. For attack detection rate and speed improvement, they also implemented an enhanced history-based IP filtering scheme (eHIPF). They combined both the hybrid machine learning model and the eHIPF scheme by using a novel mechanism approach to mitigate DDoS for the SDN-based cloud platform.

Chandola *et al.* [30] described three categories of anomalies. They described collective anomalies, point and contextual anomalies. Point anomaly compares an individual data event with collective data events. An average case is an application-bug that creates a threat. An inconsistency is contextual if there is a change in the context of the data. This is mostly controlled with the help of dataset structure. A grouped anomaly is anomaly that consists over the entire dataset. DDoS flooding is an example that creates a complete harmful and coordinated data-set. This approach is ordinarily completed after training and recognition stages. This stage trains the classifier with input data and the classifier proficiency depends upon it. Input contains events, patterns and possible outputs. The data may be in the form of uni-variate and multivariate data. In case of more than one variable the data is also a combination of the multiple datasets. The input data is labeled. These labels decide whether the data is normal or attacked. The classifier learns from those labels to classify the test data. The dataset for research consists of both training and testing data. KDD'99 is an example of this. It has roughly 490K vectors which are single connection [31]. This single vector has 41 attributes. Each of these attributes is normal or attacked. There are four classes of attacked data. These are DOS, Remote to Local, User-to-Root, and a Probing attack. Rules based learning is another name of supervised machine learning techniques. Such a learning method uses the labeled instances for learning of patterns and then creates its own rules for classification of the data. This identification of DDoS attack is done with the help of labels. This learning is the simplest way of learning and classifying. It is the same as like someone trying to classify the shades of light. These colors can be also used by the camera to match the new colors to label them. These colored examples can then also be used for the classification of car color based on the same labeled data. We can differentiate the learning methods by seeing the labels. If these are labeled dataset in the training data then the technique is rule based supervised learning [23]. Table 2 presents a comparison of the research discussed.

In this paper, we highlight DDoS attack trends, existing DDoS attack detection techniques, detection of DDoS attack routes, and state of the art mitigation techniques at the initial stage. We also inspect the industrial DDoS mitigation solutions that prevent and respond to network attacks. We compared the accuracy of detection, specificity, mechanisms, and specificity with existing solutions. These approaches are compared to our proposed method. Our contributions in this paper can be summarized as follows. We have developed a mechanism that not only detects the presence of DDoS attacks but also identifies the route of attack and starts a process of mitigation at the initial stage of a DDoS attack. We proposed an algorithm that integrates the optimized SVM and SNORT IPS to detect the attack at initial stage, identifying the path of the attack and options for mitigating the DDoS attack. The experimental results show that the proposed method can find the route of host machine from which a DDoS attack started within its initial stage and that the proposed mechanism rapidly mitigates the DDoS attack in the network.

The rest of the paper organized as follows. Section III provides an overview of materials and methods of our proposed method. In Section IV, we present the results of proposed methodologies and provide a detailed discussion on the implementation of the method. Section V concludes the paper and provides future directions.

III. MATERIALS AND METHODS

The protection method is designed based on traffic behavior analysis, packet header validation, used protocol validation and traffic matching with datasets. The protection method prevents the malicious traffic to reach the destination after analysis of network traffic for odd behavior or network abnormalities. This method works as an inline intrusion prevention system because it not only removes the malicious traffic by dropping it but also rerouting such traffic from the primary route to the secondary route for traffic redirection. These functionalities can be performed autonomously. This method becomes extraordinary by adding additional functionalities of continuous traffic monitoring, behavior analysis, statistical analysis, proactive DDoS attack intelligence, and by providing a rigorous DDoS secured environment.

A. DESIGN OF PROPOSED DDOS PROTECTION METHOD

The DDoS protection method offers comprehensive and consistent network traffic monitoring for malicious activities through investigating the packets header information utilizing supervised learning and contrasting network traffic behavior, with KDDCUP99, DAPRA datasets and updated DDoS attack datasets. Since recovering a lot of network packets require high preparation rate and is extremely costly. In specific networks, the threshold value varies from packet information or higher than the threshold value with respect to a possible DDoS attack and needs to be monitored. We used an individual packet threshold for every protocol to overcome this issue and identify threshold values accurately.

Considering assessments, we have chosen the finest threshold value per network protocol by checking per unit time of the most extreme network packets in chose condition where the original threshold values are adjustable. The packets are isolated and an examination of the planned network is performed. Our proposed method uses these configurations to choose the validity of the malicious packets. The detection sensor of proposed method is set up in each network node by utilizing SNMP. When we train the decision tree algorithm with old data-sets the result of the detection method is an unknown value. By utilizing a decision tree algorithm has the unique qualities to separate unknown attack behavior if type of attack or attack trained with the algorithm. Results are demonstrated using the method trained with old data-sets then the decision tree algorithm.

The research also demonstrates the statement that the method can detect unknown and known malicious traffic if trained with network agent with up to date datasets. The cross-layer upgrade for optimization of transform ICT under secure multi-agent system to overcome existing distributed systems bottlenecks issues [32].

In this circumstance, proposed method if one of the agent failed to recognize attack while other neighboring DDoS agents sense a similar attack that agent before trained with old data-sets now it should be trained with up-to datasets yet it will go offline from network because agents trained with supervised learning and specific configurations need to be activated or re-activated according to requirement. In this manner, when the algorithm learning isn't with latest datasets then the additional help can be obtained from the agents share knowledge to make further actions. Meanwhile every agent sends logs of every DDoS attacks to system controller for signature database and send SNMP trap to all devices with new ACL data, new iptable information and routing information. One of agent act as main controller gather all the attacks information and forward it as a solitary email to the network admin. All the DDoS agents are comprehensively process and work as an independent controller or distributed agent which communicates with other agents inside the networks or that are sent in various networks. In this way on the off chance that controller DDoS agent quits working the other sensor take charged as controller in the system can in any case send and get SNMP trap messages along these lines help to make our proposed method mechanism solid, dependable and impervious to DDoS agent crumple or crash. For implementation of the proposed method, the planned DDoS IPS system is a SNORT integration module which is based on Ubuntu Linux. To elevate malicious network packets and allowing legitimate network packet DDoS IPS request IPTABLES by using destination IP in results.

B. DESIGN OF PROPOSED DDOS PROTECTION METHOD NETWORK MAP

The proposed DDoS protection method network map describes details of a network layout of an organization. The main risk for the network is an attack from the external network. Many times DDoS attackers forward flooded network traffic to the victim's host with packets, ACKs or requests that consume all the available resource or exhaust bandwidth like state tables or CPU and memory. For better detection and defense tools are placed at the edge of the network and Figure 1 presents proposed method for DDoS defense while Figure 3 presents the deployment architecture of the method.

The proposed method consists of primary and backup edge routers and working on High Availability (HA) mode. In HA mode, one router works as active mode and second one working in passive mode. Flow starts from an incoming packet analyzing. First check in blacklist database if attack detect then it discards on initial stage. If attack not encounter in black list database then further action for protocol analysis we have been used LS-SVM algorithm start it analysis iphdr, tcphdr, UDPhdr, icmphdr, data and iptables. If any attack detects in LS-SVM algorithm then packet drop and insert finding in signature based database. The LS-SVM is the most efficient and effective classifier for use in detecting of DDoS

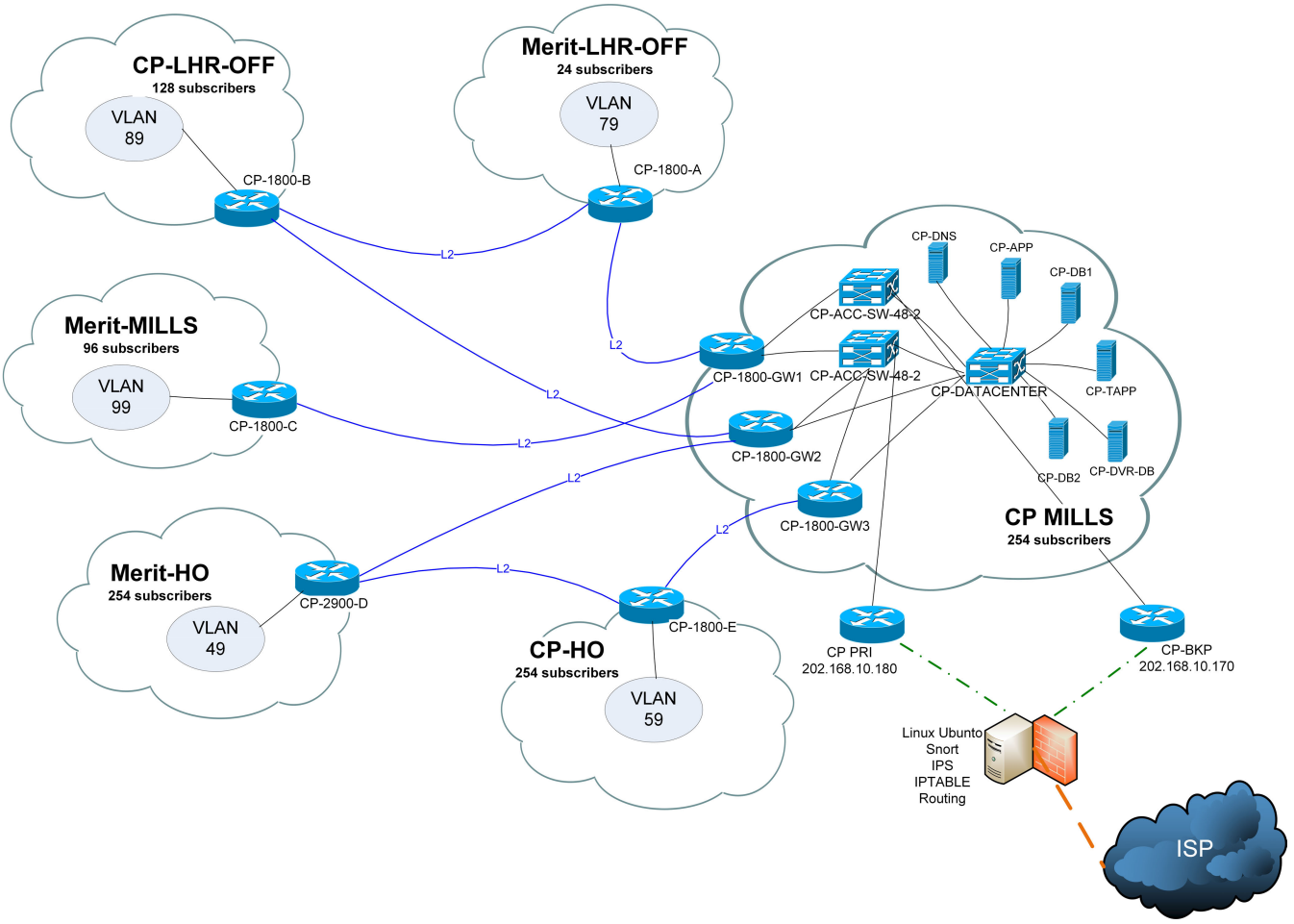


FIGURE 1. Network map of proposed method.

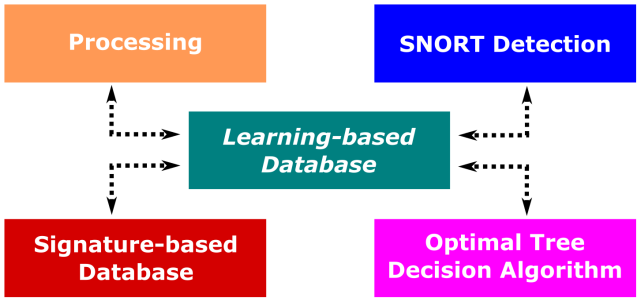


FIGURE 2. Learning mechanism of the proposed method.

attack traffic pattern [16]. Figure 2 presents the learning of the proposed DDoS protection system.

C. PROPOSED PRE-PROCESSING ALGORITHM

The Algorithm 1 shows the proposed method for mitigation of the attack.

D. LS-SVM

Least Squares Support Vector Machine (LS-SVM) is an evolutionary algorithm based on Support Vector Machine (SVM). It uses the method of LS-SVM instead of the standard SVM quadratic programming method, converting a quadratic optimization problem with inequality constraints in original space into the equation kernel space constraints, and converts the standard SVM inequality constraints into equality constraints by solving linear equations to obtain the least squares support vector machine classifier model. In this way, the solution process is transformed to solve linear equations. Since the complexity of algorithm is low and the efficiency is high, so we can apply LS-SVM to solve classification problems.

IV. RESULTS & DISCUSSION

To evaluate the proposed method, real-time network traffic should be generated which is very difficult to generate. The LOIC is one of the best tool in generating the malicious traffic to the network. The three types of DDoS attacks are used in attacking the server machine. These are HTTP, TCP and UDP based attacks. For maintaining the same amount of attack traffic throughout the experimental process, a Tcpreplay tool is implemented. For experiments results data has been taken by the snort machine to the CAS form, changed to the standard layout then LS-SVM (Least Squares Support Vector Machine) can predictable, then make the standard file

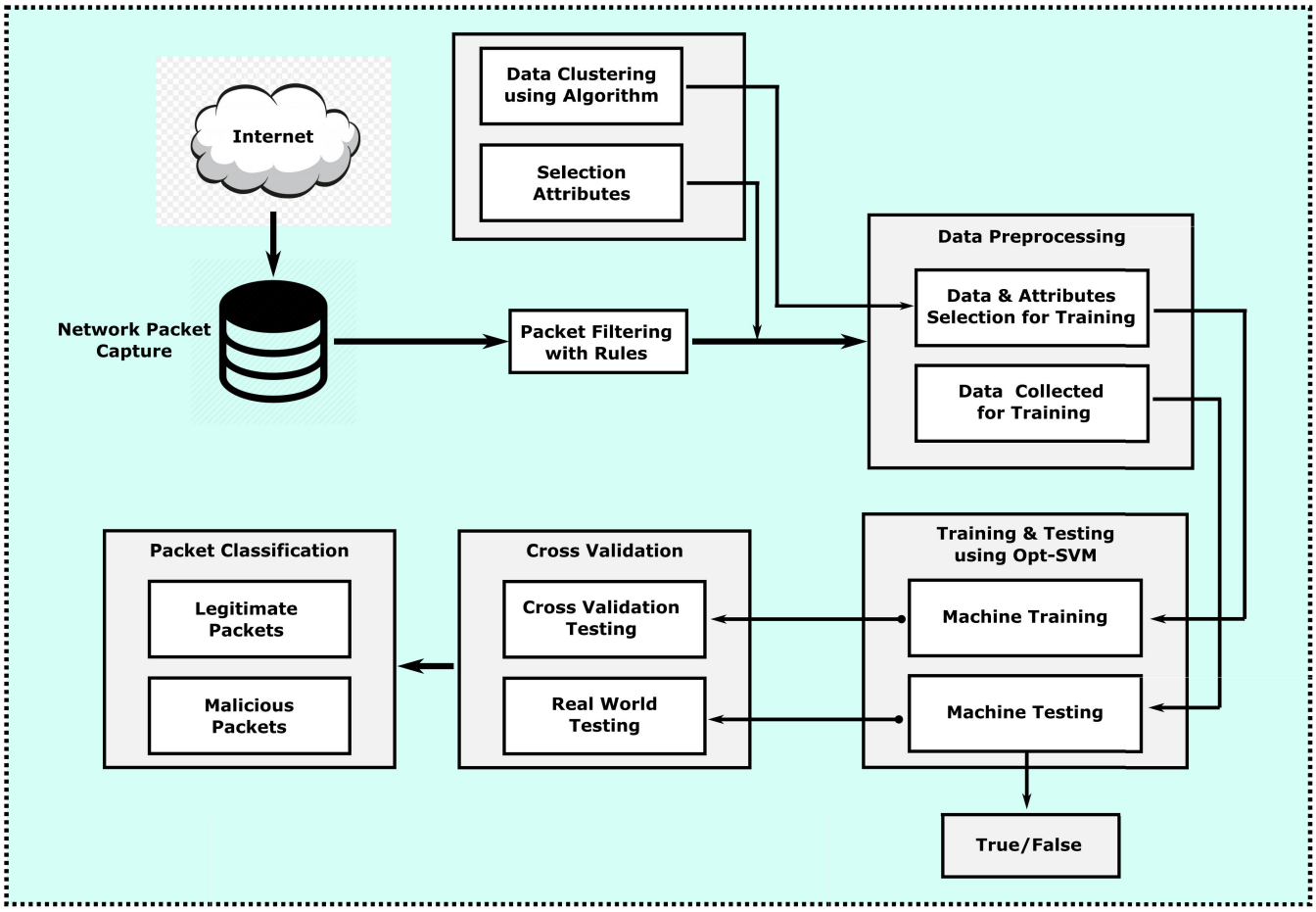


FIGURE 3. Deployment architecture of the method.

format as the training sections to do some recognition and sorting.

A. TESTBED DESIGN

Initially in this experiment, the evaluation of both IPS techniques are done against the three different profiles of DDoS attacks individually and the results are compared. To evaluate the IPS techniques, a testbed should be created such that it should support evaluation of any IPS against these attacks. We used accuracy, exposure and proficiency for identify positive outcomes and capability to identify malicious outcomes, to evaluate the proposed method of IPS. Table 3 shows the evaluation of experiments through other methods and IPS based on signature for which we recorded measureable estimations. The attack data traffic used (low rate to high rate) and legitimate for test IPS solution in a controlled network and isolated atmosphere. During experiments, we have launched 1 hour of original traffic and 1 hour of (UDP, HTTP, TCP) DDoS attacks involving 10 to 20 bots to target the destination. We used VMware VM (virtual machines) for zombies and client for attack from virtualized environment where the VM are linked to the victim machine using routers. Then we installed the IPS by using snort inline the gateway where it inspected the traffic for anomaly and abnormality.

B. IMPLEMENTATION

The LOIC tool is placed in this framework for generating the malicious traffic as this provides the GUI and easy operating. It also has the capacity of generating the real-time traffic of TCP, UDP, and HTTP flood attacks which match the behavior of the DDoS profile. The three flooding attacks are used against the apache web server. We have used three different DDoS attacks because they provide a possible view as to whether the protocols have any effect in the handling attacks. To generate the genuine traffic to the server a load testing tool JMeter is used [33]. The JMeter is used because it is an open source testing tool developed by Apache and is widely used for testing web applications. This tool provides the GUI for generating the HTTP traffic with regular intervals of time as depends on several user threads selected. We should ensure that the same amount of real time traffic should be maintained for evaluation of both IPS techniques. Generally, there are two methods to replicate the same amount of traffic each time. To use existing datasets: Using of datasets like DARPA and KDDCUP99 [34] helped in generating the traffic. Among them, the most used datasets are KDDCUP99 and DAPRA's datasets for capturing and save datasets. Since there are many datasets better than DARPA and KDDCUP99 [35] we had selected to generate and capture the traffic. So, Tcpreplay tool

Algorithm 1 Proposed Pre-Processing Algorithm **where,** n: the number of packets, D: destination address, S: source address, U: UDP header, T: TCP header, F: Flag, R: average received packets, K: TTL for attack packets, $-M$: attack packets, 1: counter for legitimate packets, $SEL\_FET()$: a new feature list of dataset with tag "M'' or " $-M''$.

Input packets
For $I = 1 : n$
  $D = data(I, 2)$
  $U = (I, 2)$
  $T = (I, M)$
  $F = (I, M)$
  $S = (I, M)$
For $J = M : n$
  $N = find(data(J, M) == S, F, T, U)\&(data(I, 2) == D)$
  If $R \geq K$
    $SEL\_FET(I, M) = data(I, M)$
    $SEL\_FET(I, 2) = -M$
  Else
    $SEL\_FET(I, M) = data(I, M)$
    $SEL\_FET(I, 2) = M$
End

is used as it has the capacity of repeating the same dataset with various options such as network speed whereas other tools like Harpoon does not generate real-time traffic [36].

C. PERFORMANCE EVALUATION

The proposed method performance is measured in terms of identification of attack (accuracy), detection rate (sensitivity) and false alarm rate (specificity) using different equations [37]. The accuracy signifies the ratio of properly recognized results over the full data used by the proposed method or true negative results, while mistakenly recognized alarm are false positive and false negative results.

The proposed method accuracy is measured by Equation 4.

- True positives (TP): truly identified true information.
- True negatives (TN): truly identified false information.
- False positives (FP): incorrectly identified information.
- False negatives (FN): incorrectly identified false information as true.

$$\text{True Positive Rate (TPR)} = \frac{TP}{P} = \frac{TP}{TP + FN} \tag{1}$$

$$\text{False Positive Rate (FPR)} = \frac{FP}{N} = \frac{FP}{FP + TN} \tag{2}$$

$$\text{False Negative Rate (FNR)} = \frac{FN}{P} = \frac{FN}{FN + TP} \tag{3}$$

$$\text{Accuracy} = \frac{TP + TN}{TP + TN + FP + FN} \tag{4}$$

The sensitivity signifies the ratio of truly recognized malicious packets over the whole range of true results gained by the proposed method. The identification of attack traffic of the proposed method is measured in Equation 5.

$$Sensitivity = \frac{TP}{TP + FP} \tag{5}$$

The specificity represents the rate of incorrectly identified abnormal packets over the entire range of negative results produced by the proposed method latency as it did not have any bearing on the rate of false positives. Because the way the method depends on the dataset, learning based change of rules, to decrease false positives, it does not expand the rate of false negatives. Any false-negative that exists in the considered method would likewise exist in an IPS without the additional tools kits. The specificity of the proposed method is measured by Equation 6.

$$Specificity = \frac{TP}{TN + FN} \tag{6}$$

$$\text{Score} = 2 \times \frac{Recall \times Precision}{Recall + Precision} \tag{7}$$

The proposed method is evaluated against the performance evaluation under both single source and multiple source attack environments using the Equation 7. False positive rate is defined by Equation 2.

D. RESULTS

The results are based on two scenarios of testing behaviors. The first phase of testing was legitimate traffic that seemed suspicious because of badly composed arrangement of snort rules. The second phase was represented as a case where an attacker made an attack on the network by LOIC tool for DDoS attack it is low level of attack tool which. First phase represents to a case in which an arrangement of seven rules were made to control the access of specific parts of the network. In the first phase of testing, out of the 23 packets sent to the network, 13 were dropped by IPS. This added up to a false positive rate of more than 50%. All traffic in this stage that was esteemed suspicious was quickly dropped. In the second period of testing, a similar traffic was replayed against the network. The principal set of packets did not coordinate against the IPS rules and were in this way directed to the backup router after the underlying arrangement of packets, then a single request generated for a connection caused an IPS rule to delete. The result was the addition of a new NAT rule in IPTABLES to drop following IP address in INPUT table and FORWARD table following rule added by scripts.

This rule caused all traffic from the following IP to drop. The second scenario was designed to emulate a situation where an attacker discovers way to attack a DDoS attack. Once more, as in the second period of testing for the first scenario, the request made to IPS inline for another NAT rule was added to the firewall that kept running closely with IPS. Now, the request was classified to suspicious traffic and was routed to backup router. The following request reached the backup router which prepared the request and restored the element of the attack packets. As the element of attack packets went through the backup router, the IPS rule to identify

the components of the attack packets read and write to the alert.log record. The snortwatch.pl script distinguished this new alert in the alert.log record and started a smooth restoration from the attack. Two new iptables rules were included as the principal rules of the IPS, as should be possible in first period of testing. This quickly kept attackers from exploiting the successful attack by cutting them from the network. As the last restriction is not critical so we chose not to investigate. Figure 4 provides the CPU load results during performing the scenarios.

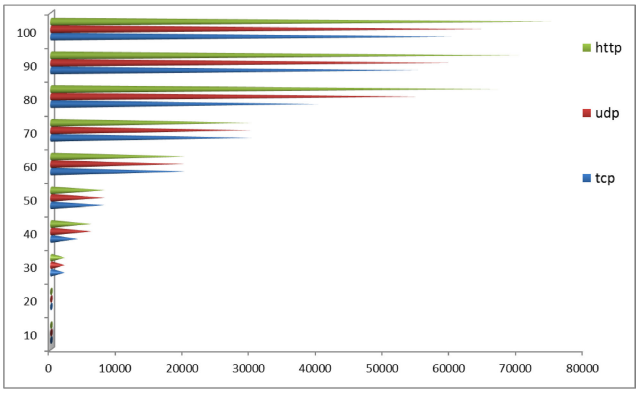


FIGURE 4. CPU load results.

The outcomes of the false negatives demonstrated that there was no effect on the false negatives rate caused by the new IPS. The first test stage saw an aggregate of around 60000 packets that were resolved to be false negatives. In the second period of testing, with fuzzy traffic, tests show a similar number of alerts for this situation of around 56000 logged which prompted a lower rate of false negatives. As said prior in the examination, this could have a few causes and the rate of false negatives between the two systems will be at least equivalent. The false positive alarms affect the performance of Snort [26]. Most essentially, the method decreased the false positive rate to zero without affecting the rate of false negatives. The outcomes similarly demonstrated a smooth procedure to recover from attack so the attack could be breaking down while legitimate users could securely keep on interacting with the network. While these outcomes were promising, they were just a beginning, as the proposed method could be extended from numerous points of view to give better insurance to protect the network, while likewise giving expanded capacities to monitoring attacks. To ensure the experiment environment is the same in evaluating the IPS techniques as in performance metric CPU load, latency, and average packets. Each iteration of the experiment is repeated ten times and the mean value is calculated and recorded in the results section. The proposed IPS method experimental results are better in terms of accuracy, detection, specificity and exposure in comparison with other IPS and Snort results given in Table 3.

This method is based on back propagation and compared it with other methods to back propagation that specifies better

TABLE 3. Traffic accuracy in normal traffic flow

Protocol	Accuracy Measurements		
	FPR	*FNR*	*TPR*
UDP	11%	0%	0%
TCP	10%	0%	0%
ICMP	3%	0%	0%

performance and accuracy. Fries did the intrusion detection using fuzzy clustering of TCP packet attributes [20], and [38] used SVM along with ACO feature subset [30]. Apart from intrusion detection, there are many other application areas where machine learning is applied as in [9], [23], [24], [31].

TABLE 4. Evaluation of results

Protocol	Machine	Accuracy	CPU Usage	Results
TCP	1-60	97.9%	66%	8%
UDP	1-70	98.5%	69%	6%
HTTP	1-80	96.2%	70%	6%

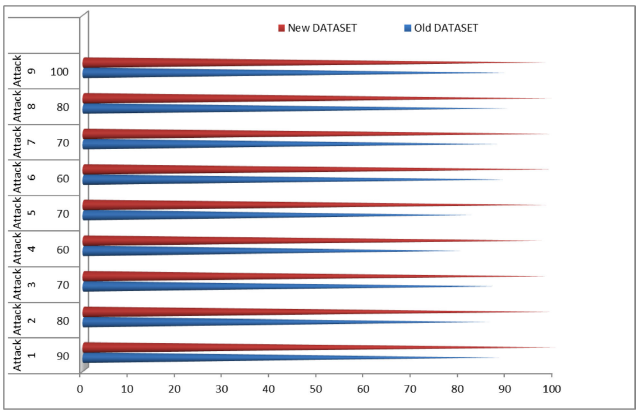


FIGURE 5. Comparison of update and old datasets results.

Authors used statistical method and K.P.C.A (Kernel Principle Component Analysis) and P.S.O (Particle Swarm Optimization) SUM DDoS Attacks detection [39], [40]. K.P.C.A is used to remove useless features and P.S.O to optimize support vector machine. Proposed IPS solution provide 97.9% detection accuracy while the percentage of unknown and known attacks was 62% and 58%. The detection results for high and low rates of DDoS attacks were 97.9% and 98.6%, individually if compare with snort simple rules 92% and 91% individually. Our proposed method has been trained with new and old datasets. We launched numerous unknown and known attacks to get better outcome of the method. Table 4, Table 5 and Figure 5 represent results of the experiments. The results in Table 9 represent that when training the agent in IPS method with old datasets then system reacted badly with 89% of exposure accuracy where the detection rate of accuracy is 85% and 40% for unknown and known attacks individually. The results in Table 7 represent that when training the agent in IPS method with latest datasets the solution's detection accuracy was 99% with 59% and 70% for unknown and known

TABLE 5. Comparison of different approaches using updated datasets

Approach	Proposed IPS	Snort	P.N.N	B.P	Chi	PSO-SVM
Accuracy	95	91	92	90	94	-
Exposure	96.7	90.4	-	-	92	96
Specificity	98.7	96	-	-	-	-

TABLE 6. Traffic accuracy in malicious traffic flow

Protocol	Accuracy Measurements		
	FPR	*FNR*	*TPR*
UDP	3.5%	1.7%	0%
TCP	11%	0.7%	0%
ICMP	18.5%	0.3%	0%

TABLE 7. Results comparison between old datasets and up-to-date datasets

Dataset Type	Accuracy	Exposure	Specifications
Old dataset	89%	85%	94%
Up-to-date dataset	98.8%	98.2%	96.3%

attacks. This showed the statistic that when trained with supervised leaning with updated and latest datasets proposed method can deliver improved results with superior accuracy in detection.

TABLE 8. Performance measurements

Detection Results	Received Packets				Average
	1000	2000	5000	6000	
Accuracy	99.5%	94.6%	96%	98%	97%
Sensitivity	95.3%	94%	98%	99%	96.5%
Specificity	96%	96%	97%	98%	96.7%

TABLE 9. Performance analysis of SVM & different algorithms

Algorithm	Accuracy 70%	Accuracy 30%
OPT_SVM	97.6	98.6
SVM	89.8	99.1
DT	45.17	55.75
LINER	55.24	67.87
MLP	65.47	76.75
Naive	30.17	45.75

We have used more feature of dataset to increases detection accuracy. Table 6 shows the traffic flow with malicious behavior. Whenever the dataset contains more features its accuracy increases [16]. Table 8 and Table 9 present the experiments and results. Figure 6 presents comparison of proposed IPS with other solution in graph upper line show the proposed IPS. The detection accuracy results for high and low rates of DDoS attacks were 97.9% and 98.6%, individually if compare with snort simple rules 92% and 91% individually. LS-SVM previous approaches, since either the percentage accuracy of previous approaches is lower than those achieved by our approach, for example 94% in [16], or are with Kappa coefficient stability measurements for example in [16]. In addition, the SNORT FPR (specificity) of the Fuzzy logic

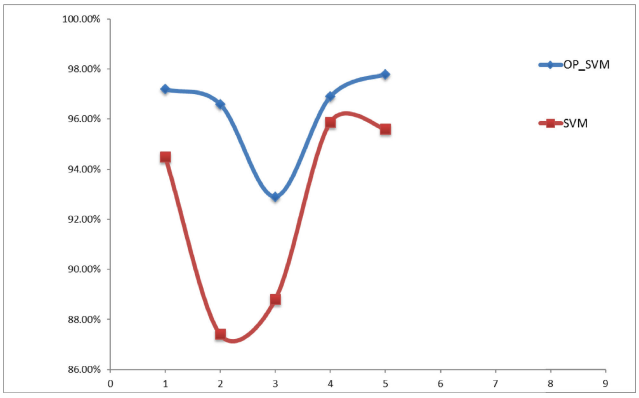


FIGURE 6. Optimized SVM & SVM chart.

algorithms are 55.2% on average [41]. Thus, we can claim that our proposed method is more effective.

V. CONCLUSION

The tests provide a proof of idea for a smart routing based IPS that is intended to reduce the impact of DDoS attacks. It showed the ability of the method to effectively and consistently recover from an attack. The successful recovery was characterized as having a reinforcement gateway of the cooperated network that could be utilized for a forensic investigation and additionally restoring the cooperated network to a protected state with the goal that it could be utilized by authentic users. Being an automatic process implemented in the method could recovery state from the attack with no human interference. The proposed IPS method can learn from malicious activity to act likewise. The learning procedure truly helped when an attacker effectively launches an attack. The proposed method goes far in lessening false positives without decreasing false negatives and opens a few ways of development that could additionally enhance the present systems of intrusion prevention. By learning from attacks instead of simply obstructing the attacker, it is conceivable that avoiding access to networks also helped in zero-day attack. We utilized trained agents to recognize TCP, HTTP and UDP attacks utilizing the fundamental key examples that recognize genuine activity from DDoS attacks. A dump record of genuine network environment is utilized to begin the learning procedure. We have assessed the proposed method with other research. The designed proposed IPS to prevent an entire network from DDoS attack and data packets sniff from achieving the objective while giving up genuine network traffic activity to go through. Additionally, assessed proposed method via training it with old existing and custom generated update datasets and it gave better results and recognized DDoS attacks that were relatively undefined with

most recent examples it was trained with. Some DDoS attacks were not recognized on the grounds that the agents were trained with old data examples and hence demonstrated that old datasets or inappropriate training can show poor results yet extraordinary DDoS cases can show better result in identifying DDoS attacks. While a pre-selected set of network traffic had a close to 48% false positive rate in the main period of testing, a similar network traffic sent to the network with the reinforcement gateway router had zero false positive. The zero day attack and multi-threading for packet processing are the only limitations of this method. This will be eliminated using SNORT3 in the future work. The future work should also includes to test the behavior of different applications under different DDoS attacks.

REFERENCES

[1] F. Al-Haidari, M. Sqalli, and K. Salah, "Impact of CPU utilization thresholds and scaling size on autoscaling cloud resources," in *Proc. IEEE 5th Int. Conf. Cloud Comput. Technol. Sci.*, vol. 2, Dec. 2013, pp. 256–261.

[2] P. Calyam, S. Rajagopalan, S. Seetharam, A. Selvadhurai, K. Salah, and R. Ramnath, "VDC-analyst: Design and verification of virtual desktop cloud resource allocations," *Comput. Netw.*, vol. 68, pp. 110–122, Aug. 2014.

[3] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," *Future Gener. Comput. Syst.*, vol. 82, pp. 395–411, May 2018.

[4] C. Gkountis, M. Taha, J. Lloret, and G. Kambourakis, "Lightweight algorithm for protecting SDN controller against DDoS attacks," in *Proc. 10th IFIP Wireless Mobile Netw. Conf. (WMNC)*, Sep. 2017, pp. 1–6.

[5] F. González-Landero, I. García-Magariño, R. Lacuesta, and J. Lloret, "ABS-DDoS: An agent-based simulator about strategies of both DDoS attacks and their defenses, to achieve efficient data forwarding in sensor networks and IoT devices," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–11, Jun. 2018.

[6] X. Yuan, C. Li, and X. Li, "DeepDefense: Identifying DDoS attack via deep learning," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2017, pp. 1–8.

[7] M. F. Majeed, V. Esichaikul, and M. No, "Use of multi-agent based platform for providing document-centric interoperability in the realm of E-government," in *Proc. Int. Conf. Adv. Inf. Technol.* Springer, 2013, pp. 141–149.

[8] F. Baker and P. Savola, "Ingress filtering for multihomed networks," Cisco Syst., Santa Barbara, CA, USA, Tech. Rep. 3704, 2004.

[9] S. Teng, C. Zheng, H. Zhu, D. Liu, and W. Zhang, "A cooperative intrusion detection model for cloud computing networks," *Int. J. Secur. Appl.*, vol. 8, no. 3, pp. 107–118, May 2014.

[10] K. Ye, "Key feature recognition algorithm of network intrusion signal based on neural network and support vector machine," *Symmetry*, vol. 11, no. 3, p. 380, Mar. 2019.

[11] M. M. Sakr, M. A. Tawfeeq, and A. B. El-Sisi, "Network intrusion detection system based PSO-SVM for cloud computing," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 3, p. 22, 2019.

[12] A. Alsirhani, S. Sampalli, and P. Bodorik, "DDoS attack detection system: Utilizing classification algorithms with apache spark," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–7.

[13] S. A. R. Shah and B. Issac, "Performance comparison of intrusion detection systems and application of machine learning to snort system," *Future Gener. Comput. Syst.*, vol. 80, pp. 157–170, Mar. 2018.

[14] M. B. Shahbaz, X. Wang, A. Behnad, and J. Samarabandu, "On efficiency enhancement of the correlation-based feature selection for intrusion detection systems," in *Proc. IEEE 7th Annu. Inf. Technol., Electron. Mobile Commun. Conf. (IEMCON)*, Oct. 2016, pp. 1–7.

[15] D. Perakovic, M. Perisa, I. Cvitic, and S. Husnjak, "Artificial neuron network implementation in detection and classification of DDoS traffic," in *Proc. 24th Telecommun. Forum (TELFOR)*, Nov. 2016, pp. 1–4.

[16] R. Aishwarya and S. Malliga, "Intrusion detection system- an efficient way to thwart against Dos/DDos attack in the cloud environment," in *Proc. Int. Conf. Recent Trends Inf. Technol.*, Apr. 2014, pp. 1–6.

[17] B. Jia, X. Huang, R. Liu, and Y. Ma, "A DDoS attack detection method based on hybrid heterogeneous multiclassifier ensemble learning," *J. Electr. Comput. Eng.*, vol. 2017, pp. 1–9, Mar. 2017.

[18] K. Singh, P. Singh, and K. Kumar, "A systematic review of IP traceback schemes for denial of service attacks," *Comput. Secur.*, vol. 56, pp. 111–139, Feb. 2016.

[19] Y. Lu and M. Wang, "An easy defense mechanism against botnet-based DDoS flooding attack originated in SDN environment using sFlow," in *Proc. 11th Int. Conf. Future Internet Technol. (CFI)*, 2016, pp. 14–20.

[20] B. Cha and J. Kim, "Study of multistage anomaly detection for secured cloud computing resources in future Internet," in *Proc. IEEE 9th Int. Conf. Dependable, Autonomic Secure Comput.*, Dec. 2011, pp. 1046–1050.

[21] S. N. Shiaeles and M. Papadaki, "FHSD: An improved IP spoof detection method for Web DDoS attacks," *Comput. J.*, vol. 58, no. 4, pp. 892–903, Apr. 2015.

[22] F. Guenane, M. Nogueira, and G. Pujolle, "Reducing DDoS attacks impact using a hybrid cloud-based firewalling architecture," in *Proc. Global Inf. Infrastruct. Netw. Symp. (GIIS)*, Sep. 2014, pp. 1–6.

[23] H. Beitollahi and G. Deconinck, "Analyzing well-known countermeasures against distributed denial of service attacks," *Comput. Commun.*, vol. 35, no. 11, pp. 1312–1332, Jun. 2012.

[24] D. Krishnan and M. Chatterjee, "An adaptive distributed intrusion detection system for cloud computing framework," in *Proc. Int. Conf. Secur. Comput. Netw. Distrib. Syst.* Springer, 2012, pp. 466–473.

[25] C. N. Modi, D. R. Patel, A. Patel, and R. Muttukrishnan, "Bayesian classifier and snort based network intrusion detection system in cloud computing," in *Proc. 3rd Int. Conf. Comput., Commun. Netw. Technol. (ICCCNT)*, Jul. 2012, pp. 1–7.

[26] C. Dou, D. Yue, Q.-L. Han, and J. M. Guerrero, "Multi-agent system-based event-triggered hybrid control scheme for energy Internet," *IEEE Access*, vol. 5, pp. 3263–3272, 2017.

[27] A. M. Lonea, D. E. Popescu, O. Prostean, and H. Tianfield, "Evaluation of experiments on detecting distributed denial of service (DDoS) attacks in Eucalyptus private cloud," in *Soft Computing Applications*. Springer, 2013, pp. 367–379.

[28] X. Xu, J. Li, H. Yu, L. Luo, X. Wei, and G. Sun, "Towards Yo-Yo attack mitigation in cloud auto-scaling mechanism," *Digit. Commun. Netw.*, Oct. 2019.

[29] T. V. Phan and M. Park, "Efficient distributed Denial-of-Service attack defense in SDN-based cloud," *IEEE Access*, vol. 7, pp. 18701–18714, 2019.

[30] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," *ACM Comput. Surv.*, vol. 41, no. 3, p. 15, 2009.

[31] M. Tavallaee, E. Bagheri, W. Lu, and A. A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in *Proc. IEEE Symp. Comput. Intell. Secur. Defense Appl.*, Jul. 2009, pp. 1–6.

[32] H. F. Rashvand, K. Salah, J. M. A. Calero, and L. Harn, "Distributed security for multi-agent systems–review and applications," *IET Inf. Secur.*, vol. 4, no. 4, pp. 188–201, 2010.

[33] R. Papadie and I. Apostol, "Analyzing websites protection mechanisms against DDoS attacks," in *Proc. 9th Int. Conf. Electron., Comput. Artif. Intell. (ECAI)*, Jun. 2017, pp. 1–6.

[34] N. Hoque, H. Kashyap, and D. K. Bhattacharyya, "Real-time DDoS attack detection using FPGA," *Comput. Commun.*, vol. 110, pp. 48–58, Sep. 2017.

[35] R. Paranthaman and B. Thuraisingham, "Malware collection and analysis," in *Proc. IEEE Int. Conf. Inf. Reuse Integr. (IRI)*, Aug. 2017, pp. 26–31.

[36] M. F. Majeed, M. N. Dailey, R. Khan, and A. Tunpan, "Pre-caching: A proactive scheme for caching video traffic in named data mesh networks," *J. Netw. Comput. Appl.*, vol. 87, pp. 116–130, Jun. 2017.

[37] S. Hosseini and M. Azizi, "The hybrid technique for DDoS detection with supervised learning algorithms," *Comput. Netw.*, vol. 158, pp. 35–45, Jul. 2019.

[38] T. Mehmood and H. B. M. Rais, "SVM for network anomaly detection using ACO feature subset," in *Proc. Int. Symp. Math. Sci. Comput. Res. (iSMSC)*, May 2015, pp. 121–126.

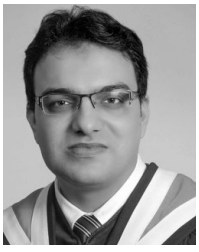
[39] X. Xu, D. Wei, and Y. Zhang, "Improved detection approach for distributed denial of service attack based on SVM," in *Proc. 3rd Pacific–Asia Conf. Circuits, Commun. Syst. (PACCS)*, Jul. 2011, pp. 1–3.

[40] J. Li, Y. Liu, and L. Gu, "DDoS attack detection based on neural network," in *Proc. 2nd Int. Symp. Aware Comput.*, Nov. 2010, pp. 196–199.

[41] A. Patil and S. Yada, "Performance analysis of anomaly detection of KDD cup dataset in R environment," *Int. J. Appl. Eng. Res.*, vol. 13, no. 6, pp. 4576–4582, 2018.

RANA ABUBAKAR (Graduate Student Member, IEEE) received the M.Sc. degree (Hons.) from Virtual University, Pakistan, in 2017. His main areas of research interest are mobile ad-hoc networks, and information and communication technologies.

ABDULAZIZ ALDEGHEISHEM received the bachelor's degree in urban planning and design from the College of Architecture and Planning, King Saud University, the master's degree in city planning from the University of Pennsylvania, Philadelphia, in 2001, and the Ph.D. degree in urban studies from the University of Illinois at Urbana-Champaign, in 2006. He is c an Associate Professor with the Department of Urban Planning, College of Architecture and Planning, King Saud University, Riyadh, Saudi Arabia. He is the Vice Head of Projects with Vision Realization Office (VRO). He is also the Supervisor of the Traffic Safety Technologies Chair. He is interested in the role of spatial information in urban planning and management. His areas of interest are urban growth and management, smart city technologies, and development.



MUHAMMAD FARAN MAJEED (Member, IEEE) received the M.S. degree (Hons.) from CECOS University, Pakistan, in 2011, and the Ph.D. degree in computer science from the Department of Information and Communication Technologies, Asian Institute of Technology, Thailand. His research interests include future internet architectures, the Internet of Things, multimedia communications, sensor networks, and agile software.

AMJAD MEHMOOD (Senior Member, IEEE) received the Ph.D. degree in wireless networks from the Kohat University of Science and Technology, Kohat, in 2014. He has got two post-docs: one from the University of Aeronautical, USA, and the other from the Guangdong Provincial Key Laboratory on Petrochemical Equipment Fault Diagnosis, Guangdong Petrochemical University Technology, Maoming, China. He is currently serving as a Research Fellow with the WMG's Cyber Security Centre (CSC), University of Warwick, Coventry, U.K. As far as academic and research experience is concerned, in 2003, he joined the Kohat University of Science and Technology, where he is serving as a Professor and the Coordinator of M.S./Ph.D. program. He is interested to work in the areas of cyber physical systems, the IoT, connected vehicles, wireless, optical communications and networking, smart grid communications and networking, network management issues and security issues, big data, cloud computing, and fault diagnosis in industrial infrastructure. He has visited many countries for sharing his research thoughts like Australia, Hong Kong, China, South Korea, Malaysia, and Thailand. He supervised many students of B.Sc., M.Sc., M.S., and Ph.D. in the above-mentioned interests. He is also been remained the part of reviewing and organizing different workshops, seminar, and training sessions on different technologies. Furthermore, he has served as a TPC, Reviewer, and a Demo Chair for numerous international conferences, including CCNC, SCPA, WICOM, INFOCOM, and SCAN. Additionally, he is a reviewer or an Associate Editor for many peer-reviewed international journals. He has published more than 60 academic articles in peer-reviewed international journals and conferences around the world. As far as his social experience is concerned, he is a Professional member of ACM and the KUST University Branch Coordinator. In 2018, he won the elections of IEEE member development and Award Committee as the Chair of Islamabad Section. By considering his performance, he has been presented an award of performance of the year 2019. As for as project hunting is concerned, he has won three projects from Higher Education Commission, Pakistan, out of which two projects have been completed while one is in progress. The in-progressed project is entitles as Intelligent Interoperable Natural Disaster Relief Operation using Ad Hoc Commission Paradigms won under National Research Project of Universities on which he and team members have been embarking, since 2018. Last but not least, he is also the Director of Research Lab at KUST named as the Reliable Optimal Smart Scalable and Efficient (ROSE) Lab.

HAFSA MARYAM received the M.S. degree in wireless networks from COMSATS University, Islamabad, Pakistan, in 2017. In 2018, she joined the Dr. Abdul Qadeer Khan Institute of Computer Science and Information Technology (KICSIT), where she is currently a Faculty Member. She has authored over eight academic articles in peer-reviewed international journals and conferences around the world. Her research interest includes information centric networks, content centric networks, vehicular networks, mobile ad-hoc networks, the IoT, wireless communications and networking, and cloud computing.

NABIL ALI ALRAJEH received the Ph.D. degree in biomedical Informatics engineering from Vanderbilt University, USA. He is currently a Professor with the Health Informatics at Biomedical Technology Department, King Saud University. He worked as a Senior Advisor for the Ministry of Higher Education, his role was in implementing development programs including educational affairs, health information systems, strategic planning, and research and innovation. His research interests include E-health applications, hospital information systems, telemedicine, intelligent tutoring systems, and wireless sensor networks.

CARSTEN MAPLE (Member, IEEE) is currently a Principal Investigator of the NCSC-EPSRC Academic Centre of Excellence in Cyber Security Research with the University and Professor of Cyber Systems Engineering in WMG. He is a co-investigator of the PETRAS National Centre of Excellence for IoT Systems Cybersecurity where he leads on Transport & Mobility. He has an international research reputation and extensive experience of institutional strategy development and interacting with external agencies. He has published over 250 peer-reviewed papers and is co-author of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit. He is also co-author of Cyberstalking in the UK, a report supported by the Crown Prosecution Service and Network for Surviving Stalking. His research has attracted millions of pounds in funding and has been widely reported through the media. He has given evidence to government committees on issues of anonymity and child safety online. Additionally he has advised executive and non-executive directors of public sector organisations and multibillion pound private organisations.

MUHAMMAD JAWAD received the B.Sc. degree (Hons.) from the Institute of Computing, Kohat University of Science Technology, Kohat, Pakistan, and the M.S. degree in software project management. His main areas of research interest are mobile ad-hoc networks and information and communication technologies, and software project management.