A REVIEW ON ARTIFICIAL INTELLIGENCE IN THE DEFENCE MECHANISIM AGAINST DDoS ATTACKS

[1]Nithin M, [2]M Manjusha, [3]Hanvitaa G, [4]Tanuja H B

[1]Student, [2] Student, [3] Student, [4] Student
Information Science and Engineering,
Alvas Institute of Engineering and Technology, Mangalore, India

***Abstract*: Artificial intelligence [AI] is the capacity of a computer software program or a machine to learn and think. It is also a field of computer science which tries to make computer programs or machines "quick-witted intelligence" develops intelligence machines that thinks and works like humans. Basically the view of AI as a computer program is a set of algorithms to process symbols and it has led to many useful applications such as visual perception, speech recognition, decision-making, and translation between languages, problem-solving, learning, planning and many more. Although the discipline of Artificial Intelligence (AI) was born in the summer of 1956 at Dartmouth College in Hanover, New Hampshire. AI has become a vital field whose influence on our daily lives will hardly be overestimated. Since the Eighties, AI has swollen into a broader study of the interaction between the body, brain, and setting, and the way intelligence emerges from such interaction. This review paper focuses on the most common defense methods against DDoS attacks that adopt AI and applied mathematics approaches. Additionally, the review classifies and illustrates the attack types, the testing properties, the evaluation methods and the testing datasets that are utilized in the methodology of the proposed defense methods. Finally, this review provides a guideline and possible points of encampments for developing improved solution models of defense methods against DDoS attacks.**

INTRODUCTION

Artificial Intelligence (AI) has a long tradition as a scientific field, with tremendous achievements accomplished in the decades behind us. It has grown dramatically and becomes more and more institutionalized. In the 21st Century. Actually, as early as the 1940s and 1950s, scientists in the field of Mathematics, Engineering, and Computer Science had explored the possibilities of artificial brains and were trying to define the intelligence of the machine. AI has been utilized into several major subjects including computer vision, natural language processing, the science of cognition and reasoning, robotics, game theory, and machine learning since the 1980s. In the context of AI's growth, we discover that the number of publications as well as the length of the author list has been increasing over the past 16 years.

Distributed Denial of Service (DDoS) attack is an intimidation trial flooded on the Internet. In DDoS attack, the network bandwidth represents victims' computer machines and resources that are depleted for sending of numerous packets toward a targeted server [1].

The source of these attacks with the help of tracking capabilities can be The associate editor coordinating the review of this manuscript and approving it for publication in the paper [2].

Detected, identified and blocked or rejected. However, due to the exponential growth of Internet usage in the last decade, attackers can select from a vast amount of vulnerable systems (hosts) and use them to start their attacks. Two main steps are needed to generate DDoS attack on a system.

The first step involves malicious packets sent by an attacker to victims' machines to disturb protocols or running applications, i.e., vulnerability attack that creates zombies [3].

Trojan horses, backdoors, or worms are usually used to recruit zombies [4].

The second step involves the attacker use these zombies to activate flooding attacks by exhausting a server or network resources including bandwidth, memory, router's processing capacities, disk/ database. Translations and content mining ar allowable for educational analysis solely Personal use is additionally allowable.DDoS attacks are launched via remotely controlled, well organized, and widely distributed zombies' botnet computers in a network. Many traffic or service requests are simultaneously or continuously sent to the target system. The target system becomes unusable, responds slowly, or crashes completely due to the attack. The identification of the original attackers is difficult for the defense methods because the attackers have spoofed IP addresses and covered within the zombies that are under their control [5].

In 2009, many zombies ar accustomed overwhelming a victim through a DDoS attack, thereby disrupting network services for popular websites, such as Facebook, Live Journal, Twitter, and Amazon [6].

Early DDoS attacks are mostly manual, and attackers must execute several steps, including detecting compromised machines to generate zombies on the Internet, port scanning, and deploying malware, before the launch of the final attack. At present, DDoS attack tools have become automated and sophisticated, thereby allowing attackers to execute all or a few of the steps automatically with minimal human effort [7].

Attackers can also configure parameter specific to the target, whereas the rest can be managed via automated tools. These automated attack tools include Trinoo, Tribe Flood Network (TFN), TFN2K, Trinity, Knight, and Stacheldraht, most of which work on Internet Relay Chat (IRC), in which compromised machines and zombies can communicate indirectly without having to disclose their identities [8].

Other attack tools are mostly agent-based, in which zombies and handlers communicate directly given knowledge of each other's identities. Flash Crowds (FC) is described as a kind of network traffic that is similar to DDoS traffic, but it comes from legitimate users [9].
FC is like DDoS attack in terms of many users gain access to a system simultaneously. In FC there is an abnormal and sudden rise in legitimate traffic because of special events such as publishing of the Olympics schedule or companies' new products like new smartphones of Samsung or Apple. The consequence of this is an early delivery response through web service, which may require prevention actions. It is difficult for defensive systems to distinguish between FC abnormal traffic from DDoS attacks because they vary in a few parameters only [10].
The parameters are low rate, infrequent arrivals and long intersession pauses.
This paper offers a thorough and detailed review of various techniques for detecting and preventing DDoS attacks, according to artificial intelligence and statistical approaches that are feasible at Open Systems Interconnection (OSI) layers model. A total number of 33 research articles, 6 networks security reports, 10 link of datasets and 6 review articles are covered in this review. The review investigates the defense methods that are deployed for detecting, mitigating, and/or preventing DDoS attacks. It classifies DDoS defense methods according to the class of vulnerability, the degree of automation, impact, and dynamics. The classification emphasizes a tangible view for many types of DDoS attack and DDoS defense methods and provides tables of relations. Moreover, this review includes a common testing datasets and evaluation methods. This review aims to improve the scope and shape the direction of DDoS research.

LITERATURE SURVEY

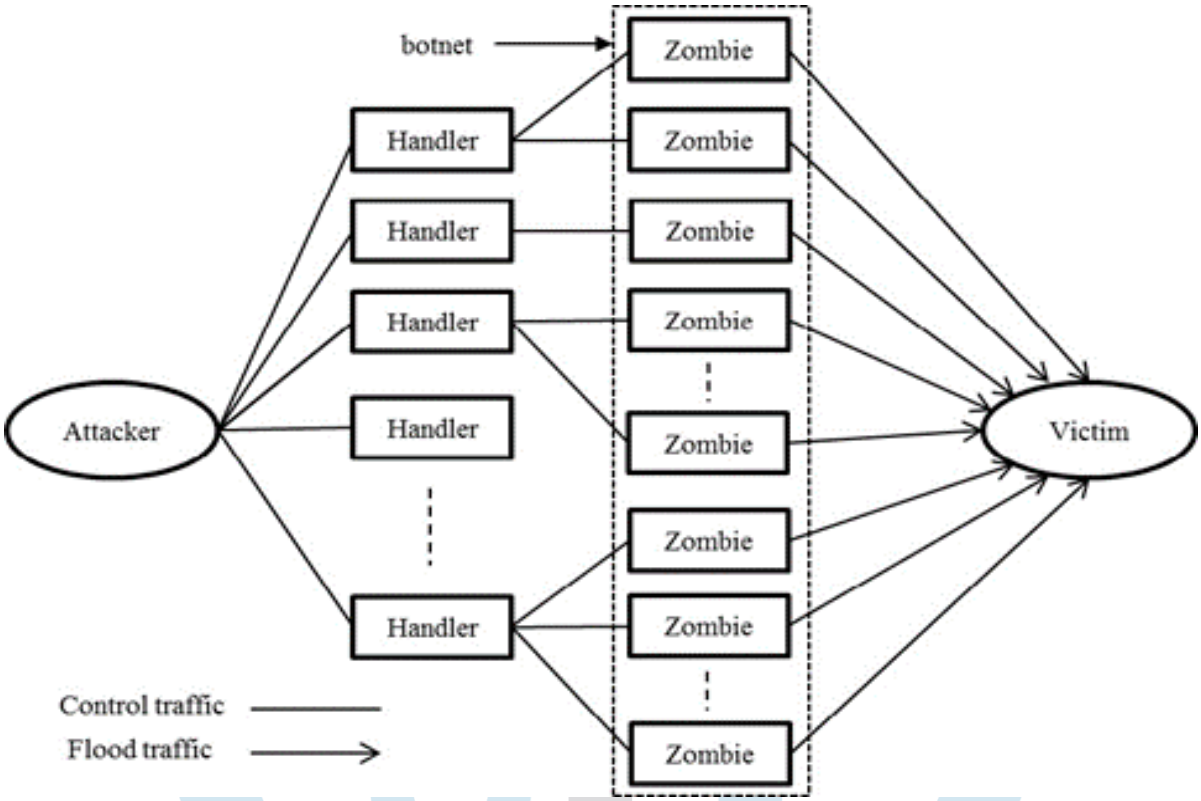
The history of the development of AI has been recent, with its origins being tracked to the mid-20th century. The genesis of AI can be credited to the contributions of various academic fields, not limited to art, history, philosophy logic and mathematics. The father of Artificial Intelligence, John McCarthy stated a definition for AI which tells that "Artificial Intelligence is the science and engineering of making intelligent machines, especially intelligent computer programs".
The two major methods that has been developed for the AI system are: "top down" method which started with the higher-level functions and implemented, and the "bottom up" method which focused at the neuron level and worked up to create higher level functions.
Different Artificial Intelligence algorithms can be used to solve a category of problems. The below mentioned are some of the algorithm used in solving the various problems using machine learning.

- **Naive Bayes** - Naive Bayes rule follows the Bayes theorem, that in contrast to all the opposite algorithms during this list, follows a probabilistic approach. This primarily suggests that, that rather than jumping straight into the information, the rule contains a set of previous possibilities set for every of the categories for your target[11].
- **Random Forest**-Think of this as a committee of Decision Trees, where each decision tree has been fed a subset of the attributes of data and predicts on the basis of that subset. The average of the votes of all decision trees are taken into account and the answer is given [12].
- **Decision tree** -The Decision Tree will basically be summarized as a flowchart-like tree structure wherever every external node denotes a take a look at on associate degree attribute and every branch represents the end result of that take a look at. The leaf nodes contain the actual predicted labels. We begin from the foundation of the tree and keep scrutiny attribute values till we have a tendency to reach a leaf node [13].

An approach to modeling and simulation of cyber-wars in Internet between the teams of software agents. According to this approach, the cybernetic opposition of malefactors and security systems is represented by the interaction of two different teams of software agents – malefactors' team and defense team. The approach is considered by an example of modeling and simulation of "Distributed Denial of Service" (DDoS) attacks and protection against them.[14]. The objective of a Distributed Denial of Service (DDoS) attack is to compile multiple systems across the Internet with infected zombies/agents and form botnets of networks. Such zombies are designed to attack a particular target or network with different types of packets. The infected systems are remotely controlled either by an attacker or by self-installed Trojans (e.g. roj/Flood-IM) that are programmed to launch packet floods. Within this context, the purpose of this paper is to detect and mitigate known and unknown DDoS attacks in real time environments. We have chosen an Artificial Neural Network (ANN) algorithm to detect DDoS attacks based on specific characteristic features (patterns) that separate DDoS attack traffic from genuine traffic [14]. Traditional architecture of internet is vulnerable to DDoS attacks and it provides an opportunity to an attacker to gain access to a large number of compromised computers by exploiting their vulnerabilities to set up attack networks or Botnets. Once attack network or Botnet has been set up, an attacker invokes a large-scale, coordinated attack against one or more targets. Here we have surveyed different types of attacks and techniques of DDoS attacks and their counter measures. The significance of this paper is that the coverage of many aspects of countering DDoS attacks including detection, defence and mitigation, traceback approaches, open issues and research challenges [15]. Software Defined Networking (SDN) has proved itself to be a backbone in the new network design. Here we propose a collaborative DDoS attack mitigation scheme using SDN. We design a secure controller-to-controller (C-to-C) protocol that allows SDN-controllers lying in different autonomous systems (AS) to securely communicate and transfer attack information with each other. This enables efficient notification along the path of an ongoing attack and effective filtering of traffic near the source of attack, thus saving valuable time and network resources. For proactive detection of DDoS attacks, by classifying the network status, to be utilized in the detection stage of the proposed anti-DDoS framework. Initially, we analyse the DDoS architecture and obtain details of its phases. Then, we investigate the procedures of DDoS attacks and select variables based on these features. Finally, we apply the k-nearest neighbour

(k-NN) method to classify the network status into each phase of DDoS attack. The simulation result showed that each phase of the attack scenario is classified well and we could detect DDoS attack in the early stage [16].

SYSTEM ARCHITECTURE



DDoS attacks have become a global menace in today's Internet. These attacks are adroit in nature and use an equivalent techniques of standard DDoS attacks except that the previous is disbursed at a larger scale than the latter via botnets. A botnet chain includes hundreds or thousands of compromised (bots, zombies, or slave agents) that are remotely controlled by one or more intruders attacking a victim[17].

For the attackers, each computer connected to the Internet presents an attractive opportunity to create zombies and mostly without their users' knowledge. Zombies are enrolled with the help of worms, Trojan horses, or backdoors with the sending of a captivating link, e-mail content, or a trust-inspiring sender address to vulnerable machines[18]. Basically, an individual attacker or a group of attackers implements different hacking techniques to exploit the vulnerability and weaknesses of computer machines connected to the Internet.

Thereby planting malicious codes that placing these computers in a vulnerable spot and assume control over these machines. Some of these machines are configured as ''handlers'' and others are configured as ''zombies''. The attackers control the handlers while the handlers' software controls the zombies. The attackers attempt to control as many computer machines as possible before starting the attack. The numbers of zombies could reach hundreds or even thousands. Successively, the large groups of zombies form a ''botnet'' of the attacks[19]. Low-rate DDoS attacks are dangerous and difficult to expose because the traffic that can be controlled by a selected link manifests as traditional. Thus, prevailing detection ways may result in an exceedingly speedy increase in high-rate DDoS attacks.

DDoS attacks are currently launched in the form of link and packet flooding. Such type of attacks has increased drastically on the Internet because attackers already know what, where, and how information is obtained. Attackers can easily launch such attacks because Internet protocols, operating systems, and web applications are constantly exposed to vulnerability. Such attacks are designed with motives, such as blackmail (to gain profit through extortion), hacktivism (to gain media attention), economic reasons (nastiness), personal reasons (disputes or revenge), and political reasons.

THE APPROACHES OF DDoS ATTACK USING AI

A] THE BAYESIAN NETWORK is defined in as a technique that determines the probabilistic associations among variables of interest. This technique is usually used for detecting attacks together with statistical schemes, which yield many advantages, such as the capability of encoding interdependencies among variables, forecasting events, and including prior data and knowledge.

Kim et al. [20] suggest the adoption of the pocket score, which can be defined as a programmed attack characterization, selective packet removal, and means of congestion control. The basic idea of this score is to prioritize packets according to per-packet score,

which determines the packet legitimacy given the values of the attributes it contains. Then, a score-based specific packet removal process is conducted at the destination, when the packet score is calculated at detecting differentiating discarding routers using a Bayesian.

In the method of Gonzalez et al[21]., a Bayesian inference prototype is applied to evaluate the reliability of proposed access routers on the basis of forwarding packets that does not modify the IP addresses of the source. In this method, a judge router collects the traffic that passes through the access routers then calculates trust scores of the access routers. The fundamental goal of these processes is to apply trust computations, management, and trust agreements among the routers to identify and filter the hostile routers.

B] FUZZY LOGIC The concept of fuzziness is used alongside the methods of identifying DDoS attack so that more emphasis is placed on network anomalies or attack. The basis of the fuzzy set theory is used in approximating the reasoning, rather than being precisely obtained through traditional predicated logic. The use of fuzzy sets, as well as their rules, are employed when a large number of input parameters such as, CPU usage time, activity rate and connection duration, which can be ambiguous when handling incomplete datasets[22].

In the work done by Shiaeles et al. [23], the detection of DDoS attack is achieved, while the time limits are improved through the use of non-asymptotic fuzzy evaluators. The evaluator is deployed on average packet inter-arrival durations. The problem is categorized into two, which are actual DDoS attack detection and victims' IP address recognition. The attack detection is achieved through the use of strict real-time boundaries, while the recognition of victims' IP address is achieved through the use of relatively lenient constraints that are able to promptly identify the victim's IP addresses. This in return begins to add anti-attack applications on the hosts that are affected using arrival time of the packet as the major statistic of DDoS attack detection**.**

In order to improve the precision capabilities of DDoS attack detection, the fuzzy classification techniques are integrated with cross-correlation by. Even though it is expected that the technique will improve precision, it does not satisfy real-time need due to the high cost of calculation. ''realtime'' identification of DDoS attack is achieved through the use of fuzzy rules together with Hurst factor. The attack is successfully identified within 13secs; this can be considered real-time in terms of specific context

C] K-NEAREST NEIGHBORS TECHNIQUE

K-Nearest Neighbors (K-NN) technique comes under an artificial intelligence technique that generates forecasts and determines by comparing the nearest graph element. Input can be categorized into groups using this nearest element, and nearby locations can be identified in real time by using this parameter geographically. Initially, K-NN has to note down IP addresses obtained to a server. Later, it has to note them down in a file and create a graph with longitude and latitude as axes [23]. A very high density demonstrated by the graph in a particular geographical area may indicate a potential DDoS.

EVALUATION METHODS

Evaluation metrics assess defensive systems by measuring their performance qualitatively and quantitatively. Numerous instances realize test scenarios that rely on specific evaluation criteria and metrics. This section covers evaluation metrics across various aspects in accordance with evaluative goals, such as detection performance, attack mitigation performance, and deployment costs.

A. QUANTITATIVE METHODS

1. PERFORMANCE METRIC

$$DR = TPR = RECALL = \frac{TP}{TP + FN}$$

DR or TP rate (TPR): The percentage of attack instances that are identified and reported correctly as attacks. This metric is useful for validating the effectiveness of the detection tool

- **TN rate:** The percentage of instances that are classified as legitimate.

- **FP rate (FPR) or false alarm ratio:**The number of legitimate instances that are classified as attacks. Its goal is to measure the effectiveness of the system in distinguishing fake and legitimate requests

2. ATTACK MITIGATION
   A. **Packet drop rate or request dropping probability:** Its goal is to assess the performance of attack mitigation. It is helpful in proving that the defense system can identify and block attacks, thereby increasing the availability of network bandwidth and resources for service.
   B. **Throughput or network traffic rate:** During an attack, throughput usually degrades because of the limited number of requests that the system serves. This metric, which can also be expressed as the rate of serviced requests, is used by authors to demonstrate the enhanced performance of the cloud service in defense and nondefense scenarios when detection and mitigation of attacks occur

B. QUALITATIVE METHODS

- **Abstraction:** Abstraction is the term used to describe how complex a person perceives or programs a system. The implication of the higher level is fewer details and the other way round.
- **Functionality:** Apart from the control of hardware and software features of experiments that are security-based, the facilitation of social and technical environments for experiments such as traffic generators, most recent tools for analysis and visualization of results, as well as diverse experimental profiles is essential.
- **Programmability:** This term describes the flexibility that a network-based experiment setup must possess, so as to able to make use of novel personalized network techniques of monitoring, detecting, filtering, improving or making the addition of practical heterogeneous hardware and router algorithms. Nonetheless, programmers who use software routers may benefit from their flexibility.

RESULT AND DISCUSSION

The related literature review papers in this field have been focused on certain aspects of DDoS security threats and solutions such as the type of attacks, defense methods, evaluation methods or testing datasets. This paper offers a thorough and detailed review of various methods to detect and prevent DDoS attacks, according to the classification of statistical and artificial intelligence approaches that are feasible at the OSI layered model. A large body of research is consulted in the preparation for this comprehensive literature review paper. A total of 151 data sources and including six review papers have been studied in order to outcome this masterpiece. The aim of this review is to provide guidelines for developing improved DDoS defensive methods and strategies and integrating effective solutions. The paper contexts on attackers' motivations that prompt such persons to flood targeted networks. It exploits and classifies the common DDoS attacks and determines the targeted particular and recognizes appropriate defensive methods of each class..

- Bayesian networks classifier is used (1) to detect and recognize DDoS attack in real-time as in ; (2) detect and defense against collective DDoS attack on HTTP as in and (3) assess the reliability of access routers when forwarding packets to detect and mitigate DDoS attack.

- Fuzzy logic technique is used to(1)reduce the ambiguity and increase the accuracy of DDoS attack detection as in; (2) perform self-adaptive judgment in order to improve the detection of DDoS attack in real-time as in; (3) dynamically estimate the intensity of DDoS flooding attack incidents in real-time.

- The K-Nearest Neighbors classifier is used to (1) classify the network status during DDoS attack in order to accurately detect and categorize the attack; (2) estimate the unknown class of requests in order to improve the anomaly traffic detection method and (3) recognize anomalous in network behavior by processing large data volumes and in a shortest possible time.

The table below show the results between AI and Static methods for detecting the DDoS Attack. The various parameters checked are complexity, Efficiency, Scalability, Precision and Accuracy and many more.

Evaluation methods	Artificial Intelligence																					Statistical									
	Bayesian Networks			Fuzzy logic			Genetic Algorithm			K-NN		Neural Network					Software Agent				SVM		Parametric				Non-parametric					
	50	51	52	53	57	58	59	60	61	62	63	66	67	69	70	71	1	73	74	75	76	85	80	82	83	84	87	88	89	90	95	98
Complexity	_	x	_	x	_	x	x	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_
Efficiency	_	_	x	_	_	_	x	_	_	x	_	_	x	_	_	_	_	_	_	x	_	x	_	_	_	_	_	_	_	_	_	_
Scalability	_	_	_	_	_	_	_	x	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_
Precision	_	_	_	_	_	x	_	_	_	_	x	_	_	x	_	_	_	_	_	_	_	_	_	x	_	x	_	_	_	_	_	_
Accuracy	x	x	x	x	x	x	x	x	x	x	x	_	x	x	x	_	_	x	x	x	x	x	x	_	_	x	x	x	x	x	x	x
F measure	_	_	_	_	_	_	_	_	_	_	x	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_
Packet drop rate	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_
Throughput	_	_	_	_	_	_	x	_	_	_	_	_	_	_	_	_	_	_	_	x	_	_	_	_	_	_	_	_	_	_	_	_
Attack impact	x	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_
Time	x	x	x	x	x	x	x	x	x	x	_	x	x	_	x	x	x	_	x	x	x	_	_	x	x	_	x	_	_	x	x	x
CPU load	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	x	_	_	_	_	_
Memory usage	_	_	_	_	_	_	_	x	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	x	_	_	x	x	_
Bandwidth	_	x	_	_	_	_	_	x	x	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	x	_	_	_	_	x
Financial cost	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	x	_	_	_	_	_
Detection Rate	_	x	_	_	_	_	x	_	x	x	x	_	x	_	_	_	_	_	x	x	_	_	_	_	_	_	_	x	_	_	x	_
Latency	x	x	_	_	_	_	_	_	x	_	_	x	_	_	_	x	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_	_

CONCLUSION

This paper attempts to provide an insight into the existing DDoS attack methodologies and a comprehensive review of the proposed solutions of numerous defense methods and techniques. The review covers a total of 129 research articles, six network security reports, ten links of the dataset and six review articles. It is applicable to web applications, web servers, web services, cloud computing, and any device with an Internet connection. The review offers a thorough and detailed review of Artificial Intelligence approaches that are utilized in preventing DDoS attacks. The paper aims to help in emerging advanced and effective defense methods for the DDoS attacks from the accumulation of the existing research.

REFERENCES

[1] I. Kotenko and A. Ulanov, ‘‘Agent-based simulation of DDOS attacks and defense mechanisms,’’ Int. J. Comput. , vol. 4, no. 2, pp. 113–123, 2014.

[2] K. Sharma and B. B. Gupta, ‘‘Taxonomy of Distributed Denial of Service (DDoS) Attacks and Defense Mechanisms in Present Era of Smartphone Devices,’’ Int. J. E-Services Mobile Appl., vol. 10, no. 2, pp. 58–74, 2018.

[3] A. Saied, R. E. Overill, and T. Radzik, ‘‘Detection of known and unknown DDoS attacks using artificial neural networks,’’ Neurocomputing, vol. 172, pp. 385–393, Jan. 2016. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S092523121501053X

[4] K. M. Prasad, A. R. Reddy, and K. V. Rao, ‘‘DoS and DDoS attacks: Defense, detection and traceback mechanisms—A survey,’’ Global J.
Comput. Sci. Technol., vol. 14, no. 7, pp. 1–19, 2014.

[5] S. Lim, J. Ha, H. Kim, Y. Kim, and S. Yong, ‘‘A SDN-oriented DDoS blocking scheme for botnet-based attacks,’’ in Proc. 6th Int. Conf. Ubiquitous Future Netw. (ICUFN), Jul. 2014, pp. 63–68.

[6] H. D’Cruze, P. Wang, R.O. Sbeit, and A. Ray, ‘‘A software-defined networking (SDN) approach to mitigating DDoS attacks,’’ Inf. Technol.New Gener. Cham, Switzerland: Springer, 2018, pp. 141–145.

[7] S. Jamali and V. Shaker, ‘‘Defense against SYN flooding attacks: A particle swarm optimization approach,’’ Comput. Elect. Eng., vol. 40, no. 6, pp. 2013–2025, 2014.

[8] A.Karim,R.B.Salleh,M.Shiraz,S.A.A.Shah,I.Awan,andN.B.Anuar, ‘‘Botnet detection techniques: Review, future trends, and issues,’’ J. Zhejiang Univ. Sci. C, vol. 15, no. 11, pp. 943–983, Nov. 2014.

[9] G. C. Kessler, ‘‘Computer security handbook,’’ in Denial-of-Service Attacks, 6th ed. London, U.K.: Wiley, 2014, ch. 18.

[10] B. Acohido and J. Swartz. ABC News Live Journal, New York.
Accessed: Aug. 2009. [Online]. Available: https://abcnews.go.com/ /story?id=8271907&page=1

[11] M. Uysal and S. R. Ranjan Swaminathan, ‘‘DDoS-resilient scheduling to counter application layer attacks under imperfect detection,’’ in Proc. 25TH IEEE Int. Conf. Comput. Commun., Apr. 2006, pp. 1–13.

[12] S. Behal, K. Kumar, and M. Sachdeva, ‘‘Characterizing DDoS attacks and flash events: Review, research gaps and future directions,’’ Comput. Sci. Rev., vol. 25, pp. 101–114, Aug. 2017.

[13] G. Oikonomou and J. Mirkovic, ‘‘Modeling human behavior for defense against flash-crowd attacks,’’ in Proc. IEEE Int. Conf. Commun., Jun. 2009, pp. 1–6.

[14] C. Douligeris and A. Mitrokotsa, ‘‘DDoS attacks and defense mechanisms: Classification and state-of-the-art,’’ Comput. Netw., vol. 44, no. 5, pp. 643–666, Apr. 2004.

[15] M. Aamir and M. A. Zaidi, ‘‘A survey on DDoS attack and defense strategies: From traditional schemes to current techniques,’’ Interdiscipl. Inf. Sci., vol. 19, no. 2, pp. 173–200, 2013.

[16] S. Behal and K. Kumar, ‘‘Trends in validation of DDoS research,’’ Procedia Comput. Sci., vol. 85, pp. 7–15, May 2016.

[17] G. Somani, M. S. Gaur, D. Sanghi, M. Conti, and R. Buyya, ‘‘DDoS attacks in cloud computing: Issues, taxonomy, and future directions,’’ Comput. Commun., vol. 107, pp. 30–48, Jul. 2017.

[18] N. S. Rao, K. C. Sekharaiah, and A. A. Rao, ‘‘A survey of distributed denial-of-service (DDoS) defense techniques in ISP domains,’’ Innov. Comput. Sci. Eng., vol. 32, pp. 221–230, May 2019.

[19] C. Zhang, Z. Cai, W. Chen, X. Luo, and J. Yin, ‘‘Flow level detection and filtering of low-rate DDoS,’’ Comput. Netw., vol. 56, no. 15, pp. 3417–3431, 2012

[20] J. Wang and G. Yang, ‘‘An intelligent method for real-time detection of DDoS attack based on fuzzy logic,’’ J. Electron., vol. 25, no. 4, pp. 511–518, Jul. 2008.

[21] Y. Li, L. Guo, Z. H. Tian, and T. B. Lu, ‘‘A lightweight web server anomaly detection method based on transductive scheme and genetic algorithms,’’ Comput. Commun., vol. 31, no. 17, pp. 4018–4025, Nov. 2008.

[22] A. Rahul, S. K. Prashanth, K. B. Suresh, and G. Anger, ‘‘Detection of intruders and flooding in Voip using IDS, jacobson fast and Hellinger distance algorithms,’’ IOSR J. Comput. Eng., vol. 2, no. 2, pp. 30–36, 2012.

[23] S. M. Lee, D. S. Kim, J. H. Lee, and J. S. Park, ‘‘Detection of DDoS attacks using optimized traffic matrix,’’ Comput. Math. Appl., vol. 63, no. 2, pp. 501–510, Jan. 2012.