Protection From Distributed Denial of Service Attack Using Fuzzy Logic

Hemalatha S (✉ hemalatharesearchphd@gmail.com)
Panimalar Institute of Technology
Vasantha Gowri N
Chaitanya Bharathi Institute of Technology
vani A
Chaitanya Bharathi Institute of Technology
Sana Qaiyum
Universiti Teknologi PETRONAS
vijayakumar P
Vellore Institute of Technology: VIT University
Sulaima Lebbe Abdul Haleem
South Eastern University of Sri Lanka

Research Article

Keywords: (DDoS) attack, Cyber Security, detection accuracy, internet, prevention, fuzzy logic

Posted Date: March 31st, 2021

DOI: https://doi.org/10.21203/rs.3.rs-349667/v1

Abstract

Distributed Denial of Service (DDoS) attacks represent an important challenge for public cloud as they invade the offender and completely delete Cloud service in order to serve the correct user and at the same time against the targets that cause system and service lack of access on infected devices. DDoS (Distributed Denial of Service) attacks are usually specific efforts to drain the resources of the victim or interrupt connections to networks by legitimate users. Traditional internet infrastructure is susceptible to DDoS assaults, and through leveraging their flaws to set up assault networks or Botnets, it offers an opening for an intruder to reach a wide number of infected machines. In order to identify and sustain improved detection accuracy, this work focuses on evaluating the different works and recommending a better solution to accommodate the cloud environment. A fuzzy logic for the detection and safety of DDOS attacks is proposed in this paper. The Fuzzy logic is used to dynamically select an algorithm from a collection of defined supervised learning that distinguish various DDoS variations and ultimately choose the relevant traffic algorithm.

Introduction

A DDoS exists when several attack sources are available. The intruder will form an army of compromised network systems to assault the server. Potential implications include that companies can miss sales due to maintenance, and the monitoring of innocent servers used as attackers is challenging. Attacks can occur in which IPs are also spoofed [1]. Usually, these key components - an intruder, an effective process, a victim/target server and innocent intermediate servers - are used as a DDoS attack. For DDoS, the bots or zombies accidentally take part in the assault. Two main methods can be used to launch Internet DDoS attacks. In the first step, the attacker sends the attacker damaging messages so that a mechanism or programme is misinterpreted.The second approach basically entails the flooding attacks on the network/transport stage/application level where an intruder executes one of both:

- Interrupt the valid user connectivity by eliminating latency, network services or router functionality.
- The services of legal users with exhaustive web servers such as Processor, storage, disk/database space, I/O connectivity.

DDoS attacks are now mostly initiated by well-organized, centrally managed, and extensively spread network Zombies or Botnet computers which are transmitting a large number of traffic or service requests to the target device continuously or simultaneously [2]. The assault results in either a sluggish, unusable answer or a total crash in the target device. Botnet zombies are typically hired using Trojan ponies, viruses, or backdoors. The security measures cause a lot of issues the actual intruder because the zombies the botnet hacker manages use duplicated Domain names. [3].Nowadays, DDoS assaults are so diverse and nuanced that they are launched in different patterns, rendering it impossible to spot static solutions. Numerous experiments have been carried out to identify and avoid DDoS attacks using classification algorithms and distributed networks [2]. Therefore, a new framework is taken to prevent threats by DDoS systematically, to efficiently properly handle patterns in DDoS attacks and the large volume of knowledge [3]. The ability of N classification algorithms, distribute processes techniques and a Fuzzy logic methodology is used for no DDoS detection method and can also progress in real to our correct knowledge.

Related Works

Nezhad et al. [4]Provide an Exponential Smoothing Transfer Standard grading system for DDoS attack detection and evaluate for a chaostic Series Data defect . The process is reviewed by the maximum cumulative calculation of Lyapunov. Their findings contain high concentrations of appreciation with respect to other approaches. Even so, to identify its effect on its efficiency and distributed period, it would also be helpful to consider further proposed structure and the use of information in public cloud.Prasad et al. [5] implement a description of the Web traffic potential system to differentiate amongst DDoS and rapid classes. To pass device reports to your center, they need Network Hazard Monitoring. Their method, nevertheless, based on case customers to limit access to public services via the protection system.Mizukoshi and Munetomo [6]suggest a Based Algorithm DDoS Defence Policy for attack, implemented in the Hadoop cluster. You are trying to solve a fixed design fault appropriate for a DDoS attack with several layouts. Their research showed that the number of Spark modules is reverse with the date of completion of a GA. Had the precision of their code been measured, they would have been more effective.Bazm et al.[7] Suggest the use of a virtual malicious machine to initiate a Network attacks as an Internet malware. Multiple machine learning techniques are proposed: sorting and classification. The method teams all VMs with same specific port and then classifies the VMs by network parameter. The system cannot, however, help a routine testing, since tracked data are transferred only to one system. It is also beneficial to evaluate the procedure for multiple classifications.Bridges et.al [8] Proposed genetic algorithm and IDS scheme focused on fuzzy. Li et.al suggested genetic algorithm-based IDS method. Genetic algorithm worked on exercise. The summary was provided by Dilpreet kaur et al[8] of multiple attacks in site log archives. RimmyChuchra et al concentrated on Network agents with their implementation to detect online assaults.S.Mirdula et al.[10] addressing the value and protection of the web application is increasingly expanding, but traditional frameworks neglect to provide web application protection. Diallo Abdoulaye Kindy et al.[11] have published a systematic web server survey on different facets of sql injection. This study also discusses SQL injection bugs, groundbreaking threats and solutions.PallaviAsrodia et al. [12] analyzed the rise in the rate of network traffic passing across their nodes every day. This paper reflects on the packet sniffer idea, its operating theory used in network traffic research. The Intrusion Detection Device network has been suggested by Sokratis et al.

Ddos Attacktypes

DDoS attack models are frequently classified into three groups: volume based assault, protocol-based assault and layer-based assault. [13][16][17].

Protocols Based Assault: Protocol Attacks are also a form of attack attempting to disrupt resources such as load-balancer configuration and other state firewall logs. This protocol-based attack aims to minimize even thousands of communications through the exhaustion of the TCP state.

Layer of Application Assault: Application Layer Attacks represent the most harmful and maximum hazard of all other kinds. Such attacks are harder to identify, since the base attack is often as minimal as possible, which is hard to identify and avoid. The most popular flood attack is the HTTP GET Flood and there are many numerous programs, such as Slowloris and Rudy. Other attacks such as DNS query flooding, sluggish assaults trying to harm the database by handling resourceful requests are overwhelmed.

Volume Based Assault: These attacks include UDP floods, ICMP floods and other network floods of spoofed packets. The aim of this attack is to saturate the bandwidth of the network and thus prevent legitimate traffic and data.

Architecture Of Distributed Denial Of Service (Ddos) Attack

Distributed Denial of Service Attack (DDoS) is one of the major threats based on the internet and the defence of such attacks is now a hot topic for research [15]. The DDoS attack utilizes many compromised hosts to send a lot of useless packets in a short space of time to the target, which will produce the assets of the destination and cause the server to be discontinued.

Such assaults presented an unprecedented danger to the internet. Many researchers have worked to identify these kinds of threats, which not only advance the network protection framework, but also constantly target techniques, which have improved appropriate attackers to evade these security systems.DDoS assault is the strongest on the Internet, where most infected machines are used. Such machines are referred to as zombies. Figure 2 below shows the DDOS assault architecture. An intruder takes the following actions in a hierarchical scheme in Figure 2

- The intruder implicitly receives access through the handlers to the officers. Handlers are picked for entry by the intruder with protection vulnerabilities in the first step.
- The intruder picks as many network providers and agents as necessary.
- Networked networks are situated beyond the network of the target and the perpetrator.
- Hosts are hacked by scanning hosts with vulnerability flaws to mount the attack form in a certain time of attack. In this stage, ICMP is typically used.
- The work of agents concurrently sends a vast number of pointless packets to a victim. The agents create those forms of TCP, UDP DDoS assault traffic.
- The victim or associated network is endangered and the provision of networks is shut down under certain kinds of DDoS assaults.
- The attackers normally target the victim using spoofing IP and random port, which makes it difficult to identify an intruder using an indirect design, as seen in Figure 2.

Ddos Preventative Assault

The most desirable security strategy for countering the DDoS attacks is avoidance of DDoS attacks. Essentially, as stated in the previous segment, DDoS attacks placed the resources of the target and the bandwidth and infrastructure of the network at tremendous risk. Thus, once an assault has already been initiated and succeeded, the victim's device will be substantially damaged. Defense against DDoS attacks is also easier against DDoS attacks, since it assures the avoidance of DDoS attack traffic and handles massive loads of attacks before the attack can succeed. This guarantees the victim's usual service. DDoS prevention of assault classification as seen in figure 3 below.

Prevention using filter: To deter attack traffic, filtering them out is quite necessary. Filtering methods discourage a victim from assaulting and being an unsuspecting intruder. Both filtering strategies are added to routers that guarantee that the device can only be reached by valid traffic.

Secure overlay: This is another DDoS avoidance method that covers a network subset. The concept is to create an overlay network over the IP network. This overlay network is the entrance to a secure network for the external network [14]. It is believed that separation can be accomplished by covering IP addresses or utilizing a distributed firewall in a secure network. This firewall guarantees that the secure network can only be reached by trustworthy traffic from the overlay network nodes. While this mechanism guarantees that DDoS attacks are avoided, it is applicable to a private network and it is not suitable to a public server [14][16][17].

Load balancing: This is a means of balancing the loads of multiple devices so that no device gets overwhelmed. The effect of the load balancing allows maintaining full efficiency and completing operation life. In situations where a server is undergoing a DDoS attack, a load balancer guarantees that data is routed to both active and unattacked servers. A bandwidth improvement is necessary on all essential connections to ensure full load balance. A large number of replicated servers and data centre are often required to minimize the loss of a single point. It also tends to reduce the attack area and allows it harder to deplete current capital and to attach saturation.

Honey pots: A honey pot is an interesting DDoS avoidance tool. Here, honey pots are less stable networks that draw attackers. A nice network imitates a legal network through which the intruder assumes that the real device has been targeted. The actual device thus remains secure. Not only is it necessary to obtain sensitive details regarding an intruder using a honey pot. This knowledge is additionally used to identify and stop a DDoS assault and its perpetrator.

Awareness-based prevention: Latest attacks by DDoS often involve IoT botnet-based DDoS user understanding. This is because the protection of IoT devices is really weak. Some DDoS assaults may also be avoided by protective steps in the ultimate user's own device. It guarantees not only their freedom from being invaded, but also that the invading force is a zombie. The following are several consumer initiatives that may deter a DDoS attack.

Executing Ddos Assault Phases

Four measures are taken to initiate a DDoS assault. This is shown in Figure 4.

Identify vulnerable hosts or agents: The intruder chooses the assaulting officers. Any device lacking antivirus protection or pirated copies of internet software is insecure and operates as a corrupted system [2]. Attackers have used these infected hosts or bots to search and hack more. The intruder uses the ample resources of these infected computers to create the attack stream.

Commitment: The intruder takes advantage of agent bugs and protection troubleshoots and downloads the attack code.

Communication: The intruder is in touch with the controllers to recognize the active agents, prepare attacks or update agents. Communication between attackers and operators

Fuzzy Logic

7.1 Architecture of Fuzzy Logic

Zadeh [as a strategy for defining and handling ambiguous information] implemented Fuzzy logic. A fuzzy collection defines a degree of membership between [0, 1], Where 1 indicates totally true ; 0-Completely False.Additional numbers between [1, 0] is a degree of fact.There are several ways to describe basic fluorescent processes, but the easiest is addressed here. Due to the two fuzzy values x and y, the following operations are defined:

(m**and** n) = minimum (a, b)

(m **or** n) = maximum (a, b)

not m = 1-a

(m**implies** n) = maximum (m,1-n)

The fuzzy logic methodology is being used to define the right form of identification of flow. In brief, we select from four candidate classifications the category classifier to identify transportation information by the fuzzy logic of each iteration. [5]. Use the fuzzy logic of an operation to select a classification method for the identification of congestion outcomes from the selection of four classification algorithms. Figure 6 shows the role in our system of the fuzzy logic. This paper proposes a fuzzy logic with three parameters: traffic length, classification methods and classification latency.

Rule Base: it shall include, on the basis of language knowledge, the rules set and the IF-THEN criteria set out by experts to regulate the decision-making framework. Latest advances in fuzzy theory have been shown to include many useful methods for controller design and tuning. Any of these developments decrease the amount of fugitive laws.

Fuzzification: is used for transforming inputs to fuzzy sets, i.e. crisp numbers. Crisp inputs consist essentially of correct sensor inputs that are transferred through the processing device, including temperature, pressure, rpm, etc.

Inference Engine: Calculates the matching degree of the existing fuzzy feedback for all rules and defines which rules to be shot by the input area. The fired laws are then merged in order to shape control acts.

Defuzzifier: is used to transform the fuzzy sets generated by the deduction motor to a crisp point. Several defuzzification approaches are possible and the optimal one for minimizing the error is used in a particular expert framework.

Figure 6 provides a device workflow summary

- The DDoS attack extracts a DDoS attack dataset, accompanied by the extraction feature, which is then saved in HDFS [5].
- The classification techniques are first eligible for their designs.
- The Fuzzy Logic System selects just next to the classification techniques equipped.
- The interpretation methods characterizes, checks and preserves the data in two databases (a) the testing period is maintained in the retrospective record and accuracy up to 110 results by each classification are retained. b) The encrypted material is included in the DDoS Attack Set Of data [4].
- The Fuzzy logic method takes as an input the precision of classification algorithms, the model training period and the amount of traffic.
- The procedure is replicated each time, where t is modified.

Methodology

Below Flow chart 7 displays the whole machine operation with some information. The IDS gathers all packets from the Traffic Sample in this design and inserts them in the flows to store within the memory [8]. In the meanwhile, the fuzzy engine gathers suspicious packets and brings them into suspicious flow. Whenever the alleged flow is done, the fuzzy engine tests for the final attack report [10].

Results And Discussion

Three situations such as standard network throughput, without optimization and optimization of fuzzy logic.

9.1 Throughput without optimization

Above table 1 and below graph 1 demonstrates the contrast of the output between iteration and round output without optimization. The blue color line represents the iteration throughput and the red color line indicates the round throughput.

Table1: Throughput (%) without optimization

S. No.	a/c to Iteration	a/c to Round
1	77	54
2	75	54.5
3	77	55
4	78	53.8

9.2 Throughput with optimization

The above table 2 and below table 2 display the contrast of the results of the performance by iteration and the performance by round for optimization. The blue color line represents the iteration throughput and the red color line indicates the round throughput.

Table2: Throughput with optimization

S. No.	a/c to Iteration	a/c to Round
1	82	58
2	79	59
3	83	54
4	80	57

9.3 Delay without optimization

The delay relation between delay by iteration and delay by round without Optimization demonstrates in Table 3 above and in Map 3 below. The blue color line shows the time delay by iteration and the red color line displays the delay by round.

Table 3: Delay without optimization

S. No.	a/c to Iteration	a/c to Round
1	14.6	0.6
2	14.1	0.57
3	13.9	0.52
4	15.7	0.63

9.4 Delay with optimization

The latency relation between time by iteration and time by round for optimization as seen in table 4 above and in figure 4 below. The blue color line shows the time delay by iteration and the red color line displays the delay by round.

Table 4: Delay with optimization

S. No.	a/c to Iteration	a/c to Round
1	5.8	0.5
2	7	0.5
3	4.4	0.39
4	5.6	0.43

9.5 Packet Delivery Ratio without Optimization

The contrast of packet distribution ratios of packet delivery by iteration ratio and packet delivery ratio by round demonstrates above table 5 and below figure 5. The blue line shows the ratio of packet delivery by iteration and the red line shows the packet delivery ratio by round.

Table 5: PDR without optimization

S. No.	a/c to Iteration	a/c to Round
1	97.6	96.5
2	99	96.4
3	98	97
4	96.9	96.9

9.6 Packet Delivery Ratio with Optimization

The packet distribution ratio as seen above table 6 and below map 6 in relation to the packet supply ratio by iteration and the packet delivery ratio by round with optimization. The blue line shows the ratio of packet delivery by iteration and the red line shows the packet delivery ratio by round.

Table 6: PDR with optimization

S. No.	a/c to Iteration	a/c to Round
1	99	97
2	98.7	97.2
3	97.9	96.8
4	98.9	96.3

Conclusion

AI approaches are getting more involved in delivering protection and in understanding. As it is acknowledged, computer defence has numerous attacks which must be stopped. The use of the genetic algorithm with the fuzzy rule set was used in this work to identify and avoid attacks in the network. The proposed algorithm has been concluded to have a reasonable accuracy score. DDoS is one of the most striking cyber threats that cloud storage and traditional servers will target. DDoS spam detection with three elements: a rating algorithm series, a distributed system and a fuzzy logic. Firstly, the performance of classification techniques is calculated. Second, different mitigation scenarios, different sizes of data gathering and the number of classification methods assess the impact of the distributed system. Thirdly, it is examined the validation and viability of the fuzzy analysis.

References

[1] Sharma, T. and Banga, V. K., March 2013, "Efficient and Enhanced Algorithm in Cloud Computing", *International Journal of Soft Computing and Engineering (IJSCE),* Volume-3, Issue-1, pp. 385-390.

[2] K. Subhashini, and G. Subbalakshmi, 2012, “Tracing sources of DDoS attacks in IP networks using machine learning automatic defence system,” *International. Journal. Electron. Commun. Comput.* Eng., 3: 164–169 .

[3] H. J. Kashyap, and D. K. Bhattacharyya, 2012 “,A DDoS attack detection mechanism based on protocol specific traffic features.”, *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology*, Coimbatore, India, 26-28 October, pp. 194–200. ACM.

[4] S. M. T. Nezhad, M. Nazari, and E. A. Gharavol, 2016, “A Novel DoS and DDoS Attacks Detection Algorithm Using ARIMA Time Series Model and Chaotic System in Computer Networks,” *IEEE Commun*. Lett., vol. 20, no. 4, pp. 700–703.

[5] K. M. Prasad, A. R. M. Reddy, and K. V. Rao, 2013, “Discriminating DDoS Attack traffic from Flash Crowds on Internet Threat Monitors (ITM) Using Entropy variations,” African J. Comput. ICT, vol. 6, no. 2, pp. 53–62.

[6] M. Mizukoshi and M. Munetomo, 2015 ,"Distributed denial of services attack protection system with genetic algorithms on Hadoop cluster computing framework," 2015 *IEEE Congress on Evolutionary Computation, CEC 2015 - Proceedings,* pp. 1575–1580.

[7] M. Bazm, R. Khatoun, Y. Begriche, L. Khoukhi, X. Chen, and A. Serhrouchni, 2015,"Malicious virtual machines detection through a clustering approach," *Proceedings of 2015 International Conference on Cloud Computing Technologies and Applications,* CloudTech .

[8] Dilpreet kaur and Sukhpreet Kaur (2013). Study on User Future Request Prediction Methods Using Web Usage Mining. IJCER.

[9] Rimmy Chuchra, Bharti Mehta and Sumandeep Kaur (2013). Use of web Mining in Network Security. *IJETAE.*

[10] S.Mirdula and D.Manivannan (2013). Neural Network Approach for Web Usage Mining. *IJRTE.*

[11] Diallo Abdoulaye Kindy and Al-Sakib Khan Pathan (2012). A Detailed Survey on Various Aspects of SQL Injection in Web Applications: Vulnerabilities, Innovative Attacks, and Remedies.

[12] Pallavi Asrodia and Hemlata Patel (2012). Network Traffic Analysis Using Packet Sniffer. *International Journal of Engineering Research and Applications (IJERA).* Vol. 2, Issue 3, pp.854-856.

[13] D. Vydeki and R. S. Bhuvaneswaran, , 2013, "Effect of clustering in designing a fuzzy based hybrid intrusion detection system for mobile ad hoc networks", *Journal of Computer Science,* vol. 9, no. 4pp. 521-525.

[14] Guo Y and Perreau S. 2010, "Detect DDoS flooding attacks in mobile ad hoc networks". *Int J Secur Network*; 5(4): 259–269.

[15] C., K. Hwang and W. Ku, 2007. "Collaborative detection of DDoS attacks over multiple network domains". *IEEE Trans. Parallel Distributed Syst*., 18: 1649-1662.

[16] Pravin Kshirsagar, Nagaraj Balakrishnan & Arpit Deepak Yadav (2020) Modelling of optimised neural network for classification and prediction of benchmark datasets, Computer Methods in Biomechanics and Biomedical Engineering: Imaging & Visualization, 8:4, 426-435, DOI: 10.1080/21681163.2019.1711457.

[17] Pravin Kshirsagar, Sudhir Akojwar & Nidhi Bajaj(2020),"A hybridised neural network and optimisation algorithms for prediction and classification of neurological disorders", International Journal of Biomedical Engineering and Technology Volume 28, Issue 4 ,DOI: 10.1504/IJBET.2018.095981

Figures

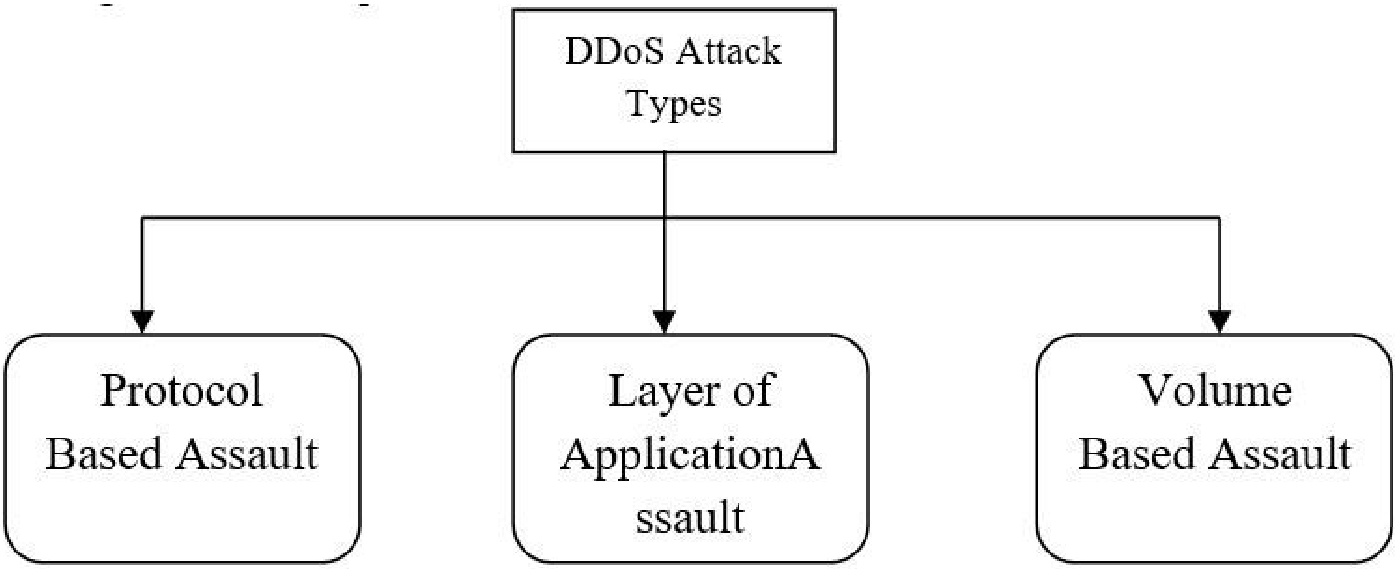

Figure 1

DDoS Attack Types

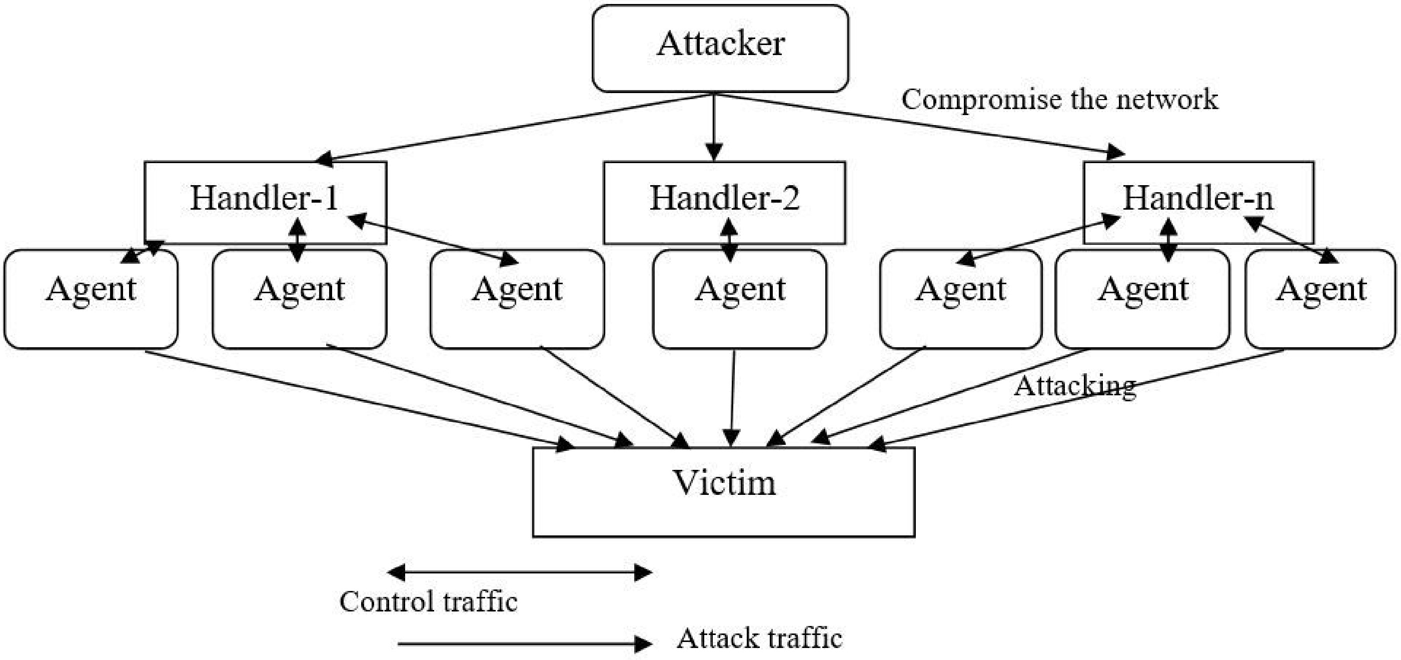

Figure 2

Architecture of DDoS attack

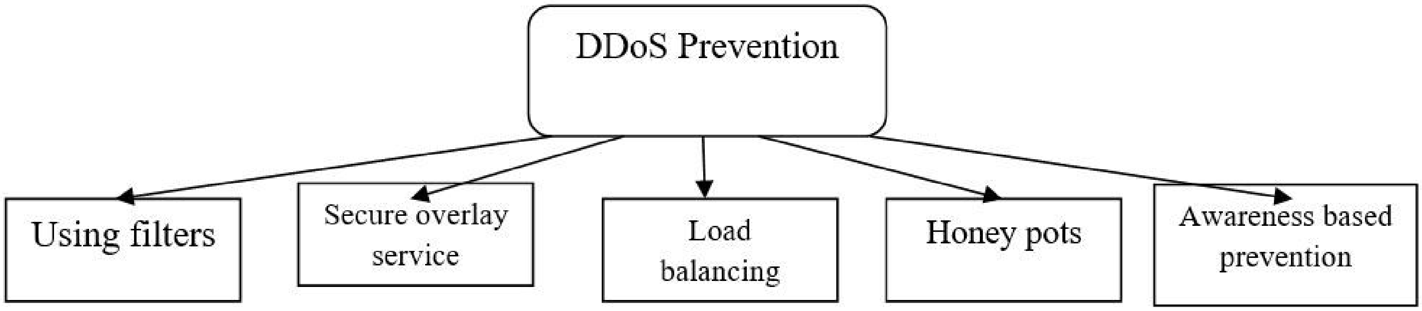

Figure 3

DDoS attack prevention

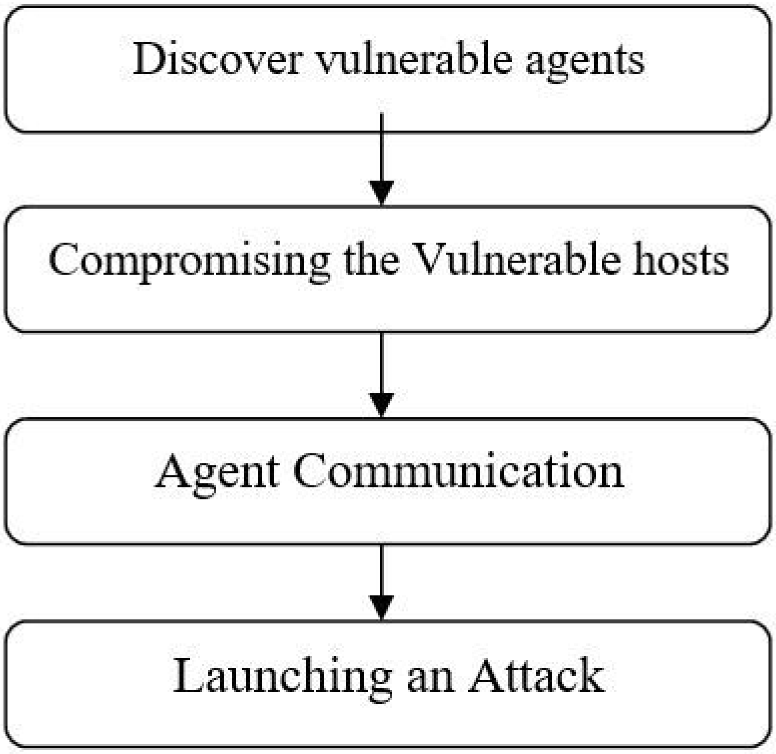

Figure 4

Phases of performing DDoS Attack

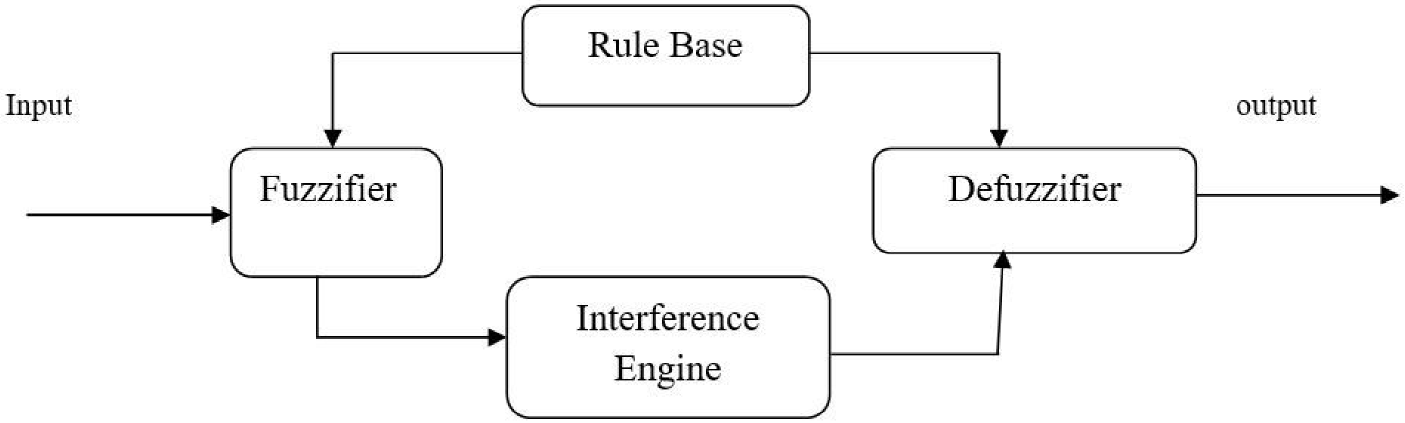

Figure 5

Architecture of Fuzzy Logic

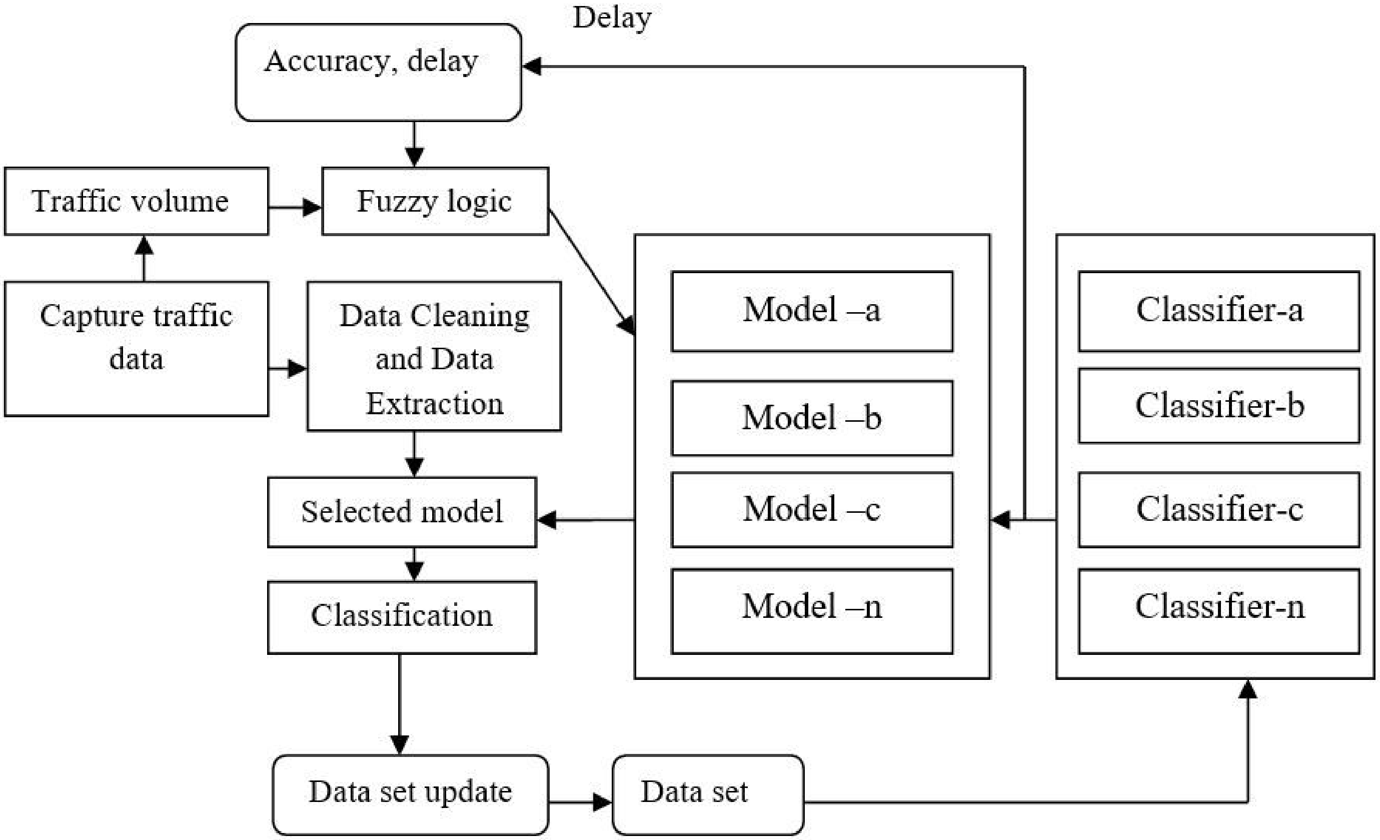

Figure 6

system workflow

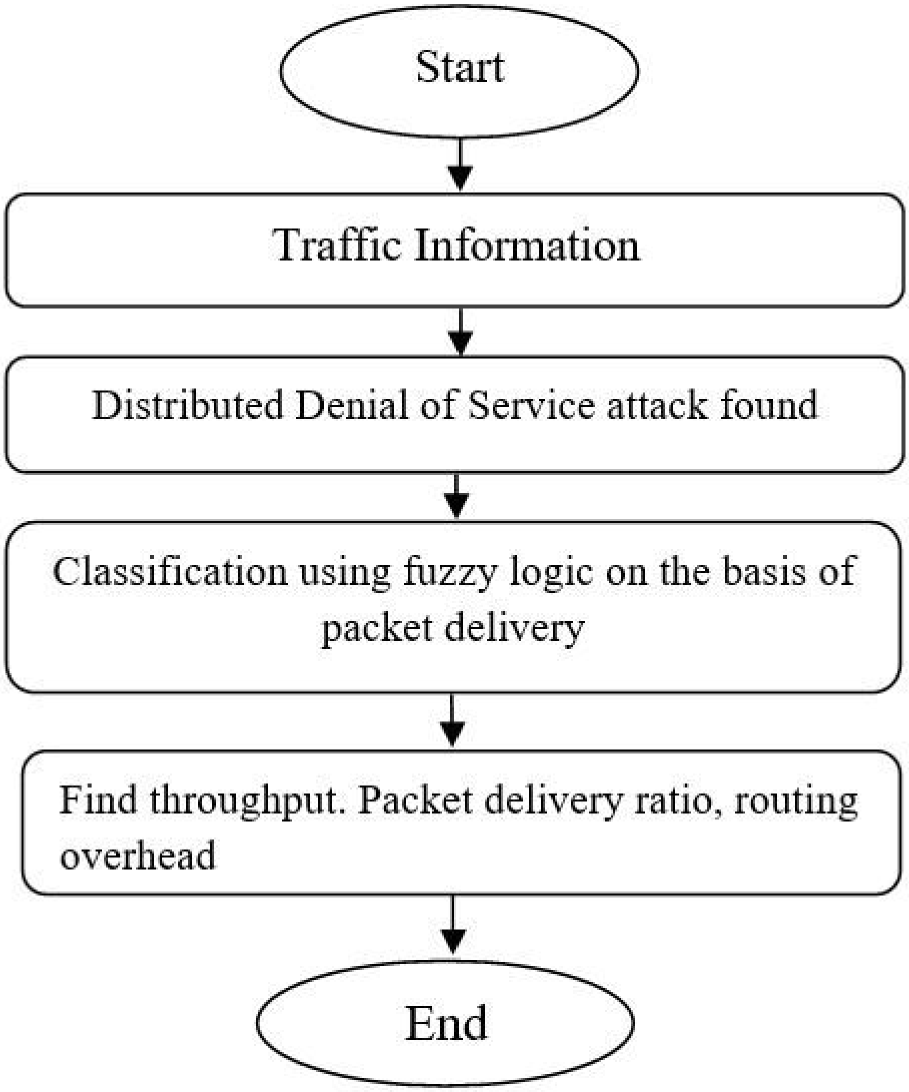
Start
Traffic Information
Distributed Denial of Service attack found
Classification using fuzzy logic on the basis of packet delivery
Find throughput. Packet delivery ratio, routing overhead
End

Figure 7

Methodology Flow Chart