FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks

Beslin Pajila (beslin.kits@gmail.com)
Francis Xavier Engineering College https://orcid.org/0000-0002-3905-2460
E. Golden Julie
Regional Campus, Anna University Tirunelveli
Y. Harold Robinson
Vellore Institute of Technology: VIT University

Research Article

Keywords: Wireless Sensor Networks, type 1 Fuzzy logic, type 2 fuzzy logic, DDoS (Distributed Denial of Service) attack, Network lifetime, Energy Consumption.

Posted Date: March 25th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-217674/v1

Version of Record: A version of this preprint was published at Wireless Personal Communications on September 3rd, 2021. See the published version at https://doi.org/10.1007/s11277-021-09040-8.

FBDR-Fuzzy based DDoS attack Detection and Recovery mechanism for wireless sensor networks

P.J.Beslin Pajila*, E. Golden Julie[1], Y. Harold Robinson[2]

Assistant Professor, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu, India*

Assistant Professor, Department of Computer Science and Engineering, Regional campus, Anna university, Tirunelveli.627007, Tamil Nadu, India[1]

School of Information Technology and Engineering, Vellore Institute of Technology, Vellore[2]

Corresponding author. Tel.: +91 8056458326 E-mail address: beslin.kits@gmail.com*

Abstract

Wireless sensor networks (WSN) is considering as one of the exploring technology. WSN has a large number of sensor nodes, which sense the environment and collect the data. The collected data are sending to the sink through the intermediate nodes. Since the sensors node data are exposed to the internet, there is a possibility of vulnerability in the WSN. The common attack that affects most of the sensor nodes is the DDoS attack. In this paper aims to identify the DDoS attack quickly and to recover sensors using the fuzzy logic mechanism. In the Fuzzy based DDoS attack Detection and Recovery mechanism (FBDR) method uses type 1 fuzzy-logic to detect the occurrence of DDoS attack in a node. Similarly fuzzy- type 2 is used for recovery DDoS attack. Both the type 1 fuzzy-based rule and type 2 fuzzy-based rule perform well in terms of identifying the DDoS attack and recover the DDoS attack. It also helps to reduce the energy consumption of each node and improves the lifetime of the network. The proposed FBDR scheme is compared with other related schemes. The experimental results represent that the FBDR method works better than other similar schemes.

Keywords: Wireless Sensor Networks, type 1 Fuzzy logic, type 2 fuzzy logic, DDoS (Distributed Denial of Service) attack, Network lifetime, Energy Consumption.

1. Introduction

In day to day life, Wireless Sensor Networks (WSN) is one of the recent developing areas. It is dynamic, quick to deploy and straight forward. It is considered as an emerging technique because of the cheap price and productivity [1].WSN has many sensor nodes, these sensor nodes are deployed in the environment to gather data and the gathered data can be sent to

sink for further processing. The sink examines and integrates the data after receiving it from the sensor node. The sink node has a connection to the outside world (end-user) through the internet [2]. In the Internet of Things (IoT) technology which contains sensor nodes for collect data, the same collected data can be forwarded through another sensor to till it reach the sink [3]. The Nodes in WSN are usually deployed in static or dynamic with limited mobility, homogeneous or heterogeneous. The static sensor nodes are deployed in the fixed position, there is no mobility. The mobile node has mobility and the cost of the hardware is high and it utilizes more energy. The heterogeneous sensor nodes have different battery power for each node in the sensor network. In homogeneous sensor nodes, each node will have the same sensing range, same battery power, communication range, power in handling capability that homogeneous sensor nodes with mobility are the better option for real-time applications. WSN has wide-ranging applications for gathering data and data transmission in the military, health care, smart grid, surveillance, etc. They are exposed to security attacks due to security reasons for effective security measures are needed to secure the sensor nodes [4].

WSN is used to monitoring the communication between the sender and receiver. The communication contains the transmission of sensed data. During passive attack never changes any data during the transmission. So it is difficult to detect the passive attack. The active attack is on the other hand usually modifies the data that is transferred between the sender and the receiver [5]. The DDoS attack, Node replication, Masquerade attack, Replay attack, Worm node, Sybil, Sinkhole, etc are some of the active attacks. Among the different active attacks, DDoS attack is one which affects the performance of WSN drastically, since it will flood the target node with a large number of packets so that the node will not be able to accept genuine requests[6]. The DDoS attack has more number of zombies so that it can create heavy traffic in the network. The zombie can also spoof the IP address and make it come under attacker control [7].

In a DDoS attack, the attacker uses multiple sources to send packets to the target node which results in more battery power usage of the target node. Because the user is flooded with more number of resources leads to less responsiveness and it consumes more energy [8]. The software used to perform DDoS attacks will have very basic logic structures and fewer memory sizes which make them extremely easy to hide and enforce. Moreover, DDoS attacks are

constantly changing their methods to overcome security systems created by network managers and researchers who are already in constant alert to alter their methodologies in handling new attacks [9]. In a distributed environment, since the traffic is distributed, it is hard to differentiate normal packets and illegitimate packets. So it is impossible to identify and stop this DDoS attack. The damage caused by a DDoS attack may lead to network or system shut down, rapid battery drainage of the sensor nodes and denial of services. Because of these issues, DDoS attack is considered as one of the serious attacks now a day's [10].

To identify the DDoS attack we use the fuzzy-based logic system. This system is considered as the most effective attack detection method, which resolves with imprecise and vague boundaries among the normal traffic and various levels of attacks. It accurately detects the occurrence of the attack and it also identifies the strength of the attack [11]. In the early 1990's fuzzy system grown because they are increasingly willing to increase systems with adaptation capabilities. The growth has created a variety of fuzzy system that makes us solve various types of problems in different application area [12]. In this paper, we discuss the detection and recovery from DDoS attacks.

The main contribution of the paper is

- ✓ Type1 Fuzzy-based rule is framed to detect DDos attacks with the input values of Energy Consumption, Response time and Packet count.
- ✓ The recovery model is constructed that the DDos attacked node will be redirected to the sink using the alternate path.
- ✓ The identification of alternate path and the sink path are computed using the Type2 Fuzzy-based rule.

The rest of the paper is organized as follows. In section 2, we present various fuzzy and machine learning techniques and comparative study between them. In section 3, we discussed the proposed fuzzy-based system. Section 4 contains the simulation results and performance evaluation and finally, section 5 covers the conclusion respectively.

2. Related works

The detection of a DDoS attack in WSN is discussed in the literature survey. Xia Zhengmin, Jianhua Li, Junhua Tang [11] proposed an intelligent fuzzy logic method which has two stages. The first stage is, the attack identification and the second stage is intelligent fuzzy logic, which was used for deciding the strength of DDoS flood attack. During the attack identification, for each new traffic, the co-efficient of the wavelet and SIC statistic was updated. SIC is the technique used to evaluate repeatedly the network change-point. After identification, the network traffic is segmented into pieces and then the strength of the attack was identified based on fuzzy logic. The Hurst parameter also used to evaluate the strength of the DDoS flood attack. An intelligent DDoS judgement method [13] was proposed to detect the DDoS attack based on judgement. The Hurst parameter is calculated based on VTP, RVTP and FRVTP. The judgement is made by the result obtained from many DDoS attacks which contain various intensity in the testbed. They analyzed the FRVTP method and traditional methods. From the comparative analysis made, it was found the FRVTP method given a better result in real-time. Fuzzy logic based defence mechanism [14] has four phases. They are learning phase, Traffic analysis, Anomaly detection, and attack prevention. In the learning phase, the rules are created and framed inside the fuzzy system. This system learns the rule that was fed inside it. In the traffic analysis phase, the traffic is analyzed (normal or abnormal traffic) and evaluated based on the rules. In the anomaly detection phase, an alarm was generated if any malicious traffic found. The unwanted packets from the malicious node are discarded traffic in the attack prevention phase. Qian Li et al [15] proposed PCA-RNN method to extract the features of the DDoS attack like flow time, slow connection, flood, etc. It is transformed into a PCA matrix for further analysis. PCA is the most efficient dimension reduction method. The correlated values are converted into values. The values are stored inside RNN to train it and the trained values are used to detect the DDoS attack. ML-based detection method [16] has two modules. The first module is pre-trained; it is already trained to find out the victim machine. The second module is online learning, it was trained by itself and updates the first module day-by-day.

The Fuzzy logic methodology [17] uses the AODV protocol to evaluate different kinds of attacks. Among the attacks, the DDoS attack is identified, based on the transfer speed of data packets, loss of data packets and the delivery ratio. FBDPS method [18], analyze the energy consumption of each node to predict the existence of the malicious node. According to this

method, the nodes are compromised in the MAC layer by DDoS attack. The compromised nodes can be identified by the energy consumption rate. Usually, the malicious node while launching the attack, the energy consumption rate of a node varies. So based on that rate we can easily differentiate the normal node and malicious node. A threshold value is used for the energy consumption and packet delivery rate to classify a different kind of malicious nodes in the MAC layer. A fuzzy Markov chain model is used in FBDPS method to analyze the energy consumption of each sensor node. FLONF method [19] detect different kinds of DDoS attack like land attack, mail bomb attack, smurf attack and ping of death attack. Four different algorithms are used to detect such attacks. The detection is based on the flow rate and the number of flows. The algorithms used in this method detect the DDoS attacks faster and the rules for detecting the attack were also simple. FRI method [20] uses a fuzzy inference system for the detection of a DDoS attack. The fuzzy inference system stores the fuzzy input into the fuzzy set and calculates it. The calculated rules are used to detect the DDoS attack more efficiently.

The IPS based protection method [21] uses fuzzy logic and Q-learning algorithm for detecting and preventing the system from the DDoS attack. It first analyzes the traffic in the network and then examines the DDoS attack utilizing learning method and artificial intelligence. In this approach, the packets are captured and the details of the packets are collected. Then the collected details are stored inside the log files and the reliability index is calculated to identify the risk of the malicious packet. Now the abnormal behaviour of the node can be identified by using neuro-fuzzy rules. The Fuzzy Q-learning method is used for the quick detection of the DDoS attack. The Fuzzy Q-learning method will investigate each packet and checks for any abnormal behaviour in the packets. If any abnormal packets are identified, then those packets will be dropped. Then the result is stored to avoid the system from the same attack in the future. The fuzzy estimator method [22] is used to detect DDoS attack and to identify the IP address of the malicious one. It is identified to avoid further intrusion of DDoS attack. But the identified IP address is not so accurate. In the Bio-inspired Bat algorithm [23] is used to identify the attack as like the bat find its prey even in dark. It is an evolutionary-based algorithm, where each bat denotes a solution. It is the best method to detect the attack even in any situation but prevention is not possible. CNN Ensemble framework [24] encounter the most sophisticated DDoS attack in SDN and the detection is more accurate. Flexible SDN-based Architecture [25] detect and reduce the Low-Rate DDoS attack. It utilizes six Machine Learning models to train the SDN-

based architecture to detect the attack more accurately. And the detection rate is up to 95%. MSCD method [26] have three parts to identifies the clone attack . The first part is to build the path of the head node and the second part is to decide the witness for each node in the network. Finally the third part is used to verify the legitimacy of the messages before sending to the head nod in the witness ring. Novel intrusion detection technique [27] with PD(Pearson's Divergence) is used to detect the intrusion that usually compromises the node. The compromised node exists for a long time in the network so that it can affect and collapse the system. Pearson's Divergence technique is used to detect the attack and it improves the accuracy of the detection.SIP based defence mechanism[28] detects SR-DRDoS attack using IP spoofing technique. This type of attack improves the CPU load to 100%. SIP mechanism has three modules named as statistics, Inspection and Action to identify the abnormal traffic to reduces the CPU load. The statistics module collects the various traffic, Inspection module compares the traffic and finally action module identify the abnormal traffic(SR-DRDoS attack) and drop or block it. IHSM Scheme [29] proposed three algorithms namely, EMABRD, SACOP and FZKA. EMABRD algorithm uses energy utilization threshold to identify the replica node. The detection rate of malicious node of SACOP algorithm is faster than EMABRD algorithm. FZKA algorithm stores the fingerprint of all the nodes in the cluster head and the finger print of the cluster heads will be stored in the base Station. So the cluster head and Base station involve in the detection of malicious node. FZKA algorithm also reduces the storage and communication overheads. OLWPRAD method[30] uses online dataset to detect the anomalies. It uses Principal Component Analysis (PCA) to manage the data. The detection of abnormal data in OLWPRAD can be done by dynamic threshold method. AIS-IDS method[31] is an effective approach to detect and reduce different kinds of flooding attack. It reduces the anomalies by dropping and blocking it. A distributed estimator framework [32] is used to detect randomly acquiring DoS attack or Data integrity attack. Each sensor is embedded with an statistical learning based detctor and it is capable enough to detect the attacks effectively. SKG Scheme [33] identify the active attacks while generating secret key. This scheme uses SVD technique and private pilot to identify the various active attacks. It usually authenticate the sender for protection against the active attacks. The DLDM Framework structure [34] is used to identify the different kinds of DDoS attack effectively, thereby it improves the throughput and it also reduces the energy consumption. EPSM [35] is proposed to detect the wormhole attack and it also used to minimize

the energy consumption and the overhead of the network. The EPSM method has two stages to identify the wormhole attack. If both the stages are unsuccessful, it means that the attack is identified and the blacklist is announced. The MSIDN method[36] is used to identified and reduce the Distributed Denial of Service attacks and Flooding based DoS in Named Data Networking. While Mitigation of the attacks it will never damage the reliable users. It also reduces the traffic and network overhead. Lower-edge routers are used for stopping the malicious node from the origin. SDN-EHCND Mechanisms[37] is used to detect and keep away from the unnecessary nodes which occur because of cloning attack. The HCND method identify clone node and remove the clone attack available in the Wireless Networks. Superimposed SDIS junction code is used to find out the clones locally and globally. SLGBM method [38] is an intrusion detection method, it has two main algorithms they SLS algorithm and Light GBM algorithm.SLS algorithm minimize the communication overhead and the Light GBM algorithm detect the various network attacks in the WSN effectively.

The summary of the related works is represented in table 1.

Fuzzy Method	**Parameter**	**Advantages**	**Disadvantages**
Intelligent fuzzy logic method[11]	SIC statistics and Hurst Parameter	Detect DDoS attack very fast, successful and brilliantly.	More time is utilized While calculating the change point of the network using SIC.
An intelligent DDoS judgement method[13]	Hurst Parameter	Detect DDoS attack in real-time	It lacks in self adaptability.
Fuzzy logic based defence mechanism[14]	Predefined learning rule(traffic parameters)	Predefined learning rule detects and mitigates DDoS attack very effectively.	Difficult to get rid of sophisticated attacks.
PCA-RNN method [15]	Prediction Time and Performance metrics	Reduces the time of detection. Good accuracy in detection	Less performance in the detection of the attack with real-time datasets.
ML-based detection method [16]	Statistical features	Detect DDoS attack with very low false positives and high	The legitimate use of the machine is reduced

		accuracy	
Fuzzy logic methodology [17]	Trust value, Data Packet transfer rate, The delivery ratio of the data packet	Different types of attacks are detected by using a single method.	Attack recovery and prevention method are not available
FBDPS[18]	Energy consumption rate	Detection of the DDoS attack was made based on the energy consumption of the node Enhance reliability and accuracy	No prevention method
FLONF [19]	Flow rate, Flow size in ICMP protocol is high	Very simple rules are used for detection. The detection rate is high.	No prevention method
FRI method [20]	Packet size, packet count, Packet rate	Reduce false positive rate value	No prevention Method
IPS based Protection [21]	Fuzzy logic and Q-learning strategy	Security against Sophisticated attack, Less buffer size	Difficult to identify other attacks.
Fuzzy estimator method [22]	Packet arrival time	Detect the DDoS before the resources consumed by the attack	It is not so accurate in identifying the attacking IP address within the time limits
Bio-inspired Bat algorithm[23]	Classification of traffic	Fast detection of DDoS attack	No prevention method
CNN Ensemble framework [24]	RNN,LSTM,CNN	Detection is more accurate	Prevention method is not available.
Flexible SDN-based Architecture [25]	Random Tree, Random Forest, Support Vector Machine	Detection is accurate ie., upto 95 % and it also mitigate the LR-DDoS attack	Prevention method is not available

MSCD method [26]	Communication load	Probability of detecting the clone attack is more	Prevention is not available and nodes are not distributed uniformly in the network.
Novel intrusion detection technique with PD(Pearson's Divergence) [27]	Probability and probability Density Function	It increases the detection accuracy	Prevention method is not available.
SIP based defence mechanism[28]	Statistics, Inspection and Action	It detect the SR-DRDoS attack more quickly and thereby reduces the CPU load.	Prevention method is not available.
IHSM Scheme [29]	Energy Consumption, Fingerprint of nodes	FZKA algorithm performs better than the other algorithms and it improves the detection rate.	Prevention method is not available.
OLWPRAD method[30]	Principal Component Analysis	The detection rate is good compared to other machine learning algorithm.	Prevention method is not available.
AIS-IDS method[31]	Fuzzy logic	Detect and reduce the flooding attacks more effectively	Need to implement the method in real time environment and prevention method is not available.
Distributed Estimator Framework [32]	False-data detector	Detect Dos attacks and linear attacks effectively.	Difficult to detect complex coordinated attacks and prevention method is also not available.
SKG Scheme [33]	SVD technique	Identify different kinds	Mitigation of the attack

	Private pilot	of active attacks more effectively.	is not available.
DLDM Framework structure [34]	Deep Learning techniques is used.	Detect the DoS attack effectively and improves the throughput.	Mitigation of the attack is not available.
The EPSM method [35]	Secured AODV Routing Protocol Algorithm is used	Detect the wormhole attack and also used to reduce the energy consumption.	Mitigation and prevention method is not available.
The MSIDN method[36]	hop-by-hop signing and verification process. lower-edge routers	Identify and reduce DDoS attacks anf flooding based attacks very effectively.	Prevention measures is not available. Collaborative actions like rate limiting and increased block periods should be included.
SDN-EHCND Mechanisms[37]	Hybrid Clone node detection mechanism Superimposed SDIS junction code and verification process	Detect the cloning attack more effectively	Attack mitigation is not available.
SLGBM method [38]	SLS algorithm Light GBM algorithm machine learning algorithms	Detect the various network attacks effectively. Accuracy rate is good. calculation time is low and improve the overall performance.	Running time is more and it does not mitigate the attacks effectively.

Table 1. Summary of related works

3. Fuzzy Based DDoS Detection and Recovery Method

3.1 Proposed work

Initially, the network has to be formed. All the sensor nodes are randomly deployed with the same energy within the specified network area. Nodes can sense the environment in the form of data, these data packets send to the sink. The packets are sent to the sink through the path which has been already calculated and identified; usually, the path is the collection of nodes. If any node in the path consumes more energy, and is flooded with data packets and has high response time then we can assume that the node is affected by DDoS attack. This prediction is made by type 1 fuzzy-based rule where energy consumption, response time and packet count is given as the input parameters. If a DDoS attack is detected, we need to mark that particular node in that path as the dead node. To avoid the loss of the packet, send the packet to the sink through the alternate path. Identify the possible alternate possible paths to the sink. These paths can be identified based on a type1 fuzzy-based rule where distance, energy consumption, and packet size is given as the input parameters for the type 2 fuzzy-based rule.

3.2 System Model:

- The nodes are deployed randomly inside the network.
- Each sensor node is mobility in nature so that it can move inside the network area.
- Each sensor node is homogenous.
- A sink may be available anywhere inside the network area.

The nodes in the WSN are not protected against the DDoS attack. Usually, this attack drains the battery power of the sensor nodes and reduces its lifetime. To detect the DDoS attack and to secure the nodes from this attack, Fuzzy based DDoS detection and Recovery method has been proposed. It uses the type 1 fuzzy-based rule to detect the DDoS attack and type 2 Fuzzy based rule to secure the nodes. The workflow diagram for the proposed is shown in figure 1.

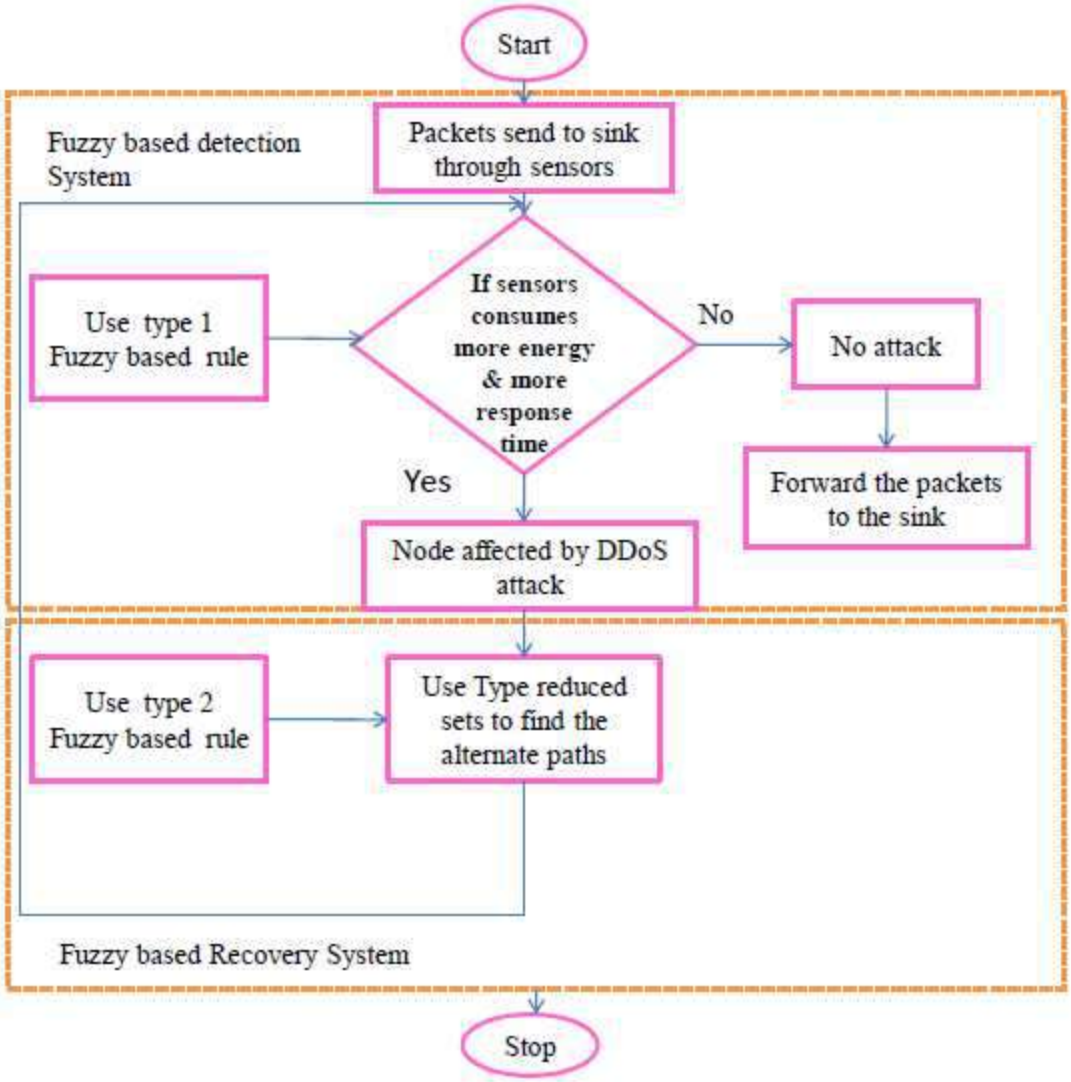

Figure 1. The workflow of the proposed system

3.3 Detection Method

The sensor node transmits the data packets through the path of nodes to reach the sink. Before passing the packets to a node, it is examined and evaluated based on the fuzzy logic. It has three input variables. They are Energy_consumption, Response_time, and Packet_count. Based on the type1 fuzzy rule, the particular node was examined whether a DDoS attack occurs or not. Fuzzy logic is used to determine the occurrence of DDoS attacks in a node based on a decision. It mainly uses true or false and “truth” degree.

The output is obtained based on the three inputs provided to the type1 fuzzy-based rule. The three inputs are considered as parameters and each input parameter has membership functions. The membership function is mainly utilized for executing the element's fuzziness in

the fuzzy set. The fuzzy set is used for solving a problem depending on its experience. The output of type 1 fuzzy-based system depends on the input supplied to the fuzzy system.

The block diagram of Type1 Fuzzy based DDoS attack detection system is shown in figure 2, it has three input parameters they are Energy_consumption, Response_time, and Packet_count. The input parameters are supplied for the fuzzification process to obtain the fuzzy-based input value with the information provided by knowledge-based rule. Then the fuzzy-based value is sent for the defuzzification process and finally, the output is obtained by the defuzzification process. Based on the obtained output value we can verify whether there is a DDoS attack inside the network.

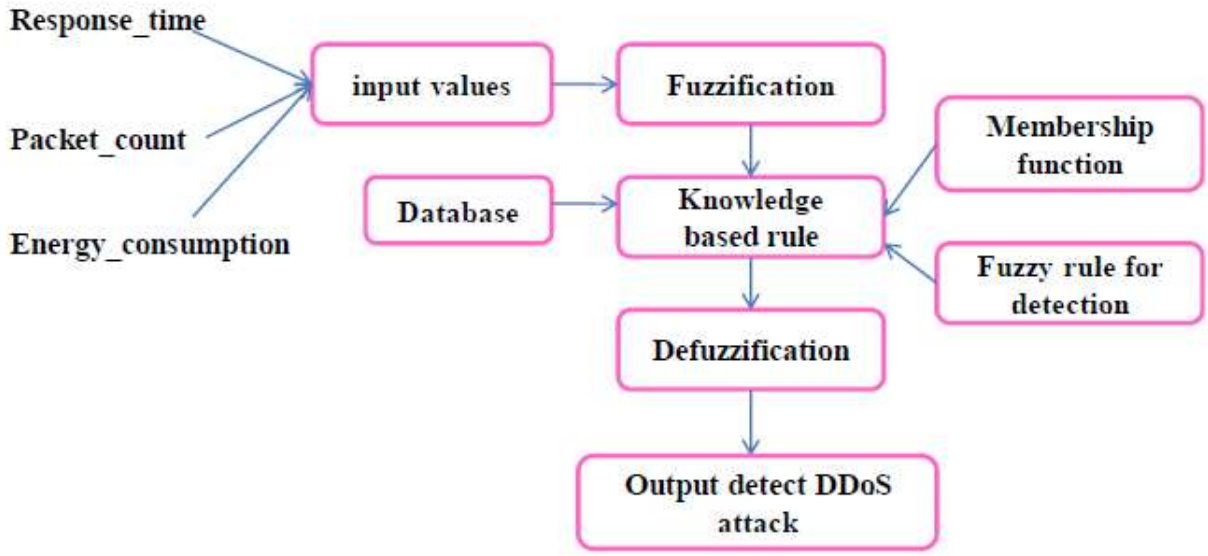

Figure 2. Type1 Fuzzy based DDoS attack detection system

The type1 fuzzy-based detection system also has three inputs parameters and each parameter has three membership functions. Based on the input parameters and the membership functions 27 rules are formed. Table 2 represents the fuzzy rule for various inputs and outputs.

Rule No.	Response Time	Energy consumption	Packet Count	DDoS attack Status
1	Less	Low	Minimum	No_attack
2	Less	Medium	Normal	No_attack
3	Less	Medium	Maximum	Predicted
4	Less	Medium	Minimum	No_attack

5	Less	Low	Normal	No_attack
6	Less	Low	Maximum	Predicted
7	Less	High	Minimum	No_attack
8	Less	High	Normal	Predicted
9	Less	High	Maximum	Occurred
10	Normal	Low	Maximum	Predicted
11	Normal	Low	Normal	No_attack
12	Normal	Low	Minimum	No_attack
13	Normal	High	Minimum	Predicted
14	Normal	High	Normal	Predicted
15	Normal	High	Maximum	Occurred
16	Normal	Medium	Maximum	Occurred
17	Normal	Medium	Minimum	No_attack
18	Normal	Medium	Normal	No_attack
19	More	High	Minimum	No_attack
20	More	High	Normal	Predicted
21	More	High	Maximum	Occurred
22	More	Medium	Maximum	Occurred
23	More	Medium	Normal	No_attack
24	More	Medium	Minimum	No_attack
25	More	Low	Minimum	No_attack
26	More	Low	Normal	No_attack
27	More	Low	Maximum	Predicted

Table 2 Rules for Type1 Fuzzy based Detection System

The algorithm1, which is mention below, represents the type 1 fuzzy-based DDoS attack detection algorithm. The current node collects the information from the next nearest hop to

which it is about to send its packets and verifies the information using type 1 fuzzy based rule and decides whether the node had been subjected to DDoS attack or not.

```
for(x1=currentnode; x1!=sink; x1++)
        for (y1=currentnode; y1!=sink; y1++)
                get nearest_hop(response_time,energy_consumption,packet_count);
                mem_func();
                fuz_rule();
        end for
end for
if (energy_consumption > Th_energy && response_time > Th_response_time &&
packet_count > Th_packet_count)
        node is declared as ddos attack
        recover()
else
        normal broadcast
end if
```

Algorithm 1: Type1 Fuzzy based DDoS attack Detection algorithm

Input Membership functions

The input and output member functions are framed by trapezoidal and triangular functions respectively. The Response_time membership function has variables like more, normal and less for evaluating the response time as shown in figure 3.

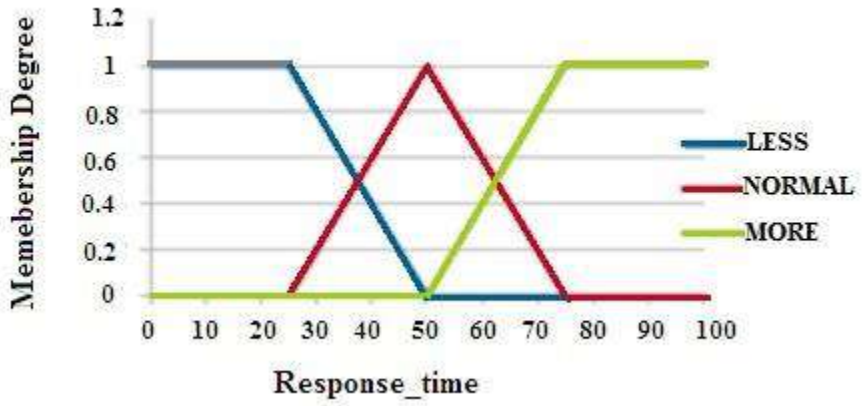

Figure 3. Membership function of Response_time

The Measurement of the membership function of Response_time for various variables like more, normal and less are represented in equations 1, 2 and 3.

$$\text{Response}_{\text{less}}(r) = \begin{cases} 1 & , r \leq 20 \\ \frac{40-r}{20} & , 20 < r \end{cases} \quad (1)$$

$$\text{Response}_{\text{normal}}(r) = \begin{cases} \frac{r-40}{15} & , 40 < r \leq 55 \\ 1 & , 55 \leq r \leq 65 \\ \frac{80-r}{15} & , 65 \leq r < 80 \end{cases} \quad (2)$$

$$\text{Response}_{\text{more}}(r) = \begin{cases} \frac{r-80}{10} & , 80 < r < 90 \\ 1 & , 90 \leq r \leq 100 \end{cases} \quad (3)$$

The Energy_consumption membership function has variables like high, medium and low for evaluating the energy consumption as shown in figure 4.

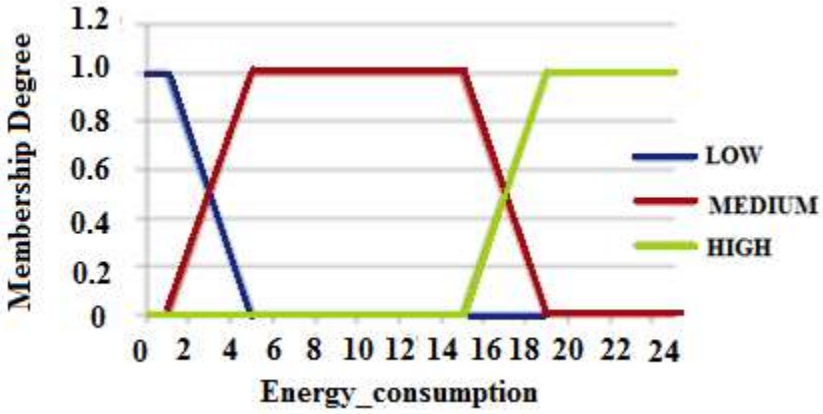

Figure 4. Membership function of Energy_consumption

The Measurement of membership functions of Energy_consumption for various variables like high, medium and low are represented in equation 4, 5 and 6.

$$\text{energy}_{\text{low}}(r) = \begin{cases} 1 & , 0 \leq r \leq 10 \\ \frac{20-r}{10} & , 10 < r \leq 20 \end{cases} \quad (4)$$

$$\text{energy}_{\text{medium}}(r) = \begin{cases} \frac{r-20}{3} & , 20 < r < 23 \\ 1 & , 23 \leq r \leq 27 \\ \frac{30-r}{3} & , 27 \leq r \leq 30 \end{cases} \quad (5)$$

$$\text{energy}_{\text{high}}(r) = \begin{cases} \frac{r-30}{7}, 30 < r < 40 \\ 1 \quad\quad ,40 \leq r \leq 49 \end{cases} \quad (6)$$

Similarly, the Packet_count membership function has variables like maximum, normal and minimum for evaluating the packet count as shown in figure 5.

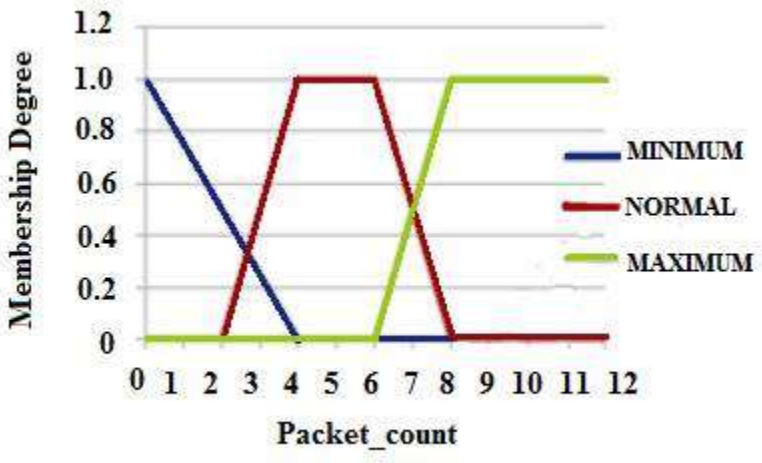

Figure 5. Membership function of Packet_count

The number of packets sent by a normal sensor node and malicious node varies, the packet count of each node can be measured accordingly [11]. The Measurement of the membership function of Packet_count for various variables like maximum, normal and minimum are represented in equation 7, 8 and 9.

$$\text{Packet}_{\text{minimum}}(r) = \begin{cases} \frac{r}{15} \quad\quad ,0 \leq r \leq 15 \\ 1 \quad\quad ,15 \leq r \leq 25 \\ \frac{40-r}{15} \quad ,25 \leq r < 40 \end{cases} \quad (7)$$

$$\text{Packet}_{\text{normal}}(r) = \begin{cases} \frac{r-40}{10}, \quad 40 \leq r \leq 50 \\ 1, \quad\quad 50 \leq r \leq 60 \\ \frac{70-r}{10}, \quad 60 < r \leq 70 \end{cases} \quad (8)$$

$$\text{Packet}_{\text{maximum}}(r) = \begin{cases} \frac{r-70}{10}, & 70 \le r < 80 \\ 1, & 80 \le r \le 90 \\ \frac{100-r}{10}, & 90 < r \le 100 \end{cases} \quad (9)$$

Fuzzy rules are fixed for the constraints of the membership functions like Response_time, Energy_consumption and Packet_count are as shown in figure 6.

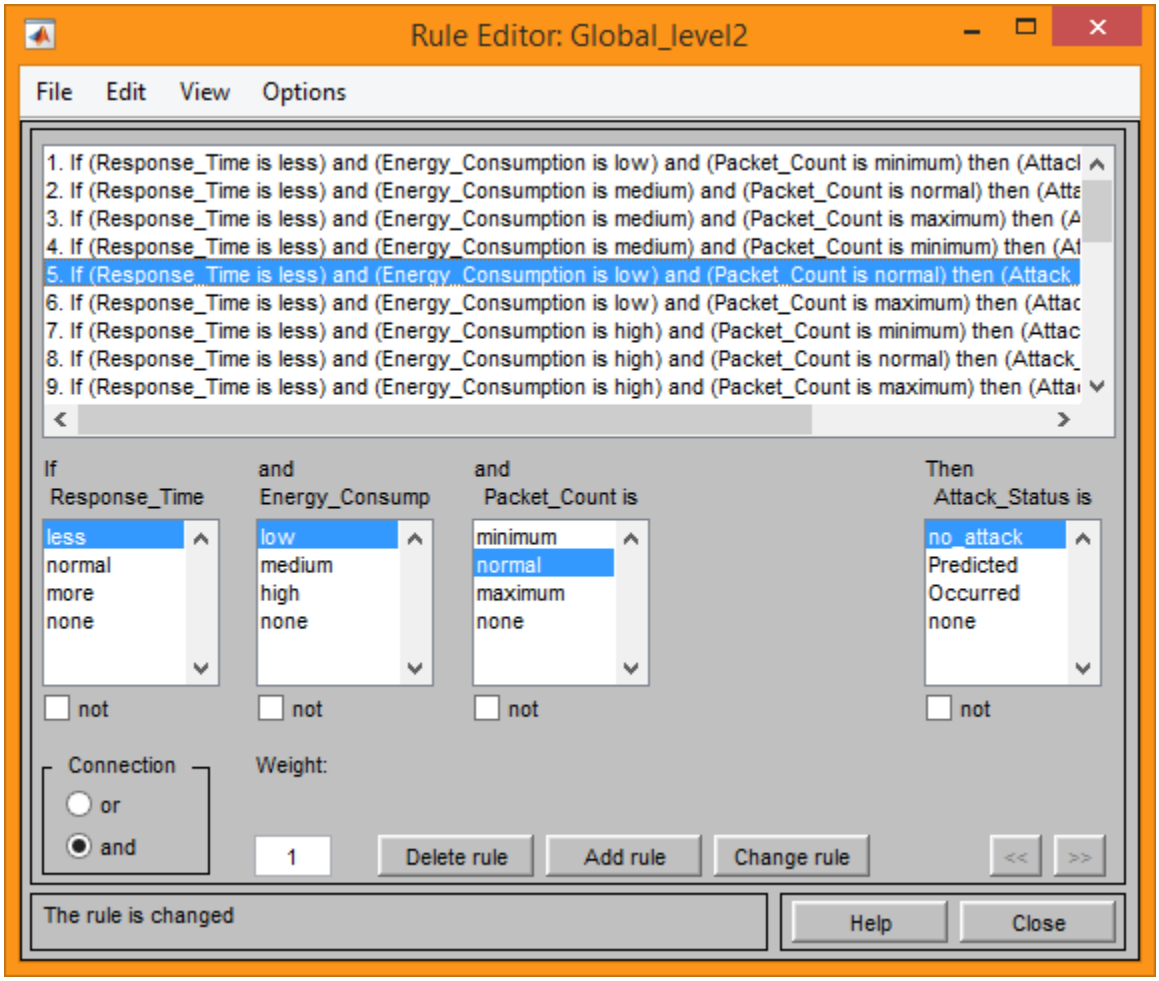

Figure 6. Rule setting for Type1 fuzzy-based DDoS attack detection system

Output Membership functions:

MATLAB's fuzzy rule viewer is shown in figure 7. IF-THEN conditions are used for generating fuzzy rules. The input and output of various membership functions are depicted in the fuzzy table2.

Membership functions for DDoS attack status:

$$\text{DDoS attack}_{\text{status}}(r) = \begin{cases} Occurred, & r = 1 \\ Prediction, & r = 0.5 \\ No\_attack, & r = 0 \end{cases} \quad (10)$$

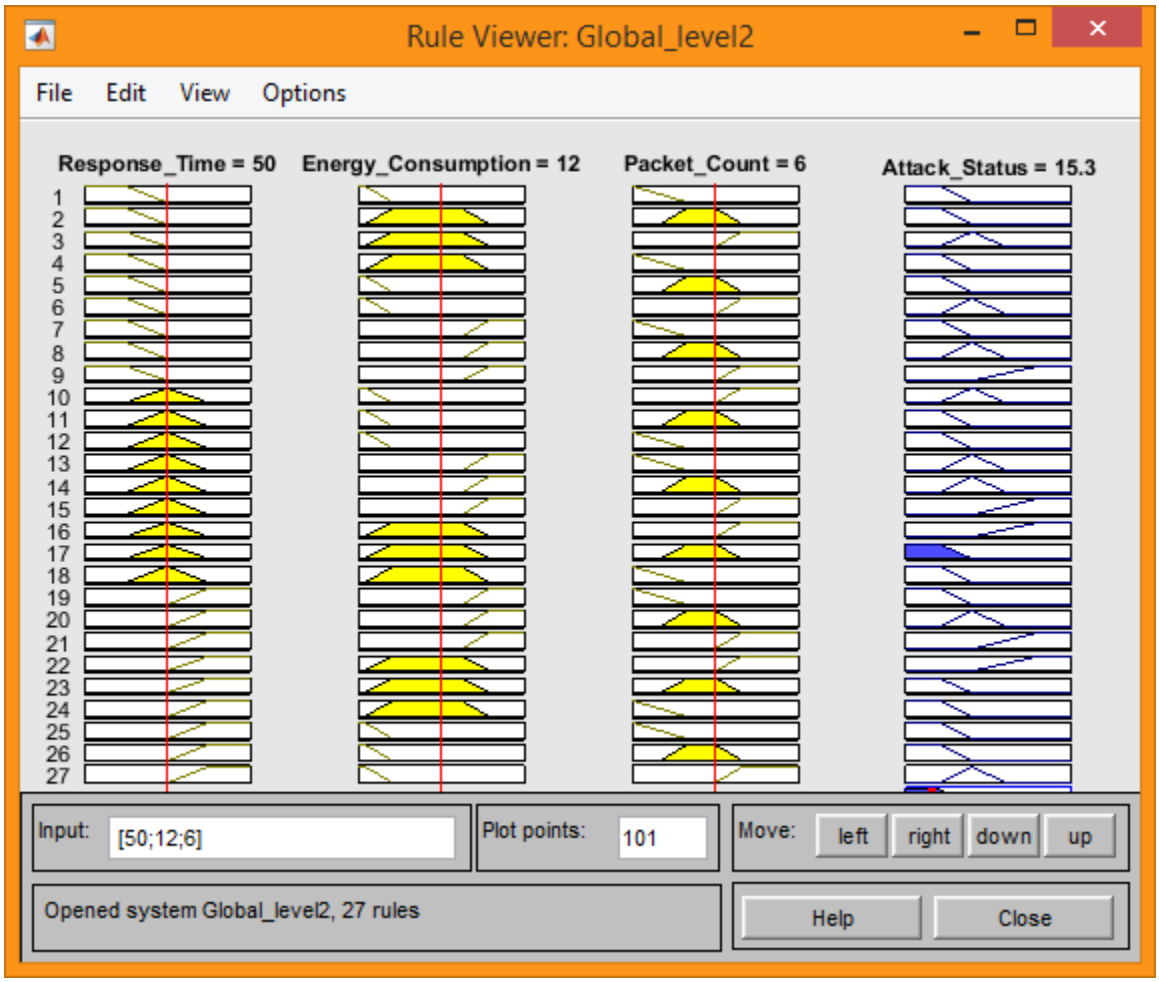

Figure 7. Rule viewer of Type1 Fuzzy based DDoS attack detection system

3.4 Recovery Method

To recover from DDoS attack we have proposed a method in which the packets which are sent to the node that is affected by the DDoS attack will be redirected to the sink through an alternate path. The alternate path is calculated in such a way that it utilizes less energy and with minimum distance. To identify the alternate paths, we use a type2 fuzzy-based rule with the inputs parameters Energy_consumption, Distance, and Packet_size. The block diagram for the type2 fuzzy-based recovery system is represented in figure 8.

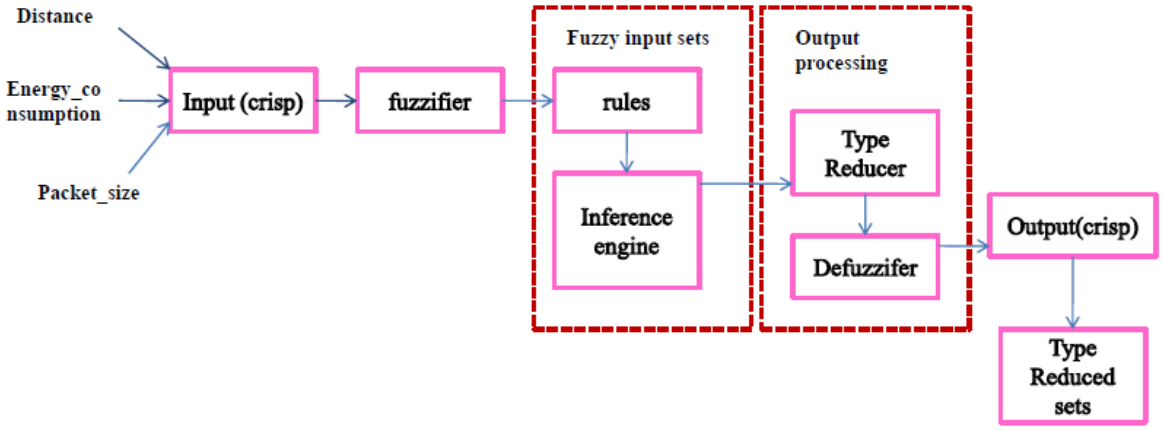

Figure 8 Block diagram of Type2 fuzzy-based recovery system

The fuzzy set has crisp input and it is given to the fuzzifier. The input (crisp) vector Inp' = (Inp_1' . . . . . .Inp_p') are represented as shown below [39]

$$\sigma \ Inp_i(Inp_i) = 1, \ \text{if } Inp_i = Inp_i' \quad (11)$$

$$\sigma \ Inp_i(Inp_i) = 0, \ \text{if } Inp_i \neq Inp_i' \quad (12)$$

The interval of the three inputs are [0,1]. The inputs are Distance, Energy_consumption and the Packet_size. The rules for the fuzzy based recovery system are represented in the table3.

Rule no.	**Distance**	**Energy_consumption**	**Packet_size**	**Sink path identification**	**Alternate path identification**
1	Near	Less	Small	Possible	Yes
2	Near	Less	Medium	Possible	Yes
3	Near	Less	Large	Slight Possible	Yes
4	Near	Medium	Small	Possible	Yes
5	Near	Medium	Medium	Possible	Yes
6	Near	Medium	Large	Not Possible	Yes
7	Near	Huge	Small	Not Possible	No

8	Near	Huge	Medium	Not Possible	No
9	Near	Huge	Large	Not Possible	No
10	Medium	Less	Small	Possible	Yes
11	Medium	Less	Medium	Possible	Yes
12	Medium	Less	Large	Slight Possible	Yes
13	Medium	Medium	Small	Possible	Yes
14	Medium	Medium	Medium	Possible	Yes
15	Medium	Medium	Large	Slight Possible	Yes
16	Medium	Huge	Small	Not Possible	No
17	Medium	Huge	Medium	Not Possible	No
18	Medium	Huge	Large	Not Possible	No
19	Far	Less	Small	Possible	Yes
20	Far	Less	Medium	Possible	Yes
21	Far	Less	Large	Slight Possible	No
22	Far	Medium	Small	Possible	Yes
23	Far	Medium	Medium	Possible	Yes
24	Far	Medium	Large	Slight possible	No
25	Far	Huge	Small	Not possible	No
26	Far	Huge	Medium	Not possible	No
27	Far	Huge	Large	Not possible	No

Table 3.Rules for fuzzy-based recovery system

Based on the assumption the parameter for the input variables like Distance is considered as ip1, Energy_consumption as ip2, and finally Packet_size as ip3. The variables for the outputs are Sink path identification as GP1 and Alternate path identification as GP2.

IF ip1 is FR1
ip2 is FR2

ip3 is FR3

……

ipn is FRn

THEN

jop1 is GP1

jop2 is GP2

Where σFRi(inpi) is the lower membership function and σFRi'(inpi) is the larger membership function.

$$fr(i) = \sigma FR1(inp1) \times \ldots\ldots \times \sigma FRp(inpp) \quad (13)$$

$$fr(i) = \sigma FR1'(inp1) \times \ldots\ldots \times \sigma FRp'(inpp) \quad (14)$$

Defuzzification

$$Dqi(y) = \frac{Dq1(y) + Dqjr(y)}{2} \quad (15)$$

The extended output,

$$Dq_{cos}^{i} = \lceil Dqj1(y), Dqjr(y) \rceil \quad (16)$$

Algorithm 2 represents the type2 fuzzy-based recovery algorithm, which is mainly used to redirect the packets to the sink through the alternate path. The current node collects the information from the next nearest hop to choose the correct path towards the sink. The path towards the sink can be identified based on decision made by type2 fuzzy based rule.

```
for(x=currentnode; x!=sink; x++)
        for (y= currentnode; y!= sink; y++)
                get nearest_nodej(distance,energy_consumption,packet_size);
                membership_fun();
                fuzzy_based_rule2();
        end for
end for
if (distance > Th_distance && energy_consumption > Th_energy && response_time > Th_response_time && packet_size > Th_packet_size)
        recover ()
else
        normal broadcast
end if
```

Algorithm 2: Type2 Fuzzy based Recovery algorithm

The Distance membership function has variables like near, medium and far for evaluating the distance as shown in figure 9.

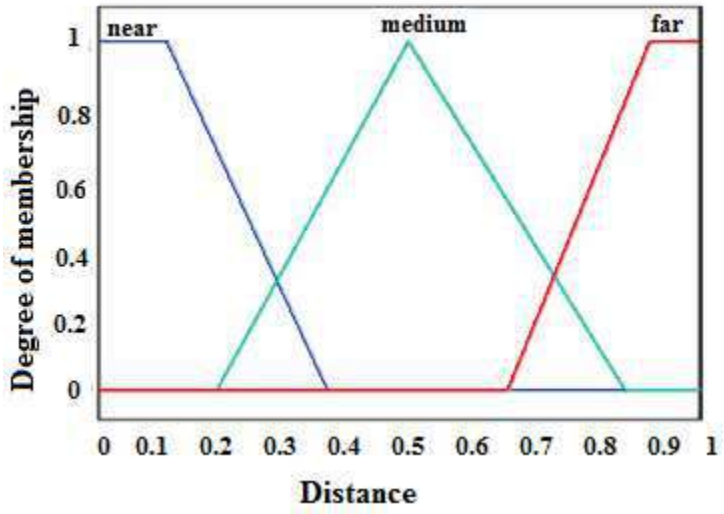

Figure 9. Membership function for Distance

The Energy_consumption membership function has variables like less, medium and huge for evaluating the energy usages as shown in figure 10.

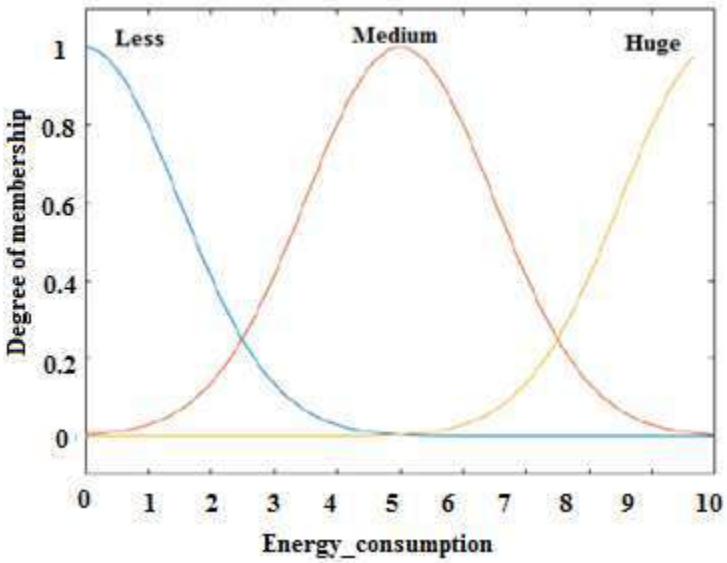

Figure 10. Membership function for Energy_consumption

The Packet_size membership function has variables like small, medium and large for evaluating the size of the packets as shown in figure 11.

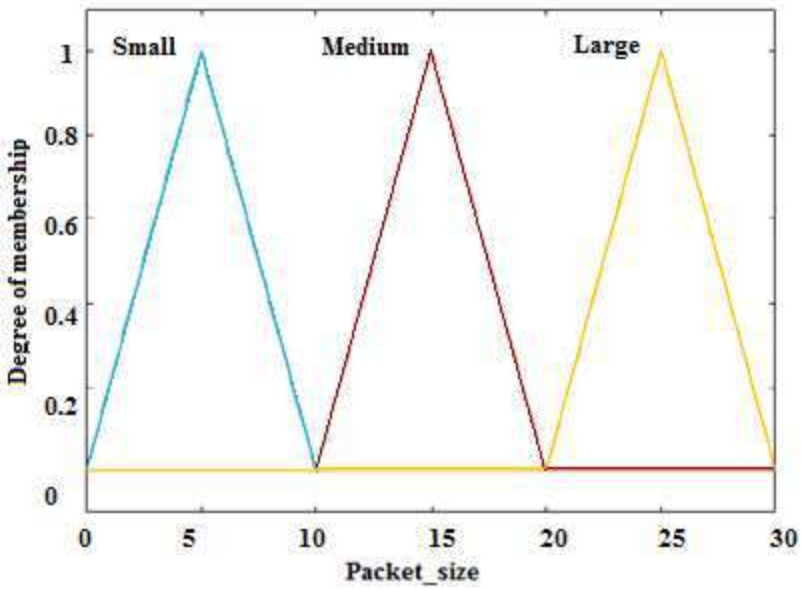

Figure 11. Membership Function of Packet_size

4. Performance Evaluation

In the proposed scheme FBDR method (Fuzzy Based Detection and Recovery method) is used to detect a DDoS attack. The sensor nodes are deployed randomly in a 500 * 500 m specified area. The sensor nodes are varied from 50 to 500. The sensor nodes are homogeneous so that all the nodes utilize the same energy, sensing range, etc. The sink is located anywhere in the specified area. The data packets from different sensor nodes are transferred to the sink. Nodes are deployed only after the calculation of the Euclidean distance.

The Euclidean distance is calculated as

$$D(Se_i,t) = \sqrt{(q_i - q)^2 + (r_i - r)^2} \quad (17)$$

The sensibility of Se_i at the point 't' can be represented as

$$(Se_i,t) = \Upsilon / D(Se_i,t)^j \quad (18)$$

Where $D(Se_i,t)$ be the distance between sensors

'Se_i' be the sensors

't' be the point at position (q, r)

Υ, j be the sensor dependent positive constant.

Euclidean distance is calculated to fix the distance between each sensor node. If the distance is less between the sensors, the sensitivity between the sensors is high so we need to calculate Euclidean distance before deploying it in a position. The proposed FBDR method reduces the usage of the buffer, energy consumption and response time. It also increases the lifetime of the network and increases the live nodes even after 450 rounds. The proposed method was evaluated and compared with the related DDoS detection strategies like the FLQL method [21], FSDNA [25], SACOP algorithm[29] and DLDMFS[34] Table 4 represents the simulation parameters.

Parameter	Value
Network Size	500 * 500 m
Nodes count	500
ID of Node	16 bit
Initial Energy of Node	1 J
Data packet Size	4000 bits
Receiver transmitter expand	1.1dBi
Sender Transmitter expand	1.1dBi
Time taken for simulation	500 s
Packets Mean time	0.01 s

Table 4. Simulation Parameters

4.1. Network Lifetime

Figure 12 represents the lifetime of the network based on the different number of sensors. It is mainly used to evaluate the capability of the FBDR method concerning the lifetime of the network. The sensor nodes taken for our simulation work are 200, 300, 400 and 500. The fuzzy-based detection and recovery method is compared with the related strategies. As the count of the sensor nodes increases the lifetime of the network also gets increased. The FBDR method can save up to 30% of network lifetime compared to the other related strategies.

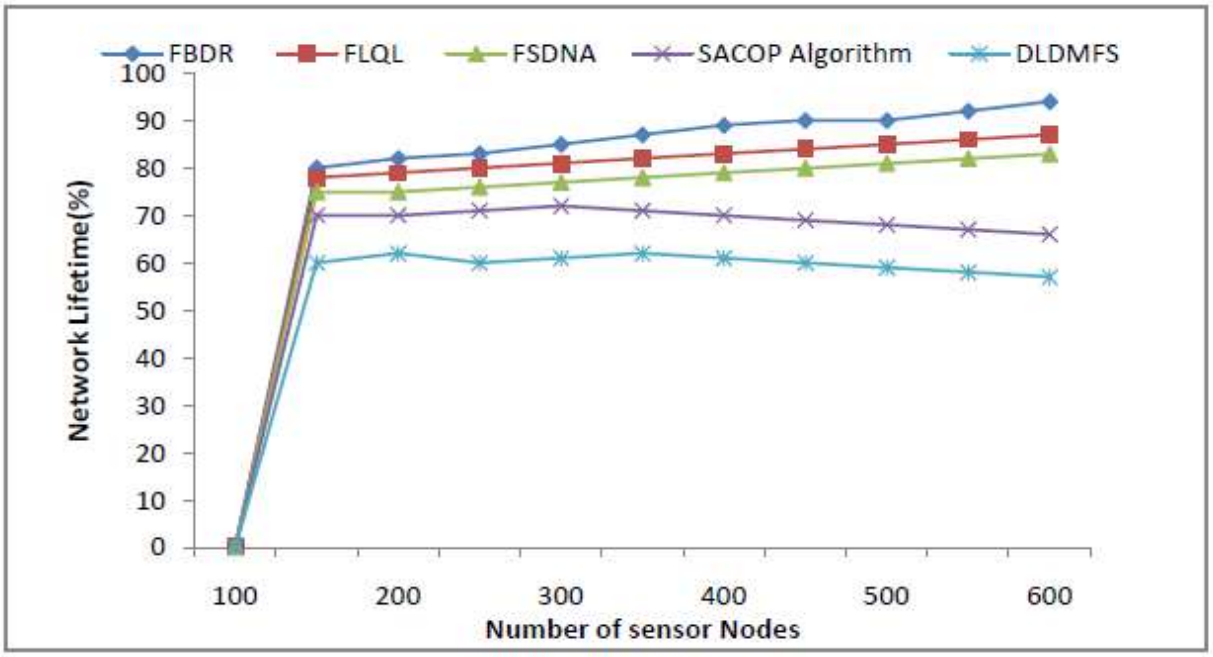

Figure 12 Lifetime of Network in terms of sensor count

4.2 Number of alive Nodes

Figure 13 represents the number of alive sensor nodes in each round. The FBDR method performs better than the other related strategies because there are alive nodes even after 450 rounds. But in the other related strategies, no more alive nodes available in 400 rounds that also affect the lifetime of the network. The distance between the sensors, while it is deploying in a position, was evaluated by the Euclidean distance equation. So that the number of alive nodes is high in this method. Because all the sensors will utilize very less energy if the distance between them is less. Since the sensors are utilizing very little energy it is alive even after 450 rounds.

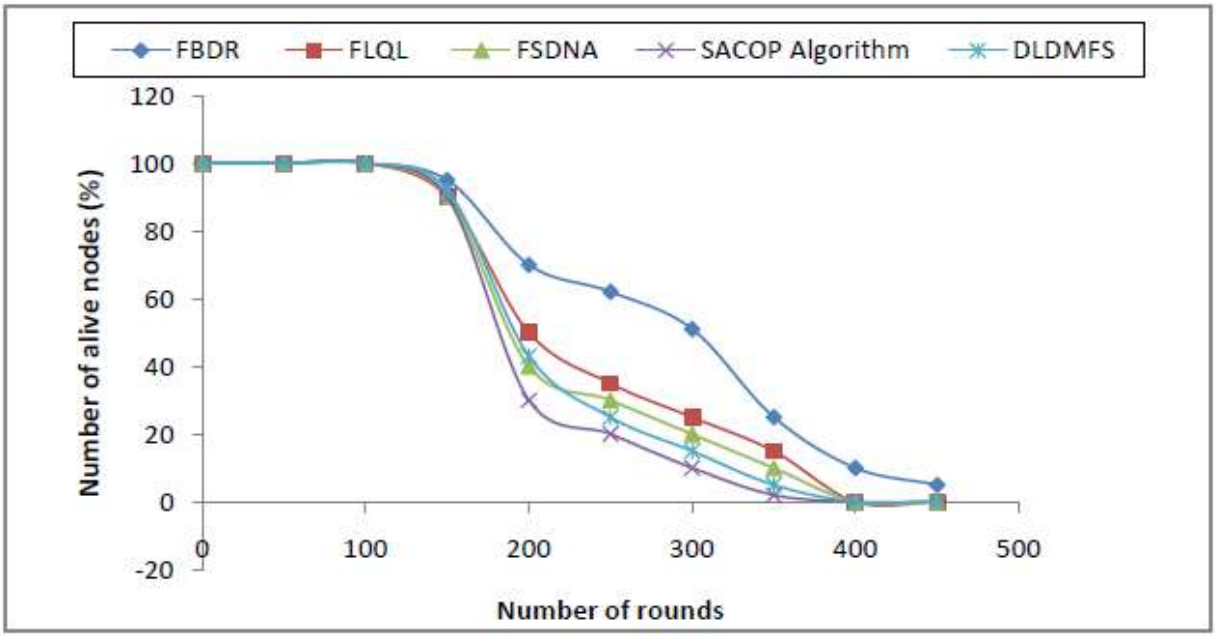

Figure 13 Number of alive nodes

4.3. Packet Drop Rate

Figure 14 represents the FBDR method with less packet drop rate than the related strategies because the FBDR method uses Fuzzy based type2 rule. It uses three types of inputs; they are Distance, Energy_consumption and Packet_size. These three inputs are used to analyze the DDoS attack affected nodes and the packets are redirected to the sink through an alternate path. Since these inputs are not available in other strategies, the number of packets loss is higher in other related strategies.

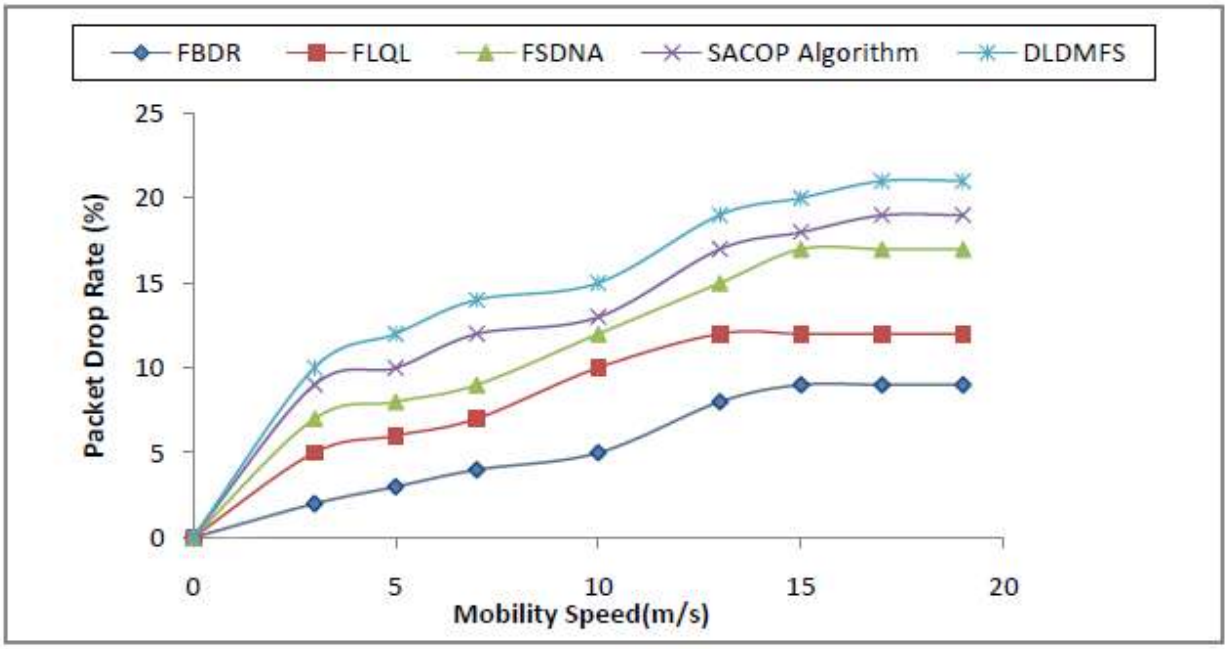

Figure 14. Packet Drop Rate in terms of Mobility speed

4.4 Energy Consumption

Figure 15 represents the energy utilization of each sensor concerning the time. The FBDR method is compared with other related strategies. Since all the sensors are deployed with less distance between each other and the fuzzy-based rule is used. The sensor consumes very less energy than the sensors in the other related strategies.

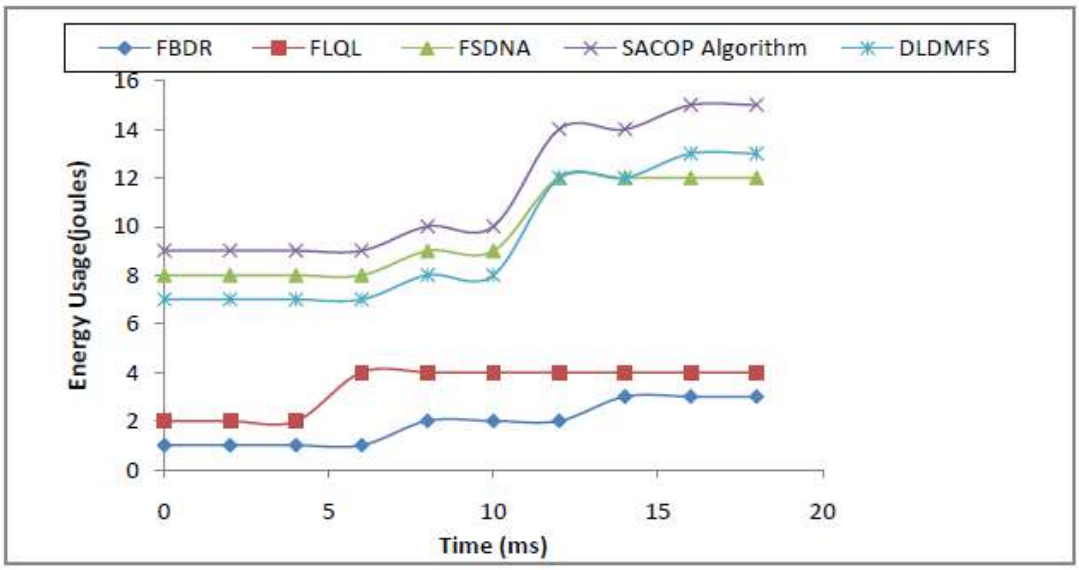

Figure 15. Energy Usage in terms of Time

4.5. Response Time

Figure 16 shows the response time concerning the time. The proposed FBDR method has 20 % less response time than the other related strategies. Since the fuzzy-based rule is used for detection and fuzzy-based type2 rule is used for recovery. The response time of our proposed FBDR method has slight improvement over the other related strategies.

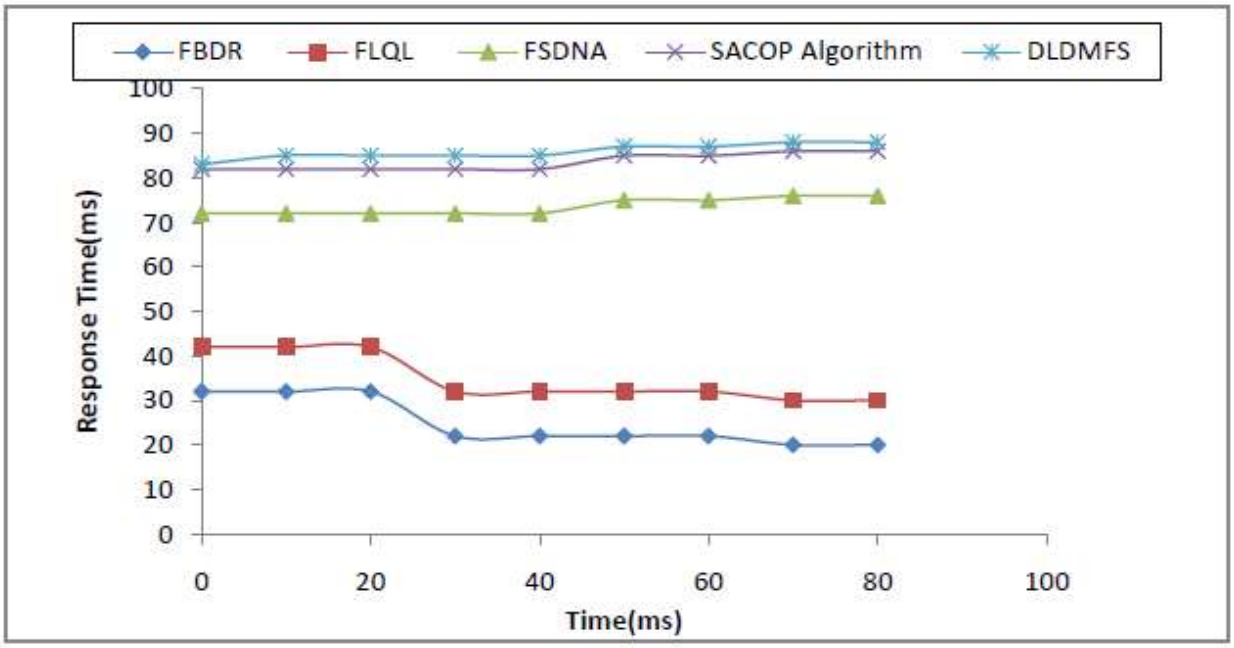

Figure 16. Response Time in terms of time

4.6. Buffer Usage

Figure 17 represents the utilization of buffer in the proposed FBDR method and other related strategies. The usage of the buffer is the main perspective for evaluating the overhead of the sensors. If the size of the buffer is less, the algorithm performs well. The FBDR method use 10 % less buffer size than the other related strategies.

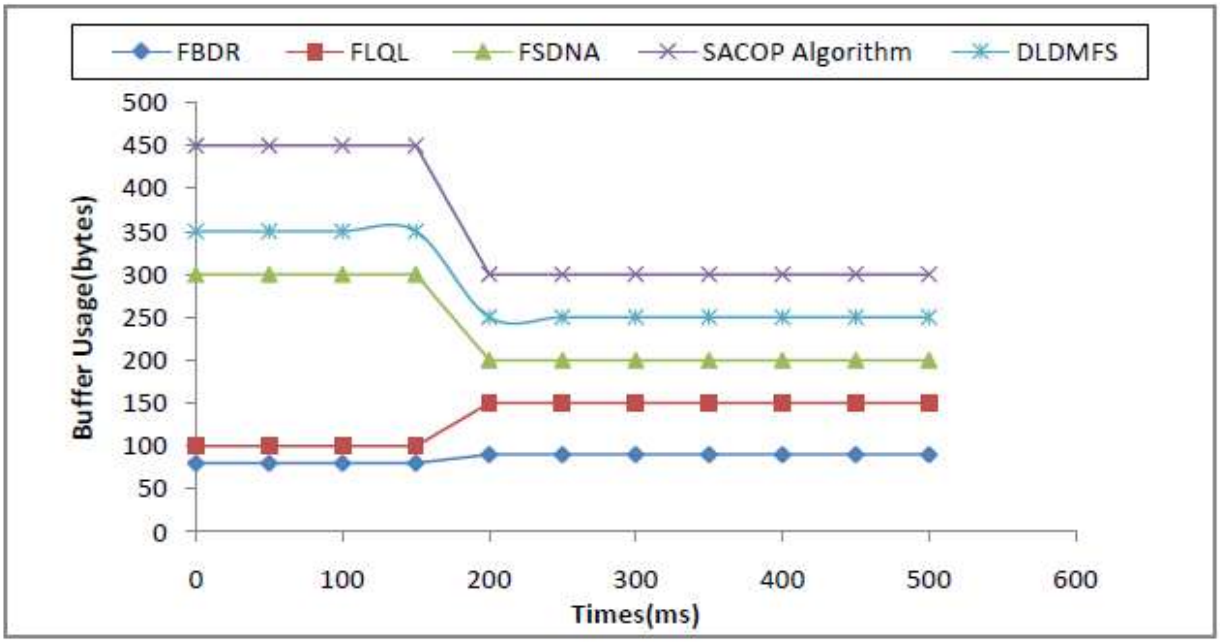

Figure 17. Buffer usage in terms of time

4.7 Detection Rate

Figure 18 represents the detection ratio in the proposed FBDR method and other related strategies. The detection rate of each strategy is evaluated and compared with each other. If the detection rate is more, the algorithm performs well. The detection rate of the proposed FBDR method is more than the other related strategies.

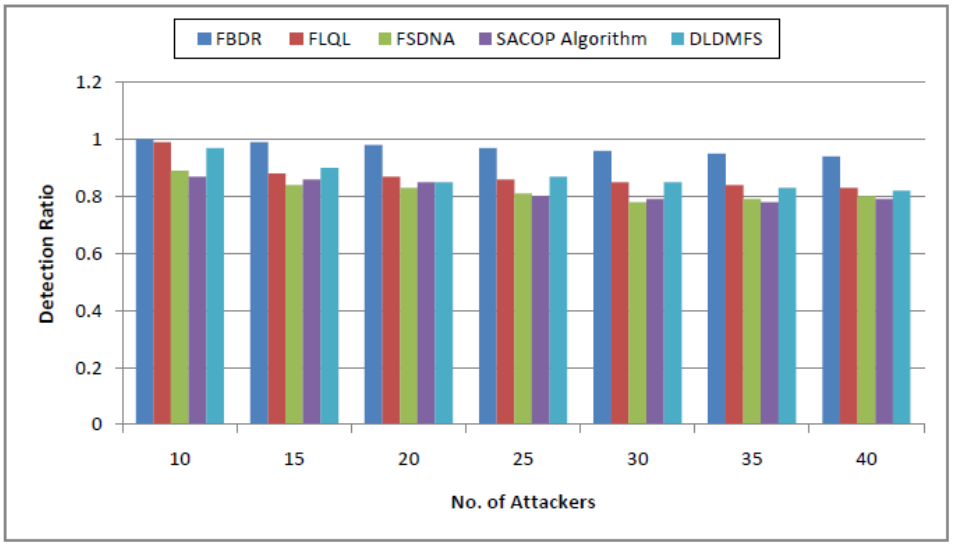

Figure 18. Detection Rate in terms of the attackers count

4.8 Execution Time

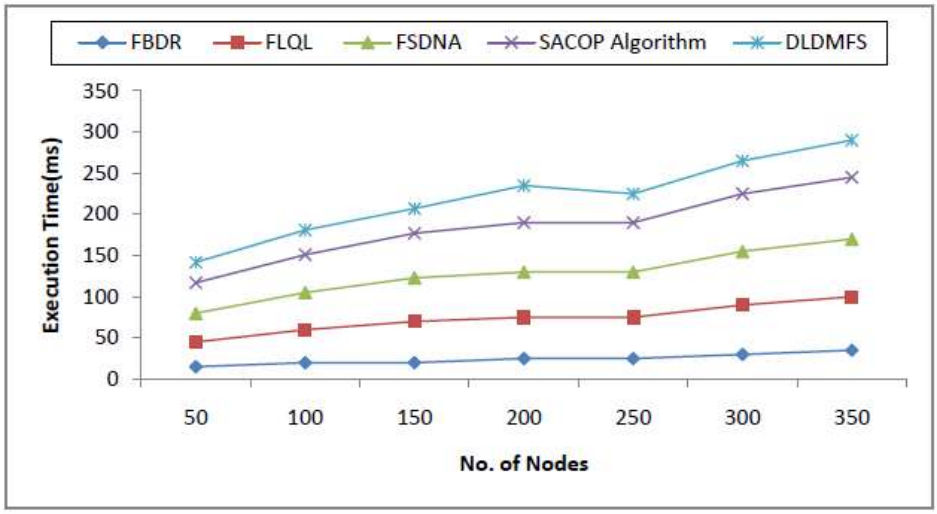

Figure 19. Execution Time in terms of the node count

Figure 19. shows the execution time of the proposed FBDR method and the other related schemes with different number of sensor nodes. It is clearly visible that the FDBR method has less execution time compared to other related strategies. The proposed FDBR method has very less execution time and also very less computational complexity compared to other related strategies.

5. Conclusion

We propose a new FBDR method to detect the DDoS attack and to redirect the data packets to the sink through the alternate path. The FBDR method analyzes the energy consumption, response time and data packet count of each sensor. The FBDR method uses type1 fuzzy-based rule to detect the occurrence of the DDoS attack. So it quickly identifies the sensor node that was affected by the DDoS attack. Moreover, to avoid packet loss, the packets are redirected to the sink through the alternate path using the recovery method. The recovery method uses type2 fuzzy-based rule. It analysis packet size, energy consumption, and distance. The proposed method saves energy usage by up to 20 % compared with the related schemes. The proposed work examines the energy efficiency of the FBDR method by analyzing the buffer usage, packet drop rate, response time and a lifetime of the network. Future work can be added to the prevention measures using the neuro-fuzzy approach.

6. References

[1]S. Patil, Sangita Chaudhari (2016), DoS attack prevention technique in Wireless Sensor Networks.7th International Conference on Communication, Computing and Virtualization. Procedia Computer Science 79, pp. 715 – 721. doi: 10.1016/j.procs.2016.03.094

[2] Gavrić, Ž., Simić, D. (2018). Overview of DOS attacks on wireless sensor networks and experimental results for simulation of interference attacks. Ingeniería e Investigación, Vol. 38, No.1, pp. 130-138. DOI: 10.15446/ ing.investig.v38n1.65453

[3]M. Farsi, M. A. Elhosseini, M. Badawy, H. Arafat Ali and H. Zain Eldin (2019), Deployment Techniques in Wireless Sensor Networks, Coverage and Connectivity: A Survey, in IEEE Access, Vol. 7, pp. 28940-28954. DOI: 10.1109/ACCESS.2019.2902072

[4]Avneet Kaur, Mandeep Kaur(2016), Performance of Node Deployment Techniques in WSN: A Review , IJSRD - International Journal for Scientific Research & Development. Vol. 4, Issue 02 | ISSN (online): 2321-0613.

[5]T. Kaur, K. K. Saluja, A. K. Sharma (2016), DDoS attack in WSN: A survey, International Conference on Recent Advances and. Innovations in engineering pp.1-5. DOI: 10.1109/ICRAIE39140.2016

[6]F. Shahzad, M. Pasha, A. Ahmad (2017), A survey of active attacks on wireless sensor networks and their countermeasures,International Journal of Computer Science and Information Security,Vol.14, No. 12. pp.54-65.

[7]R.Upadhyay,U.R.Bhatt, H.Tripathi (2016), DDOS Attack Aware DSR Routing Protocol in WSN, International Conference on Information Security & Privacy (ICISP2015), Vol.78, pp. 68 – 74. DOI: 10.1016/j.procs.2016.02.012

[8]Monika Sachdeva,, Gurvinder Singh, Krishan Kumar and Kuldip Singh(2010), DDoS Incidents and their Impact: A Review, The International Arab Journal of Information Technology. Vol. 7. No.1.

[9]Christos Douligeris, Aikaterini Mitrokotsa(2004), DDoS attacks and defence mechanisms: classification and state-of-the-art, Computer Networks. Vol. 44.pp.643–666. DOI:10.1016/j.comnet.2003.10.003

[10] Mirkovic, Jelena & Martin, Janice & Reiher, Peter. (2003). A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms. ACM SIGCOMM Computer Communications Review. Volume 34, Number 2. https://doi.org/10.1145/997150.997156

[11] Zhengmin, Xia & Lu, Songnian & Li, Jianhua & Tang, Junhua. (2010). Enhancing DDoS Flood Attack Detection via Intelligent Fuzzy Logic.. Informatica (Slovenia). 34. 497-507.

[12]Jesus Alcala-Fdez, Jose M Alonso (2016), A Survey of Fuzzy Systems Software: Taxonomy, Current Research Trends and Prospects, IEEE Transactions on Fuzzy Systems vol. 24(1). pp. 40-56. DOI: 10.1109/TFUZZ.2015.2426212

[13]Wang Jiangtao Yang Geng(2008), An Intelligent Method for Real-Time Detection Of DDoS Attack Based On Fuzzy Logic, JOURNAL OF ELECTRONICS. Vol 25. pp. 511–518. DOI 10.1007/s11767-007-0056-6

[14]N.Ch.S.N. Iyengar, Arindam Banerjee and Gopinath Ganapathy(2014), A Fuzzy Logic-based Defense Mechanism against Distributed Denial of Service Attack in Cloud Computing Environment, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 6, No. 3,

[15]Li Q., Meng L., Zhang Y., Yan J.(2019),DDoS Attacks Detection Using Machine Learning Algorithms ,Digital TV and Multimedia Communication.Communications in Computer and Information Science. Springer, Singapore. 1009. pp. 205–216 https://doi.org/10.1007/978-981-13-8138-6_17.

[16] He, T. Zhang and R. B. Lee (2017), "Machine Learning Based DDoS Attack Detection from Source Side in Cloud," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, pp. 114-120, doi: 10.1109/CSCloud.2017.58.

[17] Khare, Ashish & Rana, J. & Jain, R.. (2017). Detection of Wormhole, Blackhole and DDOS Attack in MANET using Trust Estimation under Fuzzy Logic Methodology. International Journal of Computer Network and Information Security.Vol. 9. pp. 29-35. DOI:10.5815/ijcnis.2017.07.04.

[18] C.Balarengadurai and Dr.S.Saraswathi (2013), Fuzzy Based Detection and Prediction of DDoS Attacks in IEEE 802.15.4 Low Rate Wireless Personal Area Network, IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 6, No 1. DOI: 10.1504/IJTMCC.2013.056424.

[19] Tabatabaei, S.F., Salleh, M., Abbasy, M., & Najaftorkaman, M. (2011). Denial of Service (DoS) Attack Detection by Using Fuzzy Logic over Network Flows, The 2011 International Conference On Security & Management.

[20]Mohammad Almseidin, Szilveszter Kovacs (2018). Intrusion Detection Mechanism Using Fuzzy Rule Interpolation, Journal of Theoretical and Applied Information Technology. Vol.96. No 16.

[21]Hafiz Husnain Raza Sherazia, Razi Iqbalb, Farooq Ahmadc, Zuhaib Ashfaq Khand, Muhammad Hasanain Chaudary (2019), DDoS attack detection: A key enabler for sustainable communication on the internet of vehicles, Sustainable Computing: Informatics and Systems Vol.23.pp. 13–20. https://doi.org/10.1016/j.suscom.2019.05.002

[22]Stavros N. Shiaeles, Vasilios Katos, Alexandros S. Karakos, Basil K. Papadopoulos(2012), Real-time DDoS detection using fuzzy estimators, computers & security, Vol. 31.pp.782 -790.DOI.http://dx.doi.org/10.1016/j.cose.2012.06.002.

[23] Indraneel, S. & Vuppala, Venkata. (2017). HTTP Flood attack Detection in Application Layer using Machine learning metrics and Bio inspired Bat algorithm. Applied Computing and Informatics. Vol.15.pp.59-66. doi: https://doi.org/10.1016/j.aci.2017.10.003

[24] S. Haider et al., "A Deep CNN Ensemble Framework for Efficient DDoS Attack Detection in Software Defined Networks," in IEEE Access, vol. 8, pp. 53972-53983, 2020, doi: 10.1109/ACCESS.2020.2976908.

[25] J. A. Pérez-Díaz, I. A. Valdovinos, K. -K. R. Choo and D. Zhu, "A Flexible SDN-Based Architecture for Identifying and Mitigating Low-Rate DDoS Attacks Using Machine Learning," in IEEE Access, vol. 8, pp. 155859-155872, 2020, doi: 10.1109/ACCESS.2020.3019330.

[26] C. Tang and D. Han, "A Low Resource Consumption Clone Detection Method for Multi-Base Station Wireless Sensor Networks," in IEEE Access, vol. 8, pp. 128349-128361, 2020, doi: 10.1109/ACCESS.2020.3007388.

[27] Shashank Gavel, Ajay Singh Raghuvanshi, Sudarshan Tiwari,A novel density estimation based intrusion detection technique with Pearson's divergence for Wireless Sensor Networks, ISA Transactions,2020,ISSN 0019-0578,https://doi.org/10.1016/j.isatra.2020.11.016.

[28] I. M. Tas, B. G. Unsalver and S. Baktir, "A Novel SIP Based Distributed Reflection Denial-of-Service Attack and an Effective Defense Mechanism," in IEEE Access, vol. 8, pp. 112574-112584, 2020, doi: 10.1109/ACCESS.2020.3001688.

[29] S. Anitha, P. Jayanthi, V. Chandrasekaran, An intelligent based healthcare security monitoring schemes for detection of node replication attack in wireless sensor networks, Measurement,Volume 167,2021,108272,ISSN 0263-2241, https://doi.org/10.1016/j. measure ment.2020.108272.

[30] I. Gethzi Ahila Poornima, B. Paramasivan,Anomaly detection in wireless sensor network using machine learning algorithm,Computer Communications,Volume 151,2020, Pages 331-337,ISSN 0140-3664,https://doi.org/10.1016/j.comcom.2020.01.005.

[31] G. F. Scaranti, L. F. Carvalho, S. Barbon and M. L. Proença, "Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-Defined Networks," in IEEE Access, vol. 8, pp. 100172-100184, 2020, doi: 10.1109/ACCESS.2020.2997939.

[32] Wen Yang, Xinting Zhang, Weijie Luo, Zongyu Zuo, Detection against randomly occurring complex attacks on distributed state estimation, Information Sciences, Volume 547, 2021, Pages 539-552, ISSN 0020-0255, https://doi.org/10.1016/j.ins.2020.08.008.

[33] Y. Huang, L. Jin, Z. Zhong et al., Detection and defense of active attacks for generating secret key from wireless channels in static environment.ISA Transactions (2019), https://doi.org/10.1016/j.isatra.2019.11.001.

[34] M. Premkumar, T.V.P. Sundararajan, DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks, Microprocessors and Microsystems,Volume 79, 2020,103278,ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2020.103278.

[35] W. A. Aliady and S. A. Al-Ahmadi, "Energy Preserving Secure Measure Against Wormhole Attack in Wireless Sensor Networks," in IEEE Access, vol. 7, pp. 84132-84141, 2019, doi: 10.1109/ACCESS.2019.2924283.

[36] Benmoussa, Ahmed & Tahari, Abdou & Kerrache, Chaker & Lagraa, Nasreddine & Lakas, Abderrahmane & Hussain, Rasheed & Ahmad, Farhan. (2020). MSIDN: Mitigation of Sophisticated Interest flooding-based DDoS attacks in Named Data Networking. Future Generation Computer Systems. 10.1016/j.future.2020.01.043.

[37] Devi, P.P. & Jaison, B.. (2020). Protection on Wireless Sensor Network from Clone Attack using the SDN-Enabled Hybrid Clone Node Detection Mechanisms. Computer Communications. 152. 316-322. 10.1016/j.comcom.2020.01.064.

[38] S. Jiang, J. Zhao and X. Xu, "SLGBM: An Intrusion Detection Mechanism for Wireless Sensor Networks in Smart Environments," in IEEE Access, vol. 8, pp. 169548-169558, 2020, doi: 10.1109/ACCESS.2020.3024219.

[39] Balaji, S. & Julie, Golden & Rajaram, M. & Robinson, Harold(2016), Fuzzy Based Particle Swarm Optimization Routing Technique for Load Balancing in Wireless Sensor Networks. World Academy of Science, Engineering and Technology International Journal of Computer, Electrical, Automation, Control and Information Engineering.Vol.10.pp.1384-1393.

Figures

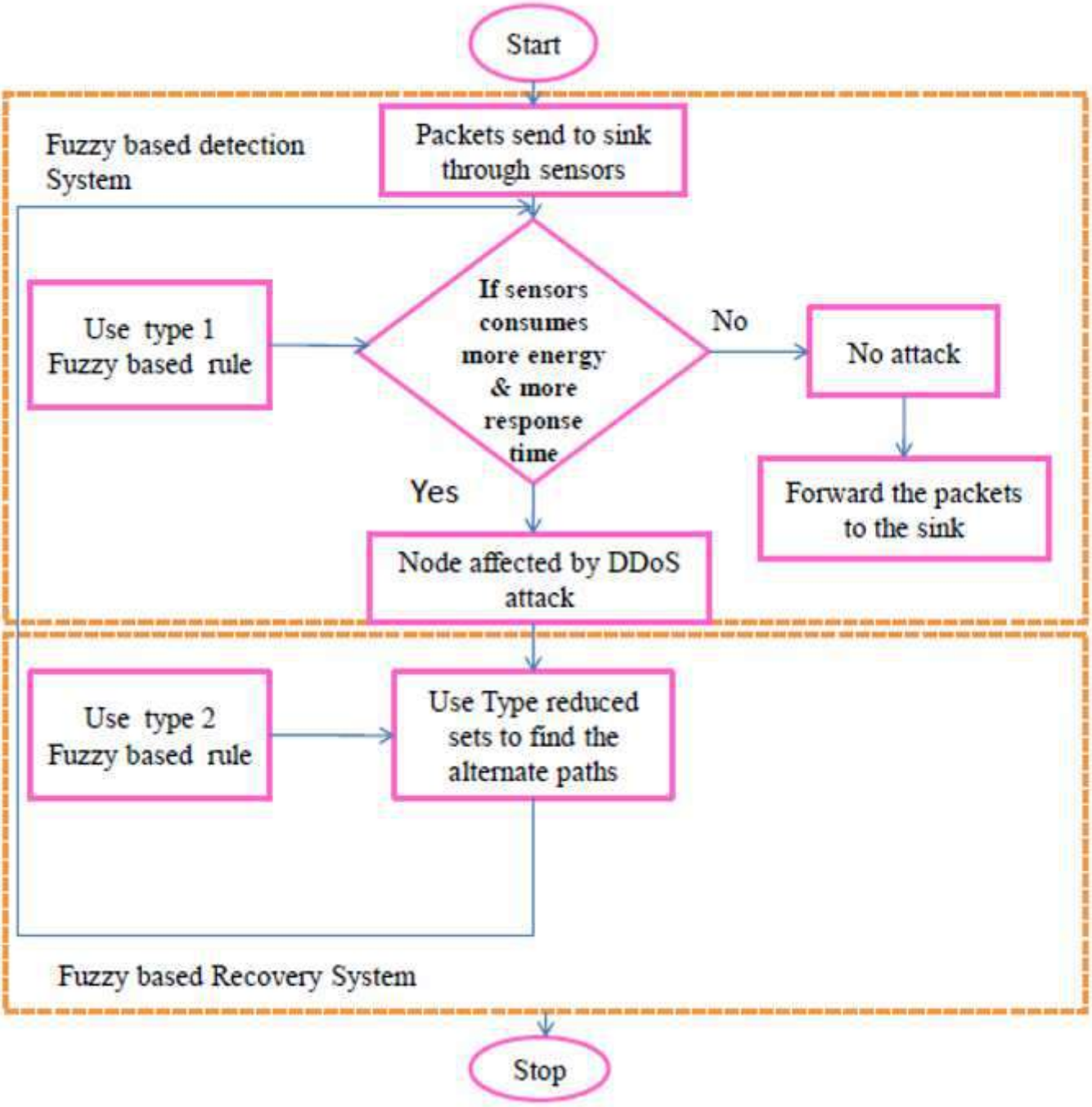

Figure 1

The workflow of the proposed system

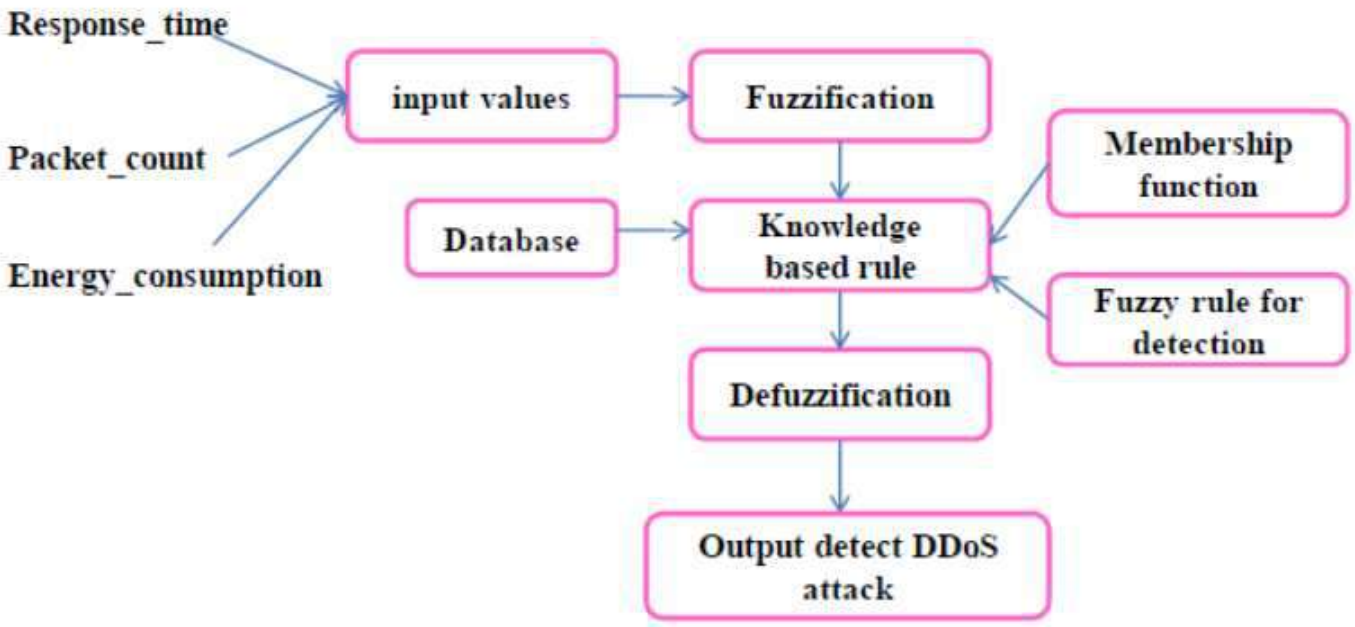

Figure 2

Type1 Fuzzy based DDoS attack detection system

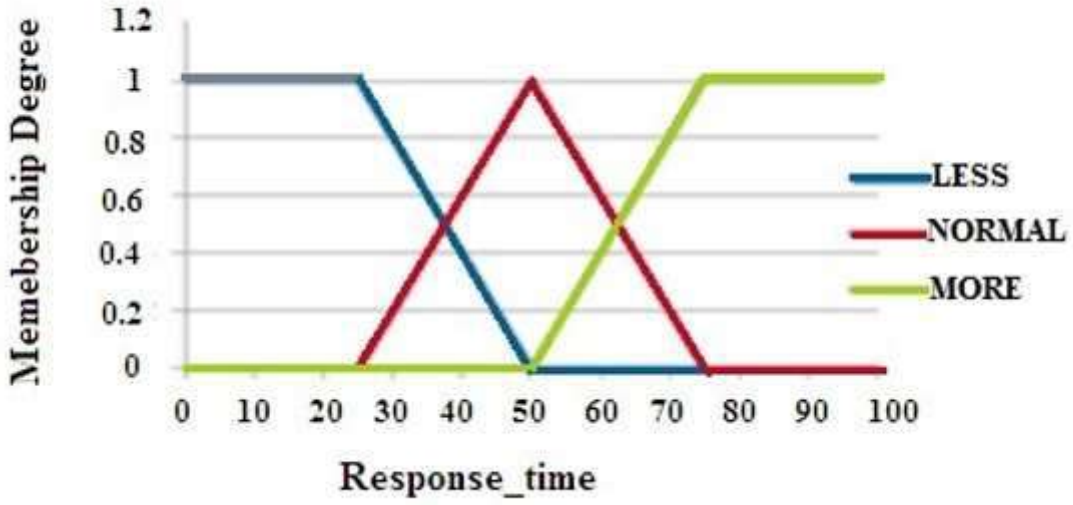

Figure 3

Membership function of Response_time

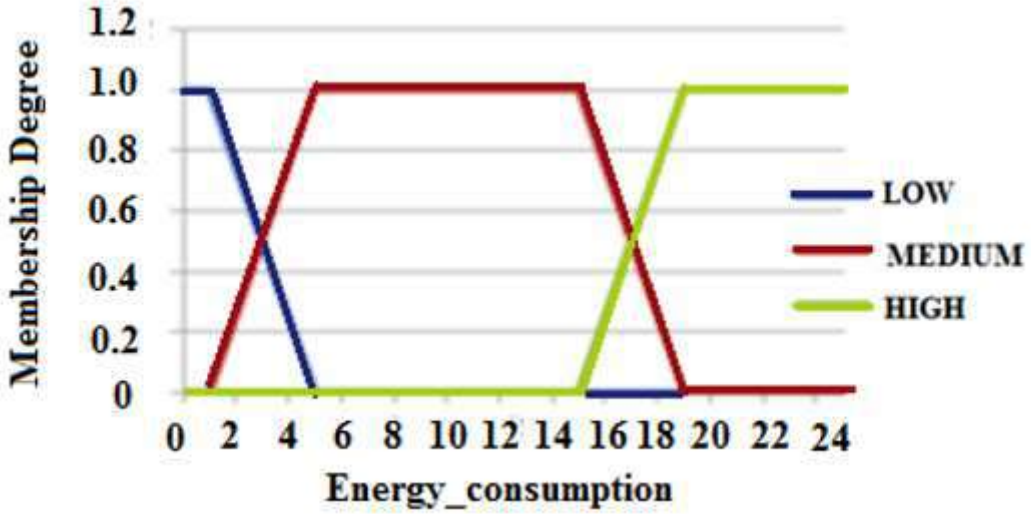

Figure 4

Membership function of Energy_consumption

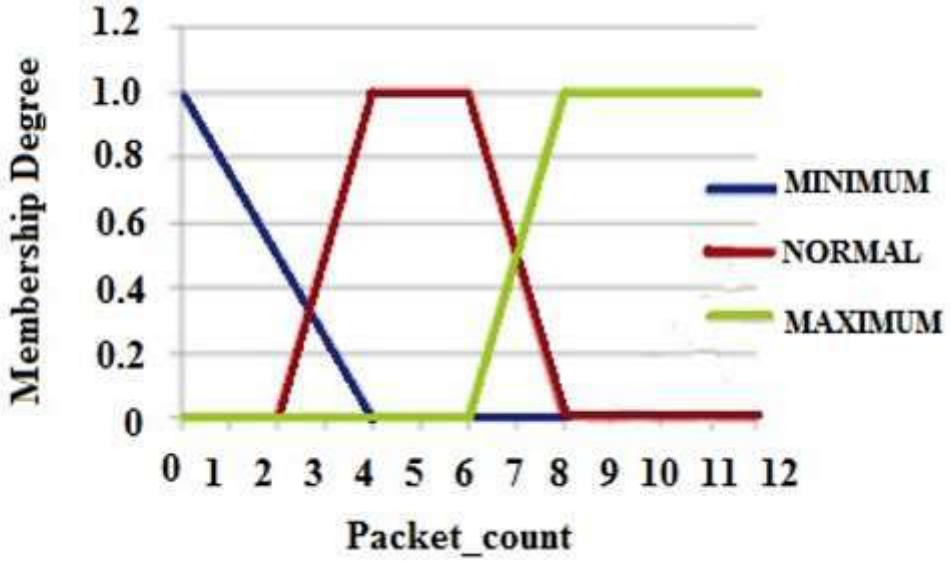

Figure 5

Membership function of Packet_count

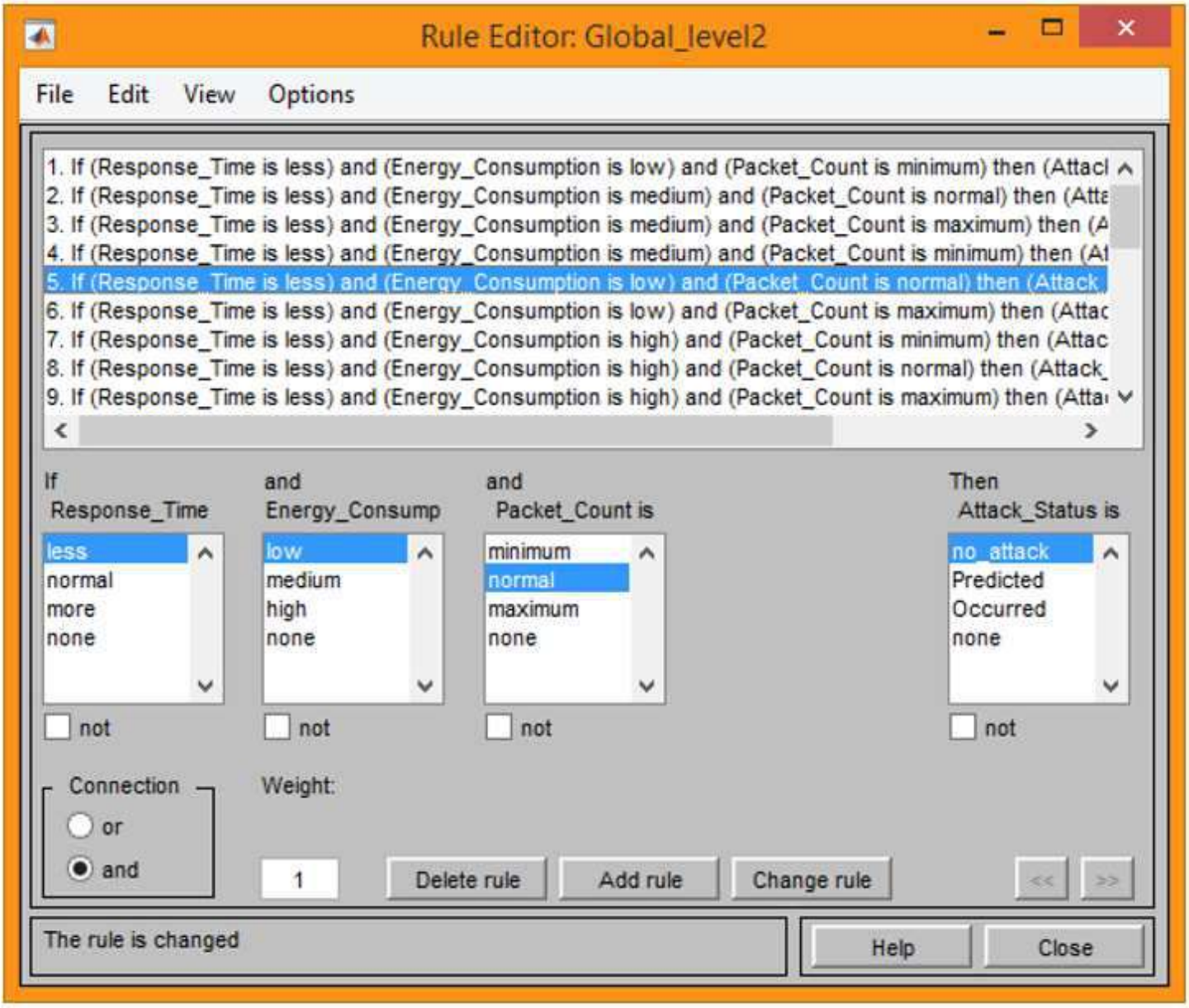

Figure 6

Rule setting for Type1 fuzzy-based DDoS attack detection system

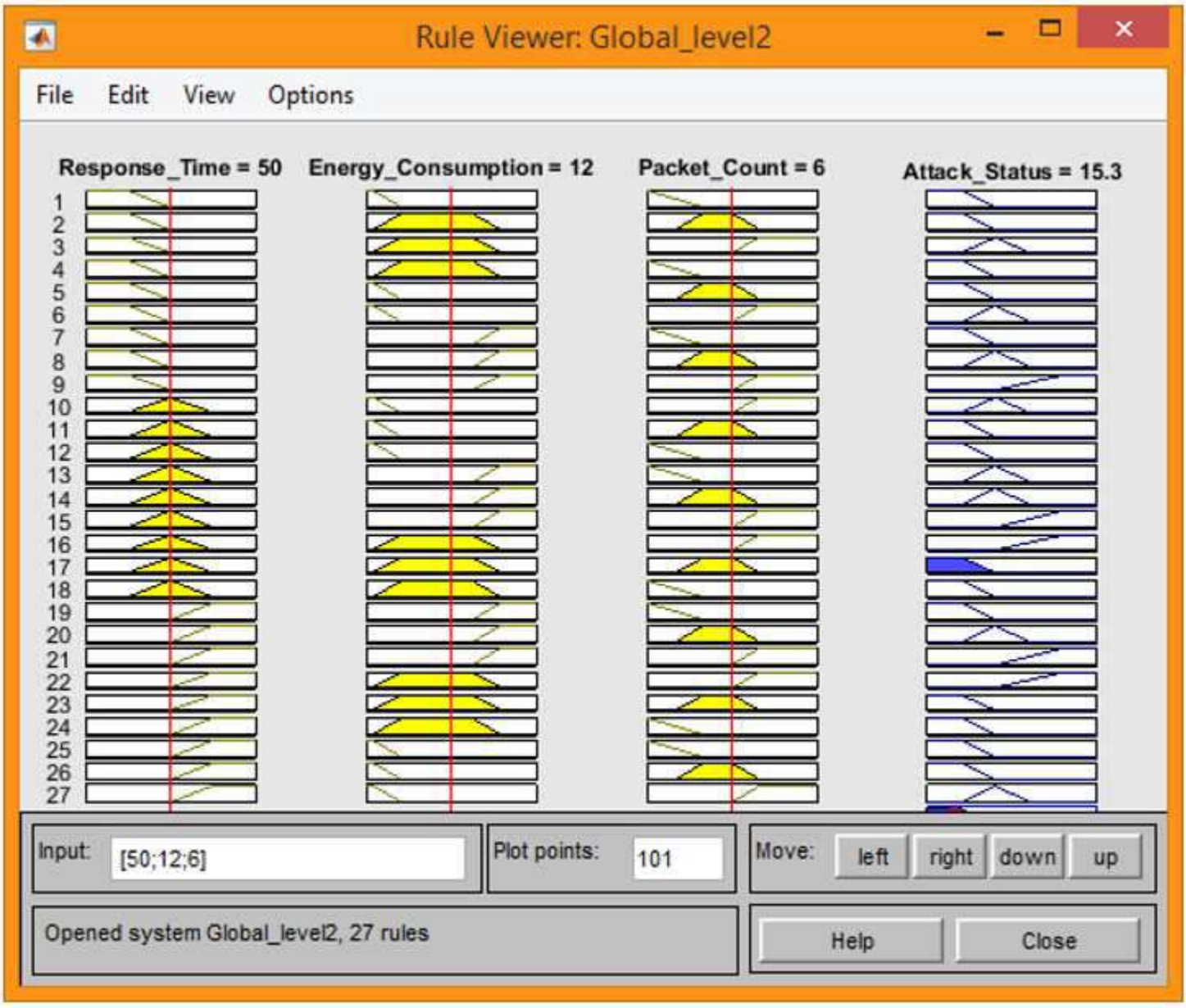

Figure 7

Rule viewer of Type1 Fuzzy based DDoS attack detection system

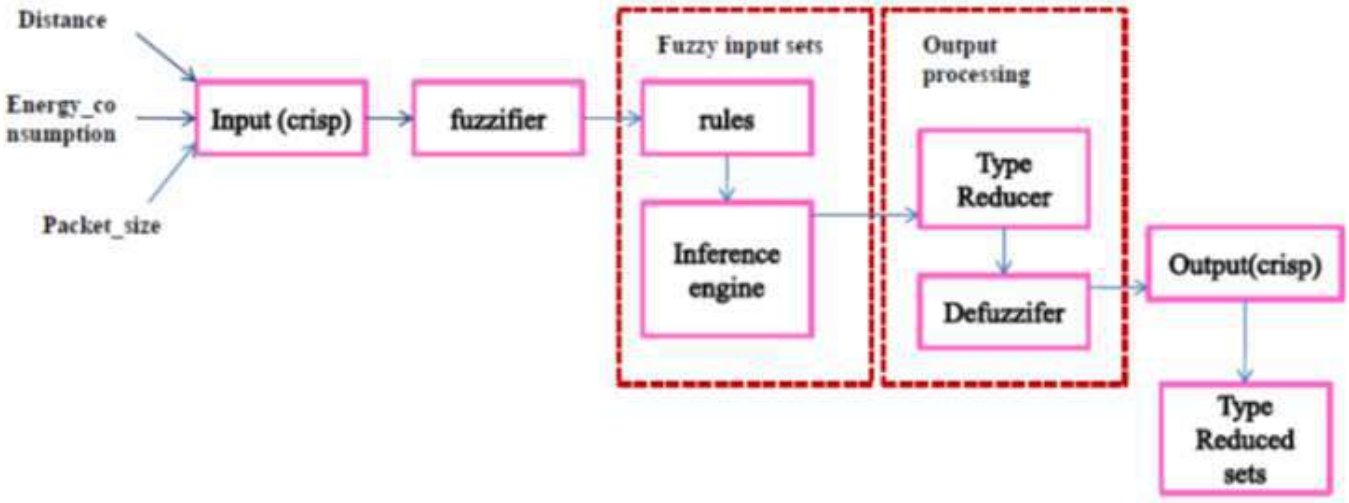

Figure 8

Block diagram of Type2 fuzzy-based recovery system

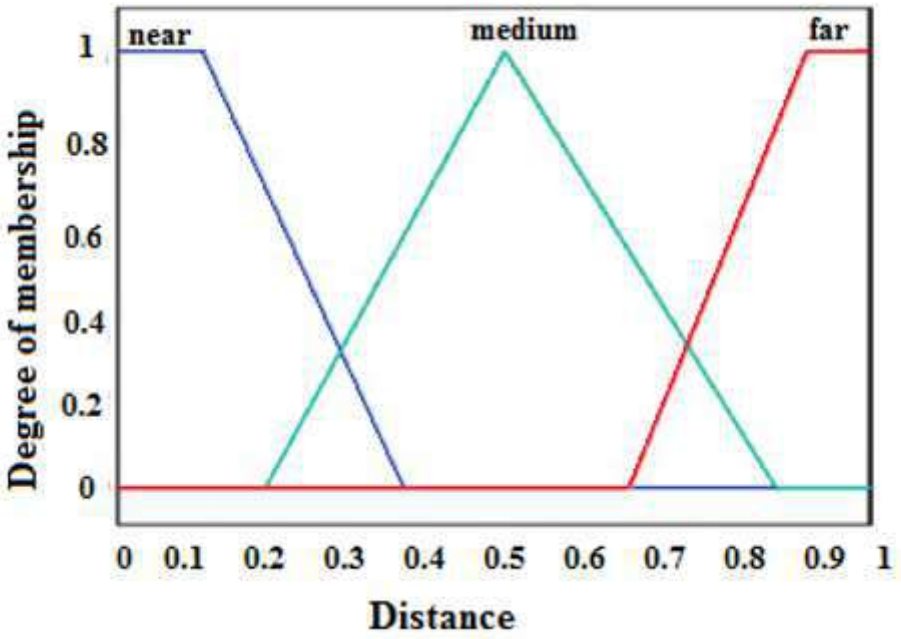

Figure 9

Membership function for Distance

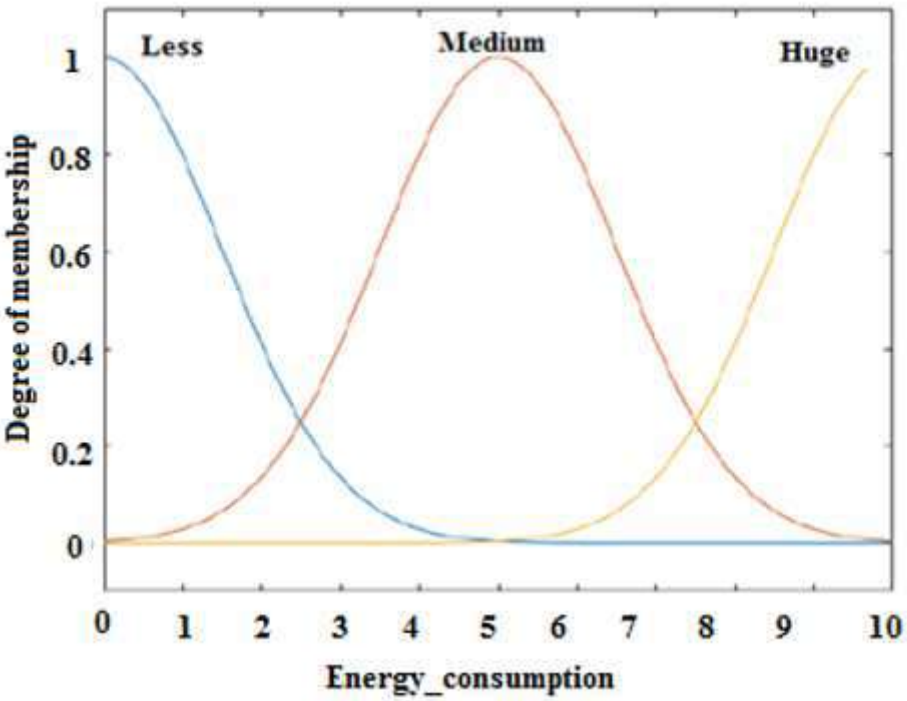

Figure 10

Membership function for Energy_consumption

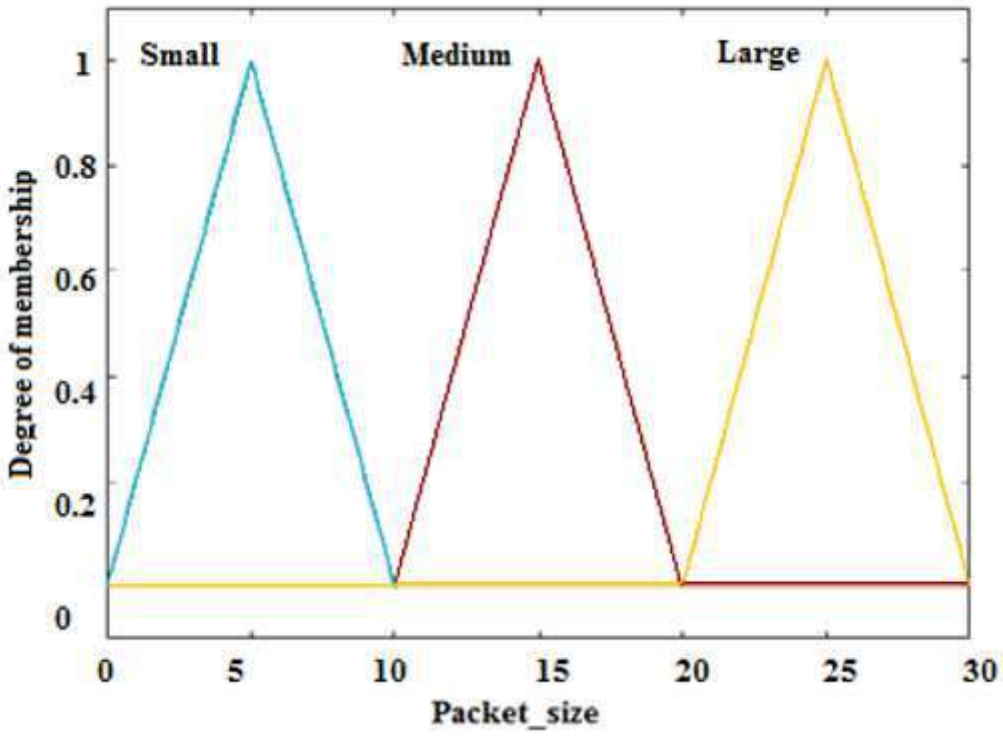

Figure 11

Membership Function of Packet_size

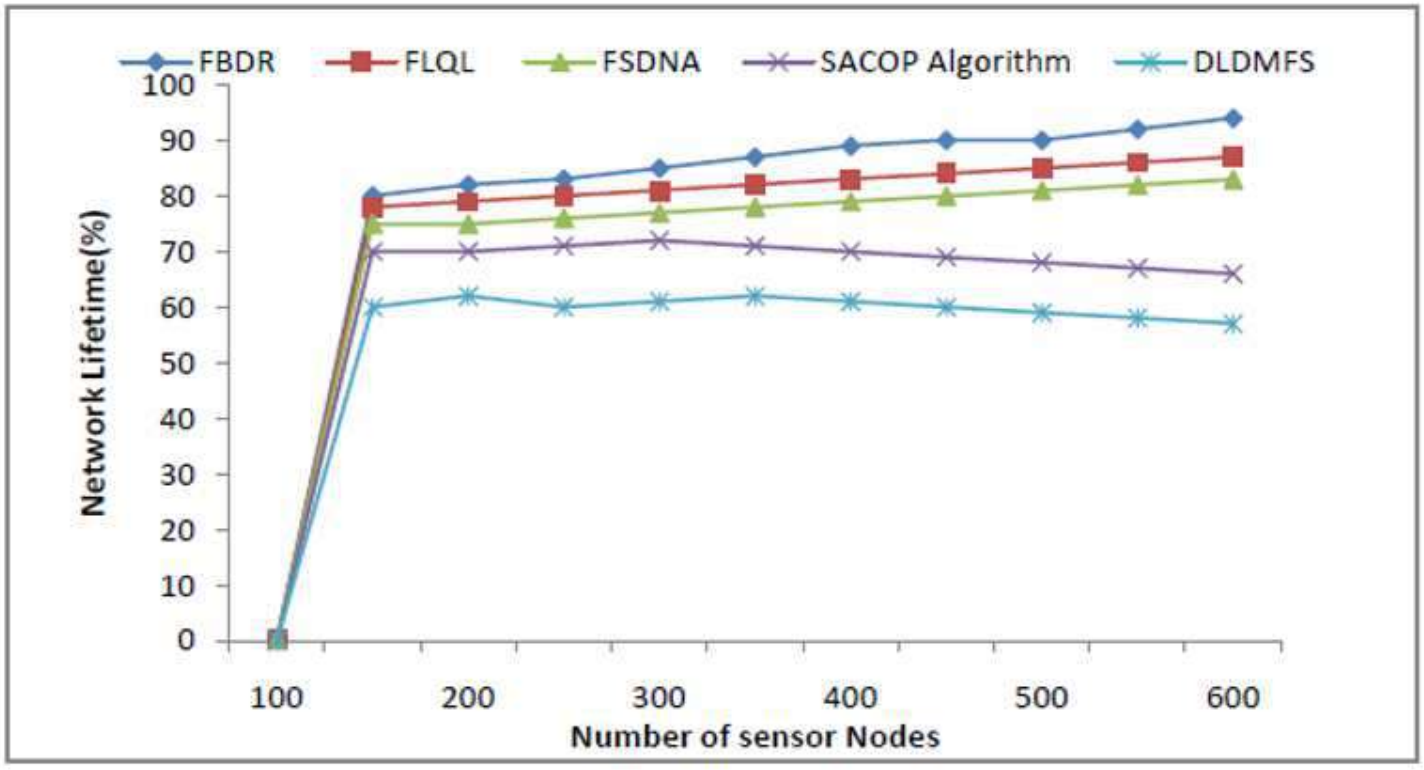

Figure 12

Lifetime of Network in terms of sensor count

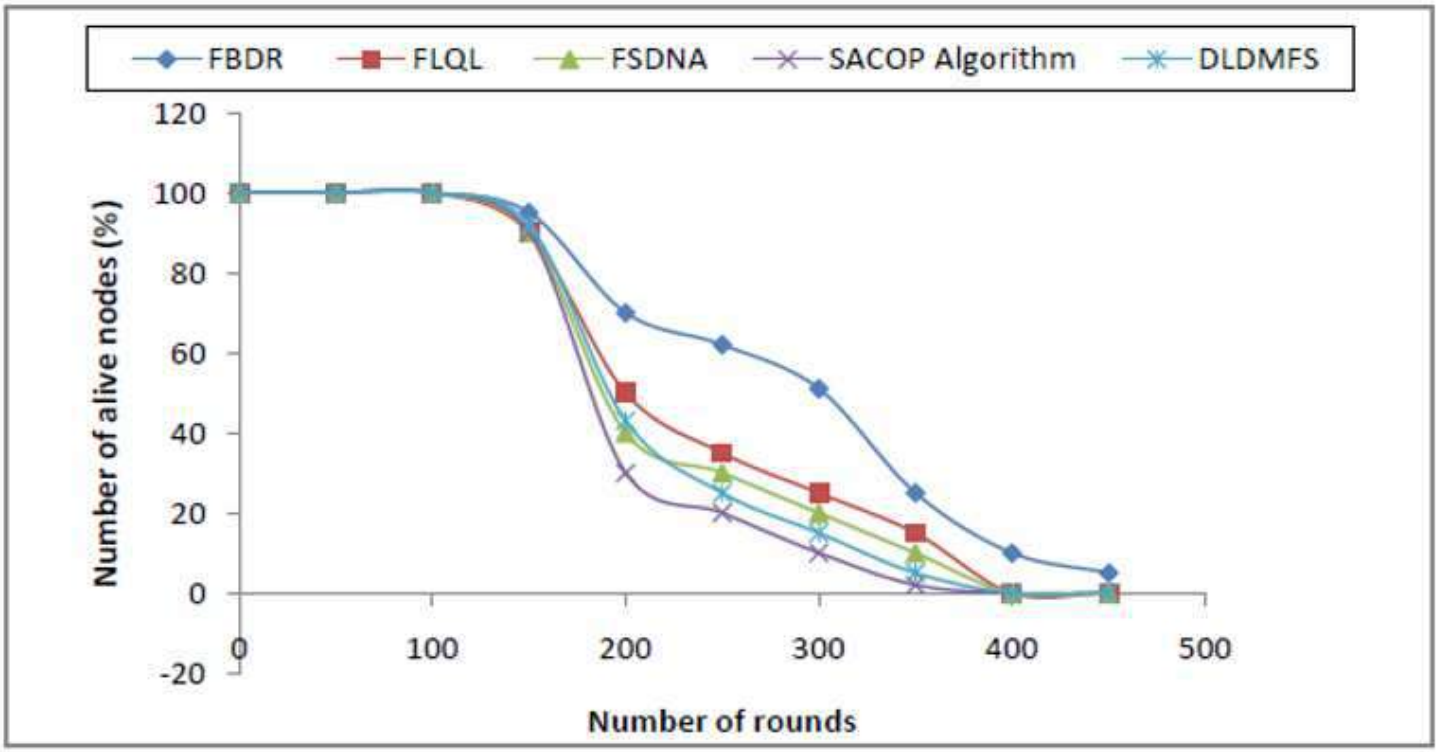

Figure 13

Number of alive nodes

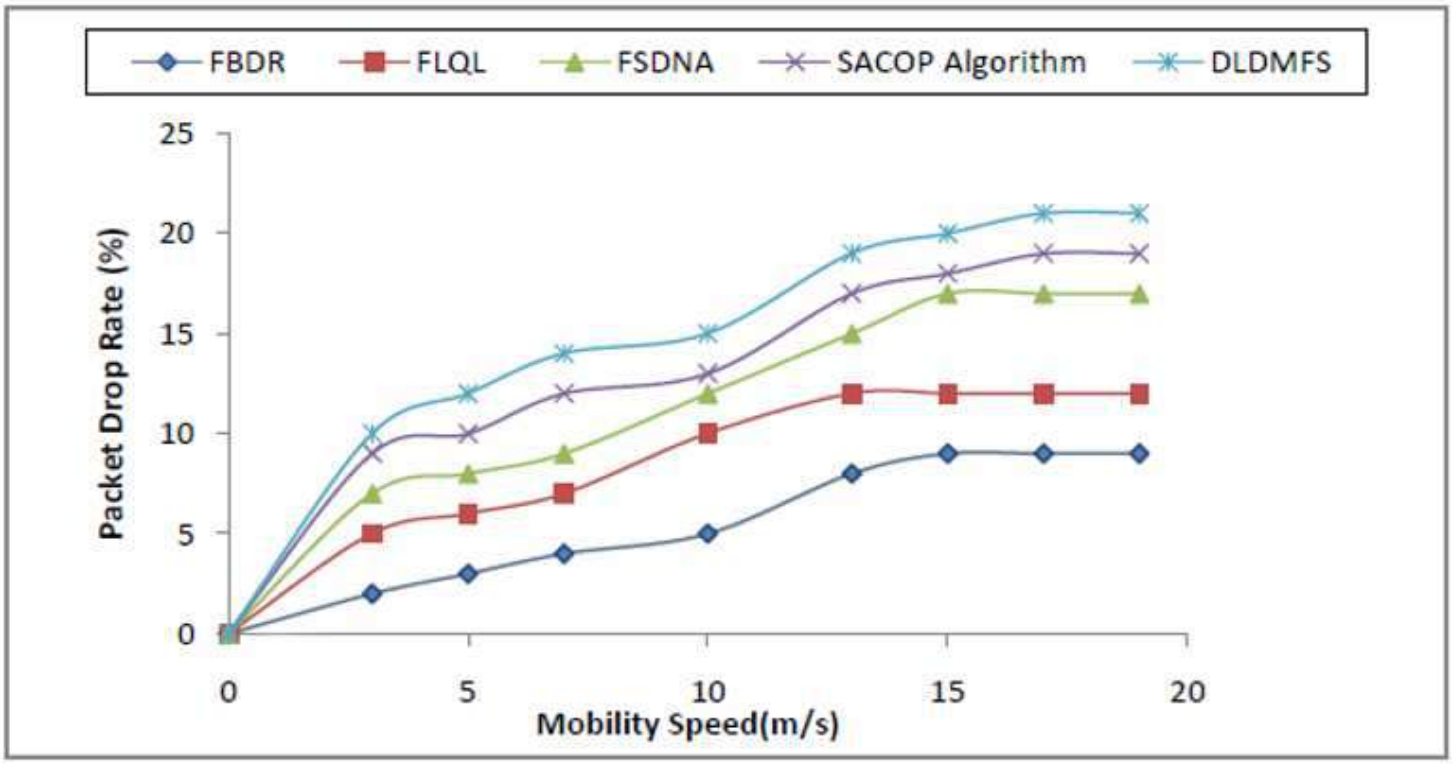

Figure 14

Packet Drop Rate in terms of Mobility speed

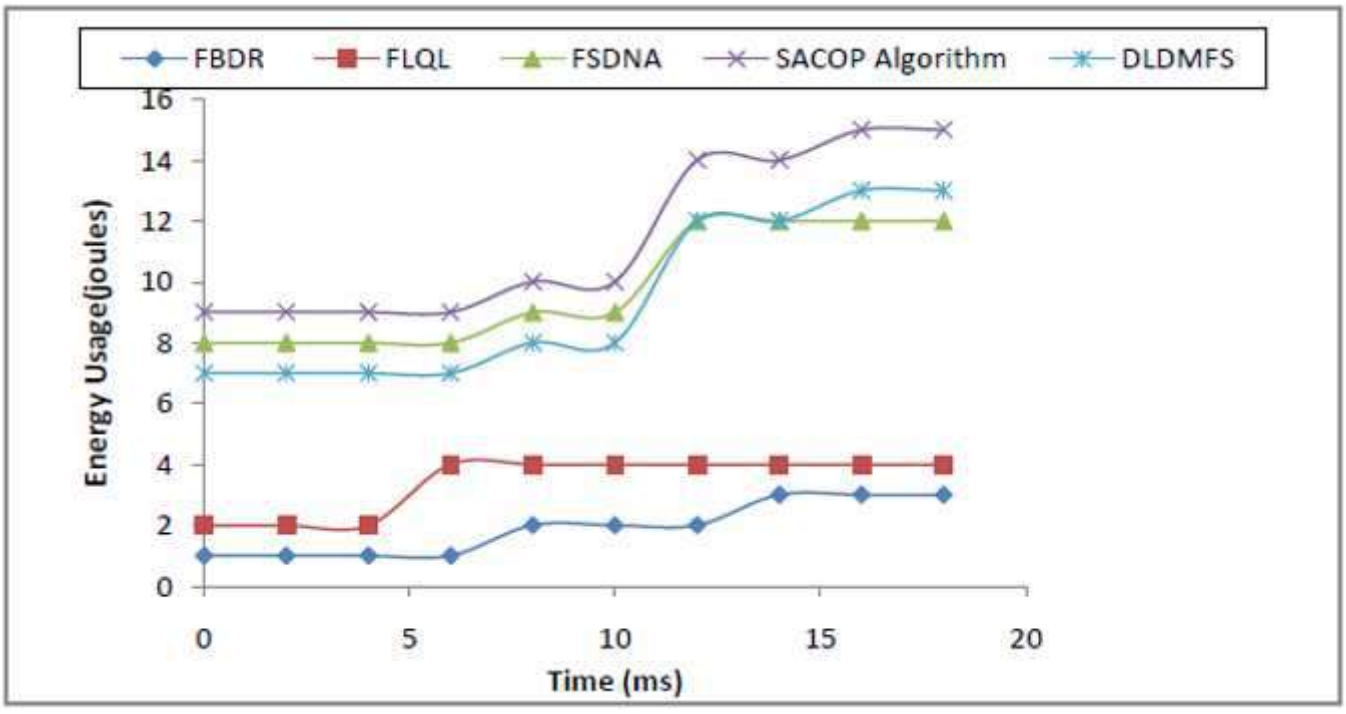

Figure 15

Energy Usage in terms of Time

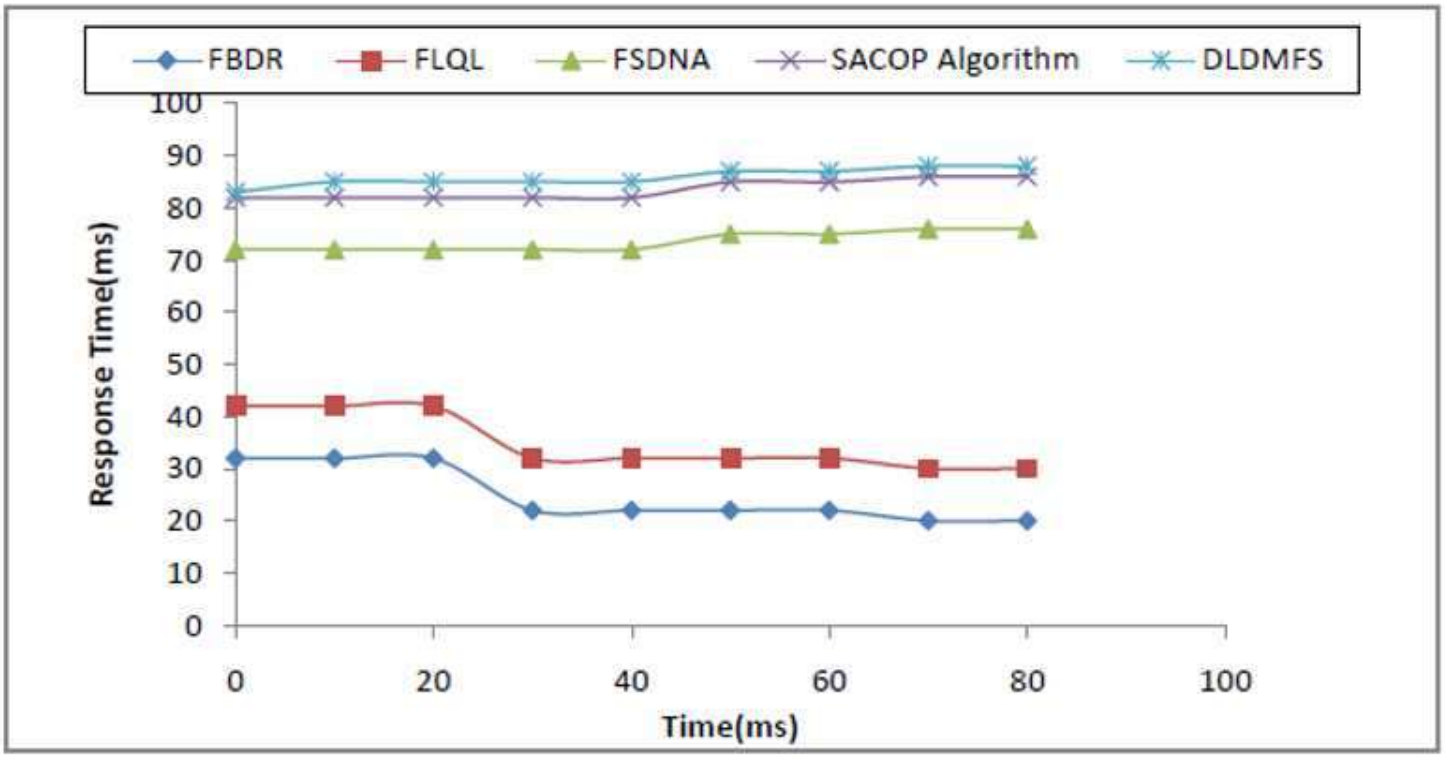

Figure 16

Response Time in terms of time

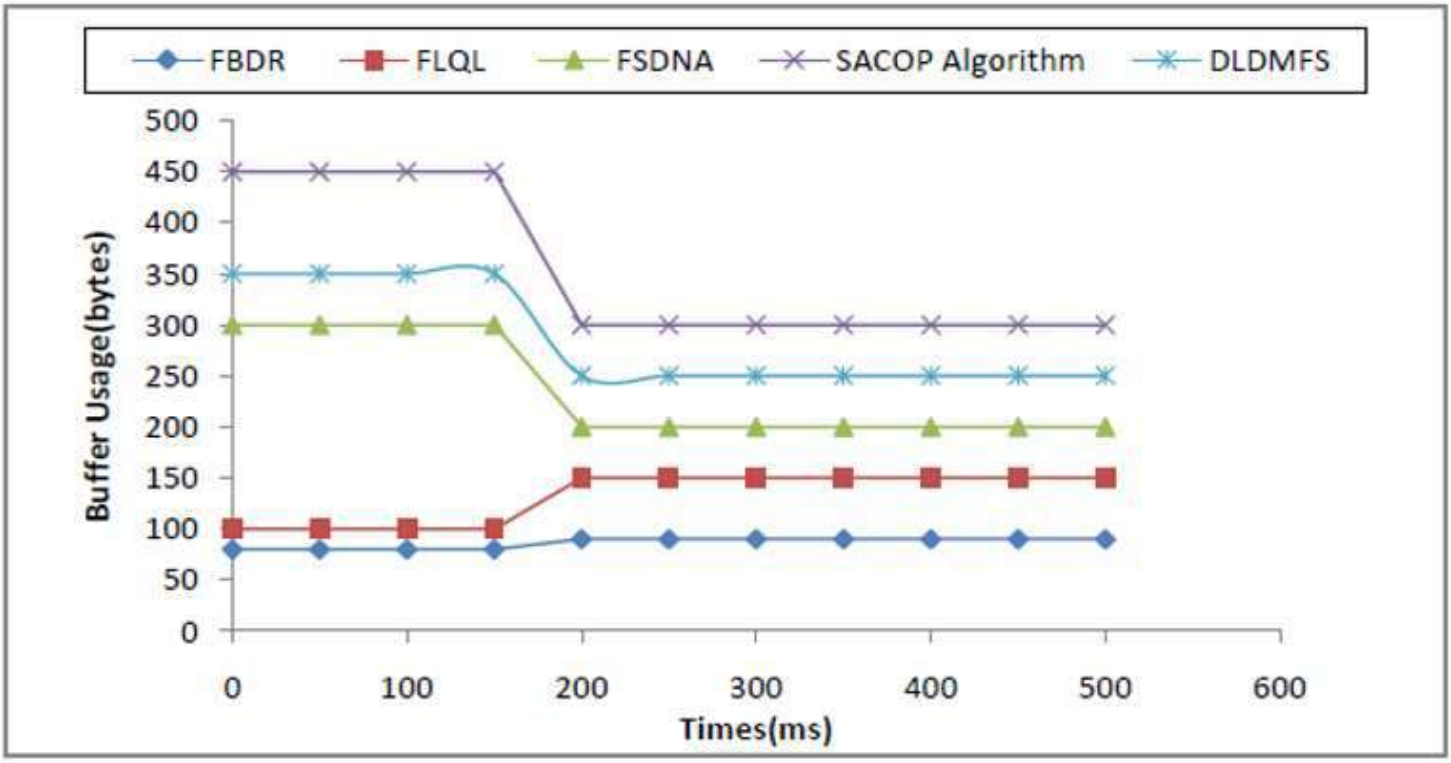

Figure 17

Buffer usage in terms of time

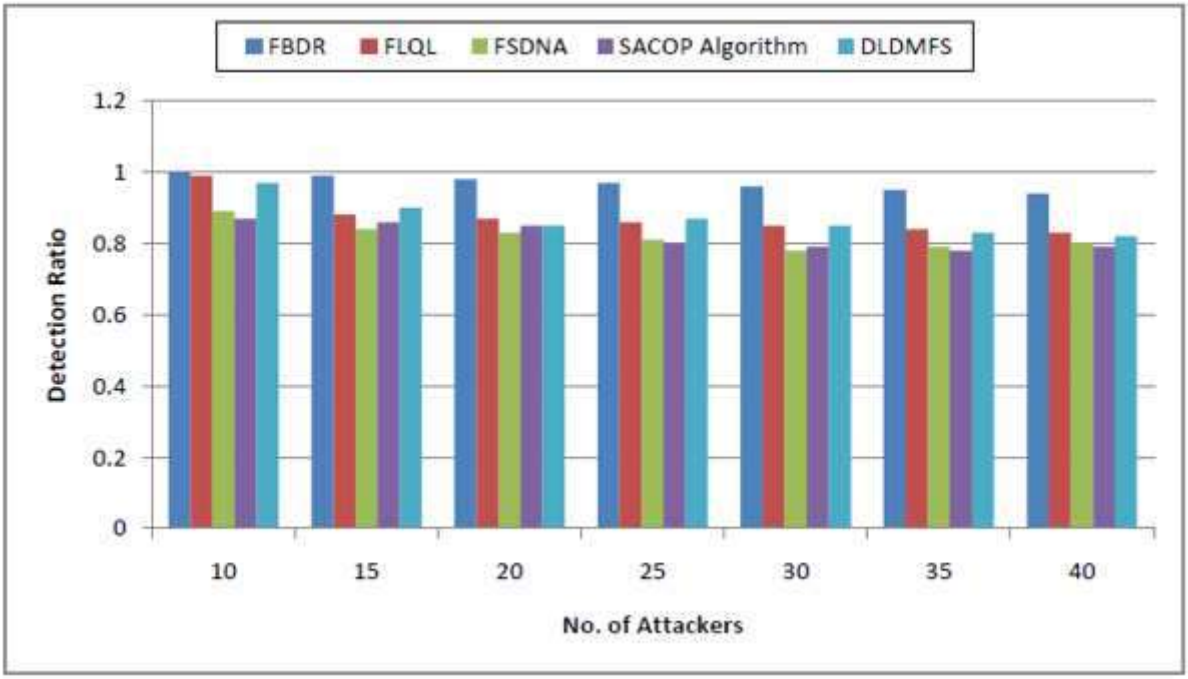

Figure 18

Detection Rate in terms of the attackers count

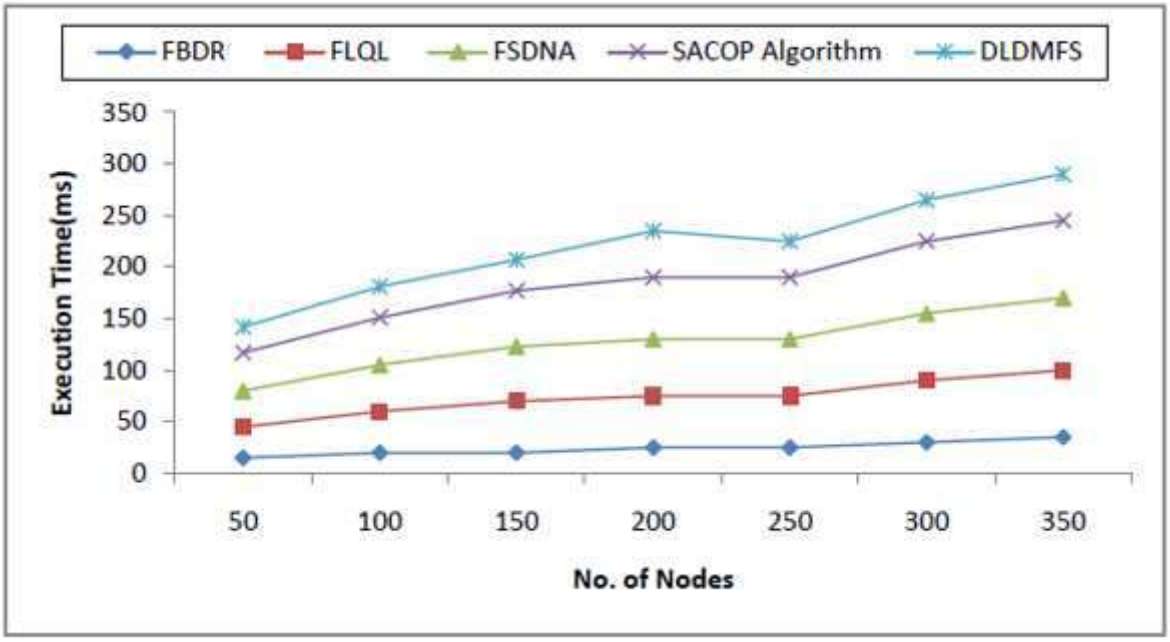

Figure 19

Execution Time in terms of the node count