Detection and Prevention of DDOS Attack by Fuzzy Rules with Grey Wolf Optimization in MANET

Aaqib Rashid[1], Rubeena Sethi[2]
[12]*ECE, Adesh Institute Of Technology Gharuan Mohali*

Abstract- Wireless sensor network is most emerging field for the research because of its large scope and optimization of power and energy. WSN is used in every field of different purposes like surveillance, monitoring and tracking etc. Due to large network and huge number of nodes connected to each other on network WSN also need a secure communication link. This research work based on the DDOS attack detection and optimization of the network by using different parameters. In this work a detailed description of attacks in wireless sensor network is presented and after this detailed literature review on the related approaches is resented. The review of different approaches and their methodology helps to improve the methodology of the work and helps to enhance the knowledge related to different types of attacks and their solution on WSN. This work presented the work on the optimization of energy and reduction in delay and packet loss during the communication on network. The optimization performed by using the grey wolf optimization algorithm which is a global optimizer which optimizes the results for effective and efficient outcomes. It improves the packet delivery rate, throughput and reduces the energy consumption and delay.

Keywords- attack, manet, fuzzy, DDOS, detection, preventation

I. INTRODUCTION

Mobile adhoc network is a type of wireless network, which includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes. It is a network of devices that can communicate the information gathered by the wireless links. The data is forwarded through multiple nodes with a gateway and the data is connected to other networks like wireless Ethernet [5][7]. These networks are used to control physical or environmental conditions like sound, pressure, temperature etc.

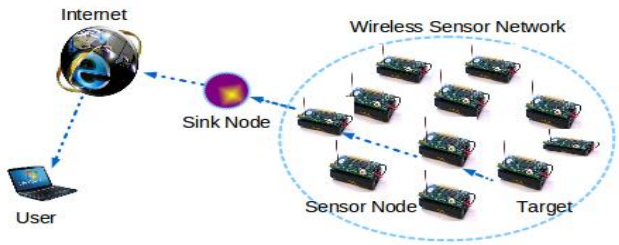


Fig.1: Mobile adhoc network

The main characteristics of the MANET are:

- *Dynamic Network Topology:* Due to wireless connection network there is no any topology for the nodes that are connected or nodes that connects after an interval of time.
- *Less Communication Failures:* Communication failure rate is less in the mobile adhoc network due to its dynamic nature, if a connection is failed then communication does not affected by it. It communicates with another connection.
- *Limited Power Consumption:* Nodes in the MANET can store very less amount of energy in it.
- *Heterogeneity of nodes:* Large numbers of nodes are able to connect in this network due to its wireless nature.
- *Deployment at large Scale:* It is easy to deploy in large area because no any additional hardware is required.
- *Scalable node capacity:*In mobile adhoc network capacity of nodes are scalable and only limited by bandwidth of gateway node.

a. MANET Architecture

There are three main components in MANET: nodes, gateways and software. Spatially distributed measured node's interface with sensors to monitor assets. The collected data transmit to gateway wirelessly, and can operate independently. It is connected to a host system where we can collect data, process, analyze and present our measurement data by using software. To extend MANET distance and reliability special type of measurement node is used such as router node. MANET is a widely used system because of its low costs and high efficiency. In a typical mobile adhoc network (MANET), sensor nodes consist of sensing, communicating, and data processing components. Sensor nodes can be used in numerous industrial, military, and agricultural applications, such as transportation traffic monitoring, environmental monitoring, smart offices, and battlefield surveillance. In these applications, sensors are deployed in an ad-hoc manner and operate autonomously. In these unattended environments, these sensors cannot be easily replaced or recharged, and energy consumption is the most critical problem that must be considered [10, 12]. The sensor is a small device which is used to detect the amount of physical parameters, event occurring, measures the presence of an object and then it converts the electrical signal value according to need it actuates a process using electrical actuators.

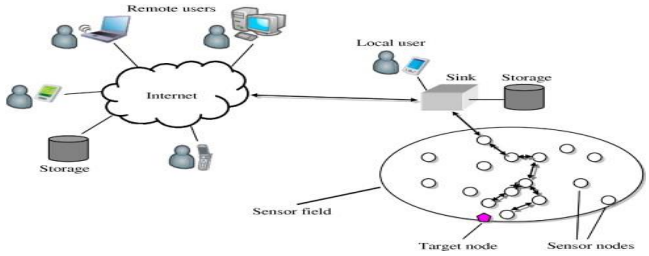


Fig.2: MANET Architecture

b. Design Issues in MANET

Following are the main design issues in the MANET which affects the performance of the system.

*1. Network Dynamic:*Routing of the messages between the nodes in MANET is more challenging task for the node stability and route stability. Stability factor is an important optimization factor with energy and bandwidth. The event can be static or dynamic it depends on the application.

*2. Node Deployment:*Node deployment in the wireless sensor actor network is deterministic or self-organizing. The nodes and sensors are deployed manually in deterministic approach and predeterministic paths are used for data routing. In self organizing nodes are scattered randomly in ad-hoc manner.

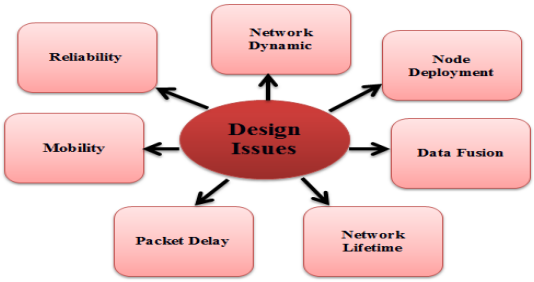


Fig.3: Design Issues of the WSAN

3. Data Fusion: The combination of data from different sources using a function such as min, max and average. These functions are done on sensor nodes for data reduction. Achieving the energy-efficient data fusion approach is a major problem for the heterogeneous network [1] [11].

*4. Network Lifetime:*The life time of the MANET is limited due to the functioning of actor nodes from battery source. Basically the life time is defined as the percentage of dead nodes below thresholds.

*5. Packet Delay:*The actor node's function in MANET is to act on the sensed data quickly and perform the required operation. It is also a design issue to design the protocols which does not considers any delay in network and nodes gives best response.

6.Reliability: The reliability of the nodes is giving the correct response by the actor nodes. Every actor nodes has a predefined time period in which it reconstructs the event, understand its intensity, location and coverage. Sometime the data sensed command may be lost due to congestion, bad connectivity and bit error.

*7. Mobility:*In WSAN, nodes are used to reduce the delay, complete the task on time and also distributed failure recovery [1].

c. Attacks on Mobile adhoc networks

Mobile adhoc network is used in various fields for the effective communication process in which user sends their information from one node to another node. Sometimes a user sends the secret information, data on the wireless network, it is very important to send this information very safely [6]. In this network sensor nodes used wireless communication and it is easy to eavesdrop. The attacker can easily inject malicious messages into the network.

Types of Attacks in MANET

1. Grey Hole Attack: This attack is modification of black hole attack. In this attack attacker node behaves like a normal node for discovering route in the network. After it discovers the route then it drop the infected packets in network. This attack is difficult to detect because packet is dropped with certainty [4].

2.Wormhole Attack: In wormhole attack, the attacker can record the data packets at one location in the network and retransmit the data from another route of the data. Wormhole attack is a serious issue that occurred into the mobile adhoc network. In the figure [3] the tunnel may be a wired link or wireless link between two nodes, this creates an illusion that the end point are very close to each other [2][10][13]. A wormhole attack has two modes.

1. Hidden mode
2. Participation mode

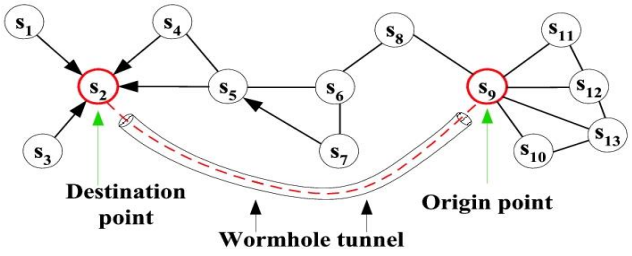


Fig.4: Wormhole Attack

3. DDOS Hole Attack: in this attack incorrect information of the routing is send to the nodes as it is low cost and it provides proper destination node. Due to incorrect routing information it leads to packet loss and manipulation in original data packets. This attack disturbs all the network process because nodes are sometime dependent on each other for information [4].There are two types of DDOS hole attack one is simple DDOS hole attack and other is using worm hole attack.The simple DDOS hole attack, malicious neighbour node behaves itself as a best route to the base station andattract the other

nodes to use this route frequently. During this route malicious node is able to tamper the data which is a big challenge in security of network.

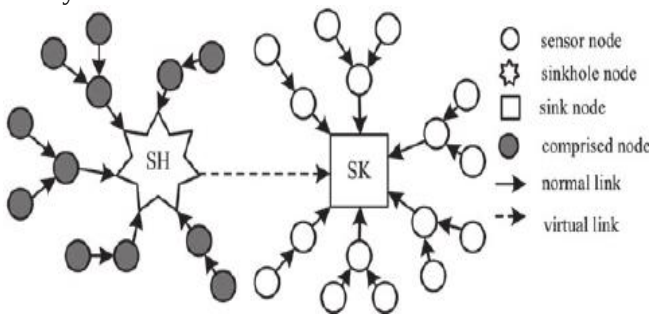


Fig.4: DDOS attack

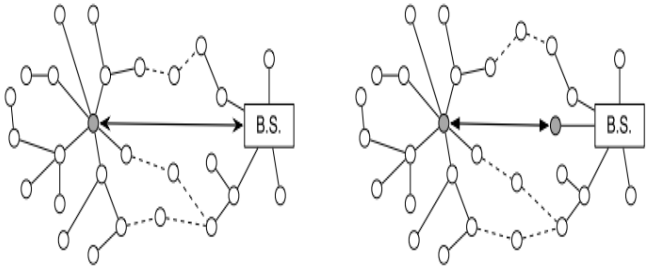


Fig.5: DDOS attack (a) and (b) DDOS hole using wormhole attack

In the other DDOS hole attack with worm hole attack, malicious node capture the node from the nearest neighbour and use the tunnel to send the packet to another colluded node. This colluded node also delivers the message to the base station.In DDOS hole attack, a malicious node acts as a black hole to draw all the site visitors within the sensor network via a compromised node growing a metaphorical DDOS hole with the adversary on the center. A compromised node is located on the center, which appears appealing to surrounding nodes and lures nearly all the site visitors destined for a base station from the sensor nodes. Thus, developing a metaphorical DDOS hole with the adversary at the center, from wherein it may appeal to the most traffic, possibly closer to the base station in order that the malicious node may be perceived as a base station. This DDOS hole attracts visitors from nearly all of the nodes to the direction through it.The main goal of our work is to effectively perceive the actual intruder (SH) in the DDOS attack. Once its miles identified, a routing protocol or a better-layer utility can easily isolate the intruder from the community to keep away from similarly loss. We assume that the base station is bodily protected or has tamper-robust hardware as a result, it acts as a vital depended on authority in our algorithm layout. The base station also has a tough understanding of the region of nodes, which will be available after the node deployment degree or received with the aid of diverse localization mechanisms.

4.Link spoofing Attack: In this attack a fake link is displayed with the neighbouring node which disturbs the routing process with the other nodes. Malicious code is sent over this link and it drops the data packets. This type of attack can be detected by OLSR protocol because it determined the node which sends the malicious code. In this types of attack message is completely lost [3].

5. Grey Hole Attack: This attack is modification of black hole attack. In this attack attacker node behaves like a normal node for discovering route in the network. After it discovers the route then it drop the infected packets in network. This attack is difficult to detect because packet is dropped with certainty [4].

6. Black Hole Attack: In this type of attack, attacker supposed to communicate packets in the network rather than discard the packets. The reason behind this attack is that a node is compromised from different number of causes. In this attack, packets are dropped from the loss network. It is not easy to detect this type of attacks [3].

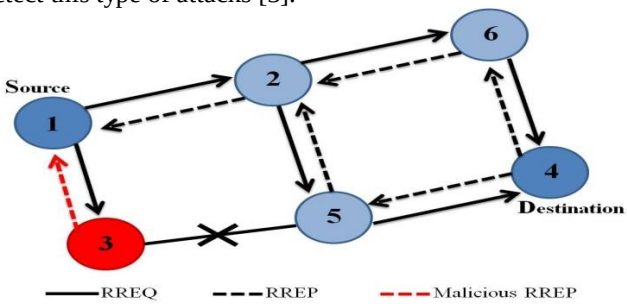


Fig.6: Black Hole Attack

II. RELATED WORK

Zhang, Zhaohui, et al. [1] explained an energy efficient DDOS hole detection approach which detects the malicious node effectively than the existing nodes. In this approach frequency of all nodes is established by m routes with optimal hops from per node to DDOS node. This method is based on the dynamic programming. This approach enhanced the detection rate and false positive rate. Devibala, K., et al. [2] proposed neighbor constraint traffic centric approach which is used to detect DDOS attack and improve the quality of the MANET. It identifies the malicious node by the data send by neighbor node. It verifies the location of the node from where data is send to the node. This method provides DDOS hole detection with high throughput and packet delivery ratio. Mittal et al. [3] proposed the major goal to analyze the effective protocol for the mobile adhoc network. This analysis shows that the access control method and authentication methods are used in the MANET. This analysis shows that most of the approaches are based on the public key cryptography, which is the most

expensive method. This paper provides a detailed comparative analysis of protocols with their advantages and disadvantages of each other.Yasin, N. Mohammaed, et al. [4] described the anomaly detection approach which detects the DDOS attack in mobile adhoc networks. This type of attack is not easy to detect due virtual path of the node. In this work Acceptance Acknowledgement approach is used to activate the digital signature system. This approach does not make any impact on the network and provides high detection rate of the malicious node. Saghar et al. [5] proposed the RAEED protocol which is used to detect the simple and intelligent tunnel attacks. This protocol helps to reduce the problem of DOS attack which disturbs the data routing and forward the data comes from the DDOS node. In future this work will be enhanced by applying formal methods to verify the communication issues. Saghar et al. [6] focused on the security issues of the mobile adhoc network. It considers the Denial-of-Service attack on the data during the routing process. In this type of attack, the attacker attracts the traffic towards it and prevents the data from the neighboring node. This paper provides a protocol for the DOS attacks called as RAEED. It detects the simple and intelligent tunnel attacks very effectively. Jan, Mian, et al. [7] proposed a lightweight payload-based mutual authentication approach for a cluster based mobile adhoc network. This is also called as PAWN approach. During the implementation process, it is implanted in two steps. First, the optimal percentages of the cluster heads are selected authenticated and allowed to communicate with the neighbouring nodes. Second, each cluster head is in a role of server and provides the authentication to the nearby nodes. This scheme is validated with various schemes and the results show that if performed very well.

Kumar et al. [8] proposed a localization algorithm which prevents from the Wormhole attack in the mobile adhoc network. This algorithm is used to identify the unauthorized nodes by using the distance estimation method and Maximum Likelihood Estimation (MLE) to calculate the required location. The results in comparison show that this algorithm performed better than the existing algorithms. Vidhya, et al. [9] worked on the detection of DDOS attack in AODV routing. This method uses energy power consumption in AODV and external energy by using battery. In this work MD5 algorithm is proposed for DDOS hole attack detection which prevent the network from the sever attack. This algorithm checks the energy transmitted by the node to the other nodes. This algorithm work effectively and enhance the packet delivery rate and throughput. It reduces the end to end delay in the network.Jahandoust, et al. [10] (2017) described the adaptive DDOS hole aware algorithm in mobile adhoc network. This work is based on the finding probability of affected nodes by DDOS attack. In this the routing of the nodes is based on AODV protocols to route packets over the most reliable nodes. The subjective model identifies the behavior of the nodes in data receiving and sending. The behavior of whole network is observed by using probabilistic automation and captures the behavior of the network which is generated at the base station. The result of the proposed approach provides low packet loss rate and effective routing between the reliable nodes. Kalnoor, et al. [11] worked on the clustered network in mobile adhoc network to detect the DDOS attack. This method is based on the agent-based quality of service to detect the DDOS attack. The agent-based approach detects the attack effectively and enhances the network performance. Agent based protocol is very helpful to provides the effective performance and throughput. Saranya et al. [12] In this paper, the author focused on the packet scheduling technique for the ad-hoc on demand distance vector (AODV) protocol. In this transitional node starts the packet scheduling and manage the memory, according to the flow of data. Data packets are stored and route repaired by the intermediate node. In the proposed scheme data packets are utilized by backup routes not to dropping it. Ma, Rui, et al. [13] proposed two types of defence strategies that are based on the monitoring the behaviour of neighbouring node and location information of the neighbouring node. In this paper, the concept of packet encapsulation is used to provide the most effective method for wormhole attack. Running a state is simulated under the normal condition and wormhole condition by using OMNET++ simulation environment. In wormhole attack, the running state applies to defence method which is based on location information and monitoring the neighbour node. The analysis results of the simulation show that it works effectively on the attacks in MANET.

III. THE PROPOSED METHOD

A. Proposed Methodology

Methodology Steps:

Step 1: Deploy the mobile adhoc network.

Step 2: Apply the leach routing process.Leach is basically a clustering based protocol which is used to reduce the energy dissipation in the networks

Step 3: Simulate the DDOS hole attack on the mobile adhoc network and parallel optimize by GWO algorithm.

Step 4: Initialize the grey wolf optimization

{

Initialize the generation counter u and randomly initialize the population of wolf P_i in which P_i(1, 2, 3,.....n).

Initialize the value of P_0 randomly.

Initialize parameters a, A and C.

}

Calculate the Fitness of the each wolf

$P_\alpha = 1^{st} Best\ wolf$

$P_\beta = T\square e\ 2^{nd}\ best\ wolf$

$P_\delta = T\square e\ 3^{rd}\ best\ wolf$

- Update the fitness function.

Update the chaotic map equation
for each search agent
Update the position of current wolf using Eq. (4)
end for
Update Parameters a, A and C.
Calculate the fitness of all wolves
$Update\ P_{\alpha}, P_{\beta} P_{\delta}.$

- Check the objective function
Replace the worst fit wolf with the best fit wolf
u=u+1

end While
Return P_{α}

- Check it optimize or not it optimized then analysis the time and dead node otherwise check the counter is greater than 0 or not. If the counter value is less than not converge and ignore the node during routing. Else again initialize the value at GWO.

}

B. ***Proposed methodology: Flowchart***

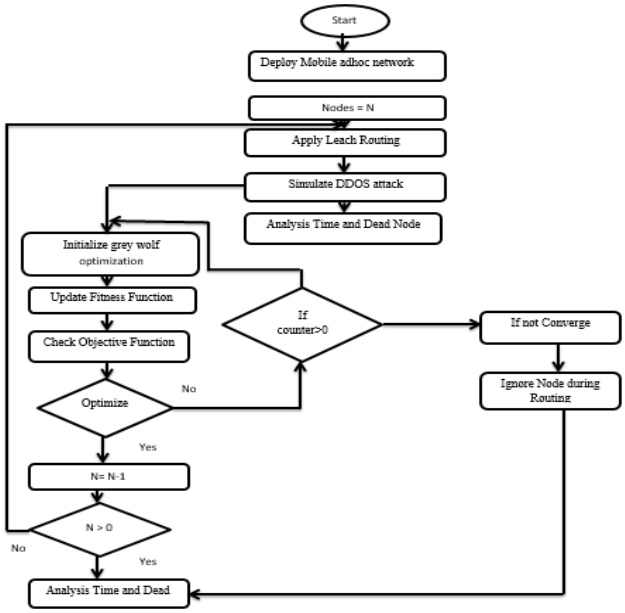


Fig.7: Proposed Flowchart

C. Algorithm Used

1. Grey Wolf Optimizer (GWO):Grey Wolf optimization algorithm is a bio-inspired algorithm which is based on the leadership and hunting behaviour of the wolves in the pack. The grey wolves prefer to live in the pack which is a group of approximate 5-12 wolves. In the pack each member has social dominant and consisting according to four different levels. The below given figure shows the social hierarchy of the wolves which plays and important role in hunting.

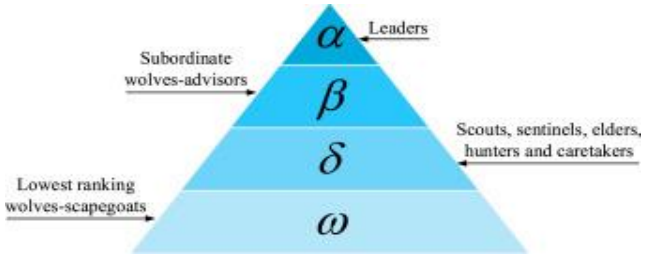


Fig.8: GWO Hierarchy [36]

1. The wolves on the first level are called alpha wolves (α) and they are leaders in the hierarchy. Wolves at this level are the guides to the hunting process in which other wolves seek, follow and hunt and work as a team. Decision making is the main task that is performed by the alpha wolves and the order by the alpha wolves is followed by all members of the pack.
2. Second level wolves are called beta (β). These wolves are called subordinates and advisors of alpha nodes. The beta wolf council helps in decision making. Beta wolves transmit alpha control to the entire packet and transmit the return to alpha.
3. The wolves of the third level are called Delta wolves (δ) and called scouts. Scout wolves at this level are responsible for monitoring boundaries and territory. The sentinel wolves are responsible for protecting the pack and the guards are responsible for the care of the wounded and injured.
4. The last and fourth level of the hierarchy are called Omega (ω). They are also called scapegoats and they must submit to all the other dominant wolves. These wolves follow the other three wolves.

Grey wolves have the ability of memorizing the prey position and encircling them. The alpha as a leader performs in the hunt. For simulating the grey wolves hunting behaviour in the mathematical model, assuming the alpha (α) is the best solution. The second optimal solution is beta (β) and the third optimal solution is delta (δ). Omega (ω) is assumed to be the candidate solutions. Alpha, beta, and delta guide the hunting while position should be updated by the omega wolves by these three best solutions consideration.

Encircling prey: Prey encircled by the grey wolves during their hunt. Encircling behaviour in the mathematical model, below equations is utilized.

$$\vec{\square}(\square + 1) = \vec{\square_{\square}}(\square) - \vec{\square}.\vec{\square}$$
$$\vec{\square} = \left|\vec{\square}.\vec{\square_{\square}}(\square) - \vec{\square}(\square)\right|$$

Where
T←iterative number
$\vec{\square}$←grey wolf position
$\vec{\square_{\square}}$←prey position

$$\vec{\square} = 2\square.\vec{\square_1} - \square$$
$$\vec{\square} = 2\vec{\square_2}$$

Where
$\vec{\square_1}$and$\vec{\square_2}$←random vector range[0,1]

The x value decreased from 2 to 0 over the iteration course.

$\vec{\square}$←random value with range [0,1] and is used for providing random weights for defining prey attractiveness.

Hunting: For grey wolves hunting behaviour simulation, assuming □, □ and □ have better knowledge about possible prey location. The three best solutions firstly and □ (other search agents) are forced for their position update in accordance to their best search agents position. Updating the wolves' positions as follows:

$$\vec{\square}(\square + 1) = \frac{\vec{\square_1}+\vec{\square_2}+\vec{\square_3}}{3} \quad (1)$$

Where $\vec{\square_1}, \vec{\square_2}, \square\square\square \vec{\square_3}$ are determined,

$$\vec{\square_1} = \left|\vec{\square_\square} - \vec{\square_1}.\vec{\square_\square}\right|$$
$$\vec{\square_2} = \left|\vec{\square_\square} - \vec{\square_2}.\vec{\square_\square}\right|$$
$$\vec{\square_3} = \left|\vec{\square_\square} - \vec{\square_3}.\vec{\square_\square}\right|$$

Where $\vec{\square_\square}, \vec{\square_\square}, \square\square\square \vec{\square_\square}$← first three best solution at a given iterative T

$\square_\square$, $\square_\square$, and $\square_\square$ are determined,

$$\vec{\square_\square} \leftarrow \left|\vec{\square_1}.\vec{\square_\square} - \vec{\square}\right|$$
$$\vec{\square_\square} \leftarrow \left|\vec{\square_2}.\vec{\square_\square} - \vec{\square}\right|$$
$$\vec{\square_\square} \leftarrow \left|\vec{\square_3}.\vec{\square_\square} - \vec{\square}\right|$$

The parameter x updating is the final process. The parameter x exploitation and exploration is updated linearly for ranging [2,0] in every iteration.

$$\square = 2 - \square\frac{2}{\square\square\square\square}$$

Where

T←iterative number

MaxI←total number of iteration

IV. RESULT ANALYSIS

This work describes the results of the proposed work and its comparison with the existing work. The parameters used for the result analysis are alive nodes, dead node, cluster heads, throughput, energy consumption and time delay. The comparison of results shows the changes according to the number of nodes changed.

A. Alive Nodes

Table 1 Alive nodes in Existing Algorithm and GWO-DDOS

No of Nodes	Without Optimization	Optimization with GWO DDOS
10	100	100
20	100	100
30	97	100
40	96	100
50	90	100
60	85	98
70	80	89
80	40	62
90	14	29
100	1	5

The above given figure 7 depicts the total number of alive nodes in the existing and proposed GWO-DDOS Approach. The blue bar of the graph represents the alive nodes in existing approach and red bar represents the alive nodes in GWO-DDOS. The alive nodes in GWO-DDOS are high than the existing which enhance the efficiency of the network.

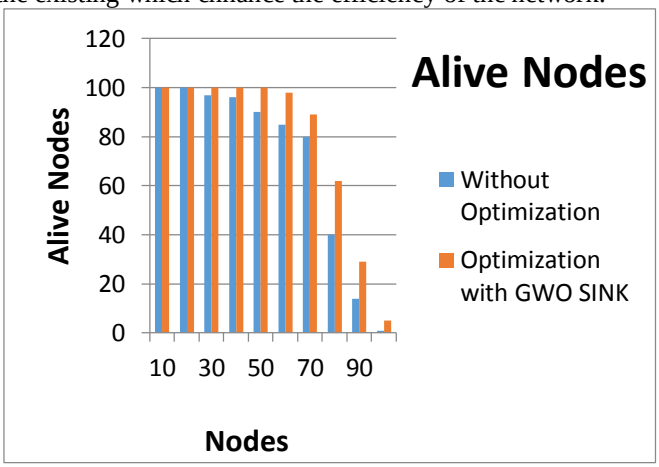


Fig.9: Alive nodes in Existing Algorithm and GWO-DDOS

B. *Throughput*

Throughput of the nodes shows the total packet delivered over the number of packet send in the given duration.

$$Throughput = \frac{\square\square.\square\square\ \square\square\square\square\square\square\square\square\ \square\square\square\square\square\square\ *\ \square\square\square\square\square\square\ \square\square\square\square*\square}{\square\square\square\square\square\ \square\square\square\square\square\square\square\square\ \square\square\ \square\square\square\square\square\square\square\square\square\square\square}$$

Table 2 Throughput in Existing Algorithm and GWO-DDOS

No of Nodes	Without Optimization	Optimization with GWO DDOS
10	1000	1000
20	1850	1850
30	2700	2820
40	3600	3750
50	4200	4300
60	5100	5250
70	5720	5880
80	6200	6500
90	6500	6900
100	6950	8550

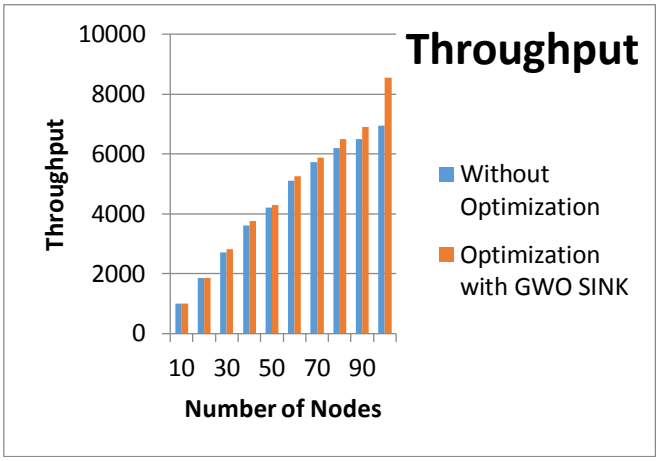


Fig.10: Throughputs in Existing Algorithm and GWO-DDOS

The above given figure 8 depicts the throughput in the existing and proposed GWO-DDOS Approach. The blue bar of the graph represents the throughput of existing approach and red bar represents the throughput of GWO-DDOS. The throughput of GWO-DDOS is high than the existing approach which enhanced the efficiency of the network. This is due to the grey wolf optimization algorithm which provides the optimal modes during the data transfer which takes less time in packet delivery and enhance the throughput of the network.

C. Dead Nodes

Table 3 Dead Nodes in Existing Algorithm and GWO-DDOS

No of Nodes	Without Optimization	Optimization with GWO DDOS
10	00	00
20	00	00
30	2	00
40	3	00
50	11	00
60	15	03
70	19	9
80	57	34
90	80	69
100	99	97

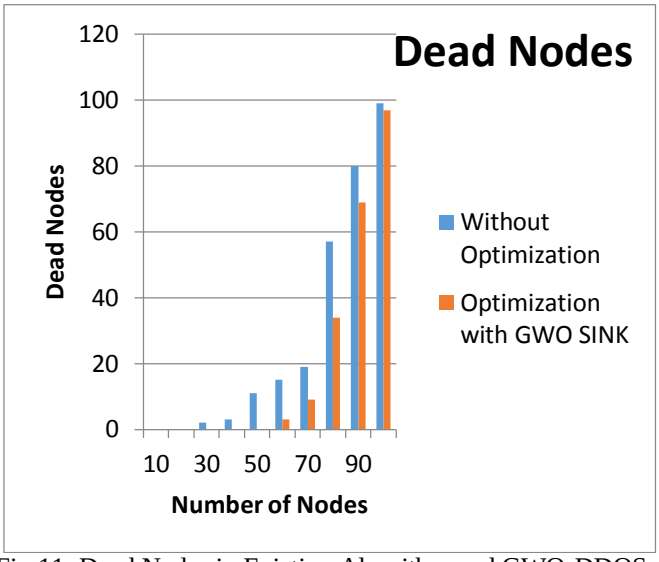


Fig.11: Dead Nodes in Existing Algorithm and GWO-DDOS

The above given figure 9 depicts the total number of dead nodes in the existing and proposed GWO-DDOS Approach. The blue bar of the graph represents the dead nodes in existing approach and red bar represents the dead nodes in GWO-DDOS. The dead nodes in GWO-DDOS are less than the existing which enhance the efficiency of the network because if dead node if high then the performance of network is degraded.

D. Time Delay

Time delay is the time period which taken by the node for the specific packet. It shows that time delay is less than network produce effective throughput.

Time Delay = Packet Sending Time (in m/sec) +Packet Delivery Time (in m/sec)

Table 4: Time Delay in Existing Algorithm and GWO-DDOS

No of Nodes	Without Optimization	Optimization with GWO DDOS
10	100	95
20	200	192
30	297	288
40	420	400
50	499	496
60	585	570
70	685	640
80	750	720
90	800	780
100	890	810

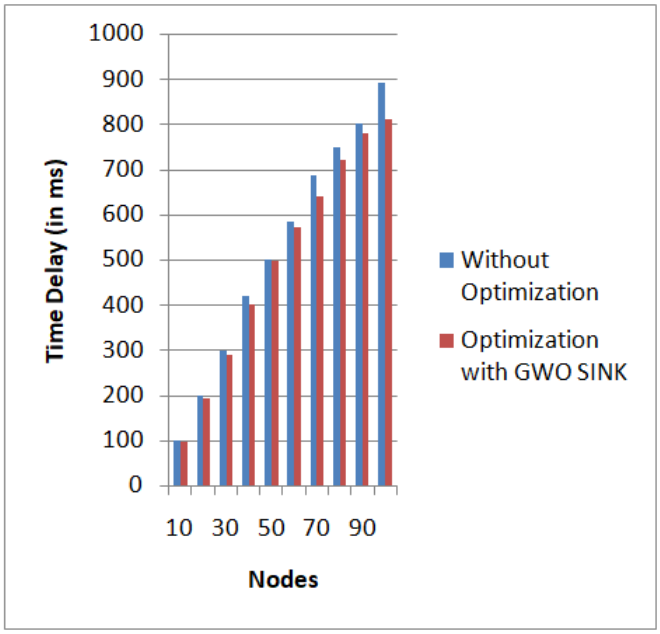


Fig.12: Time Delay in Existing Algorithm and GWO-DDOS

The above given figure 4.4 depicts the time delay in the existing and proposed GWO-DDOS Approach. The blue bar of the graph represents the time delay in existing approach and red bar represents the time delay in GWO-DDOS. The time delay in the proposed GWO-DDOS approach is less than existing approach which improves the network quality because if delay is less than packets deliver fast and enhance the communication process.

E. Energy Consumption

The below given table represents the total energy consumed by the nodes to transmit the data packets. If the nodes consume lot of energy then it is costly and less efficient. The proposed algorithm consumes less energy as compare to existing approach.

Energy Consumption= Packet Sending Energy+ Packet Delivery Energy

Table 5: Energy Consumption in Existing Algorithm and GWO-DDOS

No of Nodes	Without Optimization	Optimization with GWO DDOS
10	4.6	4.4
20	3.8	3.7
30	3.2	2.9
40	2.7	2.4
50	2.0	1.6
60	1.2	1.0
70	0.6	0.4

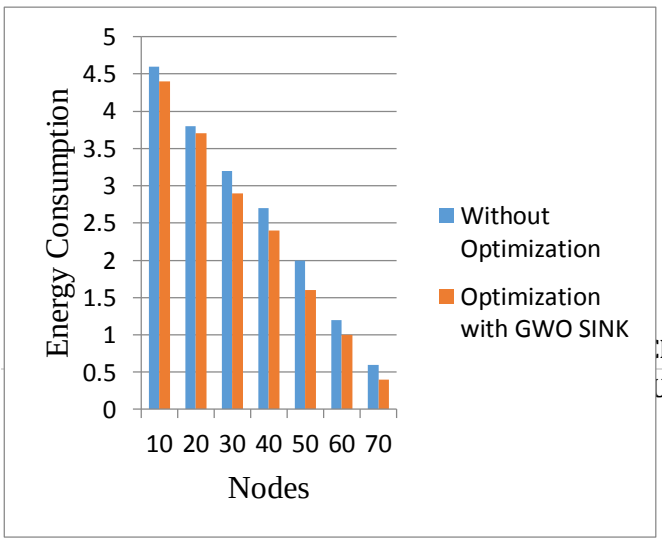


Fig.13: Energy Consumption in Existing Algorithm and GWO-DDOS

The above given figure 10 depicts the energy consumption in the existing and proposed GWO-DDOS Approach. The blue bar of the graph represents the energy consumption in existing approach and red bar represents the energy consumption in GWO-DDOS. The energy consumption in the proposed GWO-DDOS approach is less than existing approach which improves the network quality because if energy consumption is less than it also uses low resources which improves network quality.

F. Count of Cluster Heads

Cluster is a group of nodes and the group of clusters has a cluster head which controls the activities of the nodes in the clusters. The high numbers of clusters shows the high number of working or active node in the network. The number of cluster heads in the proposed algorithm is high.The number of cluster heads in the proposed algorithm is high.

Table 6 Cluster heads in Existing Algorithm and GWO-DDOS

No of Nodes	Without Optimization	Optimization with GWO DDOS
10	9.2	13.4
20	10.1	12.7
30	11.7	12.5
40	10.8	12.3
50	11.2	11.9
60	8.7	9.2
70	6.1	7.8
80	4.6	5.8
90	2.8	4.1
100	00	2.1

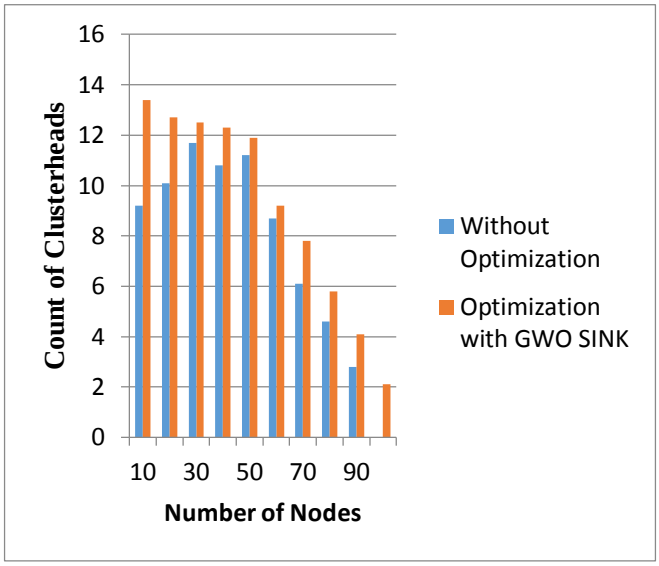


Fig.14: Cluster Heads in Existing Algorithm and GWO-DDOS

The above given figure 11 depicts the energy consumption in the existing and proposed GWO-DDOS Approach. The blue bar of the graph represents the energy consumption in existing approach and red bar represents the energy consumption in GWO-DDOS.

G. Packet Delivery Rate

Packet delivery rate is defined as the total packet delivered in the given slot of time. It shows the efficiency of the network by sending more packets in less time. It is calculated by using following formula:

PDR (Packet delivery rate) = Total number of Packets Send / Time (msec)

Table 7: Packet Delivery Rate in Existing Algorithm and GWO-DDOS

No of Nodes	Without Optimization	Optimization with GWO DDOS
10	800	1100
20	780	1050
30	750	980
40	730	900
50	690	720
60	540	700
70	400	1375
80	350	1740
90	110	2100
100	50	2400

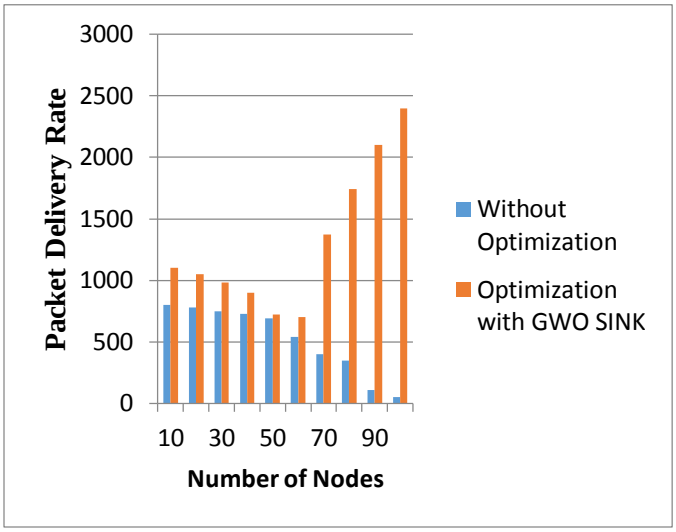


Figure 12 Packet Delivery Rate in Existing Algorithm and GWO-DDOS

The above given figure 12 depicts the packet delivery rate of the existing and proposed GWO-DDOS Approach. The blue bar of the graph represents the packet delivery rate of the existing approach red bar represents the packet delivery rate of GWO-DDOS. The packet delivery rate of the proposed approach is better than existing graph represents the packet delivery rate of the existing approach which makes communication more effective. This is due to effective GWO result and it improves the packet delivery rate.

H. Overall Result Analysis

The table given below depicts the overall result of the existing and proposed approach on various metrics. The analysis based on the alive nodes in the network, throughput of the network, dead nodes on the network, time delay, and packet delivery rate. The alive node shows the total available node during the communication on network which is high in the GWO approach.The throughput defines the total packet delivered in the given time which is more in GWO approach. The dead nodes are that node which does not active or not performs any function in the network they are high in the existing method and less in proposed approach.

Table 8 Overall results Analysis table of Existing approach and proposed GWO-DDOS approach

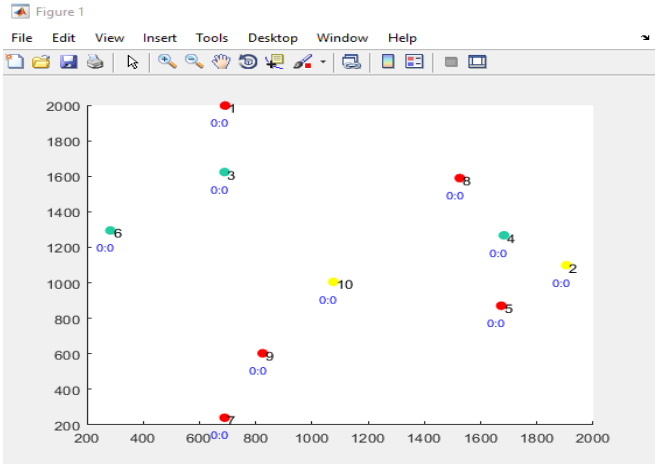
No of Nodes	Alive Nodes		Throughput		Dead Nodes		Time Delay		Packet Delivery Rate	
	Without	Optim	Withou	Optimiz	Withou	Optimiz	Withou	Optimi	Witho	Optimi

	Optimization	ization with GWO DDOS	t Optimization	ation with GWO DDOS	t Optimization	ation with GWO DDOS	t Optimization	zation with GWO DDOS	ut Optimization	zation with GWO DDOS
10	100	100	1000	1000	00	00	100	95	800	1100
20	100	100	1850	1850	00	00	200	192	780	1050
30	97	100	2700	2820	2	00	297	288	750	980
40	96	100	3600	3750	3	00	420	400	730	900
50	90	100	4200	4300	11	00	499	496	690	720
60	85	98	5100	5250	15	03	585	570	540	700
70	80	89	5720	5880	19	9	685	640	400	1375
80	40	62	6200	6500	57	34	750	720	350	1740
90	14	29	6500	6900	80	69	800	780	110	2100
100	1	5	6950	8550	99	97	890	810	50	2400

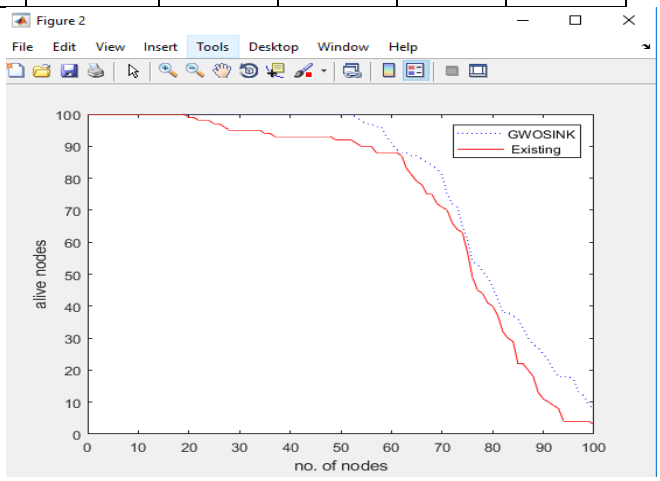
The time delay in the existing approach is high during data transfer and it also enhances the packet delivery rate and reduces the efficiency. The time delay, throughput, and packet delivery rate is improved by the grey wolf optimization algorithm in the proposed work and it also shown in the above defined graphs and their outcomes.

I. Simulation Results

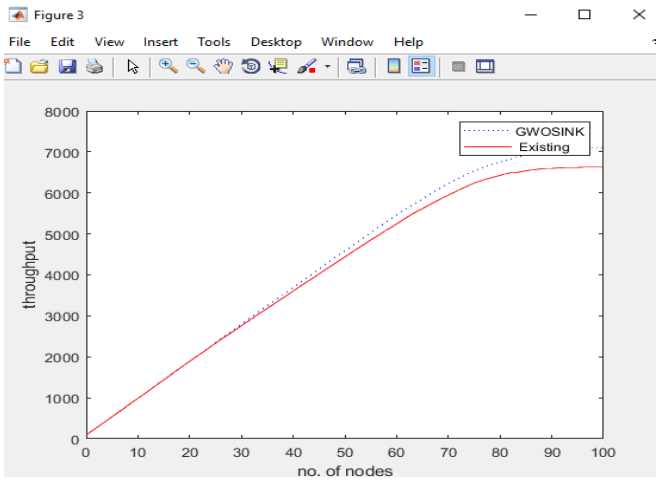
a. Nodes



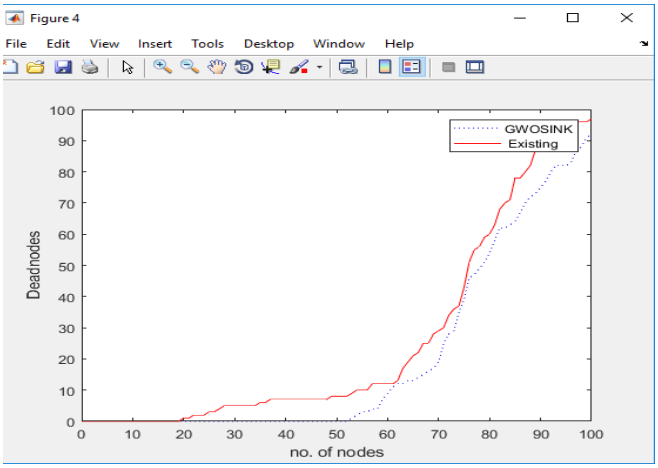
b. Alive Nodes



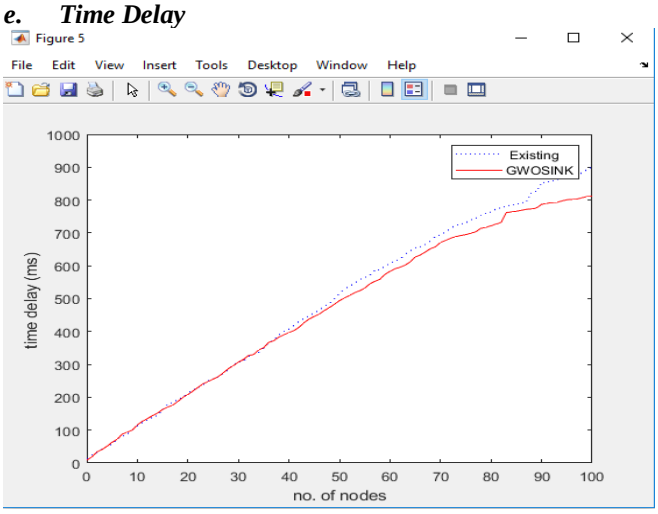
c. Throughput



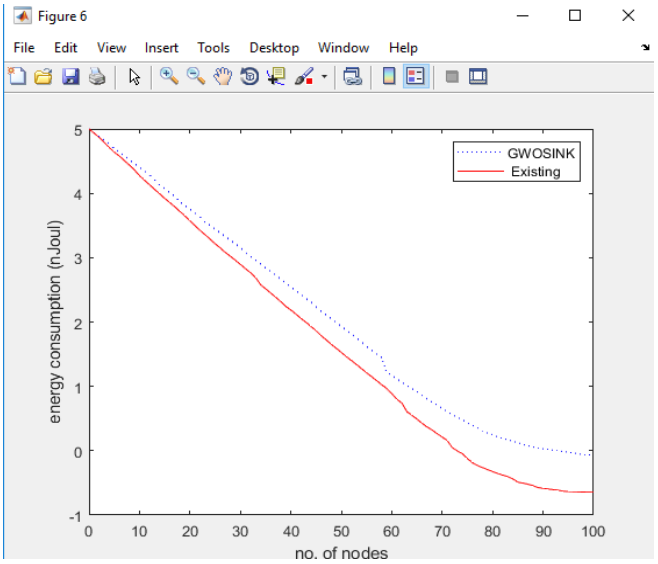
d. Dead Nodes



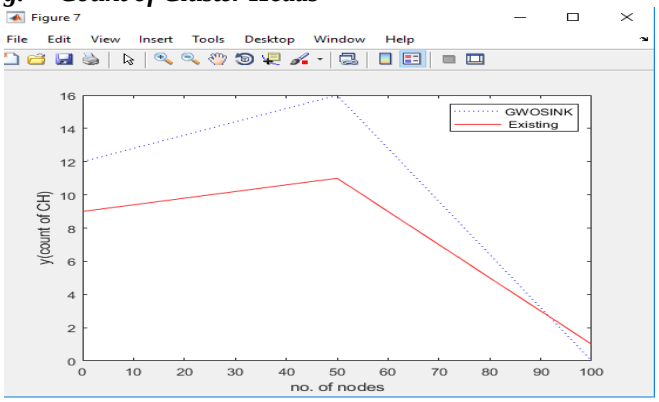
e. Time Delay



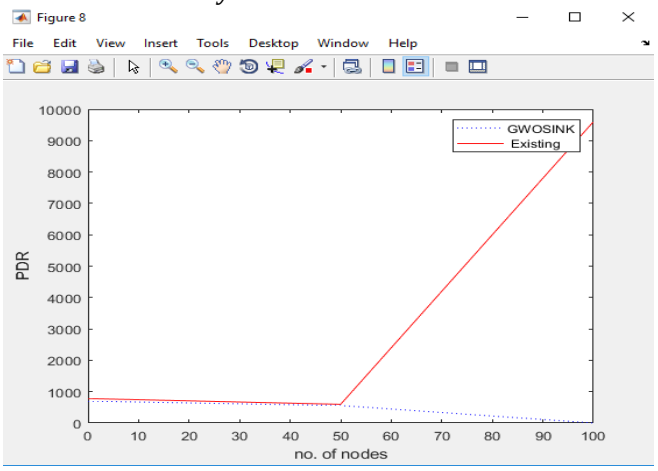
f. Energy Consumed



g. Count of Cluster Heads



h. Packet Delivery rate



V. CONCLUSION

Mobile adhoc network (MANET) contains sensor nodes which mainly used for sensing, communicating and data

processing. Sensor nodes can be used in many fields like industries, military, and agricultural applications, such as transportation traffic monitoring, environmental monitoring, smart offices, and battlefield surveillance. In these applications, sensors are deployed in an ad-hoc manner and operate autonomously. In these unattended environments, these sensors cannot be easily replaced or recharged, and energy consumption is the most critical problem that must be considered. This research work done on the mobile adhoc network by using the concept of leach routing of nodes and optimize the routing process by using Grey Wolf Optimization algorithm. The GWO algorithm provides the optimal results. The optimal result provided by GWO reduced the time delay, dead nodes and energy consumption and improve the network quality. It enhanced the packet delivery rate and number of cluster heads in mobile adhoc network.

VI. REFERENCES

[1]. Zhang, Zhaohui, et al. "M optimal routes hops strategy: detecting DDOS attacks in mobile adhoc networks." *Cluster Computing* (2018): pp: 1-9.

[2]. Mitigation approach for quality of service improvement in mobile adhoc networks." *Industry Interactive Innovations in Science, Engineering and Technology*. Springer, Singapore, 2018. pp: 357-366.

[3]. Mittal, Vikas, Sunil Gupta, and Tanupriya Choudhury. "Comparative Analysis of Authentication and Access Control Protocols against Malicious Attacks in Mobile adhoc networks." *Smart Computing and Informatics*. Springer, Singapore, 2018. pp: 255-262.

[4]. Yasin, N. Mohammaed, et al. "ADSMS: Anomaly Detection Scheme for Mitigating DDOS Hole Attack in Mobile adhoc network." *Technical Advancements in Computers and Communications (ICTACC), 2017 International Conference on*. IEEE, 2017 pp. 154-159.

[5]. Saghar, Kashif, HunainaFarid, and Ahmed Bouridane. "Formally verified solution to resolve tunnel attacks in mobile adhoc network." *Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on*. IEEE, 2017, pp. 448-455.

[6]. Vidhya, S., and T. Sasilatha. "DDOS attack Detection in MANET using Pure MD5 Algorithm." *Indian Journal of Science and Technology* 10.24 (2017).

[7]. Jahandoust, Ghazaleh, and FatemehGhassemi. "An adaptive DDOS hole aware algorithm in mobile adhoc networks." *Ad Hoc Networks* 59 (2017) pp: 24-34.

[8]. Kalnoor, Gauri, JayashreeAgarkhed, and Siddarama R. Patil. "Agent-Based QoS Routing for Intrusion Detection of DDOS attack in Clustered Mobile adhoc networks." *Proceedings of the First International Conference on Computational Intelligence and Informatics*. Springer, Singapore, 2017, pp. 571-583.

[9]. Saranya, P., Abin P. Varghese, and R. S. Balaji. "DETECTING AND PREVENTING THE WORMHOLE ATTACKS IN MOBILE ADHOC NETWORK." *traffic* 3.04 (2017).

[10]. Ma, Rui, et al. "Defences against Wormhole Attacks in Mobile adhoc networks." *International Conference on Network and System Security*. Springer, Cham, 2017, pp. 413-426.

[11]. Saghar, Kashif, HunainaFarid, and Ahmed Bouridane. "Formally verified solution to resolve tunnel attacks in mobile adhoc network." *Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on*. IEEE, 2017, pp. 448-455.

[12]. Jan, Mian, et al. "PAWN: a payload- based mutual authentication scheme for mobile adhoc networks." *Concurrency and Computation: Practice and Experience*29.17 (2017).

[13]. Kumar, Gulshan, Mritunjay Kumar Rai, and Rahul Saha. "Securing range free localization against wormhole attack using distance estimation and maximum likelihood estimation in Mobile adhoc networks." *Journal of Network and Computer* Applications 99 (2017): pp: 10-16.