Novel Approach of Black Hole Attack Detection and Prevention by Convex Optimization

GbazoeKelezonga Daniel[1], Anuj Gupta[2]
Computer Science Engineering
(Alakh Prakash Goyal) Shimla University

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. This paper 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- WSN, Prevention, optimization, Attack

I. INTRODUCTION

In a typical wireless sensor network (WSN), sensor nodes consist of detection, communication, and data processing components. Sensor nodes can be used in many industrial, military and agricultural applications, such as transport traffic monitoring, environmental monitoring, smart offices and battlefield surveillance. In these applications, the sensors are distributed ad-hoc and operate autonomously. In these unmanned environments, these sensors cannot easily be replaced or recharged, and energy consumption is the most critical problem that needs to be considered. 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.

In WSN, the attacks are mainly affecting the functionality of network layer which is responsible for the routing in MANET. There are mainly two types of attacks which are occurred in the mobile ad-hoc network.

A. Active Attack

In active attack, attacker modifies the content of data which is exchanged in the network. In this process attacker can inject the new packets, drop the packets and modify the existing data packets. This type of attacks is very harmful for the network and the senders. It is further divided into two parts the attack done by the node which present in network is called internal attack and node which attack from outside is called external attack.

B. Passive Attack

In passive attack, the attacker captures the data without altering of modifying it. This attack does not affect the normal working of the network this is the main difficulty reason in detection. This attack is done mainly to gather the information about the communication between the sender and receiver.

The rest of the paper consider the related study of black hole attack and approaches used to avoid it and the propose methodology using grey wolf optimization.

II. RELATED STUDY

Saghar et al. focused on the security issues of the wireless sensor 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 [1]. Jan, Mian, et al. proposed a lightweight payload-based mutual authentication approach for a cluster based wireless sensor 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 neighboring 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 [2].

Kumar et al. proposed a localization algorithm which prevents from the Wormhole attack in the wireless sensor 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 [3]. Amish et al. proposed a method of detection and prevention of a Worm Hole attack in the wireless sensor network. The author surveyed the many techniques and analyzed them to provide this approach. Ad-Hoc on Demand multipath distance vector routing is based on the round trip time (RTT) mechanism. NS2 simulator is used to perform the all tasks of simulation [4].

Patel et al. [proposed the two-phase detection technique for the dynamic sensor network. This algorithm is developed to overcome the wormhole attacks in the wireless network. It is very difficult to detect the attacker nodes because the network is wireless and distributed. Attackers used the private network nodes to attack the network due to private network it is a very difficult task to identify them. The proposed algorithm results show that it is an effective tool for that kind of attacks [5]. Tan, Shuaishuai et al. proposed optimized link state routing mechanism to solve the issues of attacks in the wireless sensor networks. In this protocol trust based mechanism is used with fuzzy rules to evaluate the trust values of the mobile nodes. This algorithm selects the route on the basis of maximum path trust value between the nodes. To evaluate the trust of nodes trust factor collection method is used. It generates only relevant information and do not generate extra control messages. In results it enhances the packet delivery ratio and latency and reduced the network overhead [6].

Chen, Honglong, et al. analyzed the effect of Wormhole attack in the DV-Hop localization scheme. This scheme works very effectively on Wormhole attacks. In this type of attack, the attacker sends the data packet by the wormhole link to damage the DV-Hop localization process. In DV propagation phase during the localization, it can aggravate the position error. The simulation results show the effectiveness of the proposed scheme [7]. Anwar, Raja et al. proposed a Trust Aware distance vector routing protocol (T-AODV) for providing the security to the wireless sensor network from Wormhole attacks. This approach provides better network efficiency by providing the improved packet delivery ratio, end to end delay and the number of nodes to the destination [8].

Arai, Masayuki et al. discussed about the tabu-list based multi-path routing scheme for the wireless sensor networks. In this scheme, multiple copies of the events are delivered to all nodes by different paths without using the additional communication path information. In this paper author also discussed the effects of Wormhole attacks and location-aware Wormhole attacks. The proposed method also explained the role of this protocol in Wormhole attack avoidance [9]. Ji, Shiyu et al. discussed the wormhole attack detection algorithm on wireless sensor network coding systems. In this work, the author proposed the centralized algorithm to detect the worm holes in the network. For distributed wireless network author proposed another algorithm called DAWN, a Distributed detection Algorithm against Wormhole in wireless Network coding systems. The analysis is performed for the resistance of DAWN against the collision attacks. DAWN algorithm does not depend on any location information of the nodes it only based on the local information on the network. The experimental results show the effectiveness and efficiency of the DAWN [10].

III. PROPOSED WORK

The proposed approach based on the GWO algorithm and it is a bio-inspired algorithm which is based on the leadership and hunting behavior 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.

This algorithm work on 4 different hierarchy of wolves that are

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.

Methodology Steps:

Step1 : Deploy the wireless Sensor network.
Step2 : Apply the leach routing process.
Step3 : Simulate the black hole attack on the wireless Sensor network and parallel optimize by GWO algorithm.
Step4 : {
Initialize the grey wolf optimization

- Update the fitness function.
- Check the objective function
- 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.

}

IV. RESULTS AND DISCUSSION

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

Parameters	**Value**
Network Size	100 x 100 sq. mtr.
Nodes	450
Capacity of Queue	40 Packets
Model of Mobility	Random way mobility model
Number of Maximum retransmissions allowed	03
Node's initial energy	5
Packets Size	128 bytes
Rate of Data	300 kb/s
Node's Sensing range	35 m
Time of Simulation	5 min
Average Simulation Run	06
Routing Protocol of QoS	Leach with GWO
Location of Base Station	(0,500)
Power of Transmitter	12.3 mW
Power of Receiver	13.4 mW

1. Dead Nodes

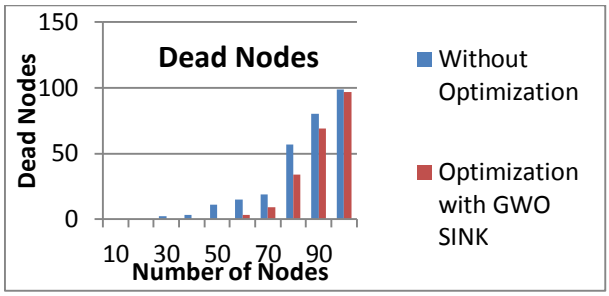


Fig.1: Dead Nodes without Optimization and proposed optimization with GWO-Black

The above given figure 4.1 depicts the total number of dead nodes without Optimization and proposed optimization with GWO-Black holeApproach. The blue bar of the graph represents the dead nodes in existing approach and red bar represents the dead nodes in GWO-Black. The dead nodes in GWO-Black hole 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.

2. Time Delay

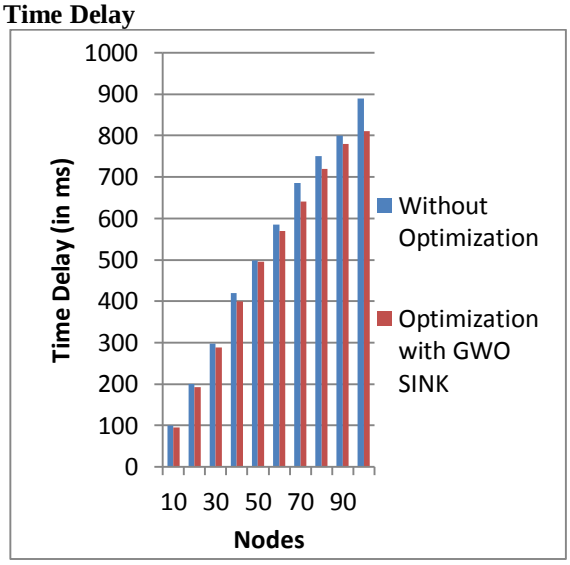


Fig.2: Time in without Optimization and proposed optimization with GWO-Black

The above given figure 4.2 depicts the time delay in without Optimization and proposed optimization with GWO-Black holeApproach. The blue bar of the graph represents the time delay in existing approach and red bar represents the time delay in GWO-Black. The time delay in the proposed GWO-Black hole 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.

3. Energy Consumption

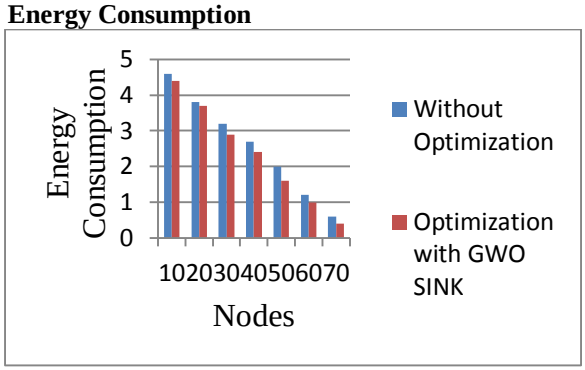


Fig.3: Energy Consumption in without Optimization and proposed optimization with GWO-Black

The above given figure 4.3 depicts the energy consumption in without Optimization and proposed optimization with GWO-Black holeApproach. The blue bar of the graph represents the energy consumption in existing approach and red bar represents the energy consumption in GWO-Black. The energy consumption in the proposed GWO-Black hole 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.

4. Cluster Head

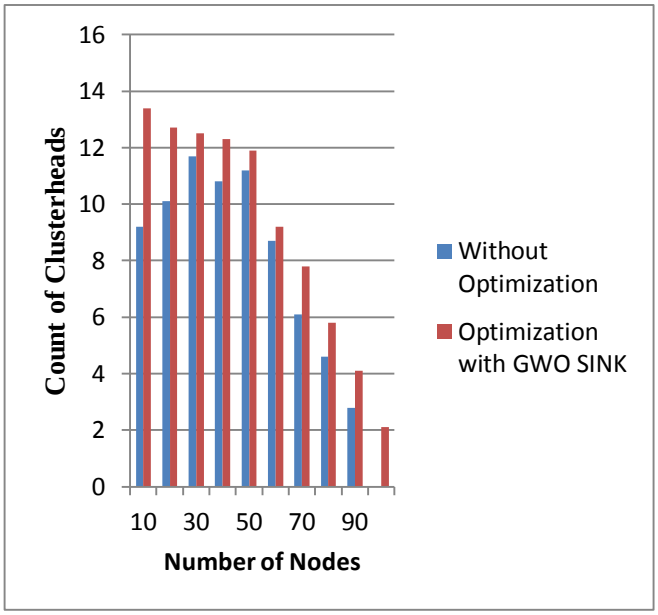


Table 4.4: Cluster Heads in without Optimization and proposed optimization with GWO-Black

The above given figure 4.4 depicts the energy consumption in the existing and proposed GWO-Black holeApproach. The blue bar of the graph represents the energy consumption in existing approach and red bar represents the energy consumption in GWO-Black.

5. Packet Delivery Rate

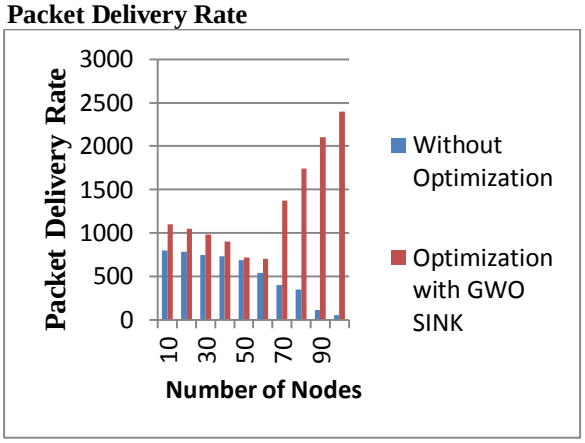


Fig.4: Packet Delivery Rate in without Optimization and proposed optimization with GWO-Black

The above given figure 4.5 depicts the packet delivery rate (PDR) of the existing and proposed GWO-Black holeApproach. The blue bar of the graph represents the PDR of the existing approach and red bar represents the PDR of GWO-Black. The PDR of the proposed approach is better than existing approach which makes communication more effective.

6. Throughput

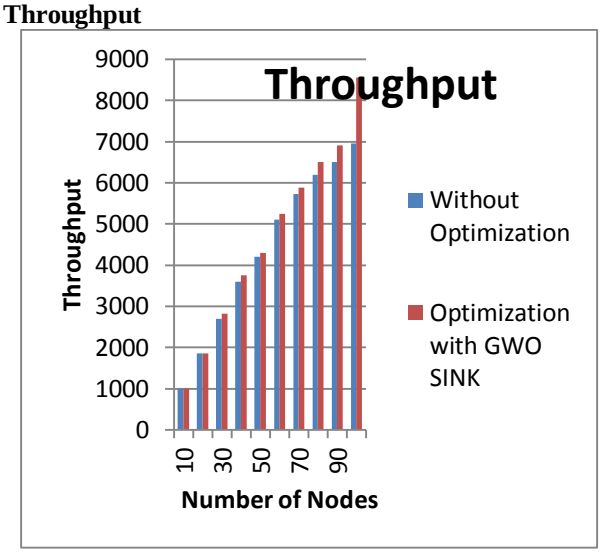


Fig.5: Packet Delivery Rate in without Optimization and optimization with GWO-Black

The above given figure 4.6 depicts the throughput in the without Optimization and proposed optimization with GWO-Black holeApproach. The blue bar of the graph represents the throughput of without Optimization approach and red bar represents the throughput of GWO-Black. The throughput of GWO-Black hole 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.

7. Alive Nodes

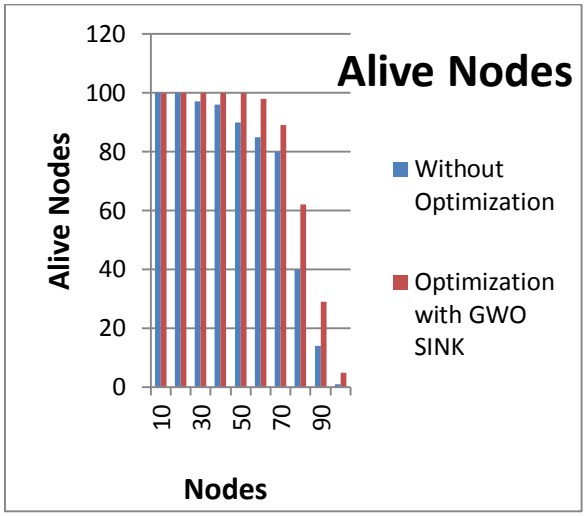
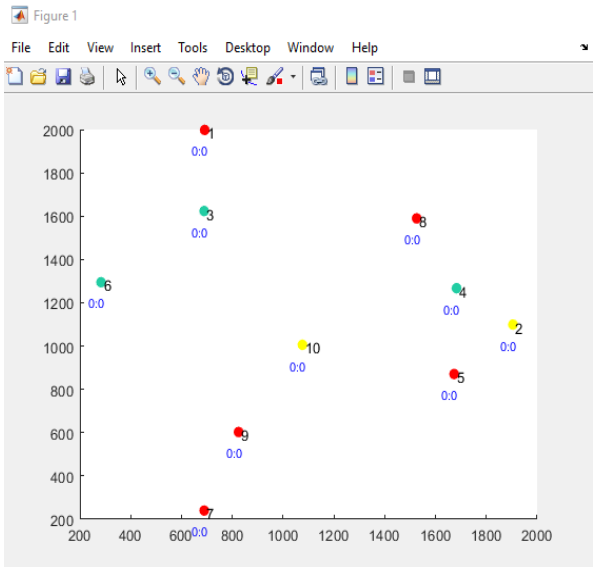


Fig.6: Alive nodes in Existing Algorithm and GWO-Black

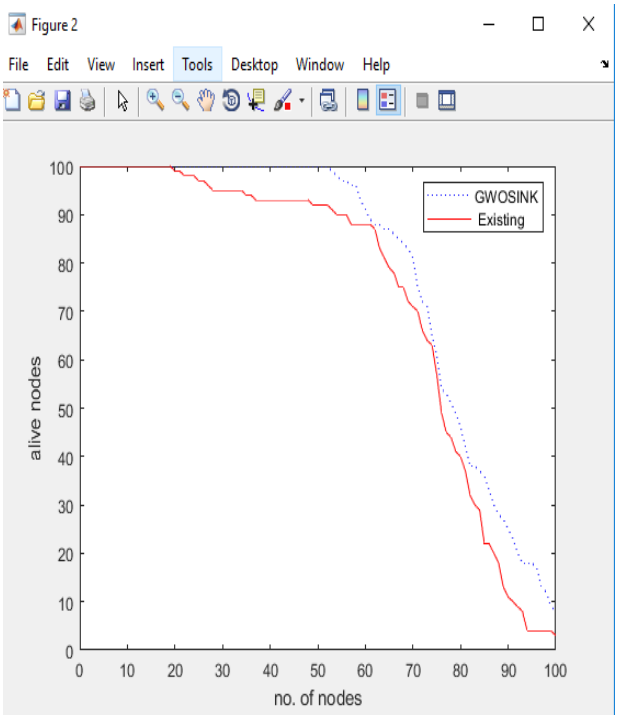
The above given figure 4.1 depicts the total number of alive nodes in the without Optimization and optimization with GWO-Black holeApproach. The blue bar of the graph represents the alive nodes in without Optimization approach and red bar represents the alive nodes in GWO-Black. The alive nodes in GWO-Black hole are high than the existing which enhance the efficiency of the network.

V. SIMULATION RESULTS

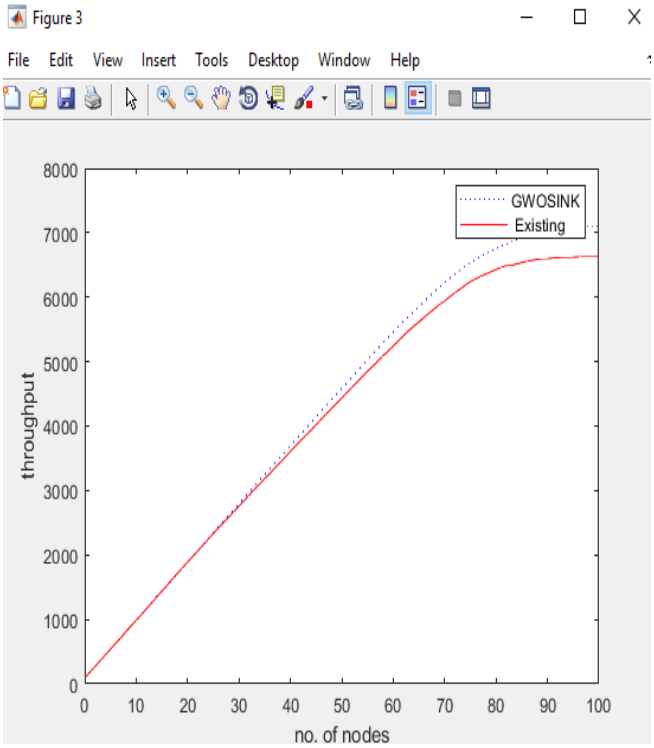
A) Nodes



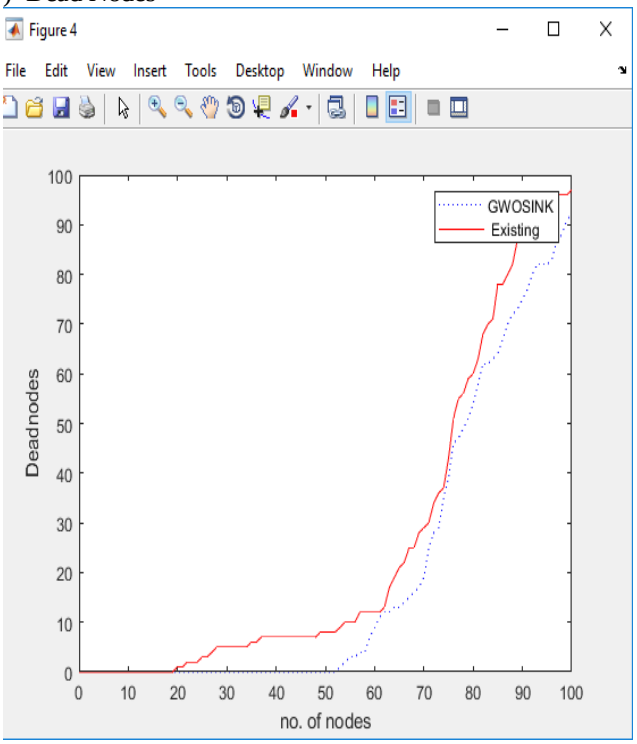
B) Alive Nodes



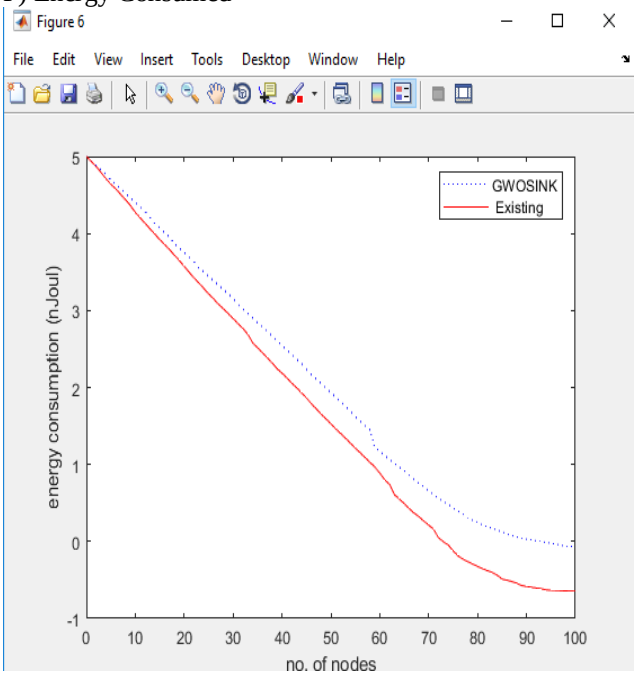
C) Throughput



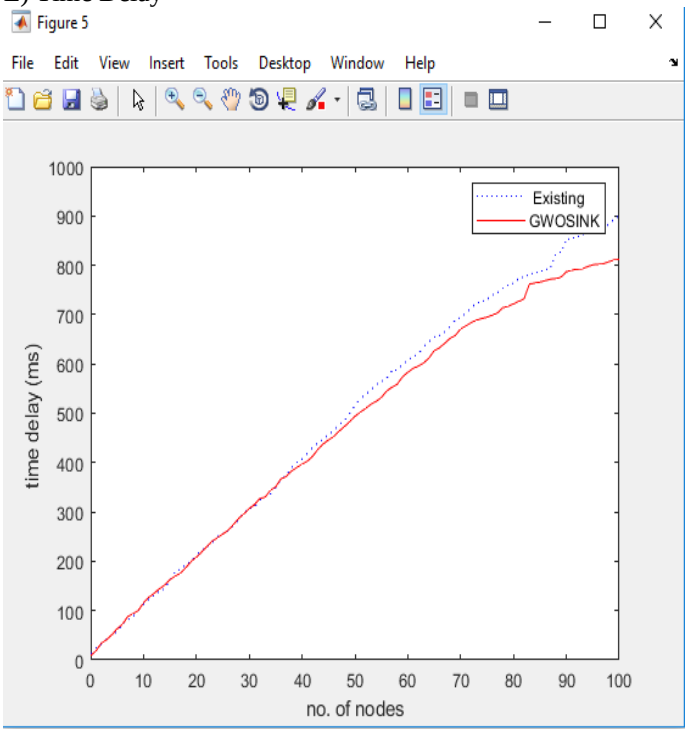
D) Dead Nodes



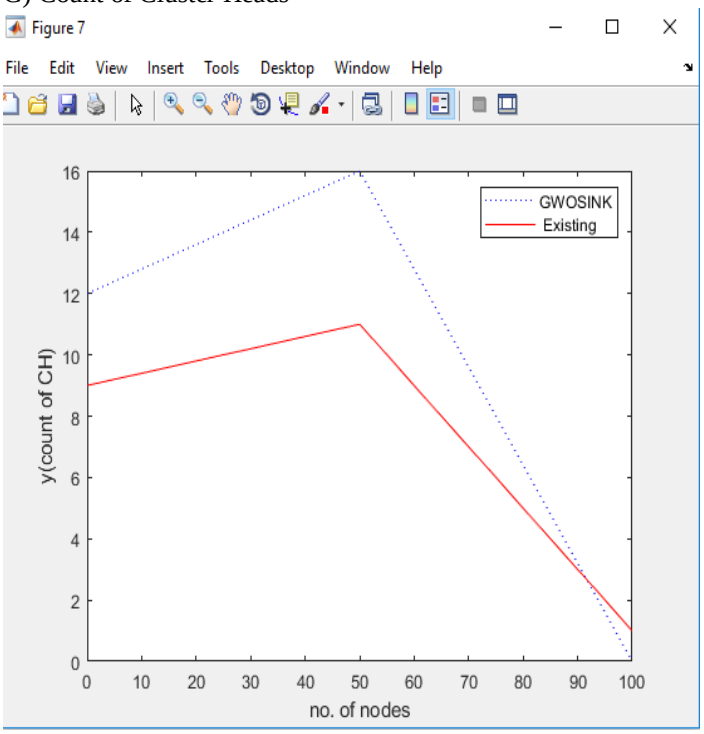
F) Energy Consumed



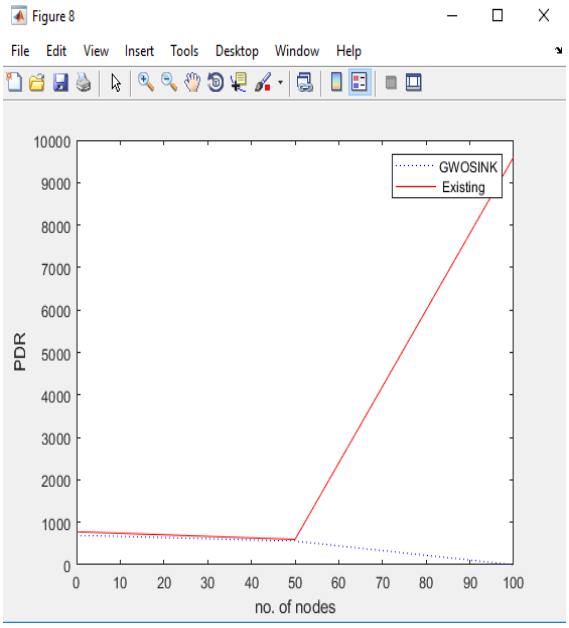
E) Time Delay



G) Count of Cluster Heads



H) Packet Delivery rate



VI. CONCLUSION

This research work done on the wireless sensor 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 wireless sensor network.

VII. REFERENCES

[1]. Saghar, Kashif, HunainaFarid, and Ahmed Bouridane. "Formally verified solution to resolve tunnel attacks in wireless sensor network." *Applied Sciences and Technology (IBCAST), 2017 14th International Bhurban Conference on*. IEEE, 2017.

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

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

[4]. Amish, Parmar, and V. B. Vaghela. "Detection and prevention of wormhole attack in wireless sensor network using AOMDV protocol." *Procedia computer science* 79 (2016): 700-707.

[5]. Patel, Manish M., and Akshai Aggarwal. "Two phase wormhole detection approach for dynamic wireless sensor networks." *Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on*. IEEE, 2016.

[6]. Tan, Shuaishuai, Xiaoping Li, and Qingkuan Dong. "Trust based routing mechanism for securing OSLR-based MANET." *Ad Hoc Networks* 30 (2015): 84-98.

[7]. Chen, Honglong, et al. "Securing DV-Hop localization against wormhole attacks in wireless sensor networks." *Pervasive and Mobile Computing* 16 (2015): 22-35.

[8]. Anwar, Raja Waseem, et al. "Enhanced trust aware routing against wormhole attacks in wireless sensor networks." *Smart Sensors and Application (ICSSA), 2015 International Conference on*. IEEE, 2015.

[9]. Arai, Masayuki. "Reliability Improvement of Multi-path Routing for Wireless Sensor Networks and Its Application to Wormhole Attack Avoidance." *Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 2015 IEEE 12th Intl Conf on*. IEEE, 2015.

[10]. Ji, Shiyu, Tingting Chen, and Sheng Zhong. "Wormhole attack detection algorithms in wireless network coding systems." *IEEE transactions on mobile computing* 14.3 (2015): 660-674.