# Novel Approach of Black Hole detection and prevention by convex optimization approach

[1]Nitin saini ,[2]Er Vivek Gupta
*[1,2]Rayat bhara university Mohali Punjab*
*([1]Nitinsn75@Gmail.com, [2]vivekgupta@rayatbahra.com)*

***Abstract***-Wireless Sensor Networks (WSN) are emerging as both an important new tier in the IT ecosystem and a rich domain of active research involving hardware and system design, networking, distributed algorithms, programming models, data management, security and social factors. algorithm is adjustable and can wage counter attacks against either single black holes or teams of malicious nodes. The proposed routing technique is suitable for network nodes that can tune their transmit power. In this paper simulate on twenty nodes with water cycle optimization.

***Keywords****- simulation; wca; optimization.*

## I. INTRODUCTION

WANET is a decentralized type of wireless network. The network is called ad-hoc because it does not depend on the pre-existing infrastructure like routers in the wired network. In this instead of each node forwarding data to the next node the determination of which nodes forward data is made dynamically on the basis of network connectivity and the routing algorithm in use. In ad hoc type of network, you can set up a wireless connection directly to another computer without having to connect to a Wi-Fi access point or router.

Network attack is usually defined as an intrusion on your network infrastructure that will first analyze your environment and collect information in order to exploit the existing open ports or vulnerabilities - this may include as well unauthorized access to your resources. In such cases where the purpose of the attack is only to learn and get some information from your system but the system resources are not altered or disabled in any way, we are dealing with a passive attack. The active attack occurs where the perpetrator accesses and either alter, disables or destroys your resources or data. An attack can be performed either from outside of the organization by unauthorized entity (Outside Attack) or from within the company by an "insider" that already has certain access to the network (Inside Attack).

### *A. Black hole attack*

An attacker can drop received routing messages, instead of relaying them as the protocol requires, in order reducing the quantity of routing information available to the other nodes. This is called black hole attack, and is a “passive” and a simple way to perform a Denial of Service. The attack can be done selectively (drop routing packets for a specified destination, a packet every n packets, a packet every t seconds, or a randomly selected portion of the packets) or in bulk (drop all packets), and may have the effect of making the destination node unreachable or downgrade communications in the network.

*B.* Type of Black hole Attack
*1)* Single black hole attack
*2)* Collaborative Black hole Attack

*a)* Single black hole attack: black hole node is that when there is single malicious node.
*b)* Collaborative Black hole Attack: Collaborative black hole node is that when there are two or more than two malicious nodes.

## II. RELATED STUDY

Sen, Jaydip et al. In this paper, routing security issues in MANETs are talked about in general, and specifically, the helpful black hole attack has been depicted in detail. A security convention has been suggested that can be used to distinguish numerous black hole hubs in a MANET and in this way recognize a safe steering way from a sourcing hub to a destination hub keeping away from the dark opening hubs. The proposed plot has been assessed by actualizing it in the system test system ns-2, and the outcomes exhibit the viability of the instrument. As a future extent of work, the proposed security instrument might be broadened with the goal that it can safeguard against different attacks like asset utilization attack and bundle dropping attack [1]. Purohit et al. performed simulation study of Black Hole and Jelly Fish attack on the wireless network. Black hole attack is one of the security threat in which the traffic is redirected to such a node that drops all the packets or the node actually does not exist in the network. Black holes refer to places in the network where incoming traffic is silently discarded or dropped. Jellyfish (JF) attack is a type of selective black hole attack. When JF node gets hold of forwarding packet it starts delaying/dropping data packets for certain amount of time before forwarding normally [12].

Singh et al. proposed a solution for the Black Hole attack in the MANET. Proposed method is completely based on the routing algorithm, ad-hoc on demand distance vector (AODV). It uses the promiscuous mode to detect malicious node (black hole).After the detection of that node information is transfer to the all nodes in the network. The results show the efficiency in throughput [3]. Biswas et al. proposed a solution for detecting and avoiding black hole attacks (both single and cooperative) and ensuring secure packet transmission along with efficient resource utilization of mobile hosts at the same time. According to the proposed method, evaluation of trust of every node in the network is based on parameters such as stability of a node defined by its mobility and pause time, remaining battery power etc. This trust of a node forms the basis of selection of the most reliable route for transmission. The simulation results show that our solution provides good performance in terms of throughput, secure routing, and efficient resource utilization [4].

Pham, Thi Ngoc Diep, et al. proposed flooding detection based on encounter records (FDER) which detects the flooding attack in mobile ad-hoc network. In this network nodes exchange their record history and the number of replicas sent over the network in a given time. The node which sends message replicas in a huge amount is detected as intruder. The proposed method also detects the burst traffic over the network. It observes the rate of message transfer by the node and reduces the delay also [5]. Singh, Kuldeep et al. Intrusion detection in mobile ad-hoc network is depends upon the parameters of the nodes. By using the threshold values of the parameters ant colony optimization algorithm is used for intrusion detection. After the detection of intrusion, recovery is done by using genetic algorithm [6].

Soni, Rajshree et al introduced velocity constrained multipath routing protocol which resolves the issues of degradation of high velocity in mobile nodes. It chooses the route which has high reliability for information transfer. It transfers the data with less delay, less packet loss and high delivery ratio [7]. Nemade, Sandip et al. In SYN Flooding attack, attacker sends a large amount of synchronization packet to the destination nodes and these nodes consumes a lot of memory. After getting the IP of the spoofed client the attacker behaves like original client node and starts sending SYN message to the server and server send SYN ACK in reply to the malicious node. The author proposed an adaptive threshold algorithm which raised alarm when it detects the SYN packets abnormally [8].

Song, et al. proposed a filtering method against the RREQ flooding attacks in MANET. In these types of attack infected nodes behaving like normal nodes and leads to congestion of network. These nodes reach the routes fastly than other nodes. The proposed method filters the nodes by their behavior and prevent from this type of attack [9]. Chang, et al. proposed a prevention method against denial-of-service attack in mobile ad-hoc network. In this paper firstly DoS attacks are explained in brief and then firewall approach is proposed for providing security against attacker nodes. This method detects the nodes before it reaches the target node [10].

## III. PROPOSED METHODLOGY

The proposed work based on the simulation of black hole network and routing by using leach routing protocol. The optimization of nodes done by using water cycle optimization. In this section flow chart of work is discussed and water cycle optimization.

### *A. Water cycle Optimization*

Water cycle optimization is a nature inspired algorithm which based on the concept of river and streams flow in the sea. This algorithm is mainly used for the computation optimization and applicable of the different graph, tress and unstructured data. This algorithm is able to compute the maximum and minimum value of the function.

Proposed methodology steps:-

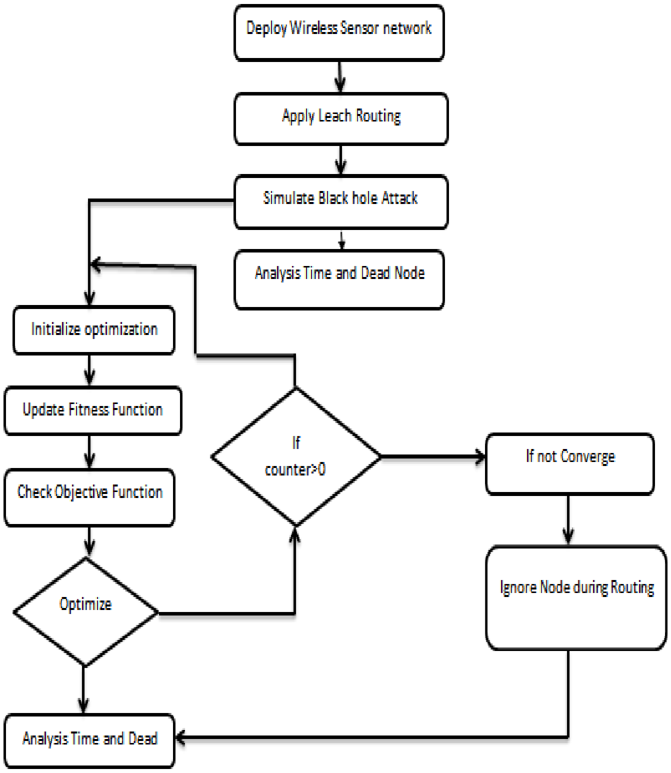
*Step1 :* Deploy the wireless Sensor network.

*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 water cycle optimization.

*Step5 :* Analyze the time and dead node



## IV. RESULTS AND DISCUSSION

This section describes the results of the proposed 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.

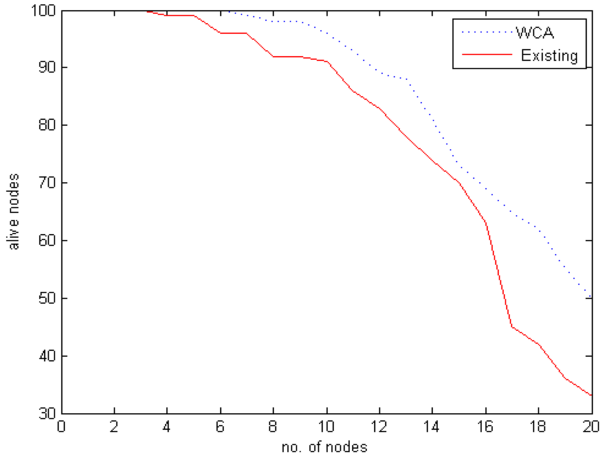


*Fig.4.1: Alive nodes in network*

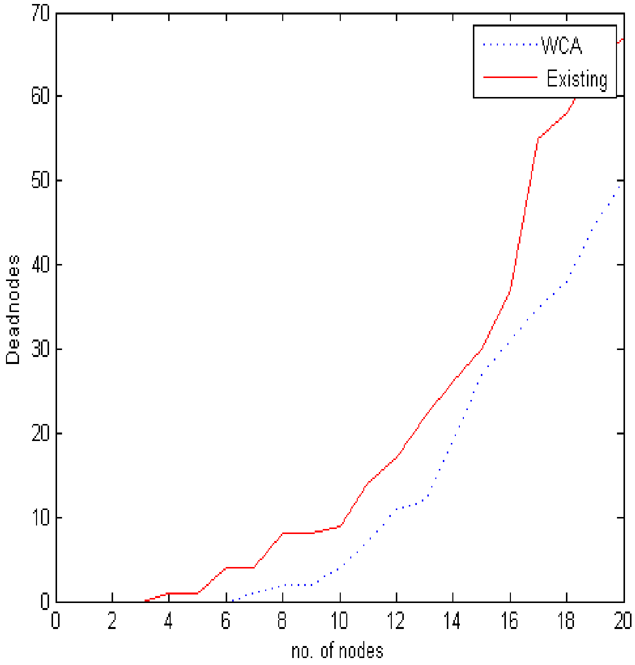


*Fig.4.2: Dead Nodes in Network*

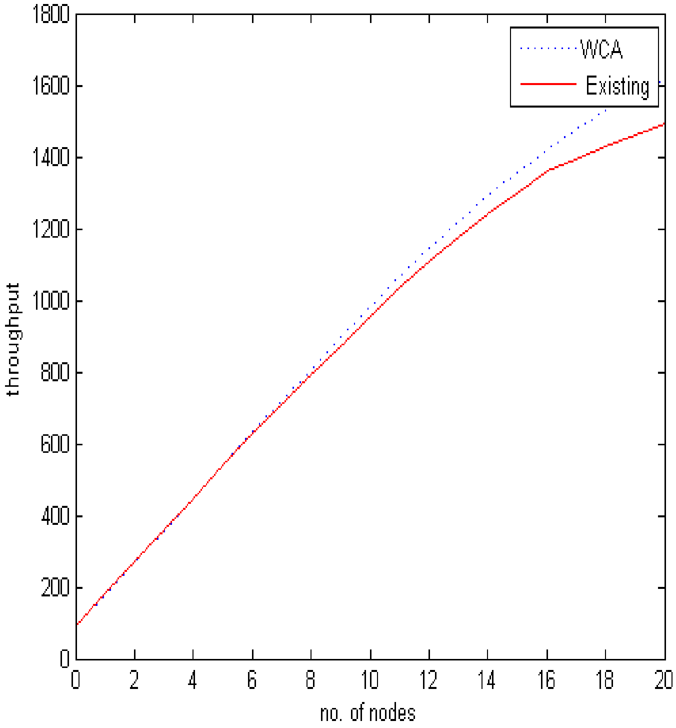


*Fig.4.3: Throughput of network*

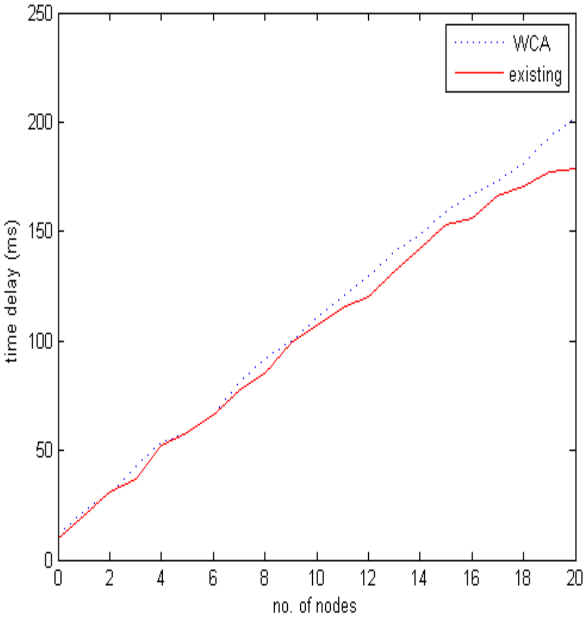


*Fig.4.4:Time delay in network*

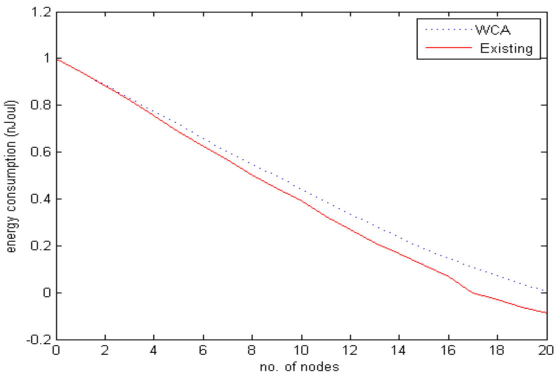


*Fig.4.5: Energy consumption in network*

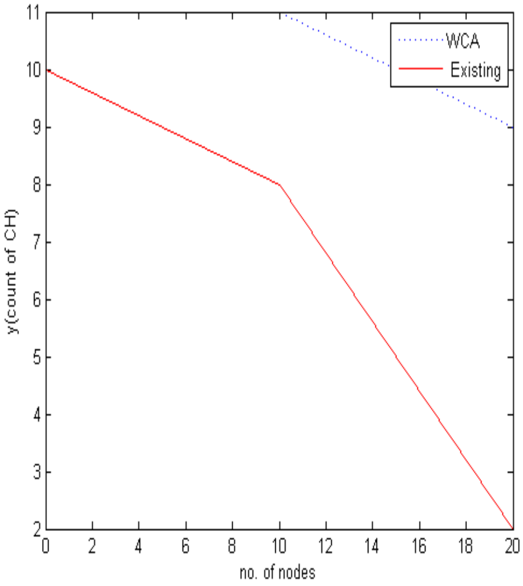


*Fig.4.6: Cluster heads in network*

## V. RESULT ANALYSIS

The above given figure 4.1-4.6 represents the comparison of result between the proposed approach and existing approach. In these graphs red curve represents the existing approach and dotted curve represents the proposed approach results. The results evaluation based on the alive node, dead node, throughput, cluster heads, time delay and throughput. The performance of the proposed approach is better and effective than existing approach.

## VI. CONCLUSION

Black hole attack is occurs, when an intermediary captures and re-programs a set of nodes in the network to block/drop the packets and generates false messages instead of forwarding correct/true information towards the base station in wireless sensor network. Nearby many techniques have been proposed in the literature for detection and prevention of black hole attack in sensor network. There are various solutions proposed in the literature which identifies black hole attack and provides successful delivery of data to the base station.

## VII. REFERENCES

[1]. Sen, Jaydip, Sripad Koilakonda, and Arijit Ukil. "A mechanism for detection of cooperative black hole attack in mobile ad hoc networks." *Intelligent Systems, Modelling and Simulation (ISMS), 2011 Second International Conference on*. IEEE, 2011.

[2]. Purohit, Nidhi, Richa Sinha, and Khushbu Maurya. "Simulation study of Black hole and Jellyfish attack on MANET using NS3." *Engineering (NUiCONE), 2011 Nirma University International Conference on*. IEEE, 2011.

[3]. Singh, Pramod Kumar, and Govind Sharma. "An efficient prevention of black hole problem in AODV routing protocol in MANET." *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. IEEE, 2012.

[4]. Biswas, Suparna, Tanumoy Nag, and Sarmistha Neogy. "Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET." *Applications and Innovations in Mobile Computing (AIMoC), 2014*. IEEE, 2014.

[5]. Pham, Thi Ngoc Diep, et al. "Detecting Flooding Attack and Accommodating Burst Traffic in Delay-Tolerant Networks." *IEEE Transactions on Vehicular Technology* 67.1 (2018): 795-808.

[6]. Singh, Kuldeep, and Karandeep Singh. "Intrusion Detection and Recovery of MANET by Using ACO Algorithm and Genetic Algorithm." *Next-Generation Networks*. Springer, Singapore, 2018. 97-109.

[7]. Soni, Rajshree, Anil Kumar Dahiya, and Sourabh Singh Verma. "Limiting Route Request Flooding Using Velocity Constraint in Multipath Routing Protocol." *Proceedings of First International Conference on Smart System, Innovations and Computing*. Springer, Singapore, 2018.

[8]. Nemade, Sandip, Manish Kumar Gurjar, and Zareena Jamaluddin. "A Novel Method for Early Detection of SYN Flooding based DoS attack in Mobile Ad Hoc Network." *Int. J. Eng. Trends Technol* 7.4 (2014): 187-191.

[9]. Song, Jian-Hua, Fan Hong, and Yu Zhang. "Notice of violation of ieee publication principles effective filtering scheme against RREQ flooding attack in mobile ad hoc networks." *Parallel and Distributed Computing, Applications and Technologies, 2006. PDCAT'06. Seventh International Conference on*. IEEE, 2006.

[10]. Chang, Rocky KC. "Defending against flooding-based distributed denial-of-service attacks: a tutorial." *IEEE communications magazine* 40.10 (2002): 42-51