Black Hole Detection and Prevention by Monitoring of Water Cycle Optimization Algorithm

Nitin saini[1], Er. Vivek Gupta[2]

[1]Student, USET, Rayat Bhara University Mohali Punjab
[2]Assistant Professor, USET, Rayat bhara University, Mohali, Punjab

---

Abstract - *Wireless Sensor Networks (WSN) are becoming popular these days in various areas like military applications, environmental application, smart homes, health monitoring etc. The nodes of a WSN sense any physical, mechanical or chemical change in the environment and send it to the base station where the user can analyze the results. WSNs have various limitations on resources like memory, processing power and battery power. Wireless Sensor Networks (WSN) in unattended environment has led to various security threats. This paper provides an overview of LEACH, the most popular clustered routing protocol of WSN and how LEACH can be compromised by Black hole used to simulate these attacks on MATLAB. The performance of WSN under attack is thoroughly investigated, by applying it on various network parameters with various node densities. It is observed that the effect of the Black Hole attack is more on the network performance as compared to the Black Hole attack on hundred numbers of nodes optimize by water cycle optimization.*

***Key Words*: WSN, optimize, WCA, Blackhole attack**

1. INTRODUCTION

Wireless ad-hoc network is more versatile than the wired network but also more vulnerable to attacks. This is due to radio transmission nature of data. In wired network intruder have to break up the physically connection of the network or physically wiretap a cable. In wireless connection attacker is able to eavesdrop on all messages within the area by packet sniffer. There are various methods of attack detection and monitor in the network some of them are Kismet, AirSnort and NetStumbler. Hence, by simply being within radio range, the intruder has access to the network and can easily intercept transmitted data without the sender even knowing (for instance, imagine a laptop computer in a vehicle parked on the street eavesdropping on the communications inside a nearby building). As the intruder is potentially invisible, it can also record, alter, and then retransmit packets as they are emitted by the sender, even pretending that packets come from a legitimate party.

2. Blackhole 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.

2.1 Type of Black hole Attack

1. Single black hole attack
2. Collaborative Black hole Attack

Single black hole attack: black hole node is that when there is single malicious node.

Collaborative Black hole Attack: Collaborative black hole node is that when there are two or more than two malicious nodes.

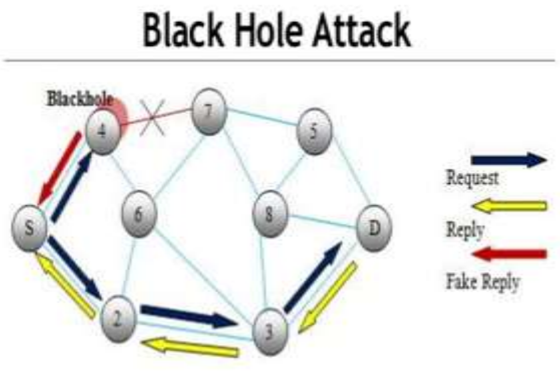

Fig -1: Blackhole attack in network node

2.2 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

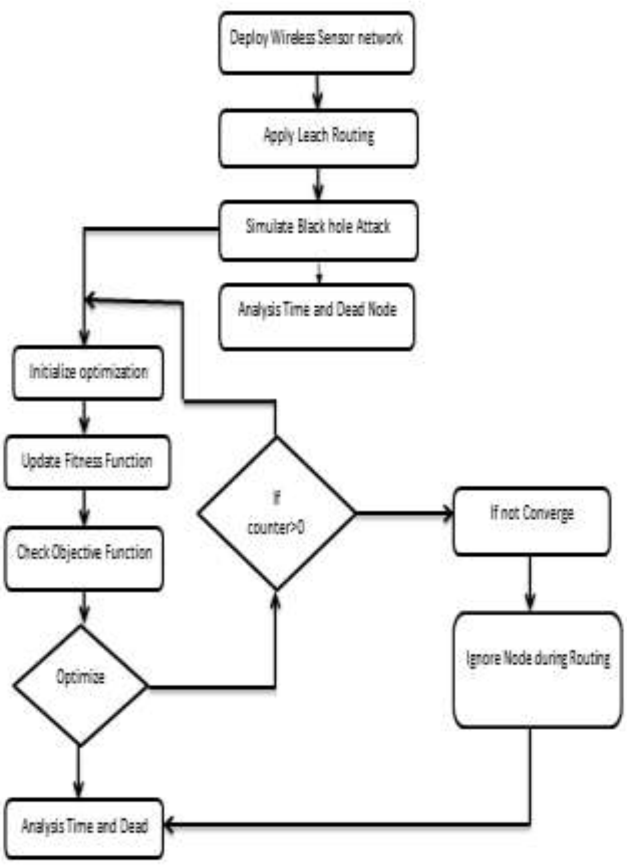

Fig -2: Research Methodology

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 WCO algorithm
Step4: Initialize the water cycle optimization. Analyze the time and dead node

2.3 RESULT AND DISCUSSION

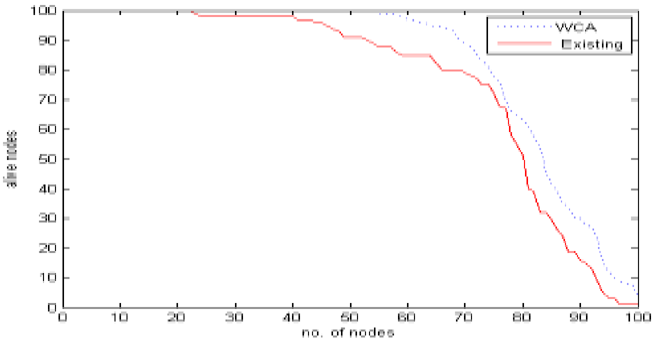

Chart -1: Alive nodes in network

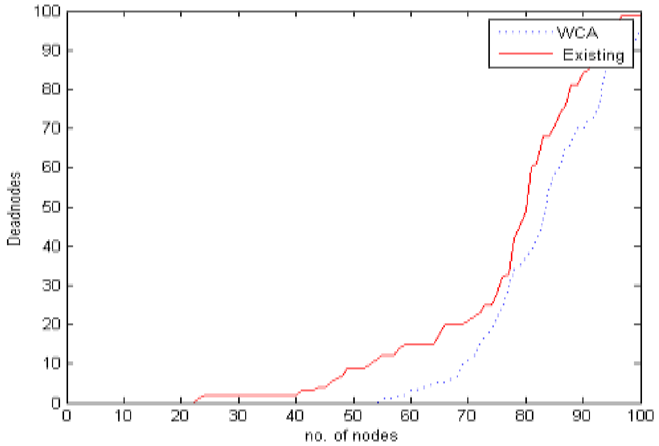

Chart -2: Dead Nodes in Network

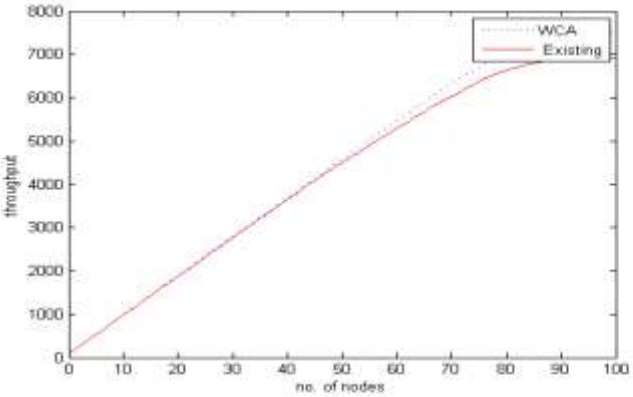

Chart -3: Throughput of network

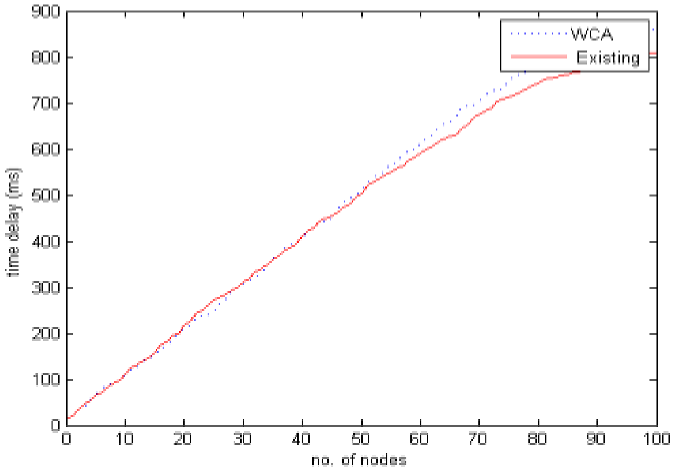

Chart -4: Time delay in network

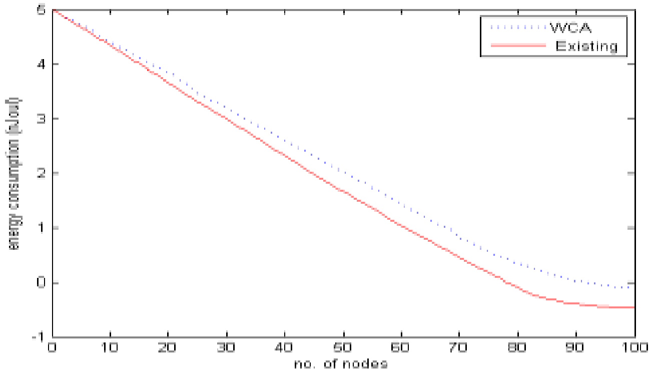

Chart -5: Energy Consumption In Network

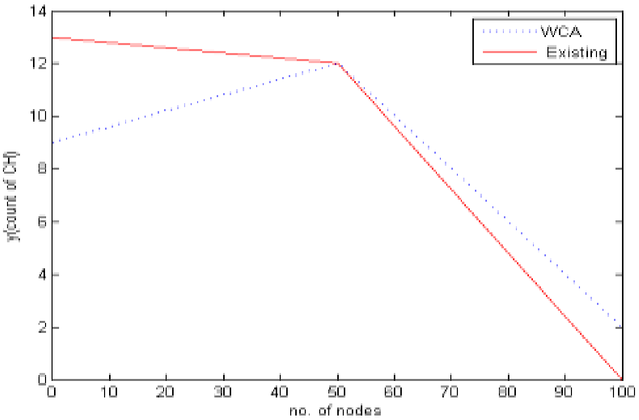

Chart -6: Cluster heads in network

2.4 RESULT ANALYSIS

The above given chart 1- 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.

3. CONCLUSION

Black-hole attack- In the black-hole attack, a malicious node advertises the wrong paths as good paths to the source node during the path finding process as in reactive routing protocols or in the route updating messages as in proactive routing protocols. Good path means the shortest path from source node to the destination node or the most stable path through the sensor network concludes that effect of the attack increases with increase in network size. Number of nodes in a cluster increases with increase in network size. The malicious node can affect the data of more nodes. We observed that the effect of the Black Hole attack. We have also floated an idea for detection of these attacks. In future, we plan to develop and simulate the detection technique on these lines.

REFERENCES

[1] Y. Yoo and D. P. Agrawal,"Why does it pay to be selfish in a MANET?",IEEE Wireless Communications, *vol. 13*, no. 6, pp. 87–97, December 2006.

[2] F. A. Kuipers, "An Overview of Algorithms for Network Survivability", International Scholarly Research Network, December 2012..

[3] J. L. Cook and J. E. Ramirez-Marquez,"Two-terminal reliability analyses for a mobile ad hoc wireless network", Reliability Engineering and System Safety, vol. 92, no. 6, pp. 821–829, June 2007.

[4] X. Xiaochuan, W. Gang, W. Keping, W. Gang, and J. Shilou,"Link reliability based hybrid routing for tactical mobile ad hoc network", Journal of Systems Engineering and Electronics, vol.19,no. 2, pp. 259–267, April 2008.

[5] Z. Ye, S. V. Krishnamurthy, and S. K.Tripathi, "A framework for reliable routing in mobile Ad Hoc networks", Proceedings of the 22nd Annual Joint Conference of the IEEE Computer and Communications , vol. 1, pp. 270–280, July2003.

[6] E.Hansler, "Comments on "a fast recursive algorithm to calculate the reliability of a communication network", IEEE Transactions on Communications, pp. 563–566, June 1972.