INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 6.078
(Volume 6, Issue 4)
Available online at: www.ijariit.com

Black hole attack detection and prevention by Grey Wolf Optimization

Gbazoe Kelezonga Daniel
AP Goyal Shimla University, Shimla, Himachal Pradesh

Anuj Gupta
AP Goyal Shimla University, Shimla, Himachal Pradesh

ABSTRACT

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— *Packet Delivery Rate, Throughput, Energy Consumption, Delay, WSN*

1. INTRODUCTION

1.1 Wireless Sensor Network

WSN 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. These networks are used to control physical or environmental conditions like sound, pressure, temperature etc.

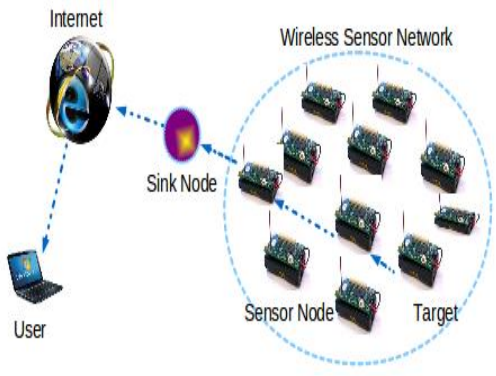


Fig. 1: Wireless Sensor Network

The main characteristics of the WSN 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 wireless sensor network due to its dynamic nature, if a connection is failed then communication does not affect by it. It communicates with another connection.
- **Limited Power Consumption:** Nodes in the WSN 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 wireless sensor network capacity of nodes are scalable and only limited by bandwidth of gateway node.

1.1.1 Attacks

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.

(c) **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.

1.1.2 Attacks on Wireless Sensor Networks

Wireless sensor 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. In this network sensor nodes used wireless communication and it is easy to eavesdrop. The attacker can easily inject malicious messages into the network.

1.1.3 Types of Attacks in WSN

- **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].

- **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 wireless sensor network. In the figure [1.3] 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]. A wormhole attack has two modes.
  (a) Hidden mode
  (b) Participation mode

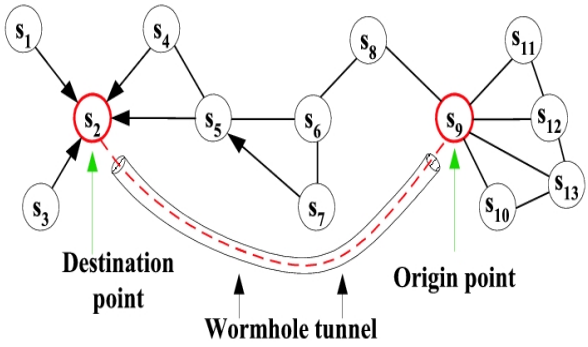


Fig. 2: Wormhole Attack

- **Sink 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].

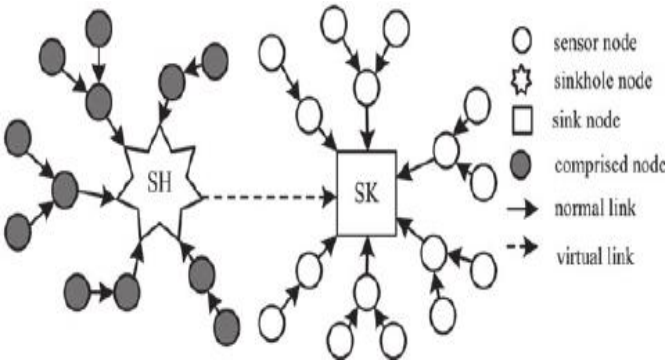


Fig. 3: Sinkhole Attack

There are two types of sink hole attack one is simple sink hole attack and other is using worm hole attack. The simple sink hole attack, malicious neighbor node behaves itself as a best route to the base station and attract 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.

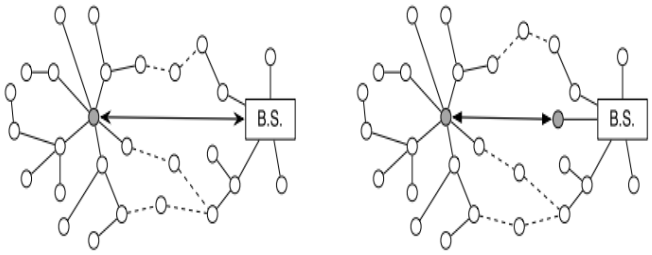


Fig. 4: Sinkhole attack (a) and (b) Sink hole using worm hole attack

In the other sink hole attack with worm hole attack, malicious node captures the node from the nearest neighbor and use the tunnel to send the packet to another colluded node. This colluded node also delivers the message to the base station.

In sink 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 sinkhole 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 sinkhole 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 sinkhole 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 sinkhole attack. Once it's 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.

2. RELATED STUDY

Zhang, Zhaohui, et al. [1] (2018) explained an energy efficient sinkhole 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 sink node. This method is based on the dynamic programming. This approach enhanced the detection rate and false positive rate.

Devibala, K., et al. [2] (2018) proposed neighbor constraint traffic centric approach which is used to detect sinkhole attack and improve the quality of the WSN. It identifies the malicious node by the data send by neighbor node. It verifies the location of the node from where data is sent to the node. This method provides sinkhole detection with high throughput and packet delivery ratio.

Mittal et al. [3] (2018) proposed the major goal to analyze the effective protocol for the wireless sensor network. This analysis shows that the access control method and authentication

methods are used in the WSN. 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] (2017) described the anomaly detection approach which detects the sinkhole attack in wireless sensor 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] (2017) 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 sink node. In future this work will be enhanced by applying formal methods to verify the communication issues.

Saghar et al. [6] (2017) 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.

Jan, Mian, et al. [7] (2017) 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.

Kumar et al. [8] (2017) 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. PROPOSED WORK

3.1 Research Motivation

Detecting the sink hole attack by consuming less effort is the main goal of this research work. In this work we check the infectious node in the network which acquire by the intruder for the sink hole attack. In the previous work, sink hole attack detection is done by using algorithm which does not gave optimal results in the outcome and need to be improvement in them. The sink hole attack detection at the appropriate time helps to increase the throughput and reduce the packet delivery time and delay in network.

3.2 Problem Statement

Reduce the confliction of attacker node by monitoring optimization approach. The problem in the previous work, solved by using the concept of optimization using grey wolf optimization. Grey Wolf Optimization (GWO) algorithm is a biological inspired algorithm and provides the facility of global optimization of the nodes.

3.3 Problem Formulation

In the wireless sensor network energy reduction is important parameter, so attacker node shows the conflicts of shortest path and energy so routing will go through attacker node and drop the packet. So, the challenge is monitoring the node behavior, in every node which reduces the energy loss and drop packet.

3.3 Problem Formulation

In the wireless sensor network energy reduction is important parameter, so attacker node shows the conflicts of shortest path and energy so routing will go through attacker node and drop the packet. So the challenge is monitoring the node behavior, in every node which reduces the energy loss and drop packet.

3.4 Objectives

(a) To study different attack and its prevention.
(b) To proposed grey wolf optimization method for monitoring behavior of nodes.
(c) To analysis the network after and before optimization.
(d) To analysis the time delay, dead node and Alive node in proposed number of rounds.

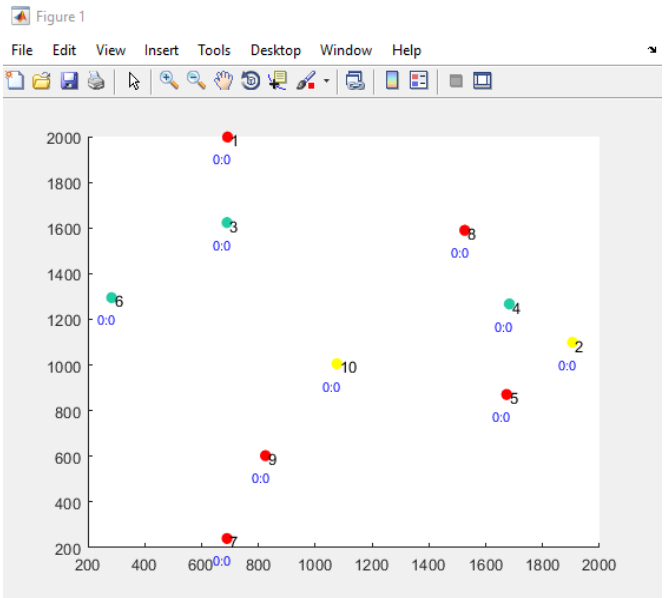
4. RESULTS AND DISCUSSION

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. 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.

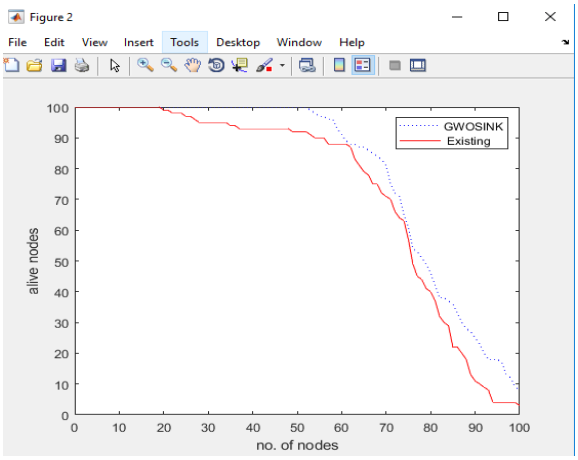
Table IX Overall results Analysis table of Existing approach and proposed GWO-Sink approach

5. SIMULATION OF RESULT WORK

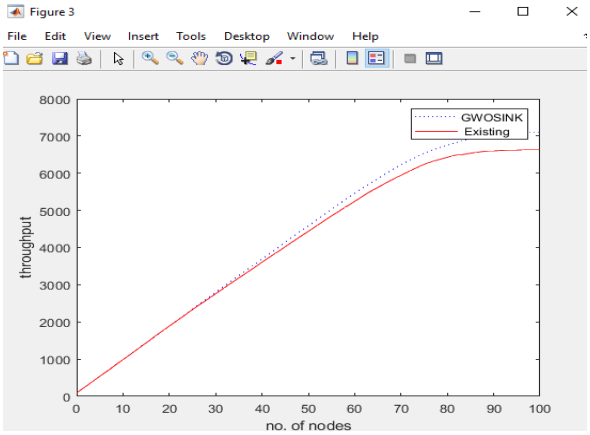
5.1 Nodes



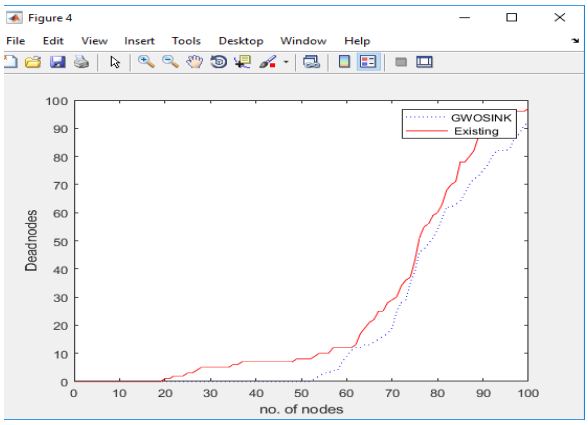
5.2 Alive Nodes



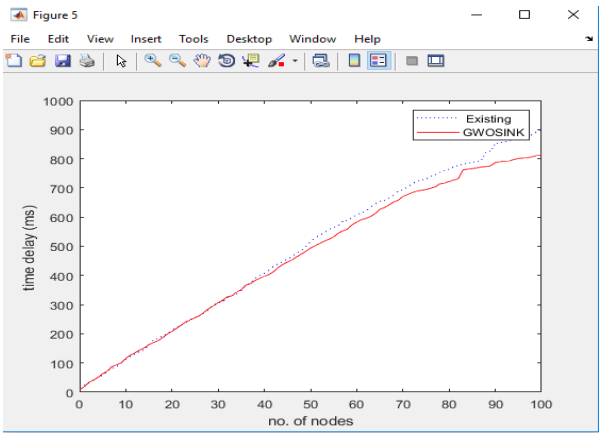
5.3 Throughput



5.4 Dead Nodes



5.4.5 Time Delay



6. CONCLUSION

Wireless sensor network (WSN) 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 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.

7. 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 Experience29.17 (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 & 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 2015s 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.

